FMC

2025 Barcelona

Seminari
Gestió
Econòmica Local

Federació de Municipis de Catalunya

Edita
Federació de Municipis de Catalunya
Via Laietana 33, 6è 1a.
08003 Barcelona
Tel. 93 310 44 04

Disseny i maquetació
www.lacuinagràfica.com

Sumari

Introducció

La Federació de Municipis de Catalunya organitza la tercera edició del Seminari de Gestió Econòmica Local destinat a l'estudi i l'aprofundiment de les novetats normatives, jurisprudencials i l'anàlisi de les bones pràctiques en el control i la gestió economicofinancera en l'àmbit local, amb l'objectiu de ser un espai de referència per als treballadors i les treballadores del sector públic local i una eina per facilitar el desenvolupament de la seva tasca, orientada a millorar l'execució de les polítiques públiques locals en el marc del bon govern i la bona administració.

En aquesta nova edició es tractaran aspectes de la fiscalitat municipal, centrats en la nova taxa de residus, el tractament de l'Impost sobre el Valor Afegit en les operacions realitzades entre les entitats que formen part del grup municipal i aspectes de l'Impost de Societats que afecten en particular les entitats dependents dels ens locals. També s'aprofundirà en aspectes de la comptabilitat pública, relatius a les normes de registre i valoració de les transferències i subvencions, i de les adscripcions i cessions de béns, així com la formulació dels comptes anuals consolidats en l'àmbit del sector públic local.

Així mateix, s'analitzarà el Reglament d'Intel·ligència artificial de la UE en el dret a la bona administració i el seu control judicial i l'aplicació de la intel·ligència artificial en els treballs de fiscalització i en el control financer de subvencions, a partir de les experiències de la Sindicatura de Comptes de Catalunya i de la Intervenció General de l'Administració de l'Estat. I per últim, s'estudiarà la problemàtica i els riscos derivats de la ciberseguretat en el control intern, en les transaccions bancàries i en la gestió d'avals.

Per finalitzar, després de l'èxit de les darreres edicions, es torna a incorporar al final de cada sessió una taula rodona on els i les ponents dialogaran i confrontaran opinions enfocades a trobar solucions als aspectes jurídics, comptables, de control intern i de la gestió econòmica dels ens locals tractats en les exposicions, amb l'objectiu de consolidar aquest Seminari com un espai de debat obert i participatiu amb els i les assistents.

Antoni Ayora Rico
Maria Petra Sáiz Antón
Director i directora del Seminari

Ponències

1a sessió

21/02/25

FISCALITAT: TAXA DE RESIDUS I ASPECTES RELLEVANTS DE L'IVA I L'IS

Implantació de la taxa residus. Consideracions jurídiques i tècniques sobre la seva implantació.

Cristina Casablanca Juez, gerenta de l'ORGT de la Diputació de Barcelona.

Impost sobre el Valor Afegit i Impost de societats. Aspectes rellevants en les entitats del sector públic local.

Jordi Casals Company, soci de Faura-Casas.

TAULA RODONA

Cristina Casablanca Juez, gerenta de l'ORGT de la Diputació de Barcelona.
Jordi Casals Company, soci de Faura-Casas.

LA TAXA DE RESIDUS. CONSIDERACIONS JURÍDIQUES I TÈCNIQUES SOBRE LA SEVA IMPLEMENTACIÓ.

Cristina Casablanca Juez
Gerent
ORGT de la Diputació de Barcelona

Contingut

1. INTRODUCCIÓ

El principi europeu que “qui contamina paga” va ser transposat a la normativa espanyola mitjançant la Llei 7/2022, de 8 d'abril, de residus i sòls contaminats per a una economia circular (llei de residus).

Aquesta Llei incorpora al Dret espanyol la Directiva (UE) 2018/851, del Parlament Europeu i del Consell, de 30 de maig de 2018, per la qual es modifica la Directiva 2008/98/CE sobre els residus, i la Directiva (UE) 2019/904 del Parlament Europeu i del Consell, de 5 de juny de 2019, relativa a la reducció de l’impacte de determinats productes de plàstic en el medi ambient.

L'article 11.3 d'aquesta llei imposa als ajuntaments l'obligatorietat d'establir una taxa o una prestació patrimonial de caràcter públic no tributari (PPPNT), que permeti implantar sistemes de pagament per generació, reflectint el cost real, directe o indirecte de les operacions de recollida, transport i tractament de residus.

Mitjançant el pagament per generació, el legislador pretén una doble finalitat extrafiscal:

1. Promoure la reducció del volum de residus generats pels contribuents.

2. Incrementar la seva separació i el seu reciclatge.

La primera finalitat hauria de comportar com a efecte principal una progressiva disminució de la despesa de la recollida, tractament i reciclat de residus, en reduir-se els mateixos; la segona, un increment de l'activitat econòmica del reciclatge, amb els seus possibles beneficis econòmics i, en tot cas, ambientals.

L'objectiu a llarg termini és anar reduint la quantia de la taxa o prestació per la disminució dels costos del servei i l'increment dels ingressos.

Des del meu punt de vista, les principals dificultats que ens estem trobant amb l’aplicació de la taxa, a grans trets, són:

1. La falta de regulació dels elements essencials de la taxa. Crec que es deixa en mans dels ajuntaments la regulació dels diferents elements tributaris de la taxa. Si s'hagués creat un impost aquesta conflictivitat no existiria (un exemple el tenim en l'Impost sobre el dipòsit de residus en abocadors, amb un desenvolupament normatiu en la pròpia Llei de residus de 13 articles). Si estiguéssim davant un impost, la igualtat tributària entre els contribuents seria la mateixa, ja que tots els ajuntaments haguessin aplicat els mateixos elements tributaris del tribut.

2. La inseguretat jurídica i la possible conflictivitat (dificultat en l'elaboració dels informes tècnico-econòmics). És imprescindible informar adequadament als contribuents, a través de la Seu electrònica, amb un seguit de preguntes freqüents, o qualsevol altre sistema que permeti tenir coneixement del que suposa aquesta nova imposició.

3. El pagament per generació (dificultat a conèixer la generació de forma individualitzada).

En els últims mesos, en premsa s'estan publicant notícies sobre la implementació de la taxa, tals com el rebuig pel ple del Congrés d'una proposició no de llei del PP per exigir que es derogui l'obligatorietat de la implementació i aplicació de la taxa.

Una altra notícia, més positiva, i en la línia d'aconseguir els objectius europeus: Europa Press ha publicat que Brussel·les avala la taxa de residus que introduirà Espanya en 2025 com a mesura viable per reduir residus.

2. ELEMENTS TRIBUTARIS DE LA TAXA DE RESIDUS

Em centraré en l'anàlisi dels diferents elements tributaris de la taxa, ja que seguint el que estableix l'estudi de l'AIReF de juliol de 2023, el 88% de les entitats locals disposen d'una ordenança fiscal reguladora de la taxa, un 6% d'una ordenança del preu públic i un 5% d'una ordenança d'una PPPNT.

Des del meu punt de vista, només caben dues figures impositives: la taxa o la prestació patrimonial de caràcter públic no tributari.

Estarem davant d'una taxa quan el servei públic de recollida de residus sigui prestat en règim de dret públic mitjançant gestió directa de forma indiferenciada o per organisme autònom.

Serà PPPNT, quan el servei públic coactiu sigui prestat en règim de dret privat mitjançant gestió directa per personificació privada (societat pública o entitat pública empresarial) o mitjançant gestió indirecta (concessionari, contractista de serveis o societat mixta). També serà necessari que la contraprestació econòmica dels usuaris la percebi el gestor de dret privat.

Si és una taxa caldrà la tramitació d'una Ordenança fiscal, i si és una PPPNT caldrà la tramitació d'una Ordenança no fiscal, ja que no estem davant d'un ingrés tributari.

2.1 Àmbit subjectiu d'aplicació de la taxa

L'obligació recollida a l'article 11.3 de la Llei de residus inclou a tots els municipis, també els de més de 5.000 habitants.

El 14 de maig de 2024, el Ministeri d'Hisenda va publicar un document sobre les qüestions rellevants en relació amb l'establiment i gestió de la taxa (a partir d'ara document-guia), que afegeix novetats destacables entorn a la gestió de la taxa que hem de tenir en compte.

L'article 12.5 de la Llei de residus atribueix la recollida, el transport i el tractament dels residus als municipis com a servei obligatori en tot el seu àmbit territorial, sense distingir la seva població, mentre que l'article 26 de la Llei 7/1985, de 2 d'abril reguladora de les bases del règim locals (LBRL), sí que distingeix en funció de la població, en establir com a servei obligatori en tots els municipis la recollida de residus, i en els de més de 5.000 també el tractament.

D'altra banda, l'article 26.2 de la LBRL, estableix que en els municipis amb població inferior a 20.000 habitants serà la Diputació Provincial o entitat equivalent la que coordinarà la prestació dels següents serveis:

a) Recollida i tractament de residus
b) Abastament d'aigua potable a domicili i evacuació i tractament de les aigües residuals
c) Neteja viària
d) Accés als nuclis de població
e) Paviment de les vies públiques
f) Enllumenat públic

Per coordinar aquesta prestació de serveis la Diputació proposarà al Ministeri d'Hisenda i Administracions públiques la forma de prestació, consistent en la prestació directa per part de la Diputació o la implementació de fórmules de gestió compartida mitjançant consorcis, mancomunitats o altres fórmules.

Quan la Diputació o entitat equivalent assumeixi la prestació d'aquests serveis repercutirà als municipis el cost efectiu del servei en funció del seu ús. Si aquests serveis estiguessin finançats per taxes i assumeix la seva prestació la Diputació, serà a aquesta a qui vagi destinada la taxa per al finançament dels serveis.

2.2 Fet imposable

L'article 20 de la Llei 58/2003, de 17 de desembre, general tributària (LGT), defineix el fet imposable com el pressupòsit fixat per la llei per configurar el tribut, la realització del qual origina el naixement de l'obligació tributària principal.

D'altra banda, l'article 20 del Text refós de la Llei reguladora de les hisendes locals, aprovat per Reial decret legislatiu 2/2004, de 5 de març (TRLRHL), defineix el fet imposable de les taxes, com:

"1. Las entidades locales, en los términos previstos en esta ley, podrán establecer tasas por la utilización privativa o el aprovechamiento especial del dominio público local, así como por la prestación de servicios públicos o la realización de actividades administrativas de competencia local que se refieran, afecten o beneficien de modo particular a los sujetos pasivos".

L'apartat quart de l'article 20, precisa que les entitats locals podran establir taxes per qualsevol dels supòsits de prestació de serveis o de realització d'activitats de competència local, i en particular assenyala alguns supòsits ("numerus apertus"). Entre ells, en el seu apartat s) recull: *"Recogida de residuos sólidos urbanos, tratamiento y eliminación de éstos, monda de pozos negros y limpieza en calles particulares".*

Amb l'aprovació de la Llei de residus, s'han clarificat les actuacions relatives al fet imposable de la taxa. L'article 2.n) de la Llei de residus recull:

"A los efectos de esta ley se entenderá por:

n) "Gestión de residuos": la recogida, el transporte, la valorización y la eliminación de los residuos, incluida la clasificación y otras operaciones previas; así como la vigilancia de estas operaciones y el mantenimiento posterior al cierre de los vertederos. Se incluyen también las actuaciones realizadas en calidad de negociantes o agente".

Per tant, ara el fet imposable es refereix a la recollida, al transport, a la valorització i a l'eliminació dels residus, així com a altres actuacions contemplades en aquest apartat n).

Des del meu punt de vista, seria recomanable que en el fet imposable de l'ordenança fiscal de la taxa de residus es faci referència a aquest apartat n) de l'article 2 de la Llei de residus, de tal manera que si es modifiqués aquest precepte, la nostra ordenança fiscal no es veurà afectada per dita modificació.

És important tenir en compte que el servei de residus és coactiu, de recepció obligatòria per part dels ciutadans, per tant, encara que els contribuents no utilitzin efectivament el servei es produeix el fet imposable, i, conseqüentment l'obligació tributària corresponent. En conseqüència, tant les segones residències com els immobles desocupats hauran de pagar la taxa de residus.

Ara bé, si el servei no es presta per part de l'ajuntament, no existeix fet imposable, i, per tant, no es pot exigir la taxa.

2.3 Supòsit de no subjecció

La LGT pot completar la delimitació del fet imposable mitjançant els supòsits de no subjecció.

L'article 21 del TRLRHL, en el seu apartat primer, estableix textualment:

"1. Las entidades locales no podrán exigir tasas por los servicios siguientes:

a) Abastecimiento de aguas en fuentes públicas.
b) Alumbrado de vías públicas.
c) Vigilancia pública en general.
d) Protección civil.
e) Limpieza de la vía pública.
f) Enseñanza en los niveles de educación obligatoria."

Entre les taxes que no podran exigir les entitats locals es contempla el servei de neteja de la via pública.

És cert, que l'article 2 de la Llei de residus, contempla dins dels residus domèstics el servei de neteja viària, tal i com ja ho contemplava la Llei de residus anterior (Llei 22/2011). Ara bé, el fet que es tracti d'un residu domèstic, no implica que s'hagi d'incloure dins del fet imposable.

El legislador ha volgut excloure del fet imposable una sèrie de supòsits relacionats a l'article 21.1 del TRLRHL, per protegir l'interès públic.

Considero que el servei de neteja de la via pública no es pot incloure dins del fet imposable, en tant la llei ho estableix com un supòsit de no subjecció per motius de salubritat pública i d'interès general.

2.4 Obligatorietat d'imposar una taxa o una PPPNT per part dels ajuntaments

L'article 11.3 de la Llei de residus estableix l'obligatorietat a les entitats locals d'establir una taxa o una PPPNT, específica, diferenciada i no deficitària, que permeti implantar sistemes de pagament per generació.

D'altra banda, l'apartat cinquè del preàmbul de la llei estableix que les taxes han de "tendir" al pagament per generació. En concret es disposa: *"El capítulo II del título preliminar está dedicado a los principios de la política de residuos y a las competencias administrativas. Se refuerza la aplicación del principio de jerarquía de residuos, mediante la obligatoriedad por parte de las administraciones competentes de usar instrumentos económicos para su efectiva consecución. Teniendo en cuenta esto, se incluye expresamente por primera vez, la obligación de que las entidades locales dispongan de una tasa o, en su caso, una prestación patrimonial de carácter público no tributaria, diferenciada y específica para los servicios que deben prestar en relación con los residuos de su competencia, tasas que deberían tender hacia el pago por generación".*

El document-guia al qual he fet referència anteriorment, disposa que la norma no imposa l'obligació taxativa d'exigir una taxa totalment individualitzada amb efectes 2025, però sí que les entitats locals hauran d'incorporar de forma gradual

elements que tinguin en compte el comportament dels ciutadans en la generació dels residus.

En base a això, i tenint en compte la disparitat de municipis espanyols, aquest document-guia distingeix tres sistemes de pagament per generació:

a. Un sistema elemental: reducció sobre una única quota en funció de determinats comportaments (exemple: aportacions a la deixalleria, participació en la separació de noves fraccions de recollida separada obligatòria, adhesió a programes voluntaris de compostatge domèstic, etc...).

b. Mitjà: quota bàsica i quota variable en funció del comportament detectat segons la zona del municipi.

c. Avançat: quota bàsica i quota variable individualitzada en funció del comportament del subjecte (exemple: prestació del servei porta a porta, contenidors intel·ligents, etc...).

Sobre aquests sistemes de pagament, l'Agència Catalana de Residus, en el mes de juny de l'any 2024 va publicar a la seva seu electrònica una nota informativa assenyalant que el sistema elemental i mitjà són sistemes d'incentius, però no de taxa justa, que només ho seria el sistema avançat.

Per tal de determinar la quota bàsica, es podrien establir els següents paràmetres:

a. Taxa domiciliària:

- Tipologia o ús cadastral de l'immoble
- El nombre de residents
- El valor cadastral
- La superfície de l'immoble
- La ubicació de l'immoble

b. Taxa comercial:

- Tipus d'activitat
- Superfície
- Ubicació de l'immoble

Respecte al cànon de l'aigua com a paràmetre per establir la quota, cal fer referència a dues sentències del Tribunal Suprem, la de l'ajuntament d'Algeciras de 19 de gener de 2024 i la de l'ajuntament de Barcelona de 13 de maig de 2024, on l'Alt Tribunal estableix*: "Atendiendo, pues, a la normativa aplicable en el momento de los hechos, podemos colegir que, continuando con la jurisprudencia*

de esta Sala, el consumo de agua presenta una correlación positiva con la generación de residuos. Esta correlación se basa en que el consumo de agua depende, entre otros factores, del número de persones que habitan en un domicilio y su nivel de renta, y ambos son indicios explicatives racionales y suficientes de la generación de residuos, tal como demanda el principio de quien contamina paga".

El Tribunal Suprem analitza la taxa sota els paràmetres de la Llei 22/2011 de residus i no en relació a las noves exigències establertes a la Directiva 2018/851 i a la Llei 7/2022.

D'altra banda, també es planteja el dubte de si existeix desigualtat en l'aplicació de la taxa, si tenim en compte que cada municipi o entitat local establirà el seus paràmetres.

Tal i com estableix el document-guia, l'incompliment dels objectius comunitaris que afecten als residus municipals podria comportar que el Regne d'Espanya fos sancionat, amb el que, en aplicació del que es disposa en l'article 8 i en la disposició addicional segona de la Llei orgànica 2/2012, de 27 d'abril, d'estabilitat pressupostària i sostenibilitat financera, aquesta sanció seria repercutida a les administracions públiques i qualssevol altres entitats integrants del sector públic responsables, la qual cosa s'aplicaria a aquelles entitats locals que no complissin amb l'establiment de la taxa/PPPNT que tingui en compte el sistema de pagament per generació i que no sigui deficitària. Addicionalment, l'existència d'aquesta taxa/PPPNT pot ser exigida com a criteri condicionant per a l'accés per part de les entitats locals als fons comunitaris.

2.5 Subjectes de la taxa

És necessari distingir els subjectes actius dels passius.

2.5.1 Subjectes actius

Respecte a la gestió de la taxa, només les entitats locals podran exigir taxes. El TRLRHL estableix un seguit d'entitats locals que poden exigir taxes:

- Municipis
- Províncies
- Àrees metropolitanes
- Mancomunitats i altres entitats municipals associatives
- Comarques i altres entitats supramunicipals

La condició per establir i exigir taxes és que es tracti d'una entitat local.

L'article 3 de la LBRL estableix quines són entitats locals territorial, assenyalant:

a. El municipi
b. La província
c. L'illa en els arxipèlags balear i canari.

D'altra banda, diu que també tenen la condició d'entitats locals:

a. Les Comarques o altres entitats que agrupin varis municipis, instituïdes per les Comunitats autònomes de conformitat amb la Lley i els corresponents Estatuts d'autonomía.
b. Les Àrees metropolitanes
c. Les Mancomunitats de municipis.

Respecte als consorcis, l'article 3 LBRL no es contempla com Entitat local, ni tampoc la legislació de la Comunitat autònoma de Catalunya.

2.5.2 Subjectes passius

El legislador distingeix, en el cas de la taxa de residus, dos subjectes passius: el contribuent i el substitut.

Fixa com a subjecte passiu en concepte de contribuent a els qui sol·licitin o resultin beneficiats o afectats pel servei en qüestió (article 23.1.b. TRLRHL), és a dir, els ocupants dels immobles (com per exemple poden ser els propietaris, arrendataris, usufructuaris, precaristes, etc.).

Aquest precepte estableix: *"Son sujetos pasivos de las tasas, en concepto de contribuyentes, las personas físicas y jurídicas así como las entidades a que se refiere el artículo 35.4 de la LGT: b) Que soliciten o resulten beneficiadas o afectadas por los servicios o actividades locales que presten o realicen las entidades locales, conforme a alguno de los supuestos previstos en el artículo 20.4 de esta ley*."

Ara bé, amb la finalitat de facilitar a l'Administració tributària la gestió de la taxa, el legislador ha utilitzat la figura del substitut (definida a l'article 36.3 LGT), perquè en aquest cas es traslladi al propietari de l'immoble l'obligació tributària principal, amb la possibilitat de repercutir, si escau, les quotes sobre els respectius beneficiaris (article 23. 2.a. TRLRHL).

Textualment l'article 23.2.a del TRLRHL assenyala: *"Tendrán la condición de sustitutos del contribuyente: a) En las tasas establecidas por razón de servicios o actividades que beneficien o afecten a los ocupantes de viviendas o locales, los propietarios de dichos inmuebles, quienes podrán repercutir, en su caso, las cuotas sobre los respectivos beneficiarios."*

D'altra banda, l'article 36.3 de la LGT disposa: "*Es sustituto el sujeto pasivo que, por imposición de la ley y en lugar del contribuyente, está obligado a cumplir la obligación*

tributaria principal, así como las obligaciones formales inherentes a la misma. El sustituto podrá exigir del contribuyente el importe de las obligaciones tributarias satisfechas, salvo que la ley señale otra cosa."

A primera vista, en aquells casos en els quals el contribuent i el substitut no són la mateixa persona, com per exemple, en els lloguers (en els quals el contribuent és l'inquilí, i el propietari és el substitut) poden generar-se dubtes raonables sobre l'aparent conflicte entre la voluntat del legislador en la Llei de residus, (que imposa als ens locals la implementació de sistemes de pagament per generació en virtut del principi qui contamina paga), i la voluntat del legislador en el TRLRHL (que mitjançant la figura del substitut, trasllada el pagament de la taxa al propietari de l'immoble). A priori, en aquests casos podria semblar que l'ocupant contamina (subjecte passiu a títol de contribuent), però no paga, en fer-se càrrec el propietari (subjecte passiu a títol de substitut). No obstant això, de l'estudi de la norma tributària, des del meu punt de vista, es conclou que no hi ha tal controvèrsia ni contradicció entre la voluntat d'ambdues normes.

El contribuent és l'obligat tributari en base al comportament del qual es determina la quota tributària de la taxa, així com les possibles reduccions de la mateixa (STS de 23 de juny de 1986 i STS de 24 de gener de 2013).

Aquesta última sentència assenyala:

> *"La realización del hecho imponible determina el nacimiento de la obligación tributaria con cargo al contribuyente, es decir, a la persona que, situada en las circunstancias que configuran el elemento subjetivo del hecho imponible, realiza, según la Ley, este hecho. Con relación a él, en consecuencia, debe determinarse la existencia y cuantificación de tal obligación, las posibles exenciones, etc. La realización del presupuesto de hecho de la sustitución, siempre lógicamente posterior a la realización del hecho imponible, determina la transmisión de la obligación tributaria del contribuyente al sustituto y la asunción por éste y por mandato de la Ley, de tal obligación como una obligación propia.*
> *(…)*
>
> *El sustituto, cuando así lo impone la Ley, se coloca en lugar del contribuyente en el momento del cumplimiento y no del nacimiento de la obligación tributaria. La Ley impone la transmisión de la deuda del contribuyente al sustituto, de tal modo que éste está obligado a cumplir la obligación del contribuyente como propia".*

Als efectes d'identificació de l'usuari (i posterior quantificació dels residus generats), crec que és convenient tenir en compte la referència cadastral o la unitat tributària com identificador de l'objecte tributari.

El pressupòsit de fet de la substitució (article 36 LGT) és sempre diferent i posterior al pressupòsit de fet que origina la realització del fet imposable. En aquest sentit, únicament es trasllada l'obligació tributària principal al substitut (propietari en la taxa de gestió de residus), però sense alterar ni incidir en la relació jurídic-tributària inicial.

Precisament per no realitzar el fet imposable ni ser titular de la capacitat econòmica gravada, la subjecció fiscal del substitut té com a rescabalament el dret a repercutir al contribuent l'import de les obligacions satisfetes (article 36.3 LGT). Això és a causa que assumeix com a pròpia una càrrega contra el seu patrimoni, per un imperatiu legal.

Aquest desplaçament de l'obligat final al pagament no altera la relació jurídic-tributària inicial, per la qual cosa cap dels seus elements (fet imposable- subjecte passiu contribuent- determinació de la quota tributària) es veuen alterats, ni les circumstàncies del substitut tenen influència alguna en cap d'aquests elements.

Aquest mecanisme legal té com a principal finalitat facilitar la gestió dels tributs per motius purament funcionals i pragmàtics en la gestió tributària, entesa en el seu sentit més ampli. Al respecte, cal portar a col·lació la sentència del Tribunal Suprem de 24 de setembre de 1999, la qual assenyala:

"Con el fin de garantizar, asegurar, reforzar, en suma conseguir que las obligaciones tributarias sean cumplidas, nuestro Derecho Tributario regula diversas instituciones que se pueden sistematizar del siguiente modo: a) Utilización de sujetos pasivos peculiares, que no existen en el Derecho privado, como son los sujetos sustitutos, con retención o sin ella, y los sujetos retenedores, sin sustitución, además del sujeto contribuyente que es el que ha realizado el hecho imponible (arts. 30, 31 y 32 de la LGT). La justificación de la existencia jurídica de los sujetos sustitutos y retenedores es puramente funcional y pragmática".

En la mateixa línia, la sentència del Tribunal Suprem de 25 d'abril de 2022 estableix: *"(…) una regulación abierta, como la vista, se adapta mejor a un ordenamiento jurídico dinámico y presto para regular aquellas situaciones que demanda la realidad, sin que, como se ha dicho, se comprometan las reglas o los principios que deben presidir la estructuración de los elementos configuradores de los tributos, como es, en este caso, el sujeto pasivo".*

Tenint en compte l'anterior, pel que fa a la part variable de la taxa per la gestió de residus (en la qual es té en compte el volum de residus generats per determinar la quota tributària), quan el contribuent no coincideixi amb el substitut (lloguers, usdefruits, precaris, etc.,) igualment es complirà la voluntat del legislador amb el principi de "qui contamina paga", ja que el subjecte passiu que utilitza el servei i genera els residus que configuren aquesta part variable (contribuent), és veritablement qui "contribueix" (realitza el fet imposable, i és el subjecte passiu establert per llei). Posteriorment, es veu desplaçat pel substitut per un imperatiu legal els motius del qual són merament funcionals i pragmàtics, però la seva aparició no influeix en absolut ni en el fet imposable, ni en la determinació de la quota tributària de la taxa. Tal és així, que el contribuent mai perd la seva condició com a tal. A més, el substitut podrà repercutir l'import satisfet al contribuent que és la persona que genera els residus. Ara bé, és destacable que, per exemple, en el cas de l'usdefruit

en l'IBI, el propietari de l'immoble no assumeix el pagament de l'impost, però en canvi sí assumeix el pagament de la taxa de gestió de residus com a substitut.

Pel que fa a l'aplicació de reduccions per motius de capacitat econòmica, hem de seguir la mateixa lògica a l'efecte de determinar qui és el subjecte que ha de tenir-se en compte per justificar la seva aplicació. Les reduccions determinen la quota tributària que assumeix el subjecte passiu contribuent, amb anterioritat a traslladar-se l'obligació de pagament al substitut. Precisament per aquest motiu, sempre han de tenir-se en compte les circumstàncies del contribuent prestatari del servei, i no les del substitut, ja que el pressupòsit de fet que l'inclou en l'equació és posterior a la realització del fet imposable i a la determinació de la quota tributària, quedant relegat a assumir el pagament, i podent repercutir al contribuent. Malgrat que la sol·licitud de l'aplicació de les reduccions pot efectuar-se per tots dos subjectes passius, sempre seran en relació amb el contribuent (qui realitza el fet imposable i utilitza el servei i genera els residus), i no del substitut que és un simple instrument de la llei per facilitar la gestió tributària.

En aquest sentit es pronuncia la sentència del Tribunal Suprem de 23 de juny de 1986:

"Los beneficios tributarios, como reducciones, bonificaciones o exenciones que se configuran en los artículos 10, 14 y 15 de la Ley 230/1963 son en muchos supuestos manifestaciones de la actividad administrativa de fomento como modalidades de signo positivo y contenido económico, en su calidad de auxilio financiero, a costa del erario público, e indirecto para estimular la iniciativa privada en un determinado sector. Ahora bien, el beneficiario de la ayuda directa o no es siempre el titular de la actividad. Como la posición tributaria de vendedor y comprador no es fungible, comunicable o intercambiable (aun cuando lo sean sus consecuencias económicas), resulta claro que tampoco es posible extender el ámbito de una exención otorgada por razón de una actividad educativa a quien no la ejerce y se desentiende definitivamente de la que va a ser su base física, el terreno. Así lo establece el artículo 520 de la Ley de Régimen Local, cuyo párrafo tercero pone en claro que el derecho de exención habrá de referirse siempre a la persona o entidad sobre la cual recaiga este arbitrio, con total abstracción de la persona o entidad obligada al pago. En el sentido que se viene exponiendo se pronuncian, entre otras, nuestras sentencias de 5 de Junio de 1972 (RJ 1972\2583) y 7 de Octubre de 1983 (RJ 1983\5041)".

Recordem que l'Ajuntament no pot modificar el subjecte passiu del tribut, ja que existeix reserva de llei en la determinació dels elements tributaris de la taxa.

2.6 Informe tecnicoeconòmic

Com he avançat a la introducció, un dels reptes principals en que s'enfronten els tècnics municipals és l'elaboració d'un informe econòmico-financer que sigui el més ajustat possible.

Amb l'aprovació de la Llei de residus, les dificultats han augmentat considerablement, tenint en compte el que regula l'article 24.2 del TRLRHL i el principi incorporat a l'article 11.3 de la llei de residus.

L'article 24.2 del TRLRHL disposa: *"En general, y con arreglo a lo previsto en el párrafo siguiente, el importe de las tasas por la prestación de un servicio o por la realización de una actividad no podrá exceder, en su conjunto, del coste real o previsible del servicio o actividad de que se trate o, en su defecto, del valor de la prestación recibida.*

Para la determinación de dicho importe se tomarán en consideración los costes directos e indirectos, inclusive los de carácter financiero, amortización del inmovilizado y, en su caso, los necesarios para garantizar el mantenimiento y un desarrollo razonable del servicio o actividad por cuya prestación o realización se exige la tasa, todo ello con independencia del presupuesto u organismo que lo satisfaga. El mantenimiento y desarrollo razonable del servicio o actividad de que se trate se calculará con arreglo al presupuesto y proyecto aprobados por el órgano competente."

Per tant, l'import de la taxa de residus per la prestació del servei no pot excedir, en el seu conjunt, del cost real o previsible del servei.

Aquest principi de les taxes que el Tribunal Suprem s'ha encarregat de ratificar en innumerables ocasions, topa amb el principi establert a l'article 11.3 de la Llei de residus quan assenyala que la taxa no pot ser deficitària.

Davant d'aquest problemàtica d'intentar reflectir tot el cost del servei sense superar el cost real, el document-guia del Ministeri estableix que la previsió de la Llei de residus és un principi i no imposa als ajuntaments una absoluta precisió en la cobertura dels costos del servei, sinó que aquesta cobertura s'aproximi al màxim al cost real del servei. Per tant, ha de ser interpretat com el necessari compliment d'un principi i no com la imposició als ajuntaments d'una absoluta precisió en la cobertura del cost del servei.

L'informe de l'AIReF de juny de 2023 estableix que, en l'actualitat, les taxes de residus només estan cobrint un 60% del cost del servei. Per tant, sembla que encara queda molt marge per cobrir.

Dit això, des del meu punt de vista, l'objecte de l'informe hauria de tenir en compte dos paràmetres imprescindibles:

1. S'ha de verificar que es compleix amb el principi d'equivalència. Sobre la base que les taxes són tributs, la llei ha volgut que s'orientessin sota el principi d'equivalència. El Tribunal Suprem en sentència de 18 de desembre del 2000,

estableix al respecte: "*La equivalencia entre coste del servicio e importe estimado de las tasas por la prestación del mismo se refiere a "su conjunto", como dice el art. 24 de la Ley de Haciendas Locales...; no cabe, por lo tanto, exigir esa equivalencia en cada liquidación, ni que en cada expediente liquidatorio se incluya un estudio económico particularizado de la adecuación, caso por caso*".

2. S'ha d'aproximar al màxim a l'encàrrec legal d'establir una taxa no deficitària.

D'altra banda, recomano que el càlcul de la taxa es realitzi de manera separada respecte als residus domiciliaris envers els comercials.

En relació als dubtes que pugui haver-hi en relació als costos i ingressos que s'han de tenir en compte, el document-guia estableix que han de ser tots aquells que reflecteixin els costos i ingressos reals per la prestació del servei. A títol merament exemplificatiu, assenyala els següents:

A. Costos directes	**Cost estimat per a l'exercici**
Personal	
Contracte recollida residus	
Manteniment i reparacions maquinària i vehicles	
Assegurança de béns destinats al servei de gestió de residus	
De transport	
Tributs (*)	
Lloguers de terrenys, construccions, maquinaria	
Subministrament d'energia elèctrica, agua, gas, combustibles	
Cost total tractament diferents fraccions de residus	
Cost amortització	
Costos financers	

B. Costos indirectes	**Cost estimat per a l'exercici**
Personal ajuntament	
Altres (costos control qualitat, campanyes publicitàries, etc...)	

(*) Dins de l'apartat de tributs es contemplarà l'Impost sobre el dipòsit de residus en abocadors, l'IVA i la taxa per la prestació del servei per part

d'una altra entitat supramunicipal del servei de gestió o recaptació de la taxa de residus.

Respecte als ingressos relatius a la responsabilitat ampliada del productor (SRAP) i venda de materials i energia, tindríem:

Ingressos	**Import total**
Retorn venda materials (plàstic, paper, etc...)	
Retorn venda energia	
Retorn per l'aplicació ampliada del productor	
Altres retorns	

2.7 Quota tributària

L'import de la taxa ha de reflectir els costos i ingressos als quals es refereix la llei de residus.

Pel càlcul de la quota tributària, i tenint en compte un model avançat, el model d'ordenança fiscal que l'Organisme de Gestió Tributària proposa als ajuntaments es basa en el següent:

1. Residus domiciliaris:

a. Part bàsica;

- Cobreix els costos estructurals del servei
- Es calcula sobre la base d'una tarifa segons el tipus d'immoble
- Les reduccions sobre aquesta part bàsica són les relatives a la capacitat econòmica regulades a l'article 24.4 del TRLRHL

b. Part variable;

- Immobles amb recollida porta a porta i/o amb contenidors tancats amb identificació de l'usuari: en funció de la quantitat i tipus de residus generats per unitat d'immoble
- Immobles amb àrees tancades com a sistema únic de recollida. En funció del nombre d'entrades anuals a les àrees tancades

- Reduccions article 11.4 Llei de residus: aportacions deixalleria, compostatge domèstic, etc…

2. Residus comercials;

a. Part bàsica;

- Diferents tarifes segons el tipus d'activitat

- Incorporem una tarifa pels habitatges de lloguer turístic, coliving, etc..., ja que considerem que estem davant d'activitats.

b. Part variable;

- En funció de la quantitat i tipus de residu generat per unitat de local

L'Organisme de Gestió Tributària en el seu model d'ordenança fiscal ha establert un percentatge màxim de reducció, ja que entenem que si es redueix tota la quota íntegrament estaríem davant una exempció no prevista en la normativa.

2.8 Beneficis fiscals: reduccions i bonificacions

L'article 9.1, primer paràgraf del TRLRHL estableix textualment: "*No podrán reconocerse otros beneficios fiscales en los tributos locales que los expresamente previstos en las normes con rango de ley o los derivados de la aplicación de tratados internacionales*".

Cal fer la distinció entre exempcions, bonificacions i reduccions.

a. Exempcions

L'article 22 de la LGT estableix que són supòsits d'exempció aquells en què, tot i realitzar-se el fet imposable, la llei eximeix del compliment de l'obligació tributària principal.

En el cas de les taxes, l'apartat segon de l'article 21 del TRLRHL només estableix un supòsit d'exempció que no aplica a la taxa de residus. Textualment, l'article 21.2 estableix:

"*El Estado, las comunidades autónomas y las entidades locales no estarán obligados al pago de las tasas por utilización privativa o aprovechamiento especial del dominio público por los aprovechamientos inherentes a los*

servicios públicos de comunicaciones que exploten directamente y por todos los que inmediatamente interesen a la seguridad ciudadana o a la defensa nacional".

b. Reduccions

En la taxa de residus, l'ajuntament pot regular a la seva ordenança fiscal dos tipus de reduccions:

1. La contemplada a l'article 24.4 del TRLRHL, relativa a la capacitat econòmica. Aquest precepte disposa que per a la determinació de la quantia de les taxes podran tenir-se en compte criteris genèrics de capacitat econòmica dels subjectes obligats al pagament.

   Si l'ajuntament vol establir reduccions per famílies nombroses o monoparentals haurà de tenir en compte aquesta capacitat econòmica dels subjectes obligats al pagament.

2. Les recollides a l'article 11.4 de la Llei de residus on s'estableix que las taxes o PPPNT podran tenir en compte, entre d'altres, les particularitats següents:

   a) La inclusió de sistemes per incentivar la recollida separada en habitatges de lloguer vacacional i similar.

   b) La diferenciació o reducció en el supòsit de pràctiques de compostatge domèstic o comunitari o de separació i recollida separada de matèria orgànica compostable.

   c) La diferenciació o reducció en el supòsit de participació en recollides separades per a la posterior preparació per a la reutilització i reciclat, per exemple, en punts nets o en els punts de lliurament alternatius acordats per l'entitat local.

   d) La diferenciació o reducció per a les persones i les unitats familiars en situació de risc d'exclusió social.

   Respecte a la reducció per persones o unitats familiars en situació de risc d'exclusió social, al no existir un registre públic, ni estatal ni autonòmic, que relacioni les persones en aquesta situació, haurà de ser l'ordenança fiscal la que estableixi els aspectes formals i substantius d'aquesta reducció.

c. Bonificacions

La Llei de residus introdueix una bonificació a l'apartat sisè de l'article 24 del TRLRH, que aplica per a la taxa de residus comercials.

La finalitat d'aquesta bonificació és la reducció del residu alimentari. Seran les ordenances fiscals les que hauran d'establir els aspectes substantius i formals de la mateixa.

L'article 24.6 del TRLRHL disposa que *"Les entitats locals podran establir mitjançant ordenança una bonificació de fins a un 95 per cent de la quota íntegra de les taxes o si escau, de les prestacions patrimonials de caràcter públic no tributari, que s'exigeixin per la prestació del servei de recollida de residus sòlids urbans per a aquelles empreses de distribució alimentària i de restauració que tinguin establerts, amb caràcter prioritari, en col·laboració amb entitats d'economia social sense d'ànim de lucre, sistemes de gestió que redueixin de forma significativa i verificable els residus alimentaris, sempre que el funcionament d'aquests sistemes hagi estat prèviament verificat per l'entitat local."*

La dificultat en aquesta bonificació està a verificar el sistema utilitzat per a la reducció dels residus alimentaris.

El model d'ordenança fiscal de l'Organisme de Gestió Tributària estableix que la sol·licitud de la bonificació s'haurà de presentar-se abans de l'1 de març, i la mateix haurà d'anar acompanyada de la següent documentació:

- Memòria explicativa del sistema de gestió implantat
- Identificació de les entitats d'economia social sense ànim de lucre

El tècnic municipal haurà d'emetre informe de valoració justificatiu dels requisits establerts en l'Ordenança fiscal.

S'està tramitant un projecte de llei de prevenció, de les pèrdues i el rebuig alimentari. Aquest projecte de llei pretén donar un nou enfocament centrat en la prevenció i conscienciació de tots els actors de la cadena alimentària.

La nova Llei estableix l'obligatorietat pels tots els agents de la cadena alimentaria de comptar amb un plan de prevenció de pèrdues i rebuig alimentari.

Així, l'article 6.5.b) d'aquesta lLei, estableix entre les obligacions de tots els agents de la cadena alimentària, arribar a acords o convenis per donar els seus excedents d'aliments a entitats d'iniciativa social i altres organitzacions sense ànim de lucre. Per tant, semblaria que amb la nova llei deixaria de tenir sentit aquesta bonificació.

El document-guia del Ministeri d'Hisenda deixa constància que la menor quota a satisfer pel subjecte passiu al que se li aplica una reducció o bonificació no implica que la resta dels subjectes passius hagin de pagar una major quota equivalent.

2.9 Meritació

La meritació de les taxes està regulada a l'article 26 del TRLRHL, el qual estableix:

"*1. Las tasas podrán devengarse, según la naturaleza de su hecho imponible y conforme determine la respectiva ordenanza fiscal:*

a) Cuando se inicie el uso privativo o el aprovechamiento especial, o cuando se inicie la prestación del servicio o la realización de la actividad, aunque en ambos casos podrá exigirse el depósito previo de su importe total o parcial.

b) Cuando se presente la solicitud que inicie la actuación o el expediente, que no se realizará o tramitará sin que se haya efectuado el pago correspondiente.

2. Cuando la naturaleza material de la tasa exija el devengo periódico de ésta, y así se determine en la correspondiente ordenanza fiscal, el devengo tendrá lugar el 1 de enero de cada año y el período impositivo comprenderá el año natural, salvo en los supuestos de inicio o cese en la utilización privativa, el aprovechamiento especial o el uso del servicio o actividad, en cuyo caso el período impositivo se ajustará a esa circunstancia con el consiguiente prorrateo de la cuota, en los términos que se establezcan en la correspondiente ordenanza fiscal.

3. Cuando por causas no imputables al sujeto pasivo, el servicio público, la actividad administrativa o el derecho a la utilización o aprovechamiento del dominio público no se preste o desarrolle, procederá la devolución del importe correspondiente".

La taxa de residus es merita l'1 de gener de cada any i el seu període impositiu coincideix amb l'any natural, excepte en els supòsits d'inici o cessament de l'activitat.

En el cas que l'ajuntament reguli a la seva ordenança fiscal una quota bàsica i una quota variable, l'exigibilitat de les dues quotes no té perquè produir-se en el mateix any. És a dir, la taxa es meritarà l'1 de gener per ambdues, però la quota bàsica es pot exigir el mateix any de la meritació, mentre que la quota variable es podria exigir a l'any següent, quan l'ajuntament disposi de totes les dades de generació de residus dels contribuents.

2.10 Gestió de la taxa

2.10.1 Gestió tributària

L'article 27 del TRLRHL regula la gestió del tribut, assenyalant que les entitats locals podran exigir les taxes en règim d'autoliquidació.

En el cas de la taxa que ara ens ocupa, al ser de meritació periòdica, la seva gestió es realitzarà mitjançant el sistema de padró (llistat de valors-rebuts).

L'article 102.3 de la LGT estableix que els tributs de cobrament periòdic es podran notificar edictalment. En concret, aquest precepte disposa:

"*En los tributos de cobro periódico por recibo, una vez notificada la liquidación correspondiente al alta en el respectivo registro, padrón o matrícula, podrán notificarse colectivamente las sucesivas liquidaciones mediante edictos que así lo adviertan.*

El aumento de base imponible sobre la resultante de las declaraciones deberá notificarse al contribuyente con expresión concreta de los hechos y elementos adicionales que lo motiven, excepto cuando la modificación provenga de revalorizaciones de carácter general autorizadas por las leyes".

El dubte que es planteja envers el disseny de la quota de la nova taxa de residus és sobre la quota variable, ja que aquesta serà diferent cada any en funció del comportament del contribuent (augmentant o disminuint segons aquest comportament). Si la quota augmenta, segons l'establert al segon paràgraf de l'apartat tercer de l'article 102 de la LGT, caldria realitzar una notificació individual al contribuent.

El document-guia del Ministeri d'Hisenda diu al respecte que el disseny de la quota permet, que una vegada notificada individualment la inclusió en la corresponent matrícula (padró fiscal), es puguin notificar col·lectivament les successives liquidacions, encara que existeixin variacions provocades per la generació de residus.

La consulta vinculant de la Direcció general de tributs d'1 d'agost de 2024, on es planteja una qüestió similar envers la taxa d'aigua, resol en el següent sentit:

"*En las ordenanzas fiscales reguladoras de las tasas objeto de la consulta, la cuota se determina por un cuadro de tarifas contenido en la propia ordenanza. En dicho cuadro se fija una cantidad a pagar por cada metro cúbico de consumo de agua, en función del tipo de inmueble y los distintos tramos de consumo. De esta forma, sabiendo la cantidad de metros cúbicos de consumo de agua en cada uno de los periodos, el sujeto pasivo tiene pleno conocimiento del importe de la tasa, ya que tan solo tiene que multiplicar la cantidad de metros cúbicos de agua consumida por la cuantía de euros por metro cúbico del tramo de la tarifa que corresponda al total consumido. (...), además de que el sujeto pasivo también puede tener acceso a la cantidad de agua consumida consultando el contado del agua.*
(...)
En las tasas objeto de esta consulta, con la notificación individual de la liquidación correspondiente al alta en el servicio y la comunicación del volumen de agua

consumida en cada periodo (en el propio recibo y en el contador de agua), el sujeto pasivo tiene pleno conocimiento del importe de la liquidación de la tasa en cada uno de los periodos trimestrales, cumpliéndose los requisitos de la notificación de las liquidaciones tributarias establecidas en el artículo 102.3 de la LGT".

2.10.2 Protecció de dades

Les dades de la part variable les haurà de facilitar l'empresa que presta el servei de residus.
Aquests sistemes d'implementació de sistemes de recollida amb identificació del usuari requereixen tenir en compte la normativa sobre protecció de dades per donar seguretat jurídica als municipis i als usuaris del servei.

En aquest cas, el tractament de dades personals està legitimat per l'exercici d'una missió d'interès públic.

La legislació marc de protecció de dades a nivell europeu és el Reglament relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades (Reglament UE 2016/679), que és d'aplicació directe per a tots els Estats Membres.

L'article 6 d'aquest Reglament, estableix:

"Licitud del tratamiento:

1. *El tratamiento será licito si se cumple al menos una de las siguientes condiciones:*

   e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferides al responsable del tratamiento".

Per valorar les dades tractades, seguin el que estableix la guia per la protecció de dades personals de l'Agència de Residus de Catalunya, podem distingir tres tipus de dades:

a. Dades contractuals; són les dades necessàries per fer funcionar el servei de recollida (exemple: número d'usuari, que està relacionat amb l'adreça de l'habitatge o de l'establiment comercial, dades de contacte, etc...).

   En aquest cas, no és necessari el consentiment del contribuent perquè la cobertura legal ens ve donada directament per l'aplicació de les següents lleis: la Llei de residus (article 25.2) i la Llei de bases de règim local (article 26).

b. Dades relacionades amb els residus; són les dades que es generen amb el funcionament del servei, relatives al comportament dels usuaris, als permisos atorgats, a la seva generació de residus i a si participen o no en la recollida selectiva.

   En aquest cas, tampoc necessitaríem el consentiment del contribuent pel mateix raonament que en el cas anterior (article 11.3 Llei de residus i article 20 i ss TRLRHL).

c. Dades complementàries; són les dades que no són necessàries per prestar el servei de recollida, ni per conèixer la participació de l'usuari. Són dades que estan vinculades a serveis addicionals, com per exemple el sistema d'avisos.

   En aquest cas, és necessari el consentiment del contribuent.

Ara bé, no hem d'oblidar que el contracte de prestació de serveis haurà de contemplar totes les clàusules relatives a la protecció de dades que correspongui.

Al respecte, hi ha una sèrie de consultes per part de diferents ajuntament a l'Autoritat Catalana de Protecció de Dades sobre aquest tema, que recomano llegir. Entre d'altres, destaco la consulta CNS 6/2020, la consulta CNS 60/2021 i la consulta CNS01/2024.

2.10.3 Exigència de les PPPNT

Per últim, respecte a les PPPNT es planteja el dubte si aquestes poden ser exigides per via de constrenyiment. La consulta de la Direcció general de tributs de 3 de juny de 2020 dona resposta a aquesta qüestió. En concret estableix:

"*El inicio del procedimiento de apremio en el supuesto de PPPNT deberá estar precedido del transcurso del periodo voluntario de pago de las mismas, previa notificación de la correspondiente liquidación al obligado al pago, notificación que deberá efectuarse de forma fehaciente.*

La ordenanza municipal que regule la PPPNT por el Servicio de recogida de basuras debe regular el periodo voluntario de pago de la misma.

Transcurrido el periodo voluntario de pago de la PPPNT, y ante la situación de impago de la misma a la Sociedad mercantil por parte del usuario, dicha Sociedad deberá comunicarlo al ayuntamiento o al Organismo Autónomo de Gestión Tributaria del mismo, a los efectos de que por estos últimos se proceda a practicar la correspondiente liquidación al obligado al pago, a su notificación y, en su caso, a la expedición de la providencia de apremio que inicie el procedimiento de apremio".

Aquesta mateixa consulta es pronuncia envers si les PPPNT han d'estar subjectes a l'Impost sobre el valor afegit (IVA). La Direcció general de tributs, considera que sí estan subjectes a l'impost. En el cas de les taxes, en canvi, no hi hauria subjecció.

2.10.4 Comunicació taxa

L'apartat cinquè de l'article 11 de la Llei de residus, estableix textualment:

"*5. Las entidades locales deberán comunicar estas tasas, así como los cálculos utilizados para su confección, a las autoridades competentes de las comunidades autónomas".*

Cal establir quines són les autoritats competents de les comunitats autònomes, sembla que podrien ser les agències de residus.

3. CONCLUSIONS

La Llei de residus és un instrument imprescindible per aconseguir una cultura ambiental de reciclatge. Aquesta llei incorpora dues novetats envers els residus: en primer lloc, l'obligatorietat per part de tots els municipis d'implementar una taxa o una PPPNT; i, en segon lloc, que aquesta taxa o PPPNT no sigui deficitària.

Tot i que l'article 11.3 de la Llei de residus estableix un termini de tres anys a comptar des de l'entrada en vigor (10 d'abril de 2022) per implementar aquestes prestacions, les entitats locals hauran de tenir aprovada la seva ordenança fiscal de la taxa o la no fiscal de la PPPNT, abans de l'1 de gener de 2025 (data de meritació de la taxa).

A principis de l'any 2026, caldrà fer balanç del següent:

1. Del nivell d'implementació de la taxa o de la PPPNT
2. Del sistema de pagament per generació (elemental, mitjà o avançat) adoptat per cada ajuntament
3. Del volum de recursos presentats pels contribuents i de l'anàlisi de les al·legacions
4. Dels percentatges recaptats envers els costos del servei
5. Compliment dels objectius europeus

Haurem d'espera una mica més per saber què en pensen els tribunals als respecte dels recursos contenciosos-administratius que es presentin.

En qualsevol cas, penso que davant tanta imprecisió normativa, caldria fer una reforma en profunditat per tal de regular tots els elements tributaris de la taxa, o encara millor, per eliminar la taxa i establir un impost.

S'indica l'enllaç als models d'informe tecnicoeconòmic i a les ordenances fiscals de l'Organisme de Gestió Tributària: Models ordenances fiscals tipus 2025 - Normativa - Diputació de Barcelona

Barcelona, 21 de febrer de 2025

SEMINARI
Gestió Econòmica Local

FMC

La taxa de residus. Consideracions jurídiques i tècniques sobre la seva implementació

Cristina Casablanca
Gerent de l'ORGT

Doble finalitat extra fiscal del pagament per generació:

Promoure la reducció del volum de residus

- Progressiva disminució de la despesa

Incrementar separació i reciclatge

- Increment activitat econòmica del reciclatge

Principals dificultats

Falta regulació

Inseguretat jurídica

Pagament per generació

29-11-2024 | Agència Europa Press

El Ple del Congrés ha rebutjat una proposició no de llei del PP per exigir que es derogui l'obligatorietat d'implantar i aplicar, a partir de l'abril de 2025, una taxa de residus al 100% dels municipis.

Europa Press

Brussel·les avala la taxa d'escombraries que introduirà Espanya el 2025 com a mesura viable per reduir residus.

La Comissió Europea ha avalat la nova taxa d'escombraries que han d'aplicar tots els ajuntaments d'Espanya des de l'abril de 2025 com una de les mesures viables per reduir deixalles que recull la directiva europea de residus.

ELEMENTS TRIBUTARIS DE LA TAXA

Informe AIReF

Taxa (88%)

Preu públic (6%)

PPPNT (5%)

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE HACIENDA

DIRECCIÓN GENERAL DE TRIBUTOS
Óscar del Amo Galán

EL SUBDIRECTOR GENERAL DE
TRIBUTOS LOCALES

Qüestions rellevants pel que fa a l'establiment i la gestió de la taxa local de residus sòlids urbans

1. Àmbit subjectiu d'aplicació

Llei de residus

Gestió de residus obligatoria per tots els municipis

VS

LBRL

Gestió de residus obligatoria només per municipis més 5.000 h.

2. Fet imposable

Està constituït:

- Recollida
- Transport
- Tractament (valorarització i eliminació)
- Altres actuacions (art. 2 n) Llei de residus): vigilància d'aquestes operacions, etc.

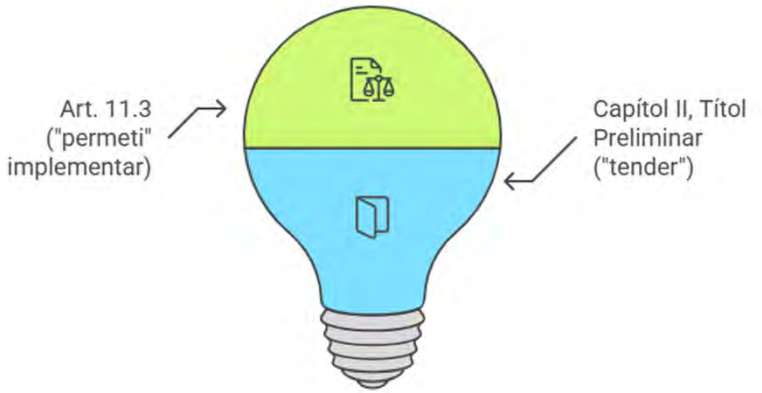
Servei coactiu: recepció obligatoria

No es pot exigir la taxa en cas de no prestació del servei.

3. Supòsit de no subjecció

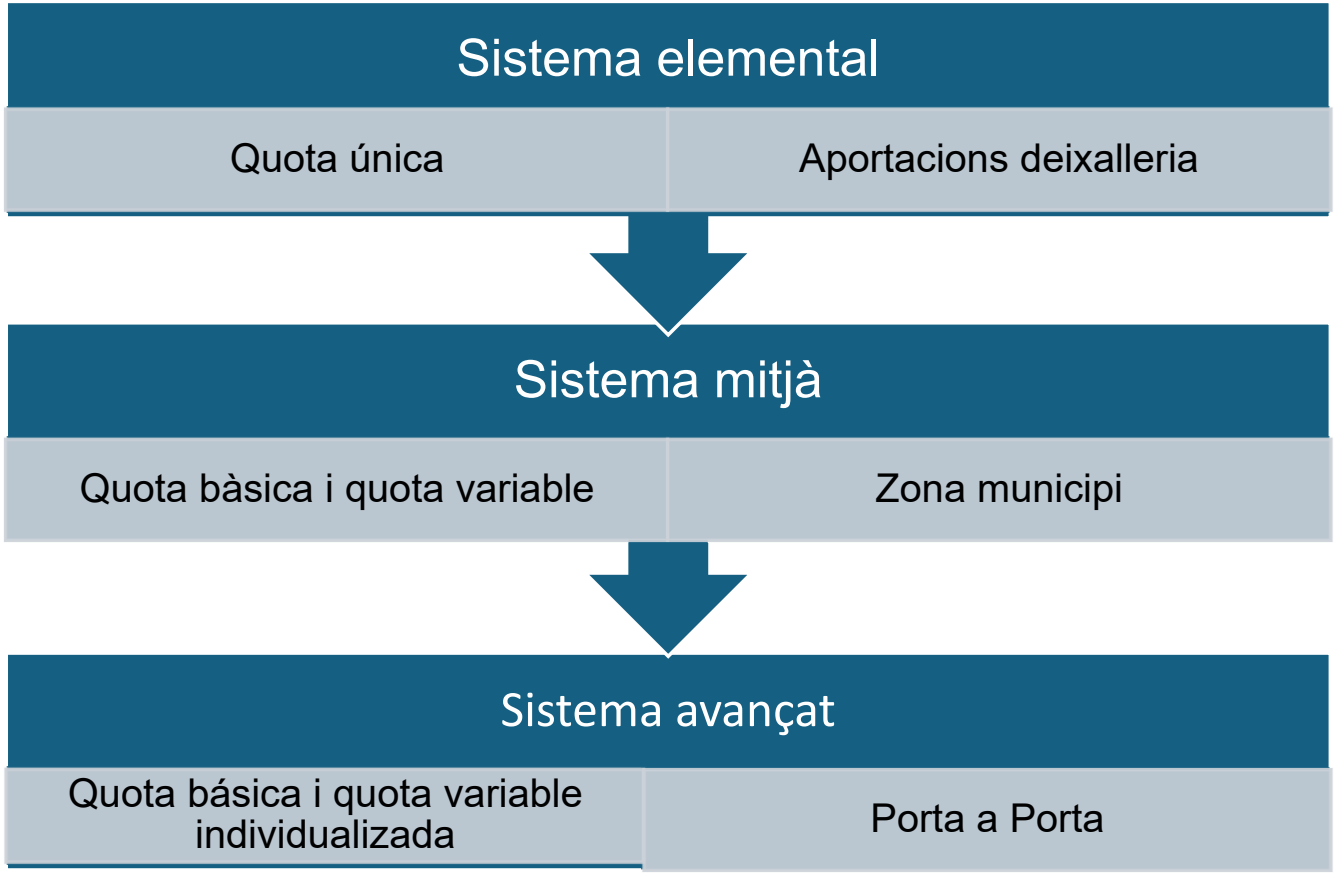
4. Obligatorietat de la taxa/PPNT

L'art. 11.3 estableix l'obligatorietat a les entitats locals d'establir una taxa o una PPPNT, específica, diferenciada i no deficitària, que permeti implantar sistemes de pagament per generació



La norma NO imposa l'obligació taxativa d'exigir una taxa totalment individualitzada.

Incorporació gradual elements de generació.


Sistema elemental
Quota única
Aportacions deixalleria
Sistema mitjà
Quota bàsica i quota variable
Zona municipi
Sistema avançat
Quota básica i quota variable individualizada
Porta a Porta

Paràmetres per fixar la quota

Residus domiciliaris

- Tipologia o ús cadastral de l'inmoble
- Valor cadastral
- Nombre d'habitants
- Superfície
- Ubicació de l'immoble

Residus comercials

- Tipus d'actividat
- Superficie
- Ubicació de l'immoble

STS 13/maig/2024

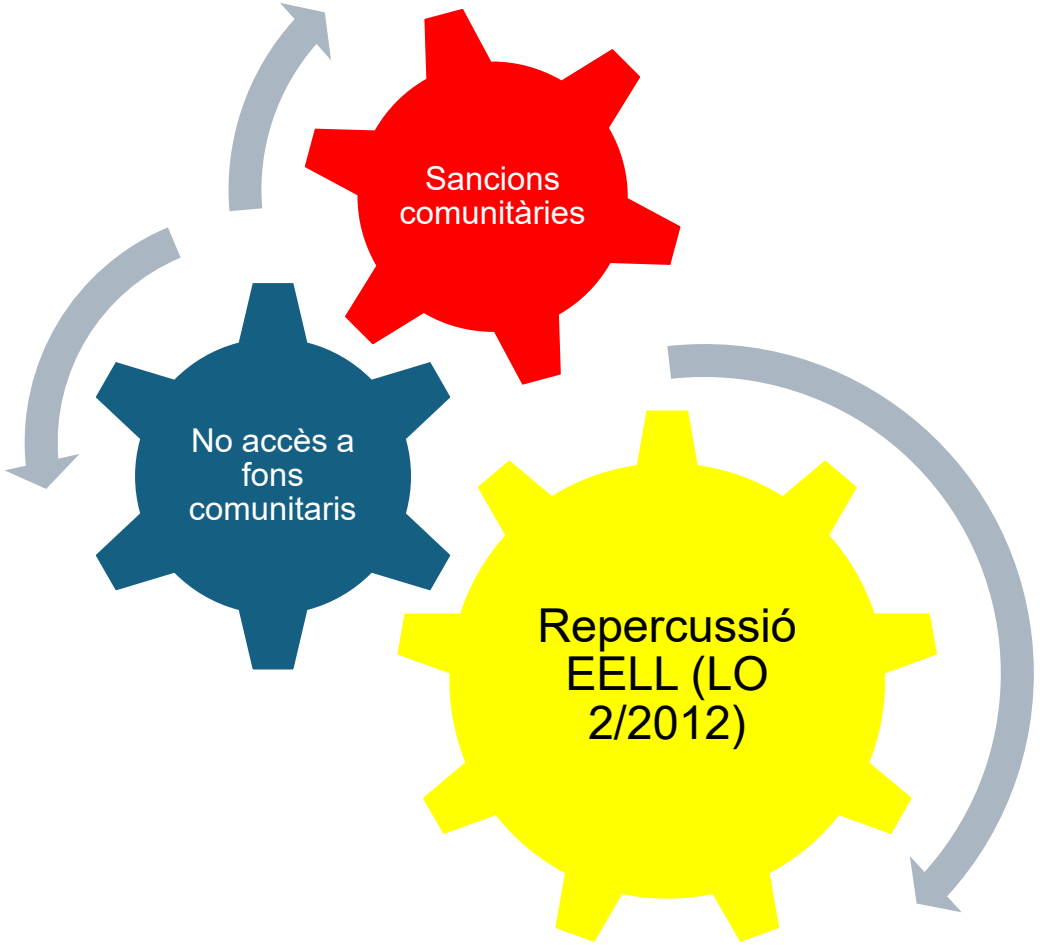
Consum d'aigua

Desigualtats en l'aplicació de la taxa

Un dels principals problemes que planteja aquesta nova taxa és la disparitat en la seva aplicació entre diferents municipis. Actualment, els ajuntaments utilitzen **diferents criteris per calcular** el cost del servei d'escombraries per ciutadà, com ara la mida de l'habitatge, el consum d'aigua o el valor cadastral. Aquests **paràmetres**, però, no reflecteixen de manera precisa la quantitat de residus generats per cada llar. Això podria portar a situacions injustes en què ciutadans que produeixen menys escombraries acabin pagant el mateix que aquells que no reciclen o generen més deixalles.

Els paràmetres són indicis només per al càlcul de la quota bàsica

Què passa en cas d'incompliment?

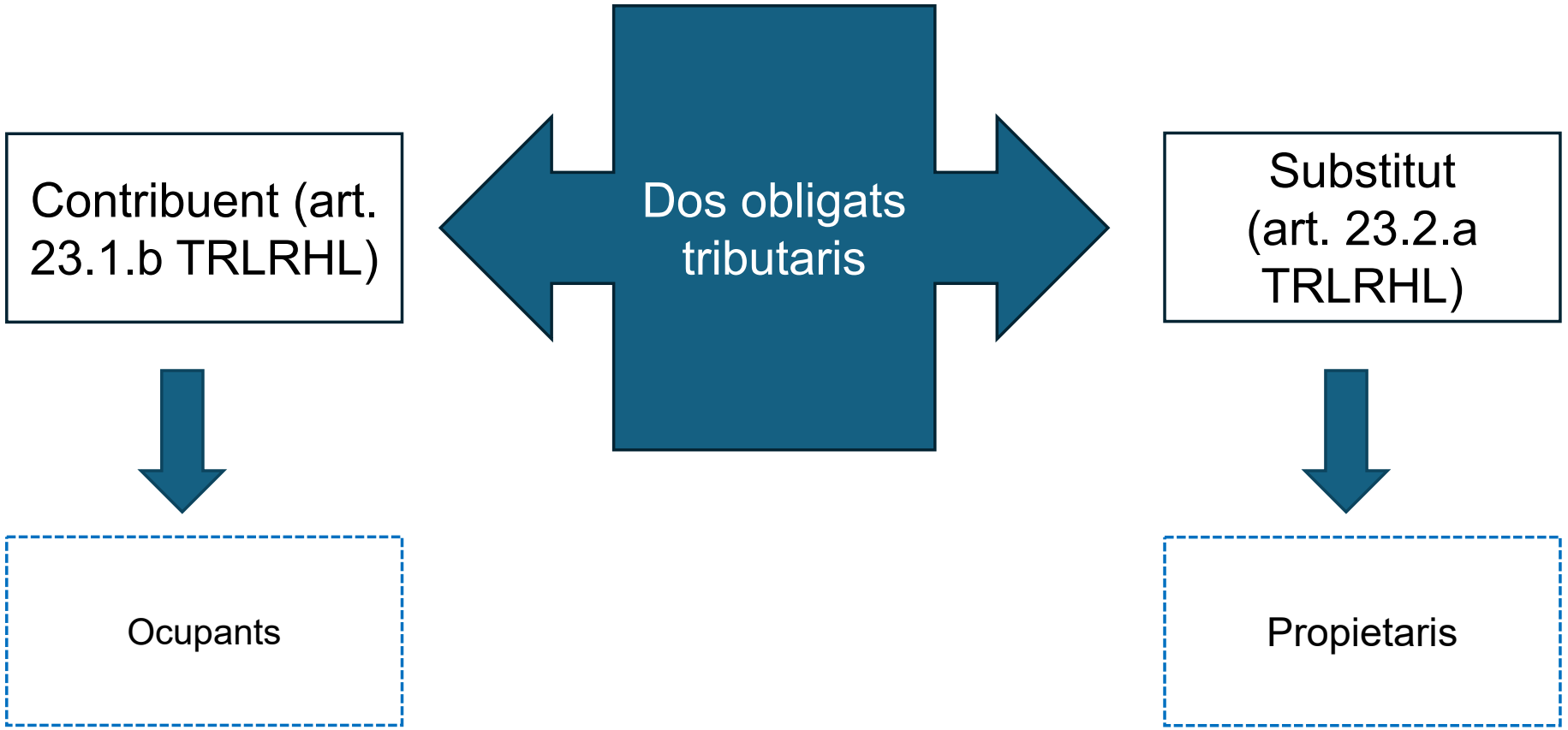


5. 1 Subjectes actius

Entitats locals que poden exigir taxes

- Municipis
- Províncies
- Àrees metropolitanes
- Mancomunitats i altres entitats supramunicipals
- Comarques i altres entitats supramunicipals.

5. 2 Subjectes passius



Punt conflictiu

Part variable de la quota

Comportament del contribuent

(referència cadastral)

Obligació de pagament: substitut

Repercutir la quota

Subjecte passiu en les reduccions i bonificacions

- Circumstàncies del contribuent.

- La sol·licitud de reduccions la poden efectuar tots dos subjectes, però sempre en relació a qui realitza el fet imposable, qui utilitza el servei i qui genera residus.

- El substitut és un simple instrument de la Llei per facilitar la gestió tributària.

6. Informe tècnicoeconòmic

Art. 24.2 TRLRHL

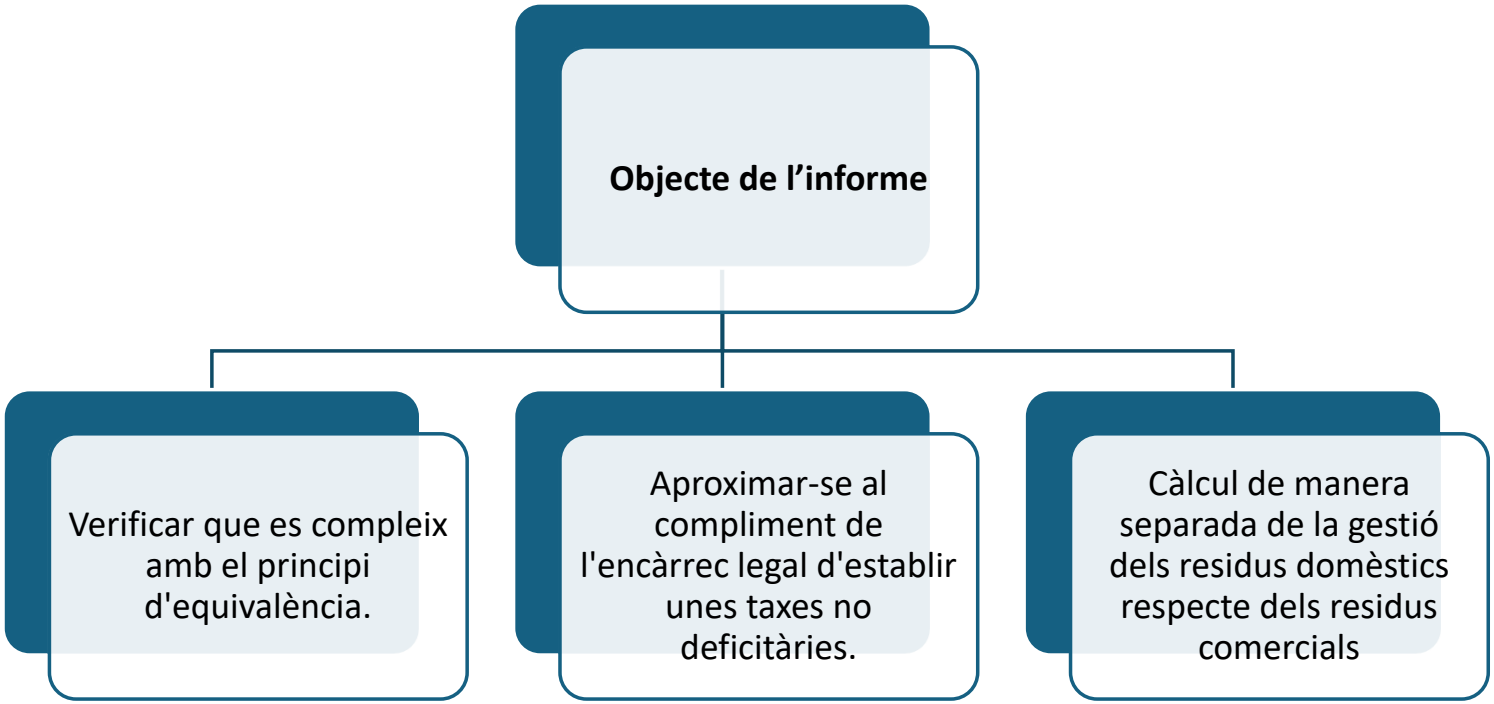
(Import taxa no pot excedir cost del servei)

Art. 11.3 Llei residus

(Taxa no deficitària)

És un principi

no es requereix una precisió en la cobertura dels costos


Objecte de l'informe
Verificar que es compleix amb el principi d'equivalència.
Aproximar-se al compliment de l'encàrrec legal d'establir unes taxes no deficitàries.
Càlcul de manera separada de la gestió dels residus domèstics respecte dels residus comercials

Costos per la gestió del servei

A) Costos directes	Costos estimats per a l'exercici (€)
De personal	
Contracte recollida residus	
Tributs	
Costos d'amortització	
Costos financers	
Altres	

B) Costos indirectes	Costos estimats per a l'exercici (€)
Personal Ajuntament	
Altres	

Ingressos relatius a la responsabilitat ampliada del productor i a la venda de materials

Ingressos	Import total
Retorn venda materials (plàstic, paper, etc...)	
Retorn venda energia	
Retorn per l'aplicació ampliada del productor	
Altres retorns	

7. Quota tributària

Model de sistema avançat: taxa de residus domèstics

Es configura la quota en dos parts:

Bàsica: diferents tarifes per tipus d'immoble:

Tarifa 1. Per cada vivienda ..... xx €
Tarifa 2. Per cada local comercial inactiu ..... xx €
Tarifa 3. Per cada local destinat a usos privats..... xx €
Tarifa 4. Per cada solar sense edificar..... xx €
Tarifa 5. Per cada local industrial i comercial (només residus domèstics)..... xx €

Reducció si s'acredita que els ingressos de la unitat familiar no superan l'import del SMI.

Variable:

- ✓ Inmobles amb recollida porta a porta/contenidors tancats amb identificació d'usuari: en funció de la quantitat i tipus de residus generats per unitat d'immoble.
- ✓ Inmobles amb árees tancades amb sistema únic de recollida: en funció del número d'entrades anuals a las àrees tancades

Model de sistema avançat: taxa de residus comercials

Es configura la quota en dues parts:

- **Bàsica: diferents tarifes segons el tipus d'activitat.**
  - Si l'activitat es desenvolupa en una vivienda –sense separació-, s'exigirà només la tarifa comercial.

Habitatges de lloguer turístic

- **Variable: en funció de la quantitat i tipus de residu generat per unitat de local comercial.**
  - Es recomana determinar l'import de cada fracció per trams de lliurament efectuades.

Volum/Pes anual lliurat

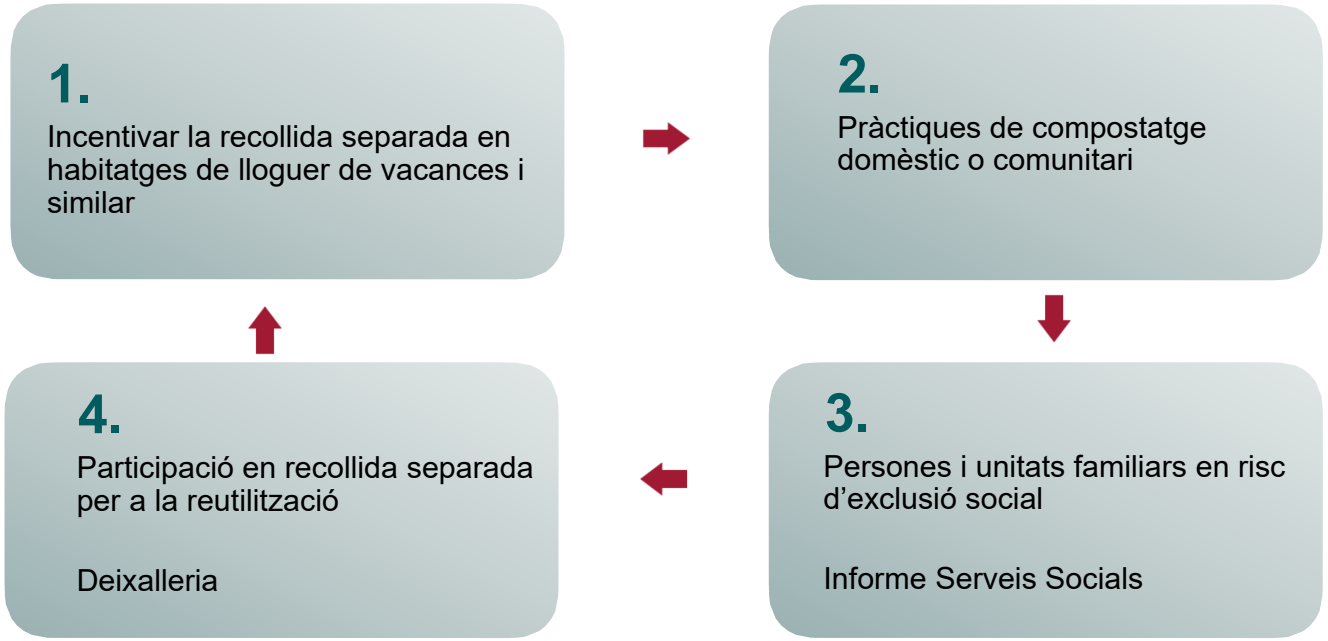
8. Beneficis fiscals: reduccions i bonificacions

Exempció: no aplica → Reduccions:
- Art. 24.4 TRLRHL
- Art. 11.4 LR

→ Bonificació:
Art. 24.6 TRLRHL

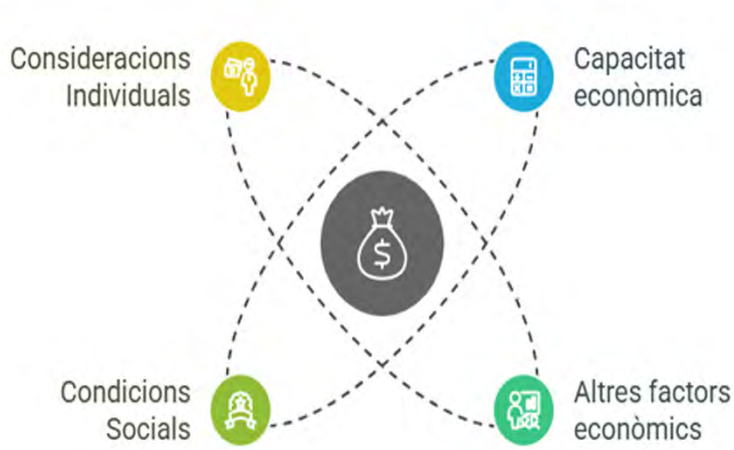
La menor quota a satisfer pel subjecte passiu NO implica més quota a pagar per a la resta.

Reduccions art. 11.4 Llei de residus



Art. 24.4 TRLRHL

“Per a la determinació de la quantia de les taxes es poden tenir en compte criteris genèrics de **capacitat econòmica** dels subjectes obligats a satisfer-les.”.”



Art. 24.6 TRLRHL

"Les EELL podran establir una bonificació de fins a un 95% de la quota íntegra de les taxes o PPPNT per a aquelles ***empreses de distribució alimentària i de restauració*** *que tinguin establerts, amb caràcter prioritari, en col·laboració amb entitats d'economia social sense ànim de lucre, sistemes de gestió que redueixin de forma significativa i verificable els residus alimentaris, sempre que el funcionament dels sistemes hagi estat prèviament verificat per l'Entitat local"*

Projecte de llei de prevenció de les pèrdues i el rebuig alimentari

9. Meritació i exigibilitat de la taxa

1. Meritació

a. Meritació: 1 de gener

b. Periode impositiu: any natural

2. Exigibilitat:

a. Quota bàsica

- S'exigeix en el mateix any de meritació.

b. Quota variable

La quota variable es pot exigir:

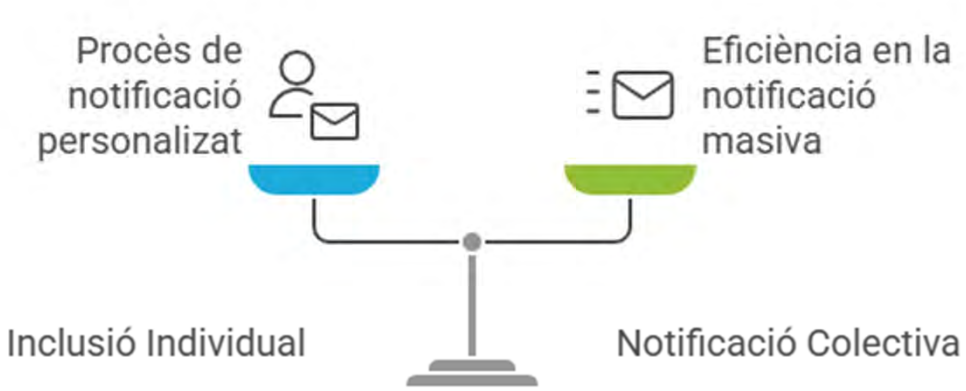
- El mateix any de la meritació juntament amb la quota bàsica.
- L'any següent al de la meritació de la taxa, en un rebut independent.

El caràcter periòdic de la taxa en determina la meritació l'1 de gener i el període impositiu coincideix amb l'any natural. Per tant, l'OF de la taxa ha d'estar aprovada i publicada abans del dia 1 de gener 2025.

Prorrateig (part bàsica)

10. Gestió de la taxa

10. 1 Gestió tributària



Consulta DGT 1/8/2024

10.2 Protecció dades quota variable

Art. 6.1.e) Reglament General de Protecció de dades :

“Licitud del tractament:

1. El tractament serà lícit si es compleixen almenys una de les següents condicions:

e) El tractament és necessari per al compliment d’una missió realitzada en interès públic o en l’exercici de poders públics conferits al responsable del tractament”

- **Dades contractuals**

Dades necessàries perquè funcioni el servei (nº usuari, dades contracte,…)

(Normativa: LBRL, Llei 7/2022, TRLRHL)

- **Dades relacionades amb els residus**

Dades que es generen amb el funcionament del servei (quina fracció s'ha aportat,…)

(Normativa: LBRL, Llei 7/2022, TRLRHL)

- **Dades complementàries**

Dades que no són necessàries per a la prestació del servei (sistema de avisos,…)

(Es requereix consentiment)

10. 3 Exigibilitat PPPNT

Com s'han de tramitar les PPPNT impagades?

Via de constrenyiment (prèvia notificació en voluntària)
Consulta DGT 3/06/2020

Les PPPNT han d'estar subjectes a l'IVA?

Si. Consulta DGT 3/06/2020

Art. 11.5 Llei de residus

Les entitats locals hauran de comunicar aquestes taxes, així com el càlcul utilitzat per la seva confecció, a les autoritats competents de les CCAA.

Qui és l'autoritat competent?

Conclusions

- Taxa obligatòria i no deficitària
- OF aprovada abans de l'1 de gener 2025
- Any 2026, balanç:
    - Nivell implementació de la taxa
    - Sistemes de pagament per generació
    - Volum de recursos
    - Percentatges recaptats
    - Compliment objectius europeus
- Reforma elements tributaris o creació d'un impost

Models ordenança fiscal i informe tècnicoeconòmic 2025: sistemes elemental i avançat
https://www.diba.cat/es/web/normativa/models-ordenances-fiscals-tipus-2025

Impost sobre el Valor Afegit i Impost sobre Societats

Aspectes rellevants en les entitats del sector públic local

Barcelona, 21 de febrer de 2025

Glossari d'abreviatures

- LLRBRL: Llei 7/1985, de 2 d'abril, Reguladora de les Bases del Règim Local
- LLIVA: Llei 37/199s de 28 de desembre, de l'Impost sobre el Valor Afegit
- LLIS: Llei 27/2014, de 27 de novembre, de l'Impost sobre Societats

---

- DGT: Direcció General de Tributs
- IVA: Impost sobre el Valor Afegit
- IS: Impost sobre Societats
- AN: Audiència Nacional
- TS: Tribunal Suprem
- TEAC: Tribunal Econòmic-Administratiu Central
- TJUE: Tribunal de Justícia de la Unió Europea
- TSJ CAT: Tribunal Superior de Justícia de Catalunya

PROGRAMA

I. L'IVA i les entitats del sector públic local

I.1. IVA i subvencions

I.2. Supòsits de no subjecció

I.3. Supòsits d'exempció

II. Impost sobre Societats i les entitats del sector públic local

II.1. La definició del sector públic a Espanya: Territorialitat i tipus d'entitats

II.2. Entitats totalment exemptes *(Art. 9.1 LLIS)*

II.3. Entitats parcialment exemptes *(Art. 9.2 LLIS)*

II.4. Bonificació per prestacions de serveis públics locals *(art. 34 LLIS)*

I. L'IVA i les entitats del sector públic local

L'IMPOST SOBRE EL VALOR AFEGIT *(IVA)*

- ✓ L'IVA és un tribut de naturalesa **indirecta** que recau sobre el **consum** i grava **els lliurament de béns i prestacions de serveis** realitzats per **empresaris o professionals**

- ✓ Estaran subjectes a l'impost els lliuraments de béns i les prestacions de serveis **realitzats per empresaris i professionals a títol onerós**, amb caràcter habitual o ocasional, en el desenvolupament d'una activitat empresarial o professional, àdhuc si es realitzen a favor dels propis socis, associats, membres o partícips de les entitats que les realitzen

- ✓ Són **activitats empresarials o professionals** les que impliquin l'ordenació per compte pròpia de factors de producció materials i humans o d'un d'ells, amb la finalitat d'intervenir en la producció o distribució de béns o serveis

- ✓ **Règim d'exempcions**. Les activitats exemptes de l'IVA són els lliuraments de béns o prestacions de servei que tot i estar subjectes a l'Impost, la Llei de l'IVA estableix que no hauran de sotmetre's a tributació. En l'IVA les exempcions tenen **caràcter objectiu**

Finançament de les activitats realitzades per les entitats del sector públic

Finançament	Tractament IVA
Transferències / Subvencions	No subjecte Subjecte (art. 78.dos.3er)
Ingressos tributaris	No subjecte (art. 7.8è)
Contraprestació	Subjecta No subjecte (art. 7.8è) Exempta (art. ´20.ú)

L'IVA i la prestació de serveis en l'àmbit del sector públic

Antecedents:

Fins 2006

Article 102 LLIVA. Règim de deduccions: Les **subvencions no vinculades a preu s'integren en el denominador de la regla de la prorrata i limiten el dret a deducció de les quotes d'IVA suportat.**

2006

Sentència TJUE de 6 d'octubre de 2005. Directiva 2006/112/CE: Les subvencions no poden limitar el dret a deducció. Es modifica redacció anterior i Subvencions no s'integren denominador prorrata.

2006 - 2015

Doctrina Administrativa (Sentències Tribunals, Consultes DGT, informes Tributs): els serveis prestats pels denominats «**ens tècnico-jurídics» de les Administracions** públiques estan No subjectes a IVA i veuran limitat el dret a deducció.

A partir de 2015

Modificació Llei 37/1992, de l'IVA, Art.7.8. Els **serveis prestats** per qualsevol ens, organismes o entitats del sector públic **a favor de les Administracions Públiques de la que depenguin o d'una altra íntegrament dependent d'aquestes**, estaran no subjectes a l'Impost sobre el Valor Afegit.

I.1. IVA I SUBVENCIONS

(Redacció introduïda per la Llei 9/2017, de 8 de novembre, amb vigència a partir del 10 de novembre de 2017)

"Article 78. Base imposable. Regla general.
Ú. La base imposable de l'impost estarà constituïda per l'import total de la contraprestació de les operacions subjectes al mateix procedent del destinatari o de terceres persones.
Dos. En particular, s'inclouen en la contraprestació:
...
3er. ***Les subvencions vinculades directament al preu*** *de les operacions subjectes a l'Impost.*
Es consideraran vinculades directament al preu de les operacions subjectes a l'Impost les subvencions establertes en funció del número d'unitats lliurades o del volum dels serveis prestats quan es determinin amb anterioritat a la realització de l'operació.
No obstant, ***no es consideraran subvencions vinculades al preu*** *ni integren en cap cas l'import de la contraprestació a que es refereix l'apartat Ú del present article, les aportacions dineraris sigui quina sigui la seva denominació, que les administracions públiques realitzin per finançar:*

- ***a) La gestió de serveis públics o de foment a la cultura*** *en els que no existeixi una distorsió significativa de la competència, sigui quina sigui la seva forma de gestió.*
- ***b) Activitats d'interès general*** *quan llurs destinataris no sigui identificable i no satisfacin cap tipus de contraprestació.*

I.1. IVA I SUBVENCIONS

(Redacció introduïda per la Llei 9/2017, de 8 de novembre, amb vigència a partir del 10 de novembre de 2017)

"Article 78. Base imposable. Regla general.
Ú. La base imposable de l'impost estarà constituïda per l'import [illegible]ació de les operacions subjectes al mateix procedent del destinatari o de terc[illegible]
Dos. En particular, s'inclouen en la contraprestació:
...
3er. ***Les subvencions vinculades directament al preu*** *de les operacions subjectes a l'Impost.*
Es consideraran vinculades directament al preu de les operacions subjectes a l'Impost les subvencions establertes en funció del número d'unitats lliurades o del volum dels serveis prestats quan es determinin amb anterioritat a la realització de l'operació.
No obstant, ***no es consideraran subvencions vinculades al preu*** *ni integren en cap cas l'import de la contraprestació a que es refereix l'apartat Ú del present article, les aportacions dineraris sigui quina sigui la seva denominació, que les administracions públiques realitzin per finançar:*

- ***a) La gestió de serveis públics o de foment a la cultura*** *en els que no existeixi una distorsió significativa de la competència, sigui quina sigui la seva forma de gestió.*
- ***b) Activitats d'interès general*** *quan llurs destinataris no sigui identificable i no satisfacin cap tipus de contraprestació.*

Sentència TJUE 27/3/2014 "Le Rayon d'Or, SRL"

IVA i Subvencions

Tipus de subvenció	S'integra a la BI?
Vinculada directament al preu	SÍ
Gestió de serveis públics o de foment a la cultura	NO
Per a finançar activitats d'interès general	NO
Per a finançar l'activitat *(transferències)*	NO
Per a la contractació de personal	NO
Par a finançar inversions *(de capital)*	NO

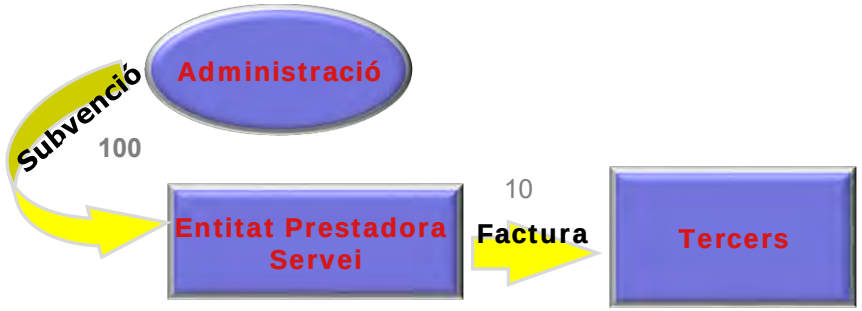
IVA i Subvencions

La Base Imposable de l'Impost (Article 78 LLIVA)

"4art. Les subvencions no vinculades al preu de les operacions, ***no considerant-se com a tals, els imports pagats per un tercer en contraprestació de les esmentades operacions****."*

Conseqüència

Quan existeixi relació directa entre la contraprestació rebuda (Subvenció) i el servei prestat la subvenció haurà d'integrar-se a la Base Imposable de l'Impost



Preu del servei	10,00
Subvenció	100,00
Base imposable	110,00
IVA 21%	+23,10
Total	133,10

I.2. SUPÒSITS DE NO SUBJECCIÓ

Article 7.8è *(Redacció introduïda per la Llei 9/2017, de 8 de novembre, amb vigència a partir del 10 de novembre de 2017)*

Tipus d'entitat del Sector públic que presta el servei	Art.7.8	Operacions no subjectes
Administració Pública	LLETRA A	Operacions a títol gratuït o amb contraprestació tributària
	LLETRA E	Serveis prestats a les seves entitats 100% participades
Altres entitats del sector públic (100% controlades per una o varies entitats del sector públic)	LLETRA A	Operacions a títol gratuït o amb contraprestació tributària
	LLETRA C	Serveis prestats en virtut d'encàrrecs de gestió (mitjans propis)
	LLETRA D	Serveis prestats per qualsevol entitat del Sector Públic íntegrament controlada per una o vàries AP a favor de les AP que la controlen o d'altres AP que en depenguin (SERVEIS INTERNS)
	LLETRA E	Serveis INTRAGRUP entre entitats 100% titularitat d'una mateixa AP

Operacions no subjectes: art. 7.8è.A

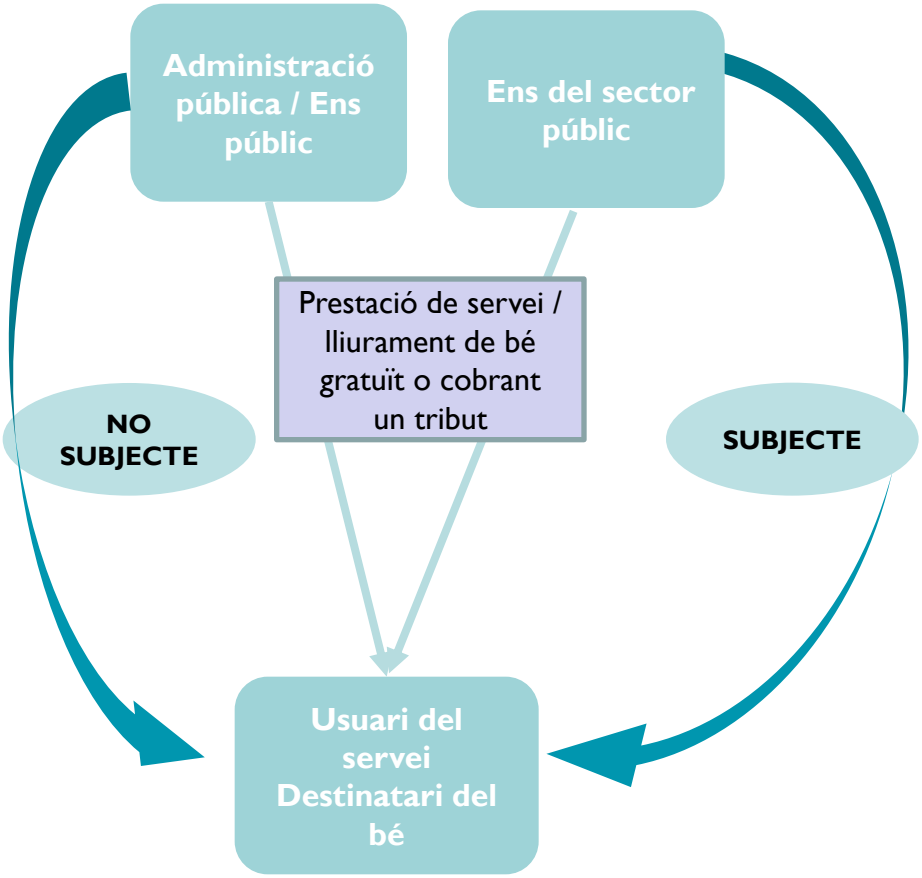
No estaran subjectes a l'impost:

...

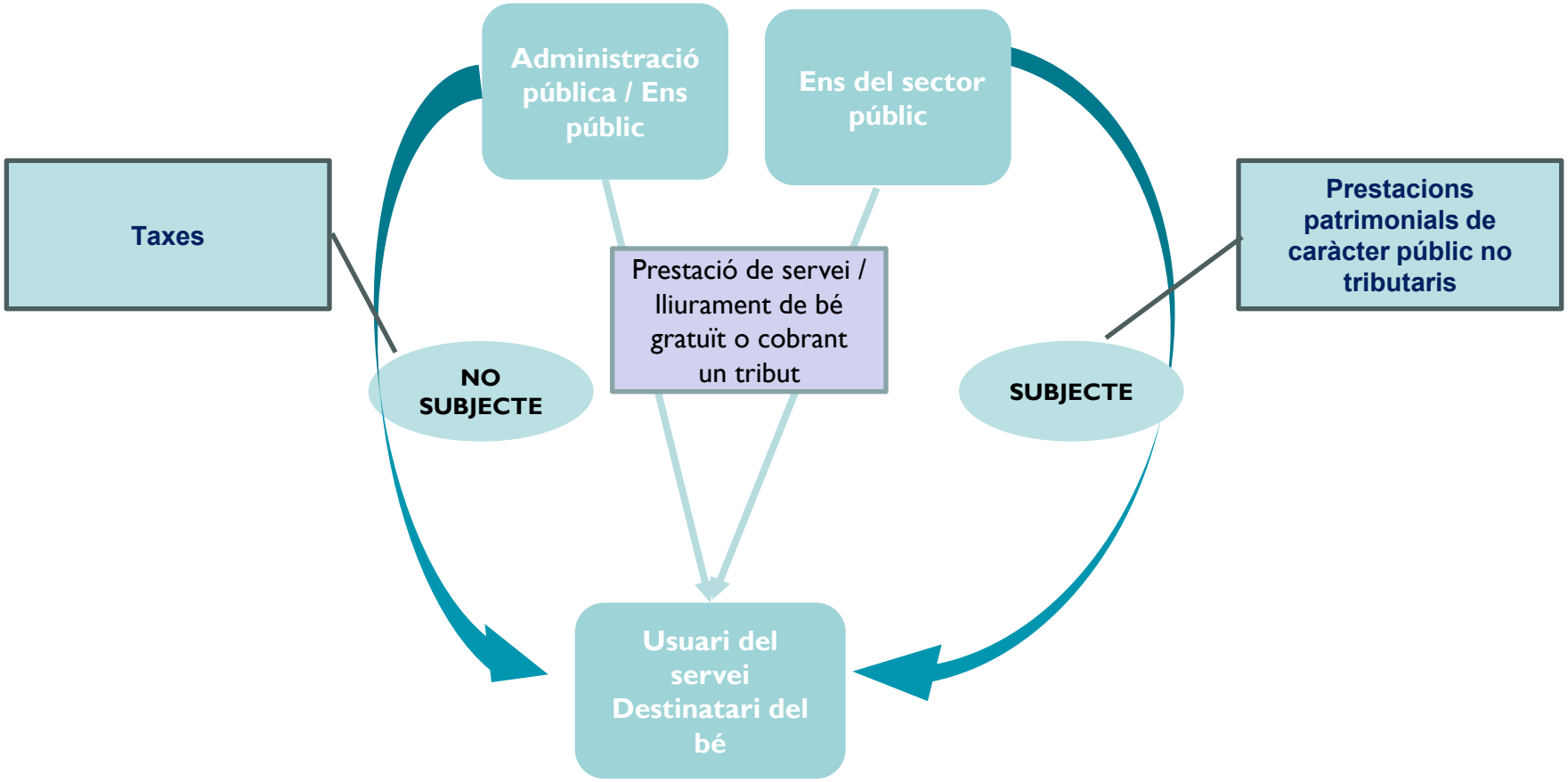
8è.

A) Els lliuraments de bens i prestacions de serveis realitzats directament per les Administracions públiques, així com les entitats a les que es refereixen els apartats C) i D) d'aquest número, sense contraprestació o mitjançant contraprestació de naturalesa tributària.

Operacions no subjectes: art. 7.8è.A



Operacions no subjectes: art. 7.8è.A



Operacions no subjectes: art. 7.8è.C

No estaran subjectes a l'impost:

...

8è.

...

*C) No estaran subjectes a l'Impost els **serveis** prestats en virtut dels encàrrecs executats pels ens, organismes i entitats del sector públic que ostentin, de conformitat amb l'establert a l'article 32 de la Llei de contractes del Sector públic, la condició de **mitjà propi personificat** del poder adjudicador que hagi ordenat l'encàrrec, en els termes establerts en l'esmentat article 32.*

Operacions no subjectes: art. 7.8è.C

Requisits *(Article 32 de la LLCSP)*

SUBJECTIUS		OBJECTIUS
Del poder adjudicador	Del mitjà propi	
Entitat inclosa en l'article 3.1 de la LLCSP	Totalitat del capital o patrimoni ha de ser de titularitat o aportació pública	Limitat a la prestació de serveis (no aplicable al lliurament de béns)
Control (conjunt) anàleg al que ostentaria sobre els seus propis serveis o unitats	Reconeixement exprés en els estatuts o acte de creació	La contraprestació s'ha d'establir per tarifes fixades pel poder adjudicador i vinculades al cost
	Més del 80% de les activitats es duguin a terme en l'exercici dels encàrrecs que li han estat confiats pels poders adjudicadors	L'encàrrec s'ha de formalitzar documentalment i publicat a la Plataforma de Contractació corresponent
	~~Justificació en la memòria i verificat per l'auditor~~	Limitació al 50% de l'import de l'encàrrec la subcontractació (llevat gestió de serveis públics i execució d'obres en encàrrecs de concessió)

Operacions no subjectes: art. 7.8è.C

Requisits *(Article 32 de la LLCSP)*

- **Control anàleg**
  (Sentència TS 1205/2024)
  El control de mitjà propis conjunt NO és individual, s'exerceix de forma col·lectiva per tots els socis i tenen caràcter funcional, no formal.

- **Activitats derivades principalment d'encàrrecs de gestió (80%)**

  • Circular conjunta, de 22 de març de 2019, de l'Advocacia General de l'Estat i la Intervenció General de l'Administració de l'Estat (IGAE)

  Variables alternatives per al càlcul:

  – Volum global del negoci
  – Volum de despeses
  – Altre indicador alternatiu

$$\text{Indicador d'activitat} = \frac{\text{Encomanes / encàrrecs}}{\text{Total activitat}} > 80\%$$

Operacions no subjectes: art. 7.8è.C

EXEMPLE CÀLCUL SEGONS VOLUM GLOBAL DE NEGOCI

	TOTAL	A Numerador	B Denominador
Subvencions	959.000		959.000
Transferències	5.825.000		
Vendes	150		150
Prestacions de serveis (encàrrecs)	1.969.000	1.969.000	1.969.000
Altres ingressos	132.000	132.000	132.000
TOTAL	8.885.150	2.101.000	3.060.150
INDICADOR (A/B)	**68,66%**		

EXEMPLE CÀLCUL SEGONS VOLUM DE DESPESES

	TOTAL	A Numerador	B Denominador
Despeses encàrrecs de gestió	2.500.000	2.500.000	2.500.000
Despeses serveis prestats a tercers	1.000.000		1.000.000
Despeses finançades per transferència	2.000.000	2.000.000	2.000.000
TOTAL	5.500.000	4.500.000	5.500.000
INDICADOR (A/B)	**81,82%**		

Operacions no subjectes: art. 7.8è.C

Requisits *(Article 32 de la LLCSP)*

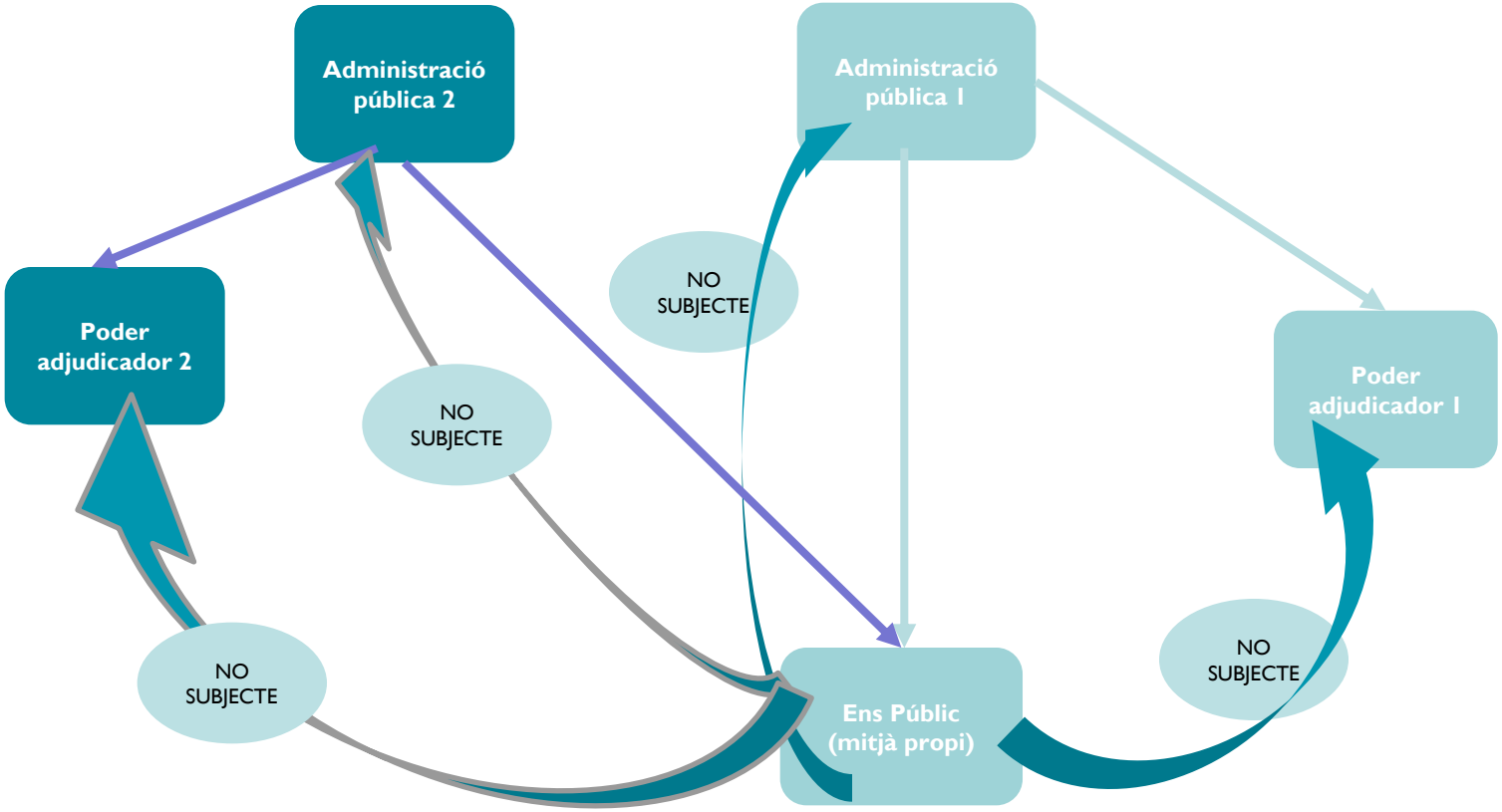
- La disposició final 40a de la Llei de pressupostos de l'estat per al 2021 (Llei 11/202), suprimeix el paràgraf 5 de l'article 32:

  5. L'incompliment sobrevingut de qualsevol dels requisits establerts en els apartats 2 o 4, segons correspongui en cada cas, comportarà la pèrdua de la condició de mitjà propi personificat i, en conseqüència, la impossibilitat de seguir efectuant encàrrecs a la persona jurídica afectada; sens perjudici de la conclusió dels encàrrecs que estiguessin en fase d'execució.

  Conseqüències a efectes d'aplicació de la no subjecció a l'IVA ?

Operacions no subjectes: art. 7.8è.C

Mitjà propi depenent de més d'una Administració pública



Operacions no subjectes: art. 7.8è.D

No estaran subjectes a l'impost:

...

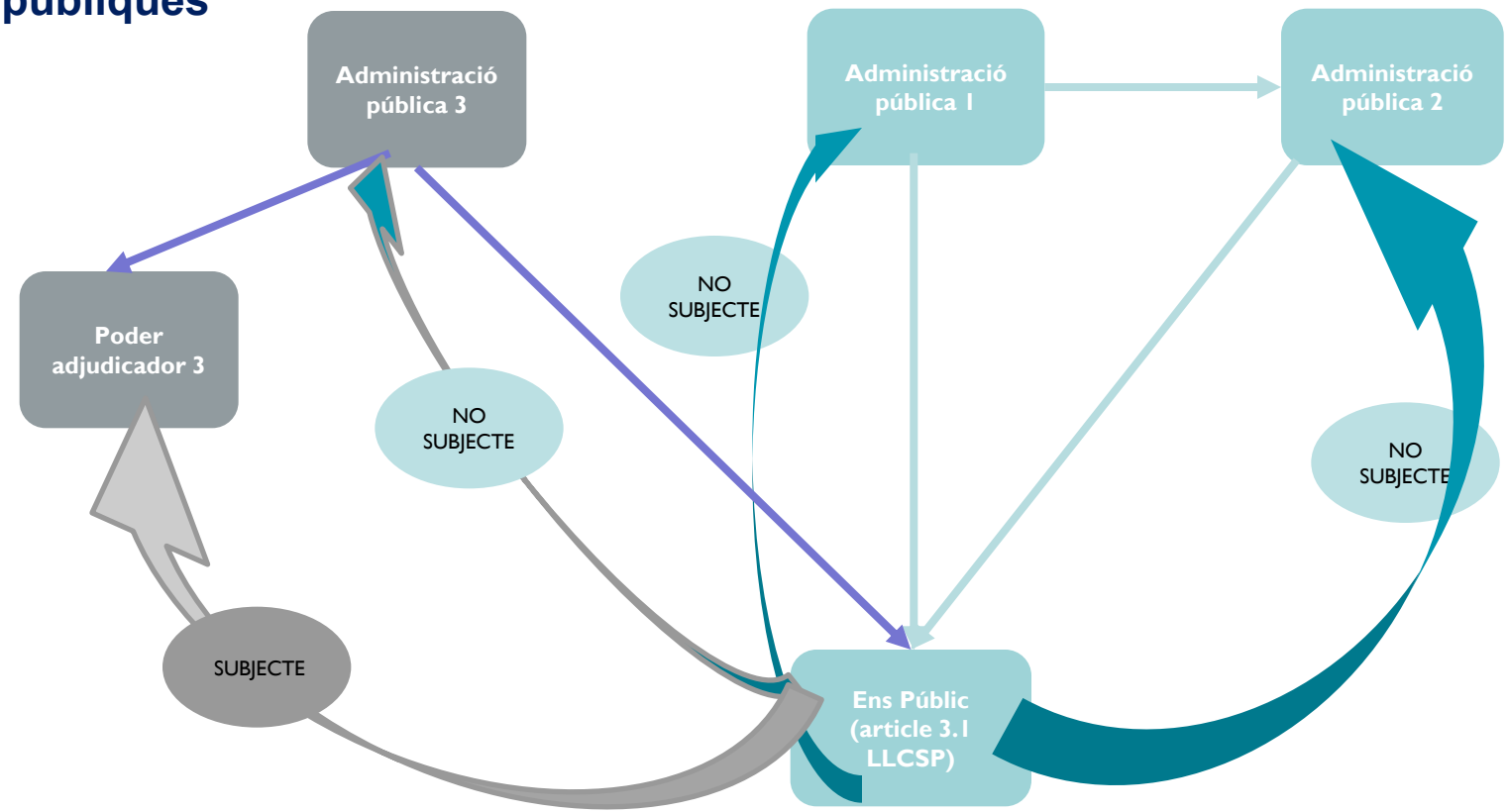
8è.

...

D) Així mateix, no estaran subjectes a l'Impost els serveis prestats per qualsevol ens, organisme o entitats del sector públic als que es refereix l'article 3.1 de la Llei de Contracte del Sector públic, a favor de les Administracions públiques de la que depenguin o d'altres íntegrament dependents d'aquestes, quan les esmentades Administracions públiques ostentin la titularitat íntegra dels mateixos.

Operacions no subjectes: art. 7.8è.D

Entitat del sector públic controlada per una o més administracions públiques

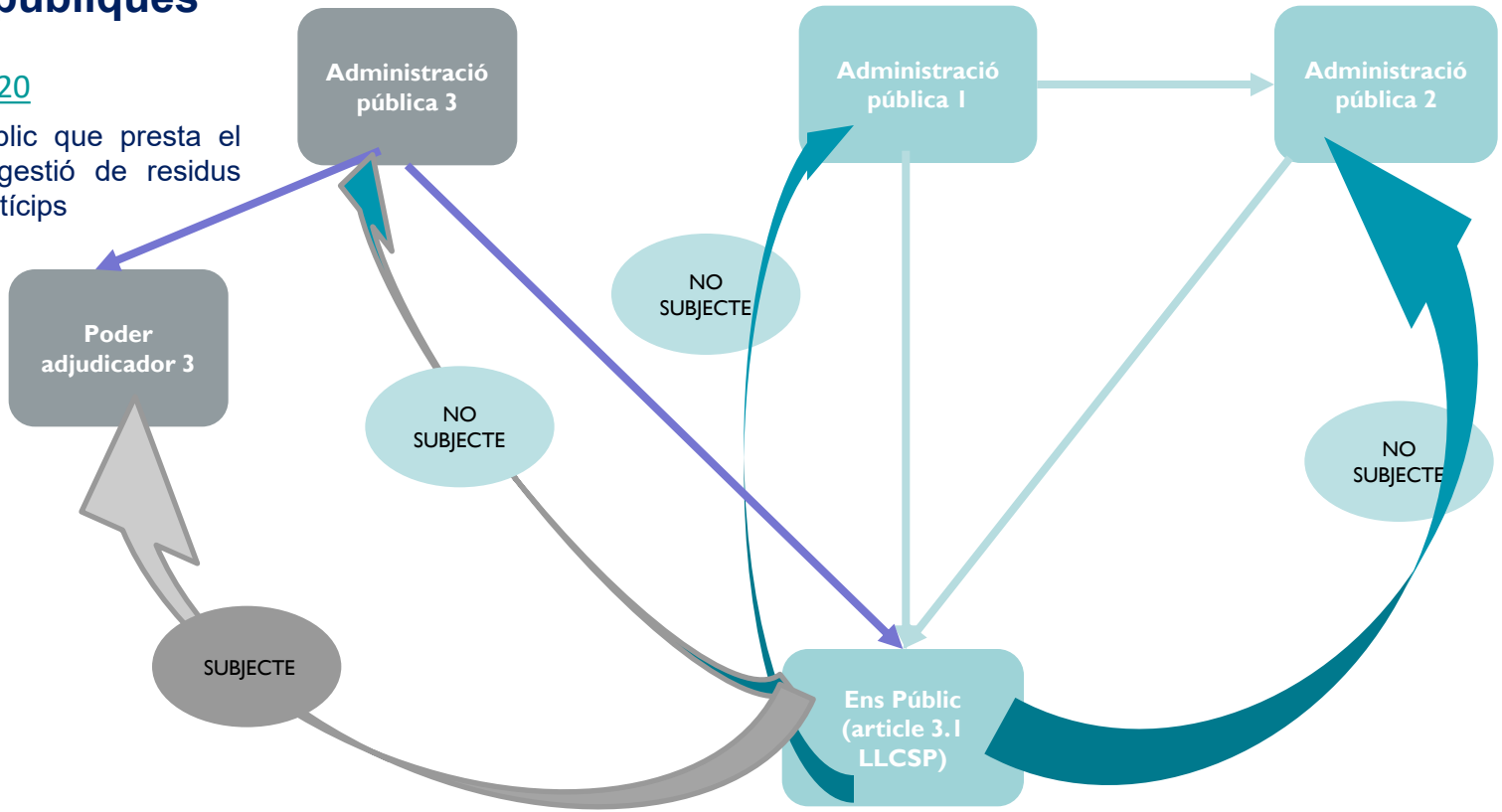


Operacions no subjectes: art. 7.8è.D

Entitat del sector públic controlada per una o més administracions públiques

DGT V0024-20

Consorci públic que presta el servei de gestió de residus sòlids als partícips



Operacions no subjectes: art. 7.8è.E

No estaran subjectes a l'impost:

...

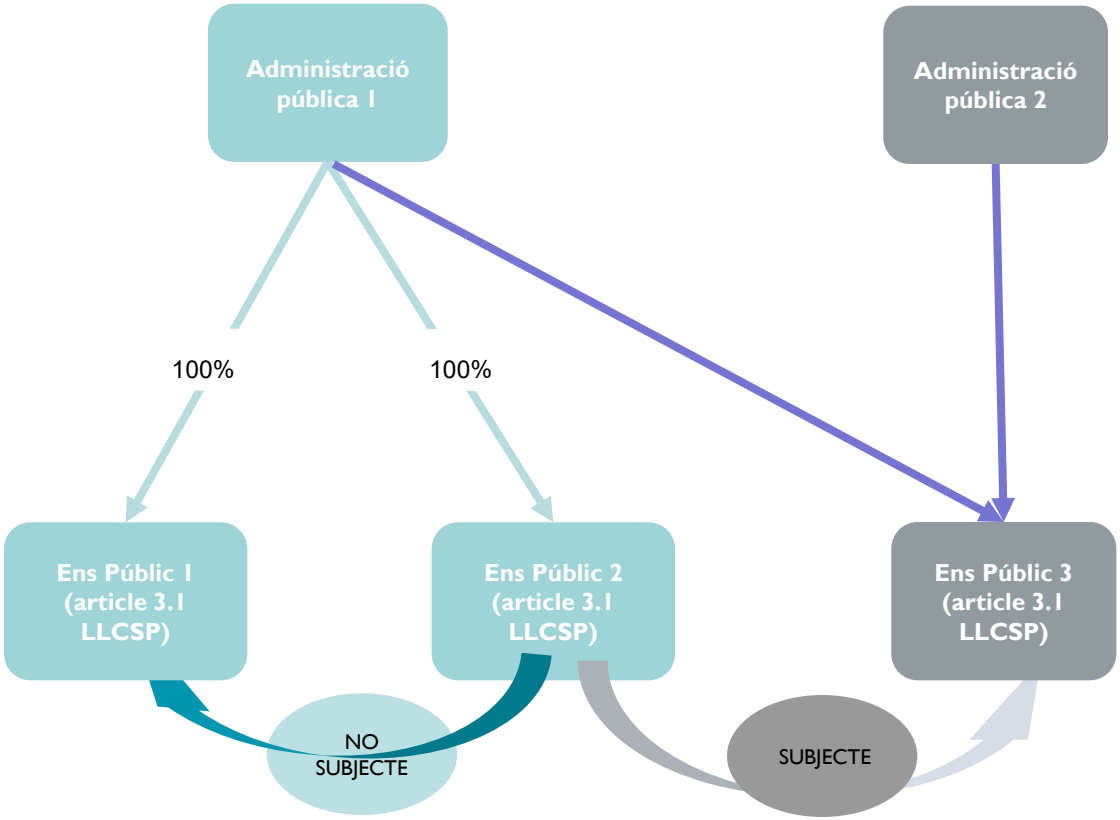
8è.

...

E) La no consideració com operacions subjectes a l'impost que estableixen els dos apartats C) i D) anteriors serà igualment aplicable als serveis prestats entre les entitats a les que es refereixen els mateixos, íntegrament dependents de la mateixa Administració Pública.

Operacions no subjectes: art. 7.8è. E

Entitats del sector públic íntegrament participades per la mateixa Administració pública



DGT V2873-20 DGT V2951-20

Universitat pública que cedeix espais a entitats i organismes oficials de la comunitat autònoma

DGT V3225-19

Societat mercantil dependent d'una altra 100% pública a qui presta serveis

DGT V3435-20

Organisme autònom que arrenda local per oficines a un altre organisme autònom

DGT 08/03/2021

Conveni entre una fundació participada per comunitat autònoma i universitat pública i una empresa pública dependent de la comunitat autònoma

Prestacions de serveis excloses de la no subjecció *(art. 7.8è.F)*

F) En tot cas, estaran subjectes a l'Impost ells lliuraments de béns i prestacions de serveis que les Administracions públiques, ens, organismes i entitats del sector públic realitzin en l'exercici de les activitats que a continuació es relacionen:

a') Telecomunicacions
b') Distribució d'aigua, gas, calor, fred, energia elèctrica i altres modalitats d'energia.
c') Transport de persones i béns
d') Serveis portuaris i aeroportuaris i explotació d'infraestructures ferroviàries incloent a aquests efectes, les concessions i autoritzacions exceptuades de la no subjecció de l'Impost pel número 9è següent
e') Obtenció, fabricació o transforació de productes per a la seva transmissió posterior
f') Intervenció sobre productes agropecuaris adreçat a la regulació del mercat d'aquets productes
g') Explotació de fires i d'exposicions de caràcter comercial
h') Magatzematge i dipòsit
i') Les oficines comercials de publicitat
j') Explotació de cantines i menjadors d'empreses, economats, cooperatives i establiments similars
k') Les d'agències de viatges
l') Les comercials o mercantils dels Ens públics de ràdio i televisió, incloses les relatives a la cessió de l'ús de les instal·lacions
m') Les d'escorxador

Prestacions de serveis excloses de la no subjecció *(art. 7.8è.F)*

F) En tot cas, estaran subjectes a l'Impost ells lliuraments de béns i prestac serveis que les Administracions públiques, ens, organismes i entitats del secto realitzin en l'exercici de les activitats que a continuació es relacionen:

DGT V3117-20

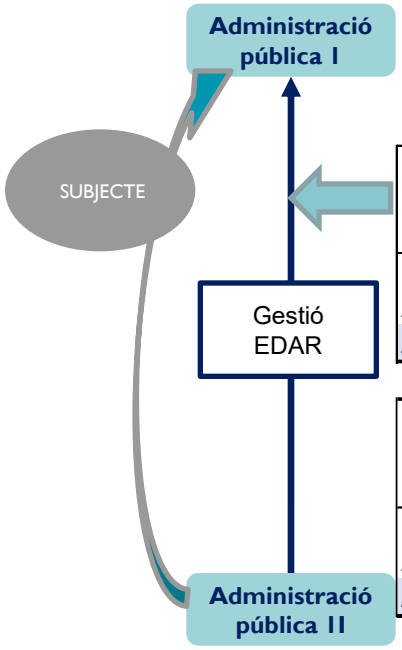
DGT V2152-20

a') Telecomunicacions
b') Distribució d'aigua, gas, calor, fred, energia elèctrica i altres modalitats d'energia.
c') Transport de persones i béns
d') Serveis portuaris i aeroportuaris i explotació d'infraestructures ferroviàries incloent a aquests efectes, les concessions i autoritzacions exceptuades de la no subjecció de l'Impost pel número 9è següent
e') Obtenció, fabricació o transforació de productes per a la seva transmissió posterior
f') Intervenció sobre productes agropecuaris adreçat a la regulació del mercat d'aquets productes
g') Explotació de fires i d'exposicions de caràcter comercial
h') Magatzematge i dipòsit
i') Les oficines comercials de publicitat
j') Explotació de cantines i menjadors d , cooperatives i establiments similars
k') Les d'agències de viatges
l') Les comercials o mercantils dels Ens públics de ràdio i televisió, incloses les relatives a la cessió de l'ús de les instal·lacions
m') Les d'escorxador

Sentència TS 239/2024

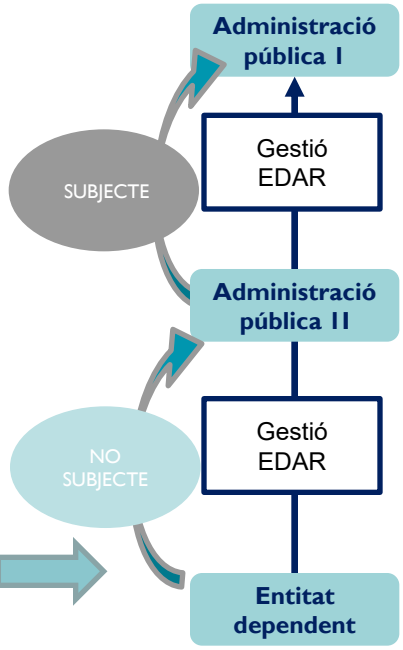
Prestacions de serveis excloses de la no subjecció *(art. 7.8è.F)*

Trencament de la neutralitat de l'IVA en la prestació de serveis de gestió de les EDAR a través d'una entitat dependent



	Factura rebuda (IVA inclòs)	Iva suportat	Cost	Iva repercutit	Total
Entitat dependent					
Administració I	1.210	210	1.000	210	1.210
Administració II	1.210	210	**1.000**		

	Factura rebuda (IVA inclòs)	Iva suportat	Cost	Iva repercutit	Total
Entitat dependent	1.210	210	1.210	0	1.210
Administració I	1.210	0	1.210	254	1.464
Administració II	1.464	254	**1.210**		



I.3. SUPÒSITS D'EXEMPCIÓ

Prestacions de serveis exemptes de l'IVA *(art. 20.Ú)*

Estan exemptes de l'IVA les següents operacions:

- Serveis d'hospitalització i assistència sanitària *(2on)*
- Serveis a les persones *(8è)*
- Ensenyament *(9è)*
- Serveis esportius *(13è)*
- Serveis culturals *(14è)*
- Transport de malalts *(16è)*
- Lliurament de terrenys o edificables *(20è)*
- Segones i ulteriors lliurament d'edificacions *(22è)*
- Arrendament d'habitatges *(23è)*

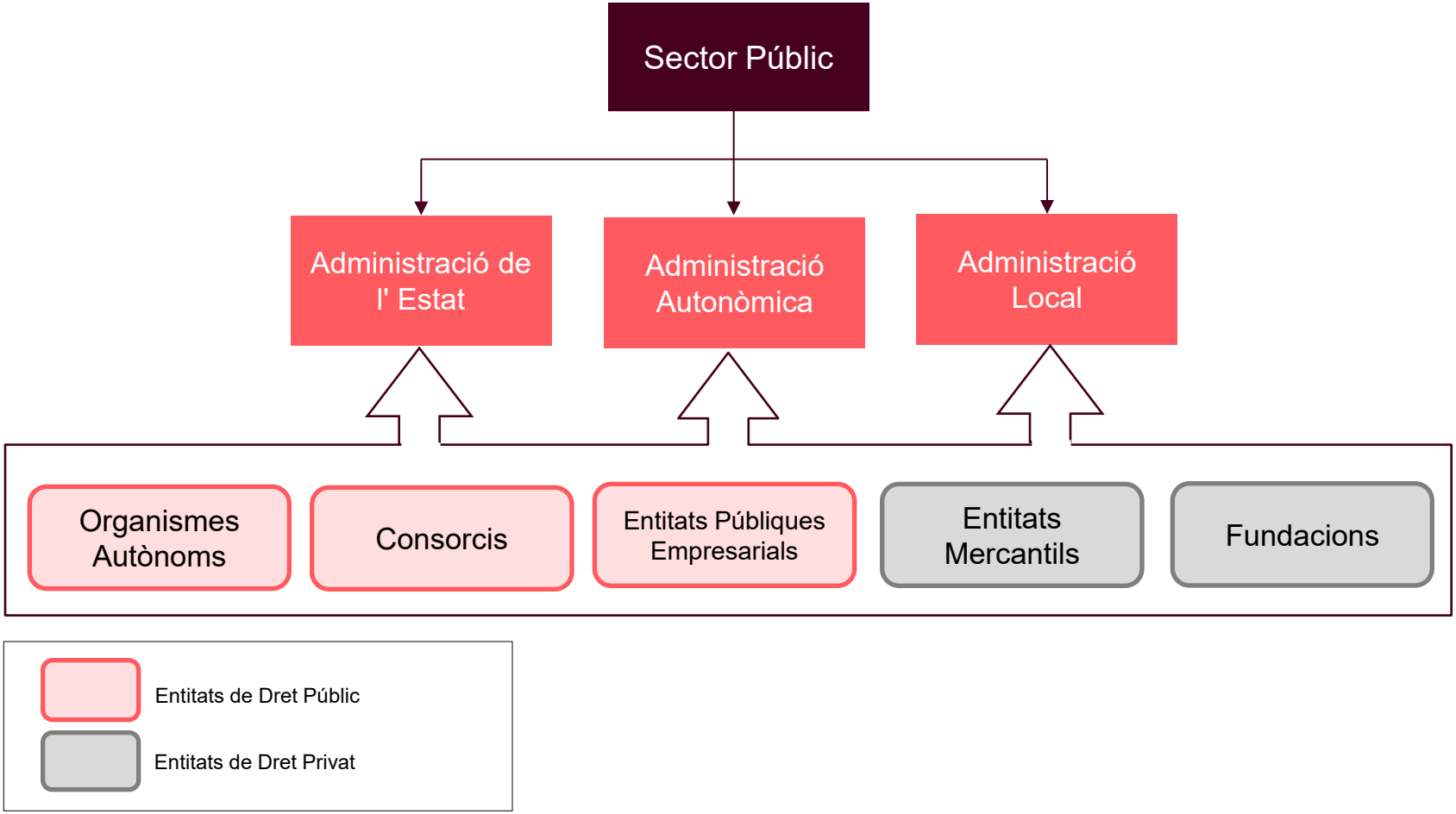
Entitats participades: ingressos percebuts de l'ajuntament

Finançament	Aportació municipal	IVA	Referència normativa	Limita el dret a deducció	Observacions
- Aportació funcionament	Subvenció	No subjecte	Art. 78.3er de la Llei 37/1992	No	Sentència del Tribunal Suprem de 27 de març de 2024 en el recurs de cassació núm. 1059/2023
- Descentralització de funcions					
- Gestió de serveis públics	Transferència	No subjecte	Art. 7.8è.D i 78.3er.a) de la Llei 37/1992	No	L'IVA suportat per la compra de béns i serveis afectes directament i exclusiva a aquesta activitat tindrà la consideració de deduïble en la seva integritat (art. 93.cinc de la Llei 37/1992)
- Activitats d'interès general	Transferència	No subjecte	Art. 7.8è.D i 78.3er.a) de la Llei 37/1992	Sí	No són deduïbles les quotes suportades en la compra de béns i prestacions de serveis destinats exclusivament a aquestes activitats (art. 93.cinc de la Llei 37/1992)
- Encomana					
- Gestió de serveis públics	Contraprestació / Subvenció	No subjecte	Art. 7.8è.C	No	L'IVA suportat per la compra de béns i serveis afectes directament i exclusiva a aquesta activitat tindrà la consideració de deduïble en la seva integritat (art. 93.cinc de la Llei 37/1992)
- Activitats d'interès general	Contraprestació / Subvenció	No subjecte	Art. 7.8è.C	Sí	No són deduïbles les quotes suportades en la compra de béns i prestacions de serveis destinats exclusivament a aquestes activitats (art. 93.cinc de la Llei 37/1992)
- Finançaments d'inversions					
	Subvenció de capital	No subjecte	Art. 78.3er de la Llei 37/1992	No	El dret a deducció de les quotes d'IVA suportat en la compra de béns d'inversió vindrà condicionat pel règim de deduccions de l'activitat a la que es trobi afecta l'actiu adquirit

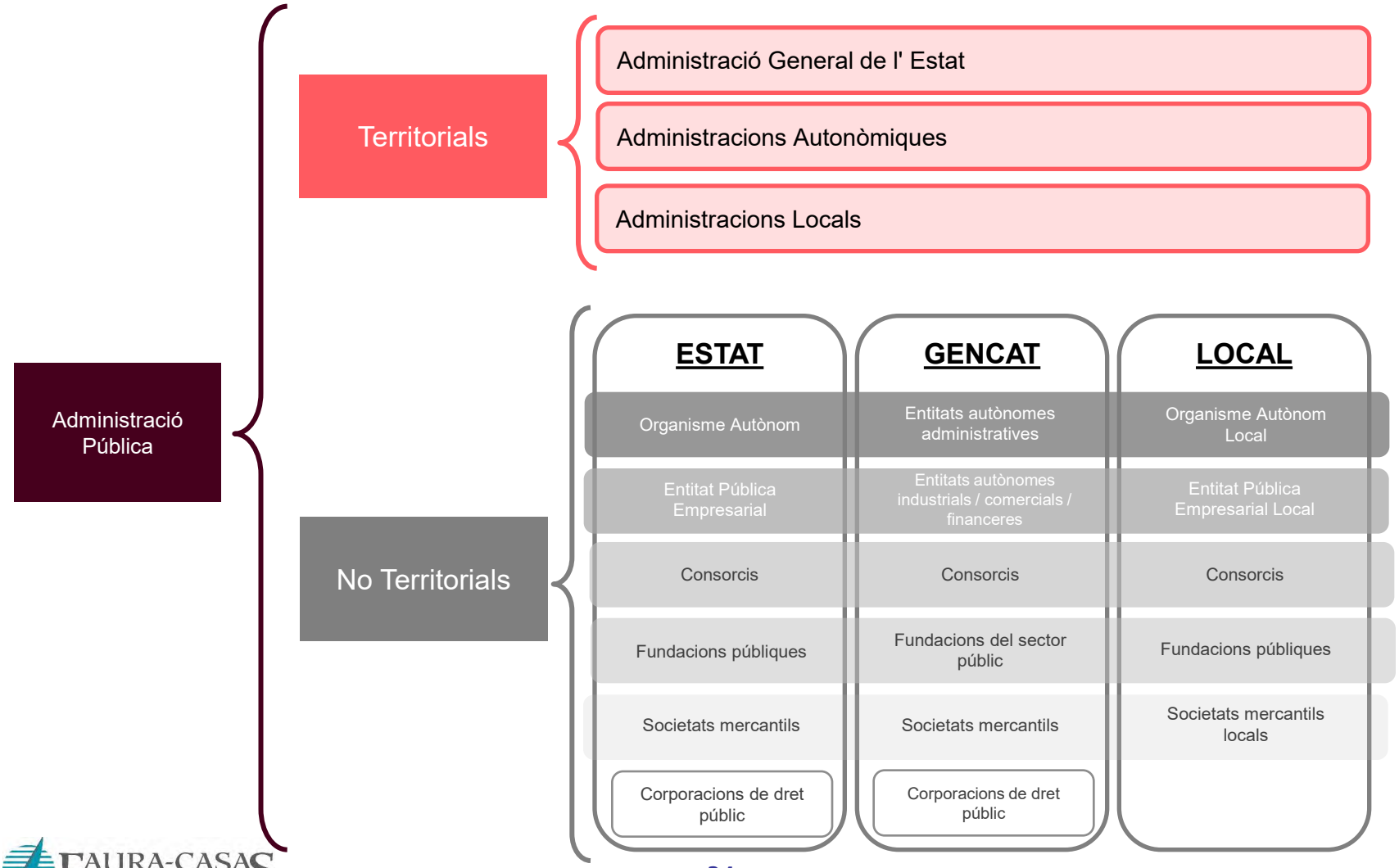
II. Impost sobre Societats i les entitats del sector públic local

II.1. LA DEFINICIÓ DEL SECTOR PÚBLIC A ESPANYA: Territorialitat i tipus d'entitats

El sector públic espanyol

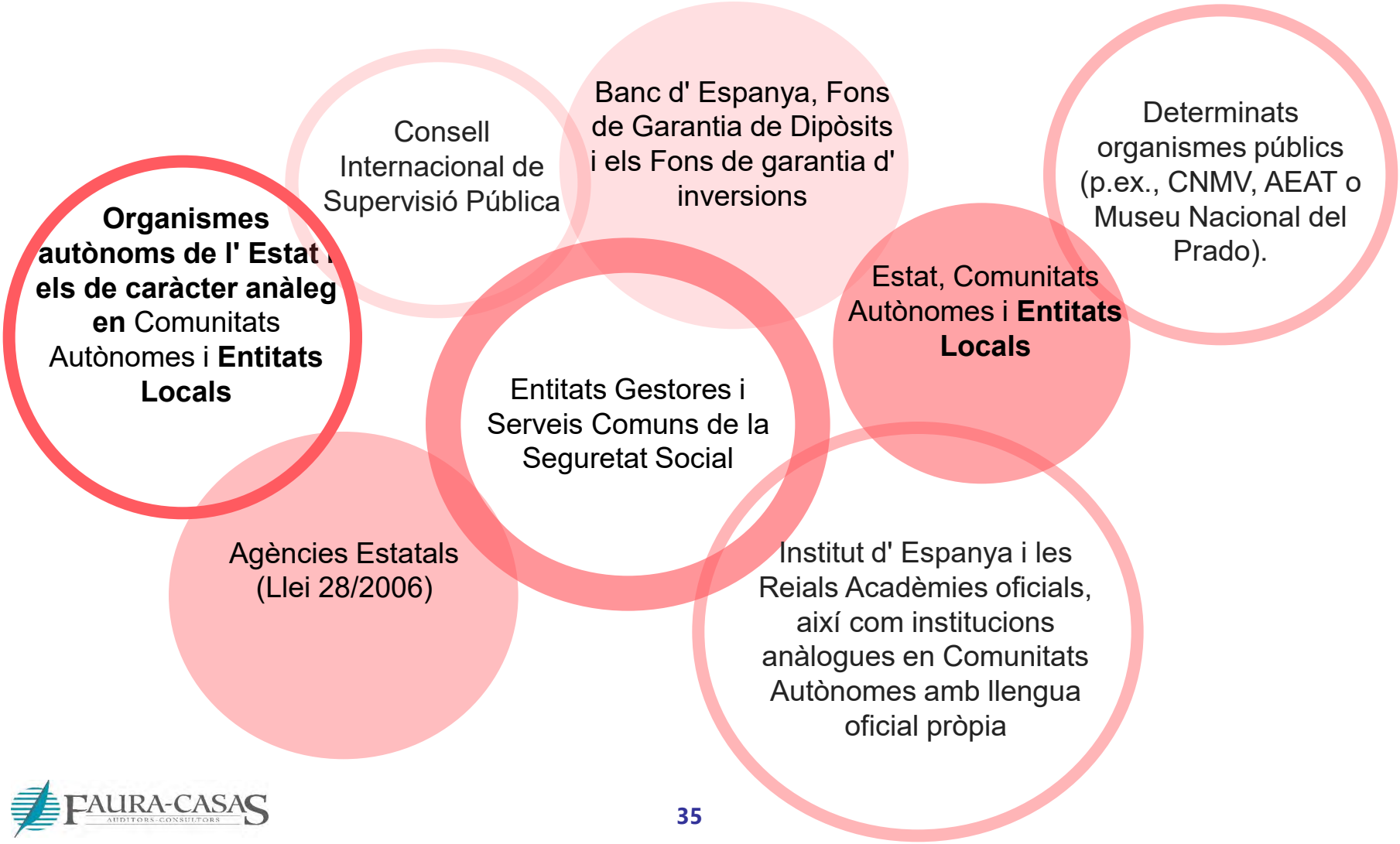


El sector públic espanyol



II.2. ENTITATS TOTALMENT EXEMPTES *(Art. 9.1 LLIS)*

Llistat d'ens públics que gaudeixen d'exempció total



Règim de les rendes obtingudes per entitats totalment exemptes

- Totes les rendes que obtinguin no tributen per l' IS.
- A causa de l'exempció, no estan subjectes a retenció les rendes percebudes (article 128.4, lletra a) LLIS).
- Això no obsta que hagin de practicar retencions, quan escaigui, sobre les rendes que satisfacin a tercers.
- No estan obligades a presentar declaració per l'IS (article 124.2 LLIS).
- No estan obligades a inscriure's en l'índex d'entitats (article 118.1 LLIS).

Entitats totalment exemptes de l'IS: criteris de l'Administració Tributària

Consulta DGT V1408-08

Fundació Pública Sanitària, organisme públic amb personalitat jurídica pròpia i adscrit al Servei de Salut de les Illes Balears.

El seu objecte és la gestió i administració d'un hospital i la realització d' activitats de promoció, prestació i gestió de recursos i serveis sanitaris assistencials a la seva zona, la docència i recerca de les ciències de la salut.

Consulta DGT V1475-16

Organisme Autònom que es va transformar en una Entitat Pública Empresarial Local, té com a finalitat bàsica la prestació del servei públic d'abastament d'aigua per a reg, que inclou l' emmagatzematge, transport, dessalat i subministrament d'aigua, així com la gestió de totes aquelles infraestructures hidràuliques o instal·lacions afectes a la mateixa mitjançant adscripció, cessió en ús o qualsevol títol admissible en Dret que li permetin la consecució dels fins assignats.

Amb caràcter general, la contraprestació percebuda per aquesta entitat per la prestació de l' esmentat servei públic consisteix en el pagament d'un preu públic per part dels usuaris.

* Véase también la consulta nº V4009-16, que analiza el caso de un consorcio público sanitario en Catalunya.

Entitats totalment exemptes de l'IS: criteris de l'Administració Tributària

Consulta DGT V2198-18

Societat (X) constituïda el 2004, que va ser posteriorment declarada com a mitjà propi instrumental i servei tècnic de l'Administració del Principat d'Astúries.

El Principat d'Astúries ostenta la íntegra titularitat del capital social de la societat, sent el seu accionista únic i documentant-se les relacions entre l'administració i l'empresa mitjançant encàrrecs de gestió.

L'objecte social de X és la provisió de tot tipus d'infraestructures i equipament d' índole sanitari i sociosanitari, així com la prestació dels serveis inherents i complementaris a la finalitat perseguida amb aquesta provisió.

Entitats totalment exemptes de l'IS: criteris de l'Administració Tributària

Ajuntament que pretén obrir un comerç per a despatx de productes de primera necessitat, així com obrir un servei de bar. Possible exempció aplicable en l' Impost sobre Societats.

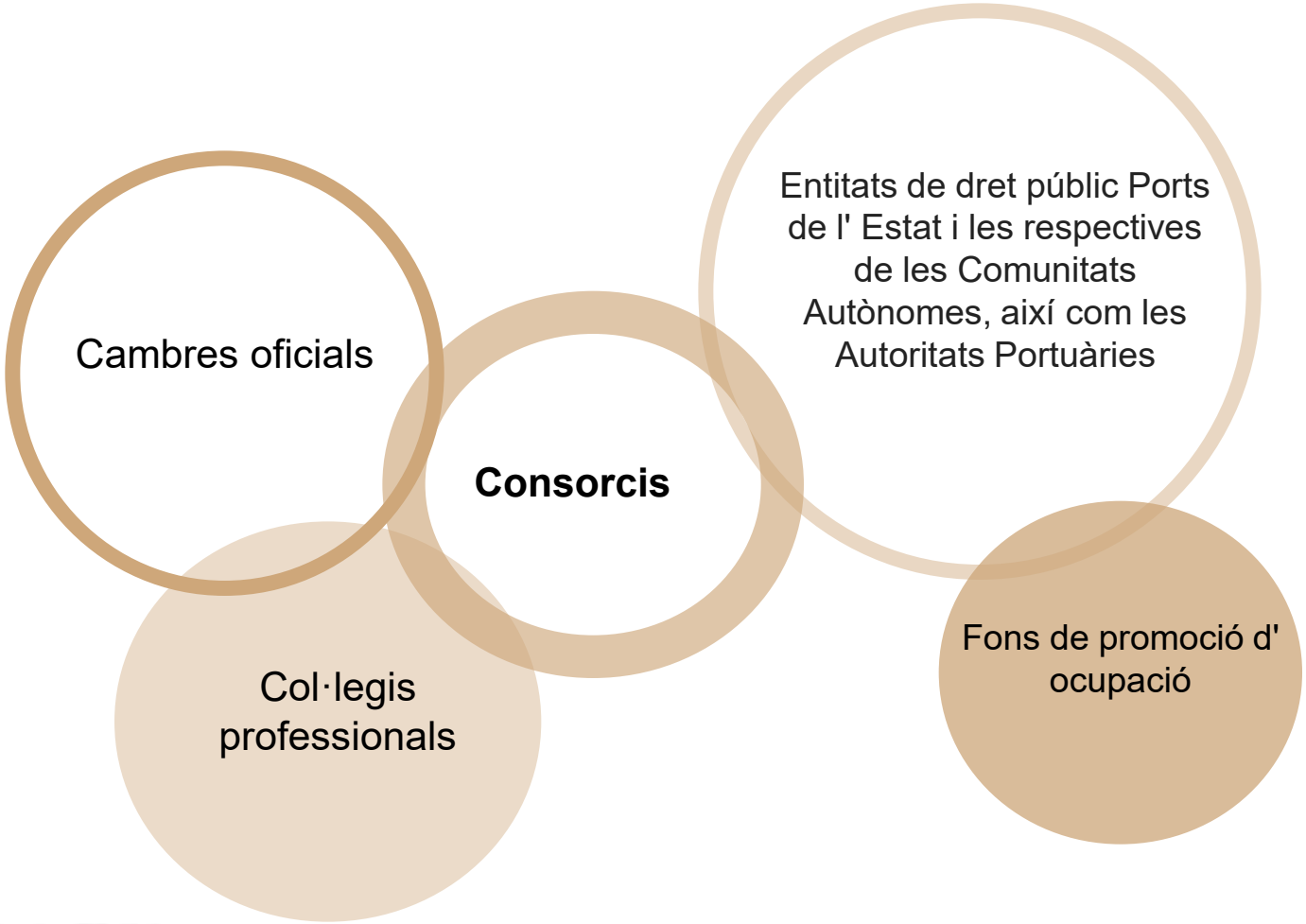
L' exempció establerta en l' Impost sobre Societats en favor de les entitats locals és de caràcter subjectiu amb independència d' on provingui la renda percebuda per aquestes. Aquesta exempció no requereix declaració expressa o autorització prèvia, sinó que resulta d' aplicació automàtica quan es compleix el supòsit de fet corresponent que en aquest cas consisteix en l' obtenció de renda per una entitat local.

Una mancomunitat de municipis. Està totalment exempta de l'Impost sobre Societats? Estan subjectes a retenció els rendiments del capital mobiliari que obtinguin?

Una mancomunitat de municipis té la consideració legal d' entitat local, per la qual cosa li resulta plenament aplicable l' exempció total de l' Impost sobre Societats prevista a l' article 9 de la LIS, no estant subjectes a retenció ni ingrés a compte, una vegada acreditada la seva condició d' entitat exempta, les rendes per ella obtingudes.

II.3. ENTITATS PARCIALMENT EXEMPTES *(Art. 9.2 LLIS)*

Llistat d'ens públics que gaudeixen d'exempció parcial



El cas particular del **consorci**: definició

Article 118 Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic

*"Els consorcis són entitats de dret públic, amb personalitat jurídica pròpia i diferenciada, creades per diverses Administracions Públiques o entitats integrants del sector públic institucional, entre si o **amb participació d'entitats privades**, per al desenvolupament d'activitats d'interès comú a totes elles dins l'àmbit de les seves competències."*

Article 113 Llei 26/2010, del 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya

*"1. Les administracions públiques de Catalunya poden constituir consorcis, o bé adherir-se a d'altres ja existents, amb altres administracions, organismes o entitats públiques, o **amb entitats privades sense ànim de lucre**, que tinguin finalitats d'interès públic concurrents.*

2. Els consorcis són entitats de dret públic, tenen caràcter associatiu, naturalesa voluntària, personalitat jurídica pròpia i capacitat per a crear i gestionar serveis i realitzar activitats i obres en els termes que estableix la normativa aplicable als organismes, administracions i entitats públiques consorciats."

Entitats parcialment exemptes de l'IS: criteris de l'Administració Tributària

Consulta DGT V1190-14

Consorci constituït entre un Ajuntament, una Diputació Provincial i la junta d' una Comunitat Autònoma, té com a objecte efectuar accions tendents a fer publicitat, promocionar i donar a conèixer un aeroport. **Es tracta d'un ens sense ànim de lucre**.

El Consorci pot percebre fons de diverses entitats, destinant-los a activitats publicitàries o promocionals.

Consulta DGT V4009-16

Consorci sanitari públic creat mitjançant acord de Govern del Departament de Salut de la Generalitat de Catalunya, constituït arrel d'un antic hospital X, i està integrat per l'Administració de la Generalitat de Catalunya a través del Servei Català de la Salut i per la Universitat de Barcelona.

El Consorci finança les seves activitats majoritàriament a traves del conveni subscrit amb el Servei Català de la Salut, per a la prestació de serveis sanitaris als beneficiaris de la Seguretat Social en l'àmbit de la Comunitat Autònoma de Catalunya.

Hauria de tributar a l'IS un consorci compost exclusivament per ens públics?

Sentència TSJ CAT 10995/2019

Consorci constituït per la Generalitat de Catalunya i integrat per la pròpia Generalitat, l'Ajuntament de Barcelona i la Universitat Pompeu Fabra Consorci sanitari públic creat mitjançant acord de Govern del Departament de Salut de la Generalitat de Catalunya, constituït arrel d'un antic hospital X, i està integrat per l'Administració de la Generalitat de Catalunya a través del Servei Català de la Salut i per la Universitat de Barcelona, amb l'objectiu d'impulsar activitats d'investigació, de desenvolupament i d'innovació biomèdica.

El tribunal considera al consorci com a entitat subjectivament exempta de l'IS d'acord amb l'article 9.1 de la LLIS, per l'establert a la lletra b) *(organismes autònoms de l'estat i entitats de dret públic d'anàleg caràcter de les comunitats autònomes i de les entitats locals):*

> *"(...) Existeix una relació de semblança entre l'esmentat Consorci, entitat pública de la comunitat autònoma, i els Organismes autònoms estatals, pel que es troba dintre del supòsit previst a l'article 9.1.b). (...)"*

II.4. BONIFICACIÓ PER PRESTACIONS DE SERVEIS PÚBLICS LOCALS *(art. 34 LLIS)*

- Bonificació del 99% de la quota derivada de rendes obtingudes per la prestació de serveis públics de competència local *(article 25.2 LLRBRL)*.

- Realitzats per entitats íntegrament públiques.

- Dependents d'entitats locals, de l'Estat o de les Comunitats Autònomes.

Serveis bonificats *(art. 25.2 LLRBRL)*

- Urbanisme.
- Medi ambient urbà.
- Cicle integral de l' aigua.
- Infraestructura viària.
- Avaluació, informació i atenció immediata a persona en situació o risc d' exclusió social.
- Policia local, protecció civil i extinció d' incendis.
- Trànsit, estacionament de vehicles i mobilitat.
- Transport col·lectiu urbà.
- Informació i promoció d'activitat turística.
- Fires, abasts, mercats, llotges i comerç ambulant.
- Protecció de la salubritat pública.
- Cementiris i activitats funeràries.
- Promoció de l' esport i instal·lacions esportives.
- Promoció de la cultura i equipaments culturals.
- Participació en la vigilància del compliment de l' escolaritat obligatòria en cooperació amb les Administracions educatives corresponents.
- Conservació, manteniment i vigilància edificis i centres educatius públics.
- Promoció ús de tecnologies de la informació i les comunicacions.
- Promoció de la igualtat entre homes i dones.

Bonificació per prestacions de serveis locals: criteris de l'Administració Tributària

Consulta DGT V2787-15

Societat 100% de capital municipal l' objecte social del qual és dur a terme la completa urbanització del Mont X, realitzant totes les gestions que fossin necessàries, en l' ordre administratiu, tècnic i econòmic, jurídic i comercial, per a la total ordenació i desenvolupament urbanístic de la zona.

Donada la seva situació de desequilibri patrimonial, en aplicació de la Disposició addicional novena de la Llei 7/1985, de 2 d'abril, reguladora de les Bases de Règim Local, la societat s'ha de dissoldre.

Abast de la bonificació regulada a l' article 34 de la LLIS.

Consulta DGT V1909-18

Societat participada íntegrament per un ajuntament, l' objecte social del qual consisteix en la promoció de sòl amb caràcter residencial, industrial i de serveis, així com la realització d' instruments de planejament, gestió i execució del planejament urbanístic.

Aplicació de la bonificació recollida a l' article 34 de la LLIS respecte dels rendiments derivats de l' activitat de promoció de sòl industrial, tant per vendes a tercers, com per la subvenció d' explotació rebuda del seu soci únic.

Bonificació per prestacions de serveis locals: criteris dels Tribunals de Justícia

Sentència TS 311/2014 de 6 de febrer de 2014

Societat mercantil de capital íntegrament d'una comunitat autònoma que té com a principals funcions l' explotació, planificació i millora del transport per ferrocarril i el manteniment i optimització de les instal·lacions de les infraestructures ferroviàries.

Procedència de l' extensió de la bonificació del 99% per la prestació de serveis públics locals als procedents d' activitats auxiliars i complementàries, en la mesura que contribueixen al finançament del cost del servei principal.

Sentència TS 1199/2016 de 26 de maig de 2016

Societat de naturalesa mercantil íntegrament participada per l' Ajuntament X que constitueix una fórmula de gestió directa dels serveis de competència municipal.

Entre els serveis de competència municipal es troben les mesures d'ordenació del trànsit de vehicles que inclouen la gestió de l'estacionament a la via pública i en aparcaments, en la seva majoria subterranis, que constitueixen domini públic municipal.

Aplicació de la bonificació sobre:

- Serveis municipals de regulació de superfície "zona blava"
- Serveis municipals de recollida de vehicles
- Explotació d'aparcaments públics subterranis

Bonificació per prestacions de serveis locals: criteris dels Tribunals de Justícia

Sentència TS de 16 de març de 2018:

Societat 100% de capital municipal l' objecte social del qual la realització dels serveis de gestió integral de residus sòlids, la neteja d'edificis i equipaments municipals, manteniment i conservació de parcs i jardins i manteniment d'instal·lacions municipals.

Abast de la bonificació als ingressos indirectes o accessoris, fins i tot als interessos meritats per imposicions a termini de quantitats provinents no de les prestacions municipals, sinó de subvencions percebudes de l' Administració.

Bonificació per prestacions de serveis locals: càlculs de la bonificació

Càlcul de la quota íntegra. Impossibilitat de bonificar una part de la quota que resulta exclusivament de les activitats no bonificades.

Davant d'una renda neta bonificada negativa, juntament amb una renda neta no bonificada positiva, la quota íntegra resultant ha de procedir únicament de les activitats no bonificades. Les rendes bonificades no tenen cap incidència en la base imposable excepte per minorar les rendes no bonificades, per la qual cosa la raó de ser de la bonificació desapareix.

Resolució TEAC de 18 de setembre de 2018

			Bonificadas	No bonificadas
Actividad 1		2.000		2.000
Actividad 2		3.000		3.000
Actividad 3		1.900	1.900	
Actividad 4		-6.000	-6.000	
BASE IMPONIBLE		**900**	-4.100	5.000
Cuota	25%	225		
Base bonificación	-4.100			
Bonificicación		**0**		
CUOTA ÍNTEGRA		**225**		

			Bonificadas	No bonificadas
Actividad 1		2.000		2.000
Actividad 2		4.000	4.000	
Suma		6.000	4.000	2.000
			66,67%	33,33%
BINs		-1.000	-667	-333
BASE IMPONIBLE		**5.000**	3.333	1.667
Cuota	25%	1.500		
Base bonificación	3.333			
Bonificicación		**825**		
CUOTA ÍNTEGRA		**675**		

MOLTES GRÀCIES!

Jordi Casals (jcasals@faura-casas.com)

Faura-Casas Auditors-Consultors, S.L.

Carrer Còrsega, 299 6ª Barcelona

Tel. 902 28 28 30

@FauraCasas (cat)

@FauraCasasAudit (esp)

Faura-Casas, Auditors-Consultors, SL

www.faura-casas.com

2a sessió

21/03/25

COMPTABILITAT LOCAL: CONSOLIDACIÓ DE COMPTES I NORMES DE REGISTRE I VALORACIÓ

La consolidació dels comptes anuals en el sector públic local.
Albert Valero Tamayo, auditor de la Sindicatura de Comptes de Catalunya.

Normes de registre i valoració del PGCP adaptat a l'administració local: transferències i subvencions, adscripcions i cessions gratuïtes de béns.
Alberto Blanco García, Oficina Nacional d'Auditoria de l'IGAE.

TAULA RODONA
Albert Valero Tamayo, auditor de la Sindicatura de Comptes de Catalunya.
Alberto Blanco García, Oficina Nacional d'Auditoria de l'IGAE.

ASPECTES FONAMENTALS EN LA PRIMERA CONSOLIDACIÓ DEL SECTOR PÚBLIC LOCAL

Albert Valero
Auditor
Sindicatura de Comptes de Catalunya. Membre del ROAC
Nota: La presentació del Seminari complementa aquest article

1. Antecedents de la consolidació del Sector Públic Local

La consolidació al sector públic local es realitzava fins l'any 2021 només de forma voluntària El Ple era el que decidia quines entitats s'havien de consolidar i quines no, sense que aquesta decisió respongués realment a criteris econòmics. **La publicació el 3 de juliol de 2021 de l'Ordre HAC/836/2021, per la qual s'aproven les normes per a la formulació de comptes anuals consolidats a l'àmbit del sector públic local (NOFCACSPL)** va pal·liar el dèficit regulador d'aquesta matèria a la normativa comptable local.

Les NOFCACSPL **culminen el procés d'harmonització comptable** que es va iniciar l'any 2002, quan es va decidir que el llenguatge comú de la comptabilitat en la Unió Europea serien les Normes Internacionals d'Informació Financera (**NIIF**)[1] que fossin adoptades per la Unió Europea

El sector públic estatal també es va incorporar en aquesta corrent harmonitzadora, prenent com a base les Normes Internacionals de Comptabilitat del Sector Públic (**NICSP** o IPSAS, pel seu acrònim en anglès de International Public Sector Accounting Standards). Aquestes normes són **l'adaptació al sector públic de les NIIF**. Per tant, **tota la normativa comptable actual, tant pública com privada, té el mateix origen.**

Aquest procés ha afavorit la unificació conceptual de la comptabilitat i la consolidació, en ambdós sectors. **Així, l'homogeneïtzació de la normativa comptable soluciona una de les dificultats que s'esgrimia per no consolidar**, que era el fet de que les diferents entitats podien

[1] Les Normes Internacionals d'Informació Financera (NIIF o IFRS, acrònim en anglès de les International Financial Reporting Standrds) són les Normes i les Interpretacions adoptades pel Consell de Normes Internacionals de Comptabilitat (IASB, acrònim de International Accounting Standards Board).
Aquestes Normes comprenen:
(a) Normes internacionals d'informació financera (NIIF);
(b) Normes Internacionals de Comptabilitat (NIC o IAS, acrònim de International Accounting Standards); i
(c) les interpretacions elaborades pel Comitè d'Interpretacions de les Normes Internacionals d'Informació Financera (acrònim IFRIC, en anglès) o l'antic Comitè d'Interpretacions (acrònim SIC, en anglès).

utilitzar plans comptables diferents, amb criteris divergents. Un cop realitzada l'harmonització, aquestes discrepàncies han estat reduïdes a la mínima expressió.

2. L'obligació de consolidar en l'àmbit local i les dispenses

En virtut de les NOFCACSPL, la presentació de comptes anuals consolidats resulta **obligatòria per a determinades entitats locals a partir de l'exercici 2022**, en concret, per aquelles incloses a l'article 211 del text refós de la Llei reguladora de les hisendes locals que són les següents:

a) **Municipis de més de 50.000 habitants**
b) **Entitats locals d'àmbit superior al municipi:**

- Diputacions,
- Consells comarcals,
- Mancomunitats de municipis,
- Entitats metropolitanes

L'obligació és efectiva per a la resta d'entitats locals a partir de l'exercici de 2024.

Les NOFCACSPL, en l'article 7, indica 3 **causes de dispensa** per presentar comptes anuals consolidades:

a) **Per pertinença a subgrup**: Si l'entitat dominant sotmesa a principis públics és alhora dependent d'una altra entitat sotmesa als principis públics i que estigui obligada a presentar comptes consolidats.
b) **Per manca de significativitat**: Quan totes les entitats dependents no posseeixen cap interès significatiu per a la imatge fidel del patrimoni, de la situació financera i dels resultats del Grup ni individualment ni en el seu conjunt
c) **Per dimensió reduïda**: Quan **l'entitat dominant estigui inclosa en l'àmbit d'aplicació del model simplificat de comptabilitat local**. Aquest model és aplicable a les següents entitats:
    a. Municipis amb pressupost inferior a 300.000 €
    b. Municipis amb pressupost entre 300.000 € i 3 milions d'€ i població inferior a 5.000 habitants
    c. Resta d'entitats locals, amb un pressupost < 3.000.000 €

3. L'objectiu primordial de la consolidació

Tal com diu la pròpia introducció a la norma, la necessitat d'obtenir uns comptes anuals consolidats prové del el creixent procés de descentralització en la prestació de serveis públics, que ha estat acompanyat de la pèrdua d'informació del grup d'entitats públiques incloses dins del mateix àmbit de control, en revelar-se els comptes anuals individuals insuficients per reflectir la gestió realitzada per totes les entitats.

Davant d'aquesta situació, es fan necessaris altres comptes anuals que mostrin **la imatge fidel** de la situació financera, patrimonial i pressupostària del grup d'entitats públiques, i que no poden ser la mera agregació dels comptes individuals .

Per tant, **l'objectiu fonamentals dels comptes anuals consolidats és obtenir la imatge fidel.**

Les mateixes NOFCACSPL esmenten fins a en 15 ocasions "la imatge fidel".

Però el que resulta més important és allò que indica l'article 48, que es transcriu literalment:

"Article 48. Documents que integren els comptes anuals consolidats.

(...)

4. Quan es consideri ***que el compliment d'aquests requisits de la informació i principis i criteris comptables*** *no sigui suficient* ***per mostrar la imatge fidel*** *esmentada, se subministrarà a la memòria la informació complementària necessària per assolir aquest objectiu.*

5. ***En aquells casos excepcionals en què aquest compliment fos incompatible amb la imatge fidel que han de proporcionar els comptes anuals consolidats, es considerarà improcedent aquesta aplicació****. En aquests casos, a la memòria consolidada es motivarà suficientment aquesta circumstància, i se n'explicarà la influència sobre el patrimoni, la situació financera i els resultats del grup."*

Per tant, a pròpia norma ens està indicant que **es poden incomplir els preceptes inclosos en la norma** si és que l'aplicació d'aquests pot distorsionar **l'objectiu fonamental dels comptes anuals consolidats: la imatge fidel.**

4. La determinació de les entitats intervinents en la consolidació

La consolidació dels comptes anuals és un repte per a totes les entitats locals, però més encara en aquelles entitats de menor dimensió que han entrat dins de de l'obligació de la consolidació en el passat exercici 2024.

La **principal qüestió** en la **primera consolidació** consisteix en **determinar quines són les entitats intervinents** en la consolidació.

Cal destacar que el concepte **d'entitats intervinent en la consolidació és més ampli que** el de **perímetre de consolidació**:

- **El perímetre de consolidació** comprèn totes aquelles **entitats sobre les que s'apliquen els mètodes i procediments de consolidació.**
- **Les entitats intervinents** en la consolidació són aquelles que estan incloses en el **perímetre de consolidació més aquelles que han estat excloses** i sobre les quals no s'apliquen els mètodes de consolidació.

Determinar adequadament les entitats intervinents en la consolidació és la base per aconseguir l'objectiu fonamental de la presentació d'uns estats financers consolidats, donant informació completa de tots els serveis públics que presta una entitat local matriu, ja sigui directament, ja sigui mitjançant qualsevol altra entitat creada o participada per mostrar la imatge fidel..

Els diferents **tipus d'entitats intervinents** en la consolidació són els següents:

- **Entitat dominant**
- **Entitats dependents**
- **Entitats multigrup**
- **Entitats associades**

4.1 Criteris de classificació de les entitats

La determinació de la tipologia de les entitats intervinents és una qüestió conceptual. Els criteris que estableix la normativa per a la qualificació de les entitats impliquen el judici. En alguns casos s'apunten algunes presumpcions quantitatives que ajuden en la determinació del tipus d'entitat, però en qualsevol cas el que determina la naturalesa de les entitats és el concepte subjacent.

Les característiques dels diferents tipus d'entitats són els següents:

a) Entitat Dominant:

L'entitat dominant és l' entitat del sector públic local, subjecta a principis comptables públics, que **ostenta, directament o indirectament, el control** sobre una altra o altres, denominades dependents.

S' entén per **control el poder de dirigir les polítiques financeres i l' activitat d' una altra entitat amb la finalitat d' obtenir rendiments econòmics o potencial de servei**.

En particular, **llevat de que existeixi una evidència clara de que altra entitat exerceix el control, es presumeix** que aquest existeix **quan es compleix almenys una de les condicions de poder i una altra de les de patrimoni net** que s' enumeren a continuació:

Condicions de poder:

i. **L' entitat té directament, o indirectament** a través d' entitats controlades, la propietat d'una **participació majoritària superior al 50% amb dret a vot** a l' altra entitat.
ii. L' entitat té la potestat, en virtut de disposició normativa o acord formal, de **nomenar o revocar la majoria dels membres de l' òrgan de govern** de l' altra entitat.
iii. L' entitat té, en virtut de disposició normativa o acord formal, **la majoria dels drets de vot** que seria possible emetre **en una junta general** de l' altra entitat.
iv. L' entitat té, en virtut de disposició normativa o acord formal, **el poder per emetre la majoria dels vots en les reunions de l'òrgan de govern,** i el control de l' altra entitat s'exerceix mitjançant aquest òrgan.
v. L' entitat **ha designat amb els seus vots la majoria dels membres de l' òrgan de govern**, que exerceixin el seu càrrec en el moment en què s' hagin de formular els comptes consolidats i durant els dos anys immediatament anteriors. En particular, es presumirà aquesta circumstància quan la majoria dels membres de l' òrgan de govern de l' entitat dependent siguin membres de l' òrgan de govern d' alguna entitat del grup.

Condicions de Patrimoni net:

i. L' entitat té **la potestat de dissoldre l' altra entitat** i obtenir un nivell important de beneficis econòmics residuals o **assumir obligacions importants**.
ii. L' entitat té la **potestat d' accedir a la distribució dels actius** de l' altra entitat, o pot ser **responsable de certes obligacions** de l' altra entitat.

b) Entitats dependents

Seran entitats dependents aquelles **sobre les que l'entitat dominant exerceixi el control**.

Les NOFCACSPL estableixen quines **entitats no poden ser dependents**[2]:

1. **Entitats de l'article 3 de la Llei 7 / 1985, de 2 d'abril, reguladora de les bases de règim local:**
   1.1. Ajuntaments (municipi)
   1.2. Diputacions (província)
   1.3. Illes
   1.4. Consells comarcals (comarques)
   1.5. Àrees metropolitanes
   1.6. Mancomunitats de municipis
2. **Entitats d'àmbit territorial inferior al municipi que tinguin personalitat jurídica pròpia**:
   2.1. Entitats Municipals descentralizades

La normativa indica que no poden ser dependents, però **enlloc es diu que no puguin ser considerades dins d'una altra tipologia d'entitats**. Per tant, res es diu en contra de que puguin ser considerades com a entitats multigrup o entitats associades.

Addicionalment, les NOFCACSPL determinen que **els consorcis i fundacions adscrits a una entitat local tindran la consideració d'entitats dependents d'aquesta entitat local[3].**

Basats en aquesta indicació**, els consorcis o fundacions** o són entitats dependents de l'entitat a la que esta adscrita, o bé **poden ser considerades entitats associades per la resta d'entitats participants en l'ens**, si es donen les circumstàncies per a ser classificades com a tals. **En cap cas podran ser considerades entitats multigrup**, atès que el control és conceptualment incompatible amb el control conjunt,

c) Entitats multigrup

D'acord amb les NOFCACSPL, són entitats multigrup, als únics efectes de la consolidació, aquelles entitats no incloses en el grup, **que són gestionades per una o diverses entitats del grup**, que participen en el seu capital social o patrimoni, conjuntament amb una altra o altres alienes al grup. És a dir, **el control de l'entitat és conjunt.**

La **gestió conjunta és l' acord estatutari o contractual** en virtut del qual dues o més entitats convenen compartir el poder de dirigir les polítiques financeres i operatives sobre una activitat econòmica, de tal manera que **les decisions estratègiques, tant financeres com operatives**

[2] Article 2.1
[3] Article 2.3

relatives a l' activitat requereixin el consentiment unànime de tots els que exerceixen la gestió conjunta.

d) Entitats associades

D'acord amb les NOFCACSPL, tindran la condició d' entitats associades, als únics efectes de la consolidació de comptes, aquelles, no incloses en el grup, en les quals **una o diverses entitats del grup exerceixin una influència significativa** per tenir una participació en el seu capital social o patrimoni que, creant amb aquesta una vinculació duradora, estigui destinada a contribuir a la seva activitat.

Hi ha influència significativa en la gestió d' una altra entitat, quan es compleixen els **dos requisits** següents:

- Que una o diverses entitats del grup **participin en el capital social o en el patrimoni** de l'entitat, i
- Que es **tingui el poder d' intervenir en les decisions de política financera i operativa de la participada**, sense arribar a gestionar-la conjuntament ni a tenir el control.

Es presumirà, llevat de prova en contrari, que es compleixen els requisits establerts en l'apartat anterior **quan una o diverses entitats del grup posseeixin, almenys, el 20 % del capital o patrimoni** de l'entitat que no pertany al grup.

Les NOFCACSPL no disposen cap altre factor a considerar sobre com determinar l'existència o no d'influència significativa. **Per aprofundir** en què es pot entendre el concepte d'influència significativa **es pot recórrer a** les Normes de Formulació de Comptes Anuals Consolidats del sector privat (NOFCAC)[4]. **Les NOFCAC són normativa supletòria de les NOFCACSPL**, d'acord amb la disposició final primera d'aquestes.

Les NOFCAC, en el seu article 5.3 introdueix **altres elements per avaluar l'existència d'influència significativa** que es transcriuen literalment :

"Així mateix, tenint participació a la societat l'existència d'influència significativa es podrà evidenciar a través de qualsevol de les següents vies:

a) ***Representació al consell d'administració o òrgan equivalent*** *de direcció de la societat participada;*

[4] Les NOFCAC es troben publicades al Reial Decret 1159/2010 de 17 de setembre, pel qual s'aproven les Normes per a la Formulació de Comptes Anuals Consolidats

b) ***Participació en els processos de fixació de polítiques****, entre les quals s'inclouen les decisions sobre dividends i altres distribucions;*

c) ***Transaccions d'importància relativa*** *amb la participada;*

d) ***Intercanvi de personal directiu****; o*

e) ***Subministrament d'informació tècnica essencial****"*

Per tant, **més enllà de la presumpció del 20% de participació, s'hauria d'atendre al concepte d'influència significativa** per determinar realment les entitats associades. Les evidències indicades per les NOFCAC, normativa supletòria, són una bona guia, en especial la representació en l'òrgan de govern de l'entitat..

4.2 Exclusions d'entitats de la consolidació

Les NOFCACSPL contemplen en **l'article 8** una sèrie de **supòsits pels quals una entitat pot ser exclosa del perímetre de consolidació** i, per tant, de l'aplicació dels mètodes i procediments de consolidació. Aquests supòsits afecten a aquelles entitats en les quals concorri alguna de les circumstàncies que, a continuació, s' indiquen:

a) Que **no tinguin un interès significatiu per a la imatge fidel** que han d' expressar els comptes anuals consolidats. Essent diverses les entitats en aquestes circumstàncies, no podran ser excloses de la consolidació més que, si en el seu conjunt, presenten un interès poc significatiu respecte a la finalitat expressada.

b) Quan hi hagi **restriccions importants i permanents** que dificultin substancialment l'exercici per l' entitat dominant dels seus drets sobre el patrimoni o la gestió de l'entitat dependent.

c) Quan **la informació necessària** per establir els comptes consolidats **només es pugui obtenir incorrent en despeses desproporcionades o amb un retard inevitable** que impossibiliti l' elaboració d' aquests comptes en el termini establert en la normativa aplicable.

4.3 Entitats no incloses en la consolidació

L'objectiu dels Comptes anuals consolidats és donar completa informació de tots els serveis que presta el grup a través de les entitats que el conformen, així com la informació pertinent de la resta d'entitats intervinents. **La no inclusió de totes les entitats en les que participa el grup defuig la informació completa que es demana al consolidat per mostrar la imatge fidel**.

A través de diferents fonts d'informació es poden detectar aquelles entitats en les que l'entitat dominant o les seves dependents hi participen i que poden no estar incloses en el procés de

consolidació. **Una relació, no exhaustiva, d'aquestes fonts que es poden utilitzar per determinar l'existència de més entitats intervinents** en la consolidació, són les següents:

- Informació de la web de l'entitat
- Informació de les web de les principals entitats dependents
- Informació de l'Inventari d'entitats del sector públic estatal, autonòmica i local de la IGAE (INVENTE)[5]
- Informació del Registre del Sector Públic Local de Catalunya (RSPLC)[6]
- Comptes anuals individuals disponibles, tant de les entitats incloses com de les excloses del perímetre de consolidació
- Inventari de béns i drets de l'entitat

Totes aquestes fonts d'informació poden posar al descobert altres entitats que serien susceptibles de ser considerades com a intervinents en la consolidació.

5. La diferència de primera consolidació i el Fons de Comerç

La primera consolidació es produeix quan una entitat entra per primer cop dins del grup, és a dir, **el moment en que passa a considerar-se entitat intervinent**. Aquest moment **no és la data del primer procés de consolidació** que, generalment, es realitzarà a final d'exercici, sinó **la data en que es participa en la seva creació o s'adquireix la participació.**

Quan es participa en una entitat que és creada o constituïda, no existeix conceptualment cap diferència en la primera consolidació, atès que l'import que s'ha aportat com a patrimoni en la creació haurà de coincidir necessàriament amb l'import recollit com a inversió en l'entitat que hi participa. Si en aquell moment es realitza la primera consolidació, l'eliminació de la inversió en la participada contra el patrimoni net d'aquesta, coincidiran els imports a eliminar, que seran igual a les aportacions efectuades.

Diferent és la problemàtica **quan l'entitat que es consolida és una entitat que s'adquireix**. En aquest cas, l'import que es desembolsa o que s'inverteix per tenir la participació rarament coincideix amb la part del patrimoni que representa aquesta inversió. D'aquesta manera, quan en consolidació es vol realitzar, **en el moment de l'adquisició, l'eliminació del valor de la inversió que apareix en l'agregat, amb la part de patrimoni net que representa aquesta**

[5] L'INVENTE té com a finalitat garantir la informació pública i l'ordenació de totes les entitats integrants del sector públic institucional, qualsevulla que sigui la seva naturalesa jurídica.

[6] El RSPLC és un registre de caràcter públic, adscrit a la Direcció General d'Administració Local, en el qual s'han d'inscriure tots els ens locals de Catalunya, així com els seus ens dependents i altres ens adscrits o vinculats

inversió, sorgeix una diferència. Aquesta és l'anomenada diferència de primera consolidació.

Les NOFCACSPL defineixen la diferència de primera consolidació en l'article 20.1 :

"*S'anomena diferència, positiva o negativa, de primera consolidació l'existent entre el valor comptable de la participació al capital o patrimoni de l'entitat dependent que posseeixi, directament o indirectament, l'entitat dominant i la part proporcional del patrimoni net representativa de la participació al capital o patrimoni de l'entitat dependent a la data de la seva adquisició".*

Si la diferència és positiva, donarà lloc, si no hi ha cap actiu a ajustar, a un actiu sorgit del procés de la consolidació anomenat fons de comerç. En cas de ser la diferència negativa, sorgeix un ingrés, la diferència negativa de consolidació.

La **problemàtica del càlcul de la diferència de primera consolidació** es pot presentar en el **cas d'haver de fer una consolidació en exercicis posteriors a la primera consolidació.** En aquest cas, per a les entitats adquirides seria necessari conèixer quina era la diferència de primera consolidació en origen, en el moment de l'adquisició. Davant aquest problema de procediment, i per evitar haver de fer una aplicació retroactiva en el temps, que en la pràctica pot resultar inviable, **les NOFCACSPL estableixen un criteri simplificador** en l'article 19.3: **es pot considerar la incorporació d'una entitat al grup en la data de començament del primer exercici en que l'entitat dominant estigués obligada a formular Comptes Anuals Consolidats.** La diferència que resulti correspondrà a un fons de comerç, si és positiva o a més reserves, si és negativa.

Aquesta problemàtica no afecta a aquelles entitats que han estat creades o constituïdes Les diferències entre patrimoni net i la inversió correspondran inequívocament a les partides de patrimoni que hagin anat acumulant aquella participació des de la seva constitució, ja siguin reserves, ja siguin ajustos per canvi de valor, ja siguin subvencions.

Per tant, en el sector públic majoritàriament no existiran Fons de comerç. Només podran existir en entitats adquirides.

NORMAS DE REGISTRO Y VALORACIÓN DEL PGCP ADAPTADO A LA ADMINISTRACIÓN LOCAL: TRANSFERENCIAS Y SUBVENCIONES, ADSCRIPCIONES Y CESIONES GRATUITAS DE USO DE BIENES Y DERECHOS

Barcelona, 21 de marzo de 2025

Alberto Blanco García
División I Planificación y Dirección de la Contabilidad Pública
OFICINA NACIONAL DE CONTABILIDAD
INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO
MINISTERIO DE HACIENDA

Normativa

Plan General Contabilidad Pública adaptado a la Administración Local (Plan de Cuentas Normal)

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

NRV 19. Adscripciones y otras cesiones gratuitas de uso de bienes y derechos:

Se incluyen aquellas operaciones por las que se **transfieren gratuitamente activos para su utilización** por la entidad receptora en un destino o fin determinado, de forma que si los bienes o derechos no se utilizaran para la finalidad prevista deberán ser objeto de reversión o devolución a la entidad aportante, tanto si lo establece así la normativa aplicable como si deriva del acuerdo suscrito entre las entidades (aportante y receptora).

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

Se registrarán y valorarán tanto en la **entidad beneficiaria o cesionaria** como en la entidad aportante o cedente de acuerdo con los criterios establecidos en la norma de reconocimiento y valoración **NRV 18 Transferencias y subvenciones**.

En el caso de que existan dudas sobre la utilización del bien o derecho para la finalidad prevista, la operación tendrá la consideración de pasivo para la entidad beneficiaria.

Se presumirá la utilización futura del bien o derecho para la finalidad prevista siempre que sea ese su uso en el momento de elaborar las cuentas anuales.

Las **adscripciones** de bienes desde una entidad publica **a sus entidades dependientes** se atenderá al apartado 4 de la NRV 18 Transferencias y subvenciones, constituyendo una **aportación patrimonial** inicial o una ampliación consecuencia de nuevas competencias.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

Concepto	Adscripción		Cesión de uso gratuita	
Sujetos	Transferido a un Organismo **dependiente**	Transferido **entre organismos dependientes**	Transferido por una entidad propietaria a una **entidad participada siendo una aportación inicial o ampliación** por nuevas competencias	Transferido a un **tercero** o a una **entidad participada sin ser aportación inicial o ampliación** por nuevas competencias
Reconocimiento y valoración	**Inversión F. / Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*	**Inversión F./ Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

Concepto	Adscripción		Cesión de uso gratuita	
Sujetos	Transferido a un Organismo **dependiente**	Transferido **entre organismos dependientes**	Transferido por una entidad propietaria a una **entidad participada siendo una aportación inicial o ampliación** por nuevas competencias	Transferido a un **tercero** o a una **entidad participada sin ser aportación inicial o ampliación** por nuevas competencias
Reconocimiento y valoración	**Inversión F. / Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*	**Inversión F./ Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1. Adscripciones:

1.1. Adscripción desde una entidad pública a sus entidades dependientes.

Siempre se va a entender que es **aportación patrimonial inicial** o posteriores **ampliaciones** por asunción de nuevas competencias. Este caso de adscripción se registrará por las entidades dominantes como **inversiones en el patrimonio** de las dependientes, valorándose de acuerdo con los criterios establecidos en la norma de valoración NRV 8 “Activos financieros” y por la entidad dependiente como **patrimonio neto**.

-NRV 19 Adscripciones y otras cesiones gratuitas de uso de bienes y derechos
-NRV 18 Transferencias y subvenciones
-NRV 8 Activos financieros

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.1. Periodo indefinido o similar a la vida económica del bien

Adscribiente (Aportante)

- Reconocimiento: momento de entrega del bien
- Valoración: Valor Razonable (VR) en el momento de la adscripción (NRV 8)
- Contabilización:

-Registrará una inversión financiera en la entidad dependiente.
-Dará de baja el inmovilizado material de su balance a valor contable.
-La diferencia entre el valor razonable de la inversión y el valor contable del bien se imputará en la Cuenta del Resultado Económico Patrimonial como una pérdida/beneficio procedentes del inmovilizado.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.1. Periodo indefinido o similar a la vida económica del bien

Adscribiente (Aportante)

- Esquema general de asientos contables:

	(250X) Participaciones a l/p en entidades del grupo **(28XX) Amortización acumulada inmovilizado** ***(67X) Pérdidas procedentes del inmovilizado***	**a**	**(2XXX) Inmovilizado** ***(77X) Beneficios procedentes del inmovilizado***	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.1. Periodo indefinido o similar a la vida económica del bien

Beneficiaria

- Reconocimiento: momento de recepción del bien
- Valoración: Valor Razonable (VR) en el momento de la adscripción
- Contabilización:

  -Registrará el elemento recibido en función de su naturaleza económica.

  -Reconocerá en el Patrimonio Neto (PN) una aportación patrimonial.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.1. Periodo indefinido o similar a la vida económica del bien

Beneficiaria

- Esquema general de asientos contables:

	(2XXX) Inmovilizado	**a**	**(1011) Aportación de bienes y Derechos**	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

Reconocimiento y valoración:

1.1.1. Periodo indefinido o similar a la vida económica del bien

EJEMPLO 1.1.1.

El Ayuntamiento “A” entrega en adscripción a su OOAA “B” un edificio para que sea su sede de manera indefinida. Se conocen los siguientes datos de la operación:

-VR edificio = 400.000€ (corresponden 100.000€ al terreno)

-Valor contable en “A”:

Terrenos:50.000€; Construcciones: 400.000€; AAIM: 200.000€

-Vida útil restante: 20 años

-Fecha operación 1-1-x1

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.1. Periodo indefinido o similar a la vida económica del bien

EJEMPLO 1.1.1.

1-1-x1. **Adscribiente (Aportante)**

400.000 **200.000**	**(2500) Participaciones a l/p en entidades del grupo** **(281) Amortización Acumulada del Inmovilizado material (AAIM)**	**a**	**(210) Terrenos** ***(211) Construcciones*** ***(771) Beneficios procedentes del inmovilizado material***	**50.000** **400.000** **150.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.1. Periodo indefinido o similar a la vida económica del bien

EJEMPLO 1.1.1.

1-1-x1. **Beneficiaria**

100.000 **300.000**	**(210) Terrenos** **(211) Construcciones**	**a**	**(1011) Aportación de bienes y Derechos**	**400.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.2. Periodo inferior a la vida económica del bien

Adscribiente (Aportante)

- Reconocimiento: momento de entrega del bien
- Valoración:
  - Valor Razonable (VR) del usufructo cedido en el momento de la adscripción (NRV 8)
  - Valor Contable (VC) del usufructo cedido en el momento de la adscripción

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.2. Periodo inferior a la vida económica del bien

Adscribiente (Aportante)

- Contabilización:

-Registrará una inversión financiera en la entidad dependiente.
-Registrará en la cuenta 299, "Deterioro de valor por usufructo cedido del inmovilizado material", un deterioro por el valor contable del usufructo cedido.
-La diferencia entre el valor razonable de la inversión y el valor contable del usufructo cedido se imputará en la Cuenta Resultado Económica Patrimonial como una pérdida/beneficio Procedentes del inmovilizado material.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.2. Periodo inferior a la vida económica del bien

Adscribiente (Aportante)

- Esquema general de asientos contables:

	(250X) Participaciones a l/p en entidades del grupo ***(67x) Pérdidas procedentes del inmovilizado***	**a**	**(299) Deterioro de valor por usufructo cedido del Inmovilizado material** ***(77x) Beneficios procedentes del inmovilizado***	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.2. Periodo inferior a la vida económica del bien

Beneficiaria

- Reconocimiento: momento de recepción del bien
- Valoración: Valor Razonable en el momento de la adscripción
- Contabilización:

  -Registrará un inmovilizado intangible por el valor razonable del derecho de uso del bien cedido a la fecha de adscripción

  -Reconocerá en el Patrimonio Neto una aportación patrimonial (por ese mismo valor).

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.2. Periodo inferior a la vida económica del bien

Beneficiaria

- Esquema general de asientos contables:

	(209) Otro inmovilizado intangible	**a**	**(1011) Aportación de bienes y derechos**	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.1.2.

El Ayuntamiento “A” entrega en adscripción a su OOAA dependiente “B” un edificio durante un periodo de 10 años. Se conocen los siguientes datos de la operación:

-Valor Razonable derecho de uso= 300.000€

-Valor Contable usufructo cedido: calculado mediante el importe acumulado de las cuotas de amortización del periodo de cesión

-Vida útil restante: 20 años

-Valor contable en “A”:

Terrenos:50.000€; Construcciones: 400.000€; AAIM: 200.000€

- Fecha operación el 1-1-x1

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.1.2.

1-1-x1. **Adscribiente (Aportante)**

300.000	**(2500)Participaciones a l/p en entidades del grupo**	**a**	**(299) Deterioro de valor por usufructo cedido del Inm. material** **VC (1-1-x1) = 200.000** **Amort. = 200000/20 años=10.000** **Amort. x años cedido =10x10000=100000** ***(771)* Beneficios procedentes del inmovilizado material**	**100.000** **200.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.1.2.

31-12-x1. **Adscribiente (Aportante)**

5.000	**(681) AMORTIZACIÓN INM. VC (1-1-x1) - deterioro= 200000-100000=100.000 Amort. = 100000/20 años=5.000**	**a**	**(2811) AAII**	**5.000**

5.000	**(299) Deterioro de valor por Usufructo cedido del Inmovilizado material**	**a**	**(799) Reversión del deterioro por el usufructo cedido del inmovilizado material.**	**5.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.1.2.

1-1-x1. **Beneficiaria**

300.000	**(209) Otro inmovilizado intangible**	**a**	**(1011) Aportación de bienes y Derechos**	**300.000**

31-12-x1. **Beneficiaria**

30.000	**(680) Amortización INM.I Amort. = 300.000/10 años=30.000**	**a**	**(2809) AAII**	**30.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

Concepto	Adscripción		Cesión de uso gratuita	
Sujetos	Transferido a un Organismo **dependiente**	Transferido **entre organismos dependientes**	Transferido por una entidad propietaria a una **entidad participada siendo una aportación inicial o ampliación** por nuevas competencias	Transferido a un **tercero** o a una **entidad participada sin ser aportación inicial o ampliación** por nuevas competencias
Reconocimiento y valoración	**Inversión F. / Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*	**Inversión F./ Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1. Adscripciones:

   1.2. Adscripción entre entidades dependientes de una misma entidad pública

   Se considerará como **subvenciones** y se registrarán y valorarán tanto en la **entidad beneficiaria o cesionaria** como en la entidad aportante o cedente de acuerdo con los criterios establecidos en la norma de reconocimiento y valoración **NRV 18 Transferencias y subvenciones**.

   En la medida que se trate de operaciones sin contraprestación directa por el beneficiario supondrán un aumento del Patrimonio Neto y una disminución del Patrimonio Neto del concedente.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.1 Periodo indefinido o similar a la vida económica del bien

Adscribiente (Aportante)

- Reconocimiento: momento de entrega del bien
- Valoración: Valor Contable en el momento de la cesión
- Contabilización:

  -Registrará un gasto por subvenciones.
  -Dará de baja el inmovilizado material de su balance a valor contable.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.1. Periodo indefinido o similar a la vida económica del bien

Adscribiente (Aportante)

- Esquema general de asientos contables:

	(651X) SUBVENCIONES **(28XX) Amortización acumulada del inmovilizado**	**a**	**(2XXX) Inmovilizado**	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.1 Periodo indefinido o similar a la vida económica del bien

Beneficiaria

- Reconocimiento: momento de recepción
- Valoración: Valor Razonable en el momento de la recepción
- Contabilización:

  -Registrará el elemento recibido en función de su naturaleza económica.
  -Se reconocerá en el Patrimonio Neto una subvención (Ingreso).
  -La subvención se imputará al resultado de cada ejercicio en proporción a la vida útil del bien, aplicando el mismo método que para la dotación a la amortización de los activos, o en su caso, cuando se produzca su enajenación o baja en inventario.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.1. Periodo indefinido o similar a la vida económica del bien

Beneficiaria

- Esquema general de asientos contables:

	(2XXX) Inmovilizado	**a**	**(940) Ingresos de subv. Para la financiación del inm. No Financiero y de activos en estado de venta**	
	(68X) AMORTIZACIÓN INM.	**a**	**(28XX) AAIM**	
	(840) Imputación de subv. para la financiación del Inm. no financiero y de activos en estado de venta	**a**	**(753) Subv. para la financiación del inm. no financiero y de activos en estado de venta imputadas al resultado del ejercicio**	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.1. Periodo indefinido o similar a la vida económica del bien

EJEMPLO 1.2.1.

La entidad pública “A” realiza una adscripción de un elemento de transporte a la entidad pública “B” por un periodo indefinido de tiempo. Además, se conocen los siguientes datos de la operación de la cesión de uso:

-Valor Razonable elemento de transporte = 6.000€

-Valor Contable en “A” = 10.000 (AAIM=5.000)= 5.000€

-Vida útil restante= 5 años

-Entrega del vehículo el 1-1-x1

-Ambas entidades públicas dependen de la misma entidad

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.1. Periodo indefinido o similar a la vida económica del bien

EJEMPLO 1.2.1.

1-1-x1. **Adscribiente (Aportante)**

5.000 **5.000**	**(651X) SUBVENCIONES** **(2818) Amortización acumulada inmovilizado material**	**a**	**(218) Elementos de Transporte**	**10.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.1. Periodo indefinido o similar a la vida económica del bien

EJEMPLO 1.2.1.

1-1-x1. **Beneficiaria**

6.000	**(218) Elementos de Transporte**	**a**	**(940) Ingresos de subv. Para la financiación del inm. No Financiero y de activos en estado de venta**	**6.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.1. Periodo indefinido o similar a la vida económica del bien

EJEMPLO 1.2.1.

31-12-x1. **Beneficiaria**

1.200	**(681) AMORTIZACIÓN INM. 6000/5=1.200**	**a**	**(2818) Amortización acumulado del inmovilizado material**	**1.200**

1.200	**(840) Imputación de subv. para la financiación del Inm. no financiero y de activos en estado de venta**	**a**	**(753) Subv. para la financiación del inm. no financiero y de activos en estado de venta imputadas al resultado del ejercicio**	**1.200**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.1. Periodo indefinido o similar a la vida económica del bien

EJEMPLO 1.2.1.

31-12-x1. **Beneficiaria**

6.000	**(940) Ingresos de subv. Para la financiación del inm. No Financiero y de activos en estado de venta**	**a**	**(840) Imputación de subv. para la financiación del Inm. no financiero y de activos en estado de venta** **(130) Subvenciones para la financiación del inmovilizado no financiero y de activos en estado de venta.**	**1.200** **4.800**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2 Periodo inferior a la vida económica del bien

Adscribiente (Aportante)

- Reconocimiento: momento de entrega del bien
- Valoración: Valor Contable del usufructo cedido en el momento de la cesión
- Contabilización:

  -Registrará un gasto por subvenciones.
  -Registrará en la cuenta 299, "Deterioro de valor por usufructo cedido del inmovilizado material", un deterioro de valor del elemento por el valor contable del usufructo cedido.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2 Periodo inferior a la vida económica del bien

Adscribiente (Aportante)

- Esquema general de asientos contables:

	(651X) Subvenciones	**a**	**(299) Deterioro de valor por Usufructo cedido del Inmovilizado material**	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2 Periodo inferior a la vida económica del bien

Beneficiaria

- Reconocimiento: momento de recepción
- Valoración: VR del usufructo cedido en el momento del reconocimiento
- Contabilización:

  -Registrará un inmovilizado intangible por el valor razonable del derecho de uso del bien cedido
  -Reconocerá en el Patrimonio Neto una subvención (Ingreso).
  -La subvención se imputará al resultado de cada ejercicio en proporción a la vida útil del inmovilizado, aplicando el mismo método que para la dotación a la amortización de los activos, o en su caso, cuando se produzca su enajenación o baja en inventario.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2 Periodo inferior a la vida económica del bien

Beneficiaria

- Esquema general de asientos contables:

	(209) Otro inmovilizado intangible	**a**	**(940) Ingresos de subv. Para la financiación del inm. No Financiero y de activos en estado de venta**	

	(68X) Amortización INM.	**a**	**(28XX) AAII**	

	(840) Imputación de subv. para la financiación del Inm. no financiero y de activos en estado de venta	**a**	**(753) Subv. para la financiación del inm. no financiero y de activos en estado de venta imputadas al resultado del ejercicio**	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.2.2.

La entidad pública “A” realiza una adscripción de un elemento de transporte a la entidad pública “B” por un periodo de 2 años. Además, se conocen los siguientes datos de la operación de la cesión de uso:

-Valor Razonable derecho de uso= 2.400€

-Valor Contable usufructo cedido: calculado mediante el importe acumulado de las cuotas de amortización del periodo de cesión

-Valor Contable en “A” = 10.000 (AAIM=5.000)= 5.000€

-Vida útil restante= 5 años

-Entrega del vehículo el 1-1-x1

-Ambas entidades públicas dependen de una misma entidad

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.2.2.

1-1-x1. **Adscribiente (Aportante)**

2.000	**(651X) Subvenciones**	**a**	**(299) Deterioro de valor por Usufructo cedido del Inmovilizado material Amortización= 5.000 / 5 años=1.000 Amort. x años cedidos = 2x1.000=2.000**	**2.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.2.2.

31-12-x1. **Adscribiente (Aportante)**

600	**(681) AMORTIZACIÓN INM. VC (1-1-x1) - deterioro= 5.000-2.000=3.000 Amort. = 3.000/5 años=600**	**a**	**(2818) AAII**	**600**

600	**(299) Deterioro de valor por Usufructo cedido del Inmovilizado material**	**a**	**(799) Reversión del deterioro por el usufructo cedido del inmovilizado material.**	**600**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.2.2.

31-12-x2. **Adscribiente (Aportante)**

750	**(681) AMORTIZACIÓN INM. VC (1-1-x2) = 5.000-2.000-600+600= VC (1-1-x2) = 3.000 Amort. = 3.000/4 años=750**	**a**	**(2818) AAII**	**750**

750	**(299) Deterioro de valor por Usufructo cedido del Inmovilizado material**	**a**	**(799) Reversión del deterioro por el usufructo cedido del inmovilizado material.**	**750**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.2.2.

31-12-x3. **Adscribiente (Aportante)**

Ha recuperado el uso del elemento de transporte el 1-1-x3.

Cálculo Amortización para el año x3:

VC (1-1-x3) = 5.000-2.000-600+600-750+750=3.000€

Amort. = 3.000/3 años=1.000€

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.2.2.

1-1-x1. **Beneficiaria**

2.400	**(209) Otro inmovilizado intangible**	**a**	**(940) Ingresos de subv. Para la financiación del inm. No Financiero y de activos en estado de venta**	**2.400**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.2.2.

31-12-x1. Beneficiaria

1.200	**(680) AMORTIZACIÓN INM.I Amort. = 2.400/2 años=1.200**	**a**	**(2809) AAII**	**1.200**

1.200	**(840) Imputación de subv. para la financiación del Inm. no financiero y de activos en estado de venta**	**a**	**(753) Subv. para la financiación del inm. no financiero y de activos en estado de venta imputadas al resultado del ejercicio**	**1.200**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.2. Periodo inferior a la vida económica del bien

EJEMPLO 1.2.2.

31-12-x1. **Beneficiaria**

2.400	**(940) Ingresos de subv. Para la financiación del inm. No Financiero y de activos en estado de venta**	**a**	**(840) Imputación de subv. para la financiación del Inm. no financiero y de activos en estado de venta**	**1.200**
			(130) Subvenciones para la financiación del inmovilizado no financiero y de activos en estado de venta.	**1.200**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.3. *Caso especial*: Por periodos de un año renovables por periodos iguales, sin duración con reserva de revocación por el cedente o sin instrumento jurídico o poco preciso

Adscribiente (Aportante)

- Reconocimiento y valoración: No dará de baja ni deteriorará el elemento cedido reconociendo, al menos anualmente, un gasto por subvención y un ingreso de acuerdo con su naturaleza en la cuenta del resultado económico patrimonial por la mejor estimación del derecho de uso cedido en cada ejercicio
- Contabilización:

  -Registrará un gasto por subvención

  -Registrará un ingreso de acuerdo con su naturaleza

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.3. *Caso especial*: Por periodos de un año renovables por periodos iguales, sin duración con reserva de revocación por el cedente o sin instrumento jurídico o poco preciso

Adscribiente (Aportante)

- Esquema general de asientos contables:

	(651X) Subvenciones	**a**	**(7XXX) Ingresos por naturaleza**	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.3. *Caso especial*: Por periodos de un año renovables por periodos iguales, sin duración con reserva de revocación por el cedente o sin instrumento jurídico o poco preciso

Beneficiaria

- Reconocimiento y valoración: No reconocerá ningún activo y reconocerá, al menos anualmente, un gasto de acuerdo con su naturaleza y un ingreso por subvención en la cuenta de resultados por la mejor estimación del derecho cedido de cada ejercicio
- Contabilización:

  -Registrará un gasto de acuerdo con su naturaleza

  -Registrará un ingreso por subvención

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.3. *Caso especial*: Por periodos de un año renovables por periodos iguales, sin duración con reserva de revocación por el cedente o sin instrumento jurídico o poco preciso

Beneficiaria

- Esquema de asientos contables:

	(6XXX) Gasto por naturaleza	**a**	**(751) Subvenciones para gastos no financieros del ejercicio**	

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.3. *Caso especial*: Por periodos de un año renovables por periodos iguales, sin duración con reserva de revocación por el cedente o sin instrumento jurídico o poco preciso

EJEMPLO 1.2.3.

La entidad pública “B” está utilizando una planta de un edificio propiedad de la entidad pública “A”. Esta utilización se está realizando sin un título jurídico. Se estima el valor de mercado del alquiler de una planta con las mismas condiciones en 10.000€ anuales. Se pide contabilizar la operación.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.3. *Caso especial*: Por periodos de un año renovables por periodos iguales, sin duración con reserva de revocación por el cedente o sin instrumento jurídico o poco preciso

EJEMPLO 1.2.3.

31-12-x1. **Adscribiente (Aportante)**

10.000	**(651X) Subvenciones**	**a**	**(776) Ingresos por arrendamientos**	**10.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

1.2.3. *Caso especial*: Por periodos de un año renovables por periodos iguales, sin duración con reserva de revocación por el cedente o sin instrumento jurídico o poco preciso

EJEMPLO 1.2.3.

31-12-x1. **Beneficiaria**

10.000	**(621) Arrendamientos y cánones**	**a**	**(751) Subvenciones para gastos no financieros del ejercicio**	**10.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

Concepto	Adscripción		Cesión de uso gratuita	
Sujetos	Transferido a un Organismo **dependiente**	Transferido **entre organismos dependientes**	Transferido por una entidad propietaria a una **entidad participada siendo una aportación inicial o ampliación** por nuevas competencias	Transferido a un **tercero** o a una **entidad participada sin ser aportación inicial o ampliación** por nuevas competencias
Reconocimiento y valoración	**Inversión F. / Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*	**Inversión F./ Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

2. Otras cesiones gratuitas de uso de bienes y derechos:

2.1. Transferido por una entidad propietaria a una entidad participada siendo una aportación inicial o ampliación por nuevas competencias

MISMO TRATAMIENTO QUE UNA ADSCRIPCIÓN DESDE UNA ENTIDAD PÚBLICA A SUS ENTIDADES DEPENDIENTES:

SE CONTABILIZA COMO UNA **APORTACIÓN PATRIMONIAL** (NRV 19 / NRV 18 / NRV 8)

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

Concepto	Adscripción		Cesión de uso gratuita	
Sujetos	Transferido a un Organismo **dependiente**	Transferido **entre organismos dependientes**	Transferido por una entidad propietaria a una **entidad participada siendo una aportación inicial o ampliación** por nuevas competencias	Transferido a un **tercero** o a una **entidad participada sin ser aportación inicial o ampliación** por nuevas competencias
Reconocimiento y valoración	**Inversión F. / Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*	**Inversión F./ Aportación patrimonial** *(NRV 19 / NRV 18 / NRV 8)*	**Subvención** *(NRV 19 / NRV 18)*

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

RECONOCIMIENTO Y VALORACIÓN:

2. Otras cesiones gratuitas de uso de bienes y derechos:

2.2. Transferido a un tercero o a una entidad participada sin ser aportación inicial o ampliación por nuevas competencias

MISMO TRATAMIENTO QUE UNA ADSCRIPCIÓN ENTRE ENTIDADES DEPENDIENTES DE UNA MISMA ENTIDAD PÚBLICA:

SE CONTABILIZA COMO UNA **SUBVENCIÓN**
(NRV 19 / NRV 18)

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

CASO PARTICULAR:

+Adscripciones y cesiones gratuitas de uso de una entidad local a un organismo público suyo que aplique el Plan General de Contabilidad.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

CASO PARTICULAR: Adscripción de una entidad local a un Organismo Público que aplique Plan General Contable

EJEMPLO 3.

El Ayuntamiento “A” entrega en adscripción a su Entidad Pública Empresarial “B” un edificio para que desarrolle una actividad especifica de interés general por un periodo indefinido. Se conocen los siguientes datos de la operación:

-VR edificio = 400.000€ (corresponden 100.000€ al terreno)

-Valor contable en “A”:

Terrenos:50.000€; Construcciones: 400.000€; AAIM: 200.000€

-Vida útil restante: 20 años

-Fecha operación 1-1-x1

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

CASO PARTICULAR: Adscripción de una entidad local a un Organismo Público que aplique Plan General Contable:

EJEMPLO 3.

1-1-x1. **Beneficiaria**

100.000 **300.000**	**(210) Terrenos** **(211) Construcciones**	**a**	**(940) Ingresos de subvenciones oficiales de capital**	**400.000**

La **EPE** (**beneficiaria**) deberá aplicar el **Plan General de contabilidad de 2007**. (NRV 18)

Así mismo también le es de aplicación la **Orden EHA/733/2010** de 25 de marzo, por la que aprueba aspectos contables de empresas públicas que operan en determinadas circunstancias.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

CASO PARTICULAR: Adscripción de una entidad local a un Organismo Público que aplique Plan General Contable:

EJEMPLO 3.

31-12-x1. **Beneficiaria**

15.000	**(681) AMORTIZACIÓN INM. 300.000/20=15.000**	**a**	**(281) Amortización acumulado del inmovilizado material**	**15.000**
15.000	**(840) Transferencia de subvenciones oficiales de capital**	**a**	**(746) Subvenciones, donaciones y legados de capital transferidos al resultado del ejercicio**	**15.000**
400.000	**(940) Ingresos de subvenciones oficiales de capital**	**a**	**(840) Transferencia de subvenciones oficiales de capital** **de venta** **(130) Subvenciones oficiales de capital**	**15.000** **385.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

CASO PARTICULAR: Adscripción de una entidad local a un Organismo Público que aplique Plan General Contable:

EJEMPLO 3.

1-1-x1. **Adscribiente (Aportante)**

250.000 **200.000**	**(651) SUBVENCIONES** **(281) AAIM**	**a**	**(210) Terrenos** ***(211) Construcciones***	**50.000** **400.000**

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

CASO PARTICULAR: Adscripción de una entidad local a un Organismo Público que aplique Plan General Contable:

EJEMPLO 4.

El Ayuntamiento “A” entrega en adscripción a su Entidad Pública Empresarial “B” un elemento de transporte para que desarrolle actividades no especificas y que no son de interés publico o general. Se conocen los siguientes datos de la operación:

-Valor Razonable elemento de transporte = 6.000€

-Valor Contable en “A” = 10.000 (AAIM=5.000)= 5.000€

-Vida útil restante= 5 años

-Entrega del vehículo el 1-1-x1

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

CASO PARTICULAR: Adscripción de una entidad local a un Organismo Público que aplique Plan General Contable:

EJEMPLO 4.

1-1-x1. **Beneficiaria**

6.000	**(218) Elementos de transporte**	**a**	**(118) Aportaciones de socios o propietarios**	**6.000**

+La **EPE** (**beneficiaria**) deberá aplicar el **Plan General de contabilidad de 2007**. (NRV 18)

Así mismo también le es de aplicación la **Orden EHA/733/2010** de 25 de marzo, por la que aprueba aspectos contables de empresas públicas que operan en determinadas circunstancias.

Adscripciones y otras cesiones gratuitas de uso de bienes y derechos

CASO PARTICULAR: Adscripción de una entidad local a un Organismo Público que aplique Plan General Contable:

EJEMPLO 4.

1-1-x1. **Adscribiente (Aportante)**

6.000 **5.000**	**(250) Participaciones a l/p en entidades del grupo** **(281) AAIM**	**a**	**(218) Elementos de transporte** ***(771) Beneficios procedentes del inmovilizado material***	**10.000** **1.000**

MUCHAS GRACIAS

Alberto Blanco García
División I Planificación y Dirección de la Contabilidad Pública
OFICINA NACIONAL DE CONTABILIDAD
INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO
MINISTERIO DE HACIENDA

Consultas, observaciones y sugerencias a través de los buzones:
CCLL@igae.hacienda.gob.es
Empresas-CCLL@igae.hacienda.gob.es

3a sessió

25/04/25

LA INTEL·LIGÈNCIA ARTIFICIAL. REGULACIÓ, EXPERIÈNCIES PRÀCTIQUES I APLICACIÓ AL CONTROL INTERN DEL SECTOR PÚBLIC LOCAL

El Reglament d'Intel·ligència Artificial de la Unió Europea de 2024. El dret a la bona administració i el seu control judicial a Espanya.
Juli Ponce Solé, catedràtic de Dret administratiu de la Universitat de Barcelona.

L'impacte de la IA en els treballs de fiscalització.
Miquel Salazar Canalda, síndic major de la Sindicatura de Comptes de Catalunya.

Aplicació de la IA en l'àmbit del control de subvencions a l'IGAE.
Ismael García Cebada, director de l'Oficina d'Informàtica Pressupostària de la Intervenció General de l'Administració de l'Estat.

TAULA RODONA
Juli Ponce Solé, catedràtic de Dret administratiu de la Universitat de Barcelona.
Miquel Salazar Canalda, síndic major de la Sindicatura de Comptes de Catalunya.
Ismael García Cebada, director de l'Oficina d'Informàtica Pressupostària de la Intervenció General de l'Administració de l'Estat.

El Reglament d'Intel·ligència Artificial de la Unió Europea de 2024, el dret a una bona administració digital i el seu control judicial a Espanya

Juli Ponce Solé, Catedràtic de Dret Administratiu. Universitat de Barcelona,

jponce@ub.edu

0. AUTOMATITZACIÓ, INTEL·LIGÈNCIA ARTIFICIAL I SIMPLIFICACIÓ I AGILITZACIÓ

1. HI HA EXEMPLES PRÀCTICS EN MARXA D'AUTOMATITZACIÓ AMB IA DE L'EXERCICI DE FUNCIONS ADMINISTRATIVES? SÍ

2. HI HA AMB POSSIBILITATS INTERESSANTS LÍMITS I PROBLEMES JURÍDICS EN L'ÚS DE LA IA EN LA SIMPLIFICACIÓ I AGILITZACIÓ? SÍ.

3. HI HA REGULACIÓ JURÍDICA VINCULANT QUE HA DE COMPLIR-SE AL RESPECTE I QUE POT CONTROLAR-SE JUDICIALMENT? SÍ. LA QÜESTIÓ DE LA RESERVA D'HUMANITAT.

4. REFLEXIONS FINALS

marcialpons.es/media/pdf/primeras_pags_Reglamento_IA.pdf

UNIVERSITAT DE BARCELONA

0.

- SIMPLIFICACIÓN

Anteproyecto de Ley de agilización administrativa y atracción de inversiones

Departamento de Presidencia, Economía y Justicia

Estadísticas

Nº de aportaciones emitidas 1

Nº de participantes (ciudadanas/os) 1

En el proceso de elaboración de una norma, puedes participar en las **consultas públicas**: Se trata de una consulta a la ciudadanía **con carácter previo a la elaboración del proyecto de una norma reglamentaria o legal**.

[Leer más >]

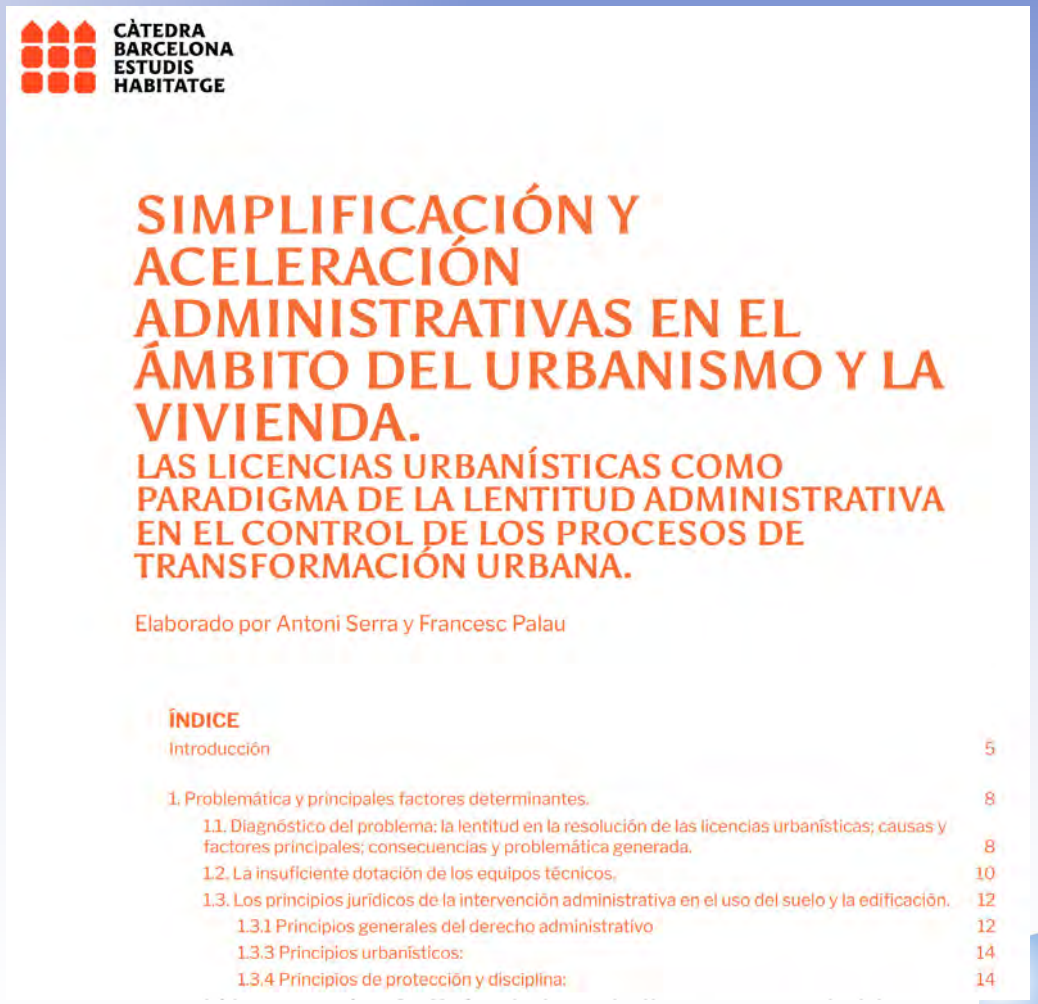
Aquí puedes participar en la consulta pública impulsada por la Comunidad Autónoma:

Agilización administrativa y atracción de inversiones

- Órgano solicitante: Departamento de Presidencia, Economía y Justicia. Gobierno de Aragón
- Fecha de inicio: **22-10-2024**
- Fecha límite para la presentación de aportaciones: **05-11-2024**

UNIVERSITAT DE BARCELONA

- https://cbeh.cat/es/documento/informe-anual-de-la-catedra-2024/



CÀTEDRA BARCELONA ESTUDIS HABITATGE

SIMPLIFICACIÓN Y ACELERACIÓN ADMINISTRATIVAS EN EL ÁMBITO DEL URBANISMO Y LA VIVIENDA.

LAS LICENCIAS URBANÍSTICAS COMO PARADIGMA DE LA LENTITUD ADMINISTRATIVA EN EL CONTROL DE LOS PROCESOS DE TRANSFORMACIÓN URBANA.

Elaborado por Antoni Serra y Francesc Palau

ÍNDICE

Complejidad burocrática

- ERRORES PERSONAS

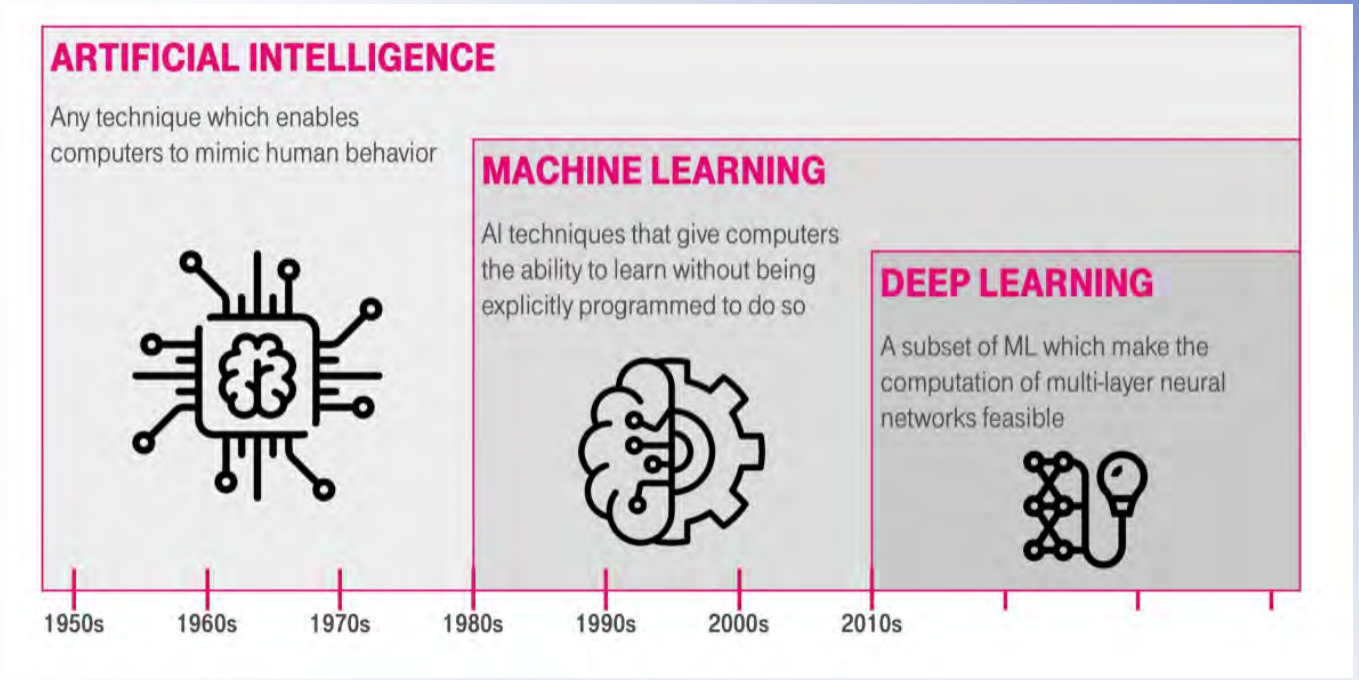
- BUROCRACIA DEFENSIVA: ERRORES SERVIDORES PÚBLICOS

UNIVERSITAT DE BARCELONA

AUTOMATIZACIÓN, SIN O CON IA...

- Datos masivos (Big data): ingentes cantidades de datos o big data, datos masivos caracterizados por su volumen, variedad y velocidad, las llamadas tres v.

- Algoritmo: secuencia de operaciones y reglas, como una ecuación matemática, diseñada por una persona o grupo de personas para resolver un problema



GENERATIVA (ej. Diputación de Girona en el ámbito de los Contratos públicos)

UNIVERSITAT DE BARCELONA

- Se otorgará el contrato a la empresa que presente una oferta que ayude a las personas con discapacidad del municipio

- **CLÁUSULA REGULADORA DEL CRITERIO SUJETO A JUICIO DE VALOR**
-

1. ÁMBITO FORMAL

Las empresas licitadoras deberán presentar un documento justificativo de su propuesta, el cual no podrá superar un máximo de 10 hojas DIN-A4, a una sola cara, con tipografía Arial 11 e interlineado 1,15. Este documento incluirá portada e índice, en su caso. Cualquier información que supere este límite o se incluya en anexos no será valorada por la Mesa de Contratación.

2. PUNTUACIÓN

La puntuación máxima asignada al criterio sujeto a juicio de valor será de 30 puntos. Si la propuesta presentada por la licitadora no alcanza una puntuación mínima de 15 puntos, la Mesa de Contratación excluirá automáticamente la oferta del procedimiento de licitación por no cumplir los requisitos mínimos establecidos.

3. ÁMBITO MATERIAL

El objetivo de la valoración es determinar el grado de incidencia de la oferta en la mejora de la inclusión social y laboral de las personas con discapacidad del municipio. A tal efecto, se establecen los siguientes subcriterios de puntuación:

a) Adecuación e impacto de las medidas propuestas (hasta 10 puntos)

- Se valora el alcance y la solidez de las medidas propuestas para favorecer la integración laboral y social de las personas con discapacidad en el municipio.
- Se puntuará positivamente la inclusión de programas de acompañamiento, formación u otras iniciativas de impacto demostrable.

b) Viabilidad y sostenibilidad de la propuesta (hasta 10 puntos)

- Se valora la coherencia y factibilidad de las acciones propuestas, incluyendo la disponibilidad de recursos materiales y humanos para su ejecución.
- Se puntuará favorablemente la continuidad de las medidas propuestas más allá de la ejecución inicial del contrato.

c) Innovación y valor añadido (hasta 10 puntos)

- Se valorarán las propuestas que introduzcan metodologías innovadoras o aporten un valor diferencial en la inclusión de personas con discapacidad.
- Se puntuará positivamente la colaboración con entidades sociales especializadas en el ámbito de la discapacidad.

Estos criterios serán evaluados por la Mesa de Contratación siguiendo un informe técnico motivado.

Artículo 146 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público

- De acuerdo con el artículo 146 de la LCSP, la valoración de los criterios dependientes de un juicio de valor se rea iz ı ı́ de manera previa a la apertura de las ofertas económicas, garantizando la transparencia y objetividad del procedimiento de contratación.

Diputació de Girona
Àrea d'Hisenda, Administració,
Promocio Econòmica i Cooperació Local
Compra Pública

GPTs personalitzats en Compra Pública

Advertència.- Els resultats generats pels models GPT personalitzats poden variar en funció de les dades proporcionades en relació als paràmetres configurats. Per aquest motiu, és imprescindible que el responsable del contracte revisi i validi el contingut abans d'utilitzar-lo com a document definitiu. Aquesta eina actua com una ajuda per agilitzar processos i oferir orientació als responsables dels contractes però no substitueix la responsabilitat del seu contingut.

1. DDG-IA és un assistent d'IA enfocat al recolzament dels tècnics de contractació alhora d'elaborar un Plec de clàusules administratives particulars (PCAP) d'obres

   https://chatgpt.com/g/g-66x4YdkxG-ddg-ia-dades-basiques-del-pcap-d-obres

2. DDG_IA és un assistent d'IA enfocat al recolzament del responsable del contracte en millorar el redactat del criteri de judici de valor a incloure al PCAP

   https://chatgpt.com/g/g-673f3686d7408191b6fd6bdaae17f513-ddg-ia-criteris-subjecte-a-judici-de-valor

UNIVERSITAT DE BARCELONA

1.

- “Cualquier tecnología suficientemente avanzada es indistinguible de la magia”, Arthur C. Clarke

- “Lejos de ser ciencia-ficción, la inteligencia artificial (IA) forma ya parte de nuestras vidas”, Comunicación 2018 UE

La inteligencia artificial en el sector público algunos ejemplos...

EL PAÍS

TECNOLOGÍA

S NOTICIAS

El Ayunta
'ANA', la
inteligen
municipa

Se trata de un 'chatbo
inteligencia artificial g
diversa tipología vincu

Noticias

ÚLTIMA HORA atresplayer

Elecciones País Vasco 2024 Actualidad Deportes Tiempo Multimedia Programas Series Newsletter

SUCESOS Al menos 14 heridos al caer un autobús en unas obras en Cornellà

Inteligencia Artificial /

El ChatGPT se cuela en los plenos de los ayuntamientos: un partido de Lalín (Pontevedra) lo usa para redactar una moción

El partido Compromiso por Lalín (CxL) ha decidido elaborar el texto de una moción a través del ChatGPT.

18 SEP 2023 | 13:0(

Bar
mo

4 de julio de 2024

• El nue
límites

Alexa, ¿quieres convertirte en mi asesora urbanística?'

El proyecto Cibeles, del Ayuntamiento y AWS, evoluciona los visores cartográficos. El altavoz ofrece los datos clave de cada parcela de la capital.

28 enero, 2021 - 02:36

GUARDAR

The Washington Post
Democracy Dies in Darkness

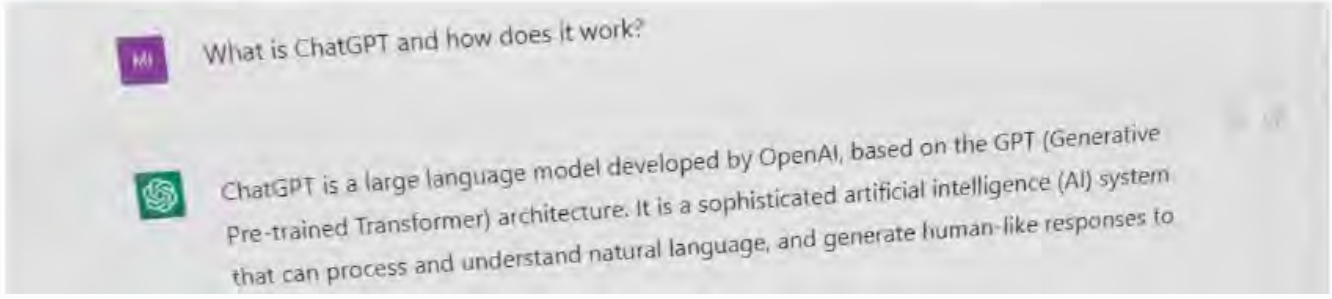
MORNING MIX

A Brazilian city passed a law about water meters. ChatGPT wrote it.

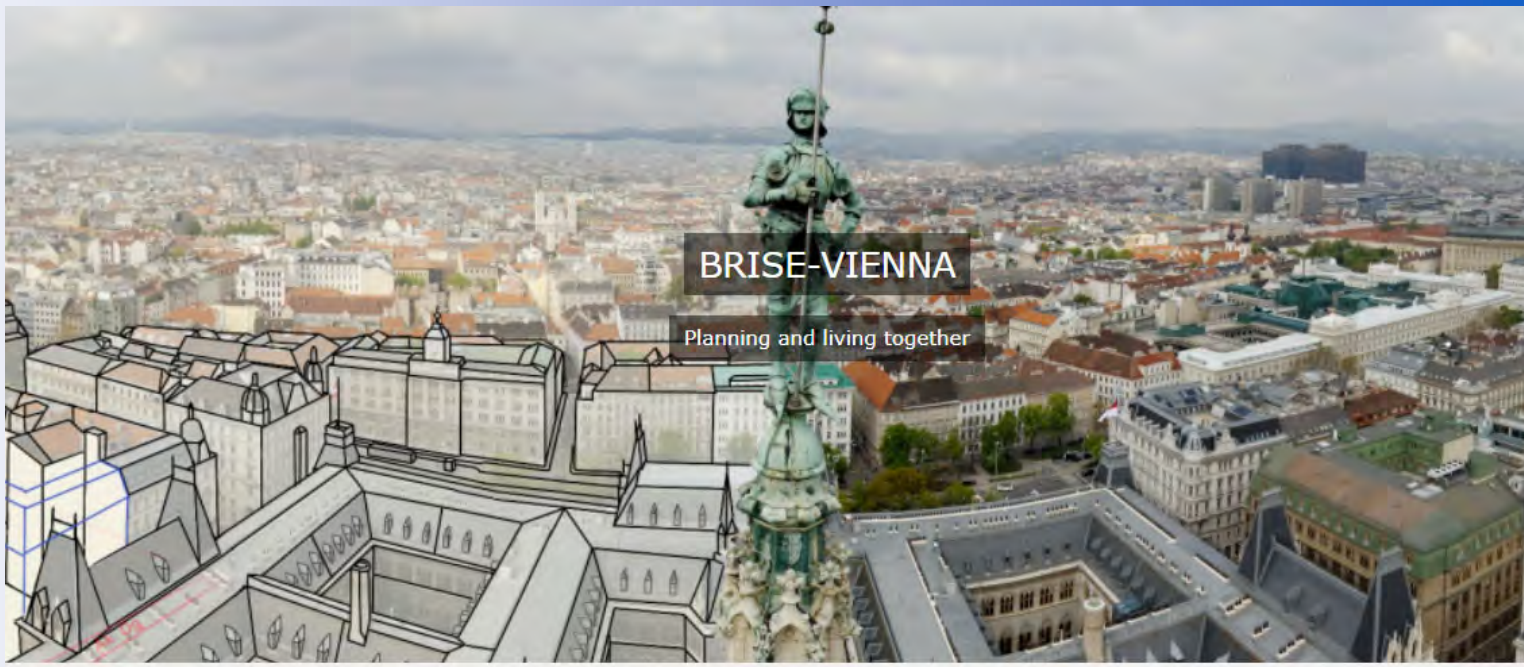
Councilman Ramiro Rosário, who sponsored the bill, revealed only after it had passed that it was written by AI

By María Luisa Paúl

December 4, 2023 at 5:57 a.m. EST



UNIVERSITAT DE BARCELONA



[BRISE-VIENNA - Planning and living together - Digitales Wien]

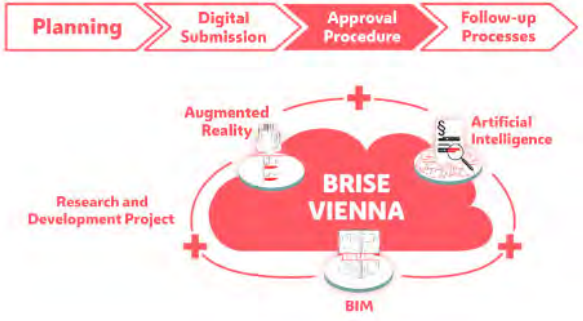
German Version

BRISE – THE FUTURE OF PUBLIC ADMINISTRATION

The BRISE digitisation project set out to improve public administration in the City of Vienna and thus the lives of the population. In a "city of short distances" like Vienna, it allows for faster and more efficient administrative processing. Digital and analogous participation processes guarantee democratic, service-oriented progress towards a modern, sustainable city administration.

BRISE – HIGH TECH SOLUTION

The BRISE project combines high-tech methods like Building Information Modelling (BIM), Artificial Intelligence (AI) and Augmented Reality (AR) to allow for a comprehensive, fully digital and automated building permit procedure. It uses digital 3D building models instead of 2D planning documents. As a result, BRISE provides an innovative basis for the entire building administration process – from planning and submission to building site inspections and, finally, handing over the finished structure.



https://www.youtube.com/watch?app=desktop&v=uU0tje2zDDg

UNIVERSITAT DE BARCELONA

MADRID

urbanismo, medio ambiente y movilidad | MADRID

ÍNDICE

Información de Firmantes del Documento
MADRID
JUAN CARLOS ALVAREZ RODRIGUEZ - DIRECTOR GENERAL
URL de Verificación: https://servint.madrid.es/VECSV_WBCONSULTAINTRA/VerificarCove.do
Fecha Firma: 07/05/2024 14:23:51
CSV : 1YMWL6E4NFN2D7AI

UNIVERSITAT DE BARCELONA

VITORIA GASTEIZ green capital

Notas de prensa

La inteligencia artificial llega a los semáforos de Vitoria-Gasteiz

Categorías: Notas de prensa — Etiquetas: inteligencia artificial, proyecto "Green light" — Komunikazio Zerbitzua / Servicio de Comunicación — 26 diciembre 2023 12:20

VITORIA GASTEIZ green capital

Notas de prensa

El Ayuntamiento recurrirá a la inteligencia artificial para agilizar la concesión de licencias

Categorías: Notas de prensa — Etiquetas: inteligencia artificial — Komunikazio Zerbitzua / Servicio de Comunicación — 4 julio 2024 11:47

- La IA se suma a la mejora de procedimientos con la que se ha reducido en 2 meses la tramitación de las licencias de actividad y en 1,2 la de obras

UNIVERSITAT DE BARCELONA

Algoritmos humanos contra algoritmos de máquinas…

Pros de los sistemas algorítmicos no humanos:

•1. **Capacidad de procesamiento** con Big Data y Algoritmos mucho mayor que los humanos

•2. Capacidad de realizar predicciones, mediante **correlaciones**

•3 **No sesgos cognitivos humanos** (ni **ruido**), pues no hay humano. Sunstein.

•4. Generan **nuevas ocupaciones laborales** relacionadas

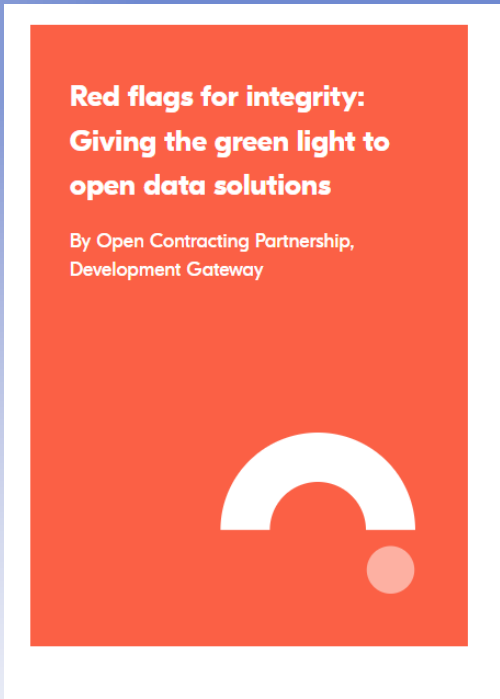
•5. Más **eficacia, eficiencia** en el sector privado; más **buena administración** en el sector público. Sentencias Consejo de Estado italiano.

•**Asociado al control de la mala administración por negligencia, del fraude y de la corrupción.**

RED FLAGS

UNIVERSITAT DE BARCELONA

- https://www.atlanticcouncil.org/wp-content/uploads/2019/06/FINALHackeandoCorrupcion.pdf
- https://www.open-contracting.org/es/2019/06/27/examinando-con-datos-las-banderas-rojas-de-compras-en-america-latina/



- Colombia, indicadores: modificaciones y cambios en los valores de los contratos
- Base de datos original en OCDS
- Representantes de la Contraloría General de la República y del capítulo local de Transparencia Internacional trabajaron con un periodista peruano del Ojo Público para explorar lo que sucede con los contratos después de que son firmados. El grupo se concentró en analizar la proporción de contratos con modificaciones y la diferencia entre el valor adjudicado y el valor final del contrato. Sus cálculos parecían indicar que casi la mitad de los procesos tenían enmiendas, una fracción más alta de la esperada, lo que los llevó a cuestionar si eso reflejaba la realidad. Identificaron un problema: al parecer, cualquier documento publicado después de la firma del contrato, como los informes de supervisión, podría estar contabilizándose como una adenda. Hemos informado a la agencia de contratación Colombia Compra Eficiente para verificar eso. Cuando el equipo intentó calcular el segundo indicador, las discrepancias entre la adjudicación y los montos finales del contrato, encontraron que todos los procesos en la muestra parecían tener exactamente el mismo valor cuando se adjudicaron y cuando finalizaron. Como esto rara vez sería el caso, revisaron procesos específicos y encontraron que podría haber un problema con la forma en que los compradores informan el valor final del contrato y lo capturan en las plataformas de adquisiciones.

UNIVERSITAT DE BARCELONA

https://www.antifrau.cat/ar/antifrau-presenta-guia-plans-mesures-antifrau-organitzacions-gestionar-

Oficina Antifrau de Catalunya

Sistemes automatitzats d'alerta en el marc dels Plans de mesures antifrau

Bruno González Valdelièvre

Cap de l'Equip d'Anàlisi de Dades
Head of Data Analysis Team

01 de desembre de 2021

Oficina Antifrau de Catalunya

Eina Arachne

- Eina tecnològica integrada de mineria i enriquiment de dades:
  - Desenvolupada per la Comissió Europea: 2009 → plenament operativa 2015
  - Oferta gratuïtament per la Comissió a les autoritats dels Estats membres amb responsabilitats de gestió i control de fons de la UE com a una eina especialment idònia de lluita antifrau

- Dades internes:
  - ✓ facilitades per les autoritats de gestió i control de fons de la UE
  - ✓ periodicitat mensual – trimestral

- Dades externes (proveïdors contractats per la Comissió Europea:
  - ✓ Orbis database
  - ✓ World Compliance

Arachne

- Mes de **100 indicadors** de risc
- 7 categories:
  - ✓ Licitació
  - ✓ gestió dels contractes
  - ✓ gestió dels fons
  - ✓ eficàcia i eficiència
  - ✓ Concentració
  - ✓ raonabilitat / altres
  - ✓ alertes reputacionals i de frau
- Dissenyats per facilitar la prevenció i detecció d'errors, conflictes d'interès o altres irregularitats i fraus en els projectes, beneficiaris, contractes i contractistes

A FAVOR	LIMITACIONES (¿problemas?)
-Principios constitucionales de buena administración: eficacia, eficiencia, economía, objetividad, racionalidad… …	Véase lo que se expone a continuación

UNIVERSITAT DE BARCELONA

Contras de los sistemas algorítmicos no humanos

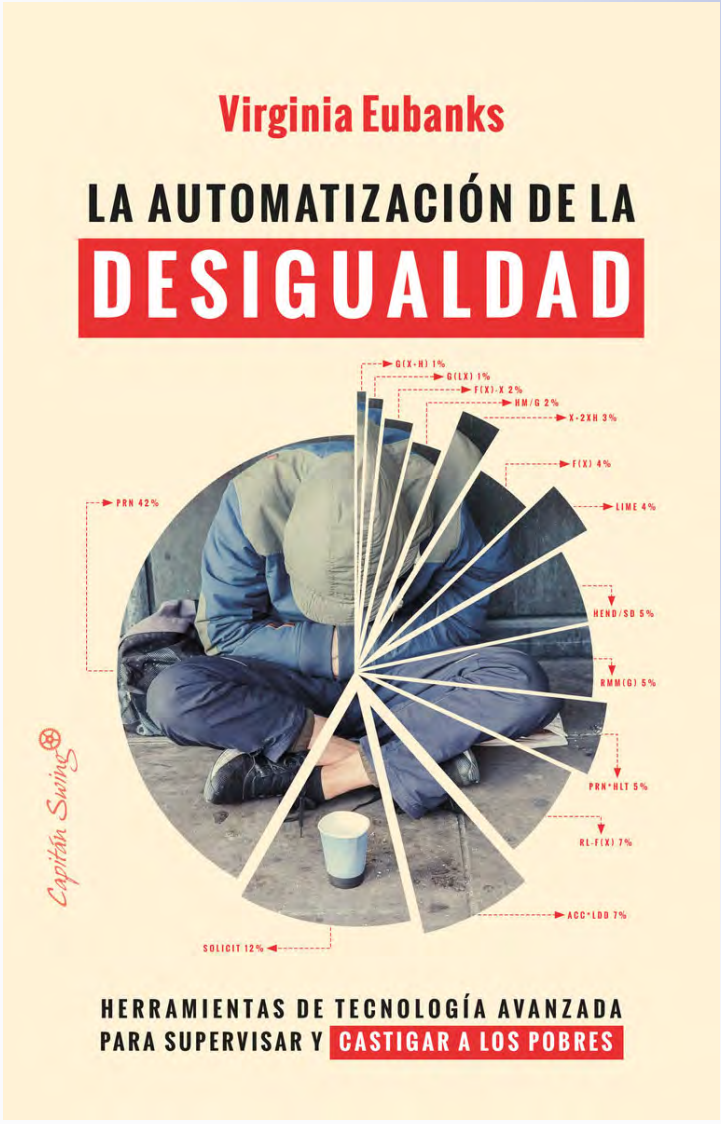
1. Conllevará una **substitución de humanos** en las tareas
2. **Impacto a gran escala,** a diferencia de problemas, errores y sesgos, humanos (libro automatización de la desigualdad).
3. **Correlaciones pueden dar lugar a errores,** no hablamos de causalidad. Ej. de errores: las personas que salen a correr contraen más cáncer. Correr causa cáncer: error, hay más variables, por ejemplo, correr en países con mucho sol implica que es el sol quien causa el cáncer. Son además incentivadoras **status quo**
4. Problema de los **errores de programación** (*bugs*)
5. Además, buena administración implica deber de diligencia debida o debido cuidado, **tomar en consideración elementos relevantes y descartar los irrelevantes**. Ejercer la discrecionalidad caso a caso teniendo en cuenta las circunstancias del caso concreto. Frente a ello, AI se basa en la ley de los grandes datos.
6. Sí **sesgos cognitivos de los programadores** (ej. confirmación, disponibilidad), de los datos (sesgo de género).
7. Algoritmos e IA pueden usar los sesgos cognitivos humanos para **manipularnos:** *dark patterns* (*Digital Services Act*), hiperacicates.
8. Riesgos de mala administración en el sector público:

    1. No hay **empatía/compasión/equidad**: algoritmos no experimentan sufrimiento: enfermedad, vejez, muerte, etc. Pueden imitar empatía, como psicópatas.
    2. No razonan con sentido común e hipótesis basadas en sentido común **(abductivamente**)como los humanos
    3. Pueden provocar insuficiente **participación y motivación** de las decisiones

UNIVERSITAT DE BARCELONA

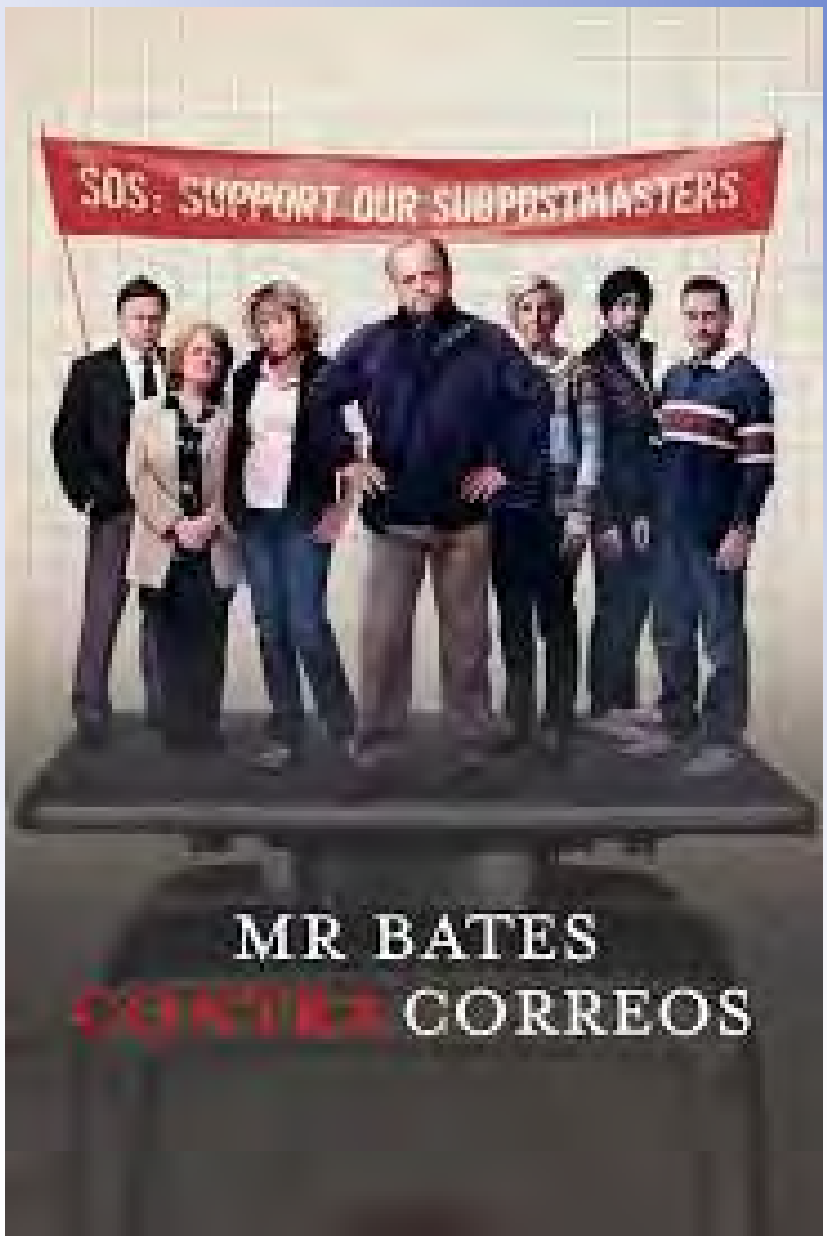
2.

- POSIBLES PROBLEMAS JURÍDICOS Y SOCIALES...


Virginia Eubanks
LA AUTOMATIZACIÓN DE LA
DESIGUALDAD
PRN 42%
LIME 4%
HEND/SD 5%
RMM(G) 5%
PRN*HLT 5%
RL-F(X) 7%
ACC*LDD 7%
SOLICIT 12%
HERRAMIENTAS DE TECNOLOGÍA AVANZADA
PARA SUPERVISAR Y CASTIGAR A LOS POBRES


CATHY O'NEIL
ARMAS DE DESTRUCCIÓN MATEMÁTICA
CÓMO EL BIG DATA AUMENTA LA DESIGUALDAD Y AMENAZA LA DEMOCRACIA

https://www.youtube.com/watch?v=VLmwdGrC-_c



UNIVERSITAT DE BARCELONA

2€/mes
Suscríbete ya

ABC Recreo

Última hora El aviso rojo por nuevas lluvias torrenciales obliga a suspender la limpieza en tres pedanías de Valencia • DIRECTO

→ ABC → El Recreo

'Hackers' piratean robots aspiradores para que insulten a sus propietarios y persigan mascotas

Este fallo informático afectó a un modelo concreto, cuya compañía ha tratado de calmar a sus clientes

• Últimas noticias

El Confidencial

Iniciar sesi

HA TENIDO OTRO PROBLEMA

No, este robot de Corea del Sur no se ha suicidado por culpa del estrés laboral

En redes sociales circula el bulo de que un robot administrativo decidió autodestruirse tirándose por las escaleras. Supuestamente, por la alta carga de trabajo a la que era sometido

El "cadáver" del robot administrativo que supuestamente se suicidó (Ayuntamiento de Gumi)

UNIVERSITAT DE BARCELONA

ERRORES...

ZBE: Barcelona multa incluso a un coche montado en una grúa (elespanol.com)

- DERECHO A LA INTIMIDAD Y (DES) PROTECCIÓN DE DATOS PERSONALES (ej. Para personalizar servicios, se elaboran perfiles ("un conjunto de datos que caracterizan una categoría de personas y que está destinada a ser aplicada a una persona").

- LIBERTAD DE PENSAMIENTO Y MANIPULACIÓN (*dark patterns*, hiperacicates) vs. libertad de pensamiento, libre desarrollo de la personalidad y principio de buena fe

- OPACIDAD (*cajas negras*) vs. Transparencia

- ARBITRARIEDAD/DISCRIMINACIÓN vs. Racionalidad y motivación (*explicabilidad*); **SESGOS**

- MALA ADMINISTRACIÓN vs. Incumplimiento buena administración y ausencia de ponderación individualizada de los factores relevantes y descarte de los irrelevantes (**ERRORES DE PROGRAMACIÓN, ERRORES EN CORRELACIÓN**)

UNIVERSITAT DE BARCELONA

3.

- Diferencia MORAL, ETICA, DERECHO

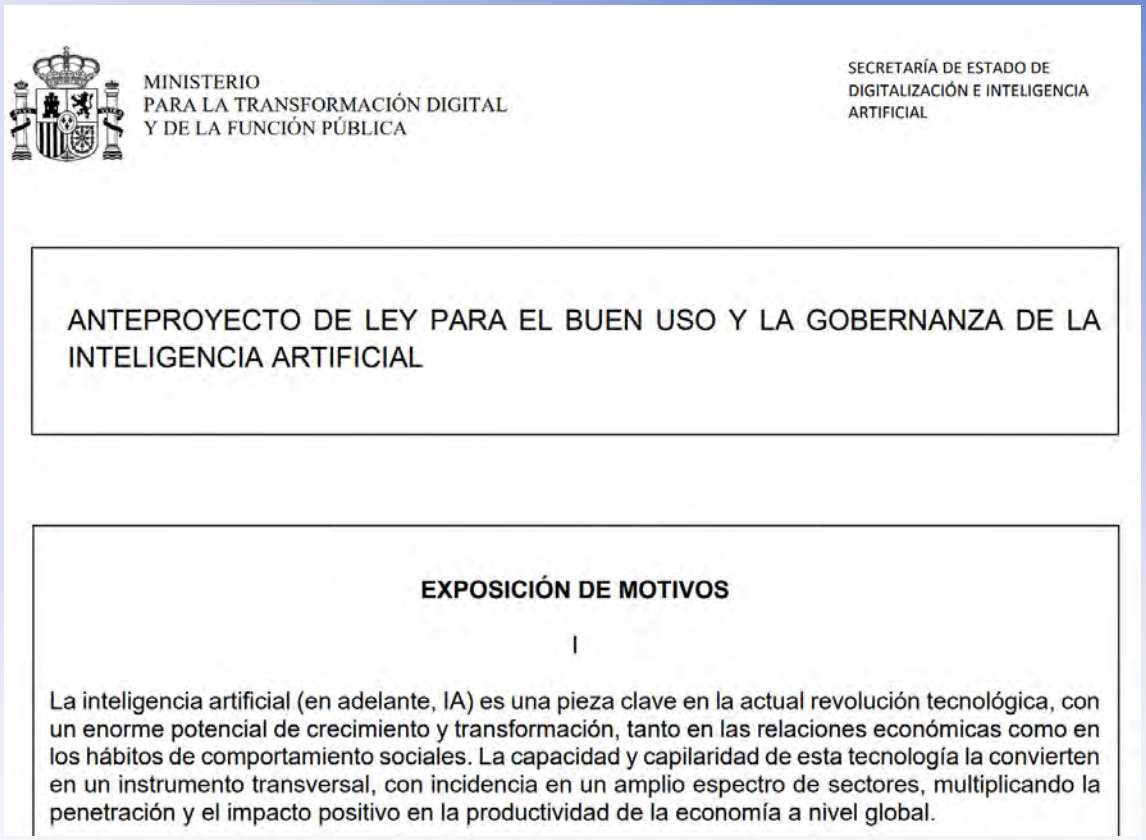
UNIVERSITAT DE BARCELONA

- 1. Regulación de la IA
  - Española: deficiente e insuficiente
  - UE: Reglamento 2024

UNIVERSITAT DE BARCELONA

ESPAÑA

- Regulación de nivel estatal:



MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE
DIGITALIZACIÓN E INTELIGENCIA
ARTIFICIAL

ANTEPROYECTO DE LEY PARA EL BUEN USO Y LA GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL

EXPOSICIÓN DE MOTIVOS

I

La inteligencia artificial (en adelante, IA) es una pieza clave en la actual revolución tecnológica, con un enorme potencial de crecimiento y transformación, tanto en las relaciones económicas como en los hábitos de comportamiento sociales. La capacidad y capilaridad de esta tecnología la convierten en un instrumento transversal, con incidencia en un amplio espectro de sectores, multiplicando la penetración y el impacto positivo en la productividad de la economía a nivel global.

- Regulación de nivel autonómico
- Regulación de nivel local

UNIVERSITAT DE BARCELONA

REGULACIÓN ESTATAL

- Art. 41 LRSP (y equivalentes en legislación tributaria o de SS).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- La ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación
- Carta de Derechos digitales de 2021
- Diversos Reales Decretos

UNIVERSITAT DE BARCELONA

Arts. 41 y 42 ley 40/2015, bases régimen jurídico de las AA.PP, 149.1.18 CE, DF 14ª.

Artículo 41. Actuación administrativa automatizada.

1. Se entiende por actuación administrativa automatizada, cualquier **acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo** y en la que **no haya intervenido de forma directa un empleado público.**

2. En caso de actuación administrativa automatizada **deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.**

Artículo 42. Sistemas de firma para la actuación administrativa automatizada.

En el ejercicio de la competencia en la actuación administrativa automatizada, **cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:** a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente

UNIVERSITAT DE BARCELONA

Ley 58/2003, de 17 de diciembre, General Tributaria (en adelante, LGT), que en su artículo 96 –bajo el título de "Utilización de tecnologías informáticas y telemáticas"– se refiere al empleo por parte de la Administración tributaria de las nuevas tecnologías en el desarrollo de su actividad:

- "Artículo 96. Utilización de tecnologías informáticas y telemáticas.
- 1. La Administración tributaria promoverá la utilización de las técnicas y medios electrónicos, informáticos y telemáticos necesarios para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que la Constitución y las leyes establezcan.
- 2. Cuando sea compatible con los medios técnicos de que disponga la Administración tributaria, los ciudadanos podrán relacionarse con ella para ejercer sus derechos y cumplir con sus obligaciones a través de técnicas y medios electrónicos, informáticos o telemáticos con las garantías y requisitos previstos en cada procedimiento.
- 3. Los procedimientos y actuaciones en los que se utilicen técnicas y medios electrónicos, informáticos y telemáticos *garantizarán la identificación de la Administración tributaria actuante y el ejercicio de su competencia. Además, cuando la Administración tributaria actúe de forma automatizada se garantizará la identificación de los órganos competentes para la programación y supervisión del sistema de información y de los órganos competentes para resolver los recursos que puedan interponerse.*
- 4. Los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por la Administración tributaria para el ejercicio de sus potestades *habrán de ser previamente aprobados por ésta en la forma que se determine reglamentariamente*.
- 5. Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por la Administración tributaria, o los que ésta emita como copias de originales almacenados por estos mismos medios, así como las imágenes electrónicas de los documentos originales o sus copias, tendrán la misma validez y eficacia que los documentos originales, siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por la normativa aplicable."

- Texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre:
- “Artículo 130. Tramitación electrónica de procedimientos en materia de Seguridad Social.
- De acuerdo con lo dispuesto en el artículo 41.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, podrán adoptarse y notificarse resoluciones de forma automatizada en los procedimientos de gestión tanto de la protección por desempleo previstos en el título III como de las restantes prestaciones del sistema de la Seguridad Social previstas en esta ley, excluidas las pensiones no contributivas, así como en los procedimientos de afiliación, cotización y recaudación.
- A tal fin, mediante resolución de la persona titular de la Dirección General del Instituto Nacional de la Seguridad Social, del Servicio Público de Empleo Estatal o de la Tesorería General de la Seguridad Social, o de la persona titular de la Dirección del Instituto Social de la Marina, según proceda, se establecerá previamente el procedimiento o procedimientos de que se trate y el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.”

https://www.boe.es/boe/dias/2024/06/07/pdfs/BOE-A-2024-11610.pdf

BOLETÍN OFICIAL DEL ESTADO
Núm. 138 Viernes 7 de junio de 2024 Sec. III. Pág. 66838

III. OTRAS DISPOSICIONES

MINISTERIO DE INCLUSIÓN, SEGURIDAD SOCIAL Y MIGRACIONES

11610 *Resolución de 29 de mayo de 2024, de la Tesorería General de la Seguridad Social, por la que se establece la tramitación automatizada de las resoluciones y otros actos administrativos relativos a la regularización anual de la cotización correspondiente a los trabajadores por cuenta propia o autónomos.*

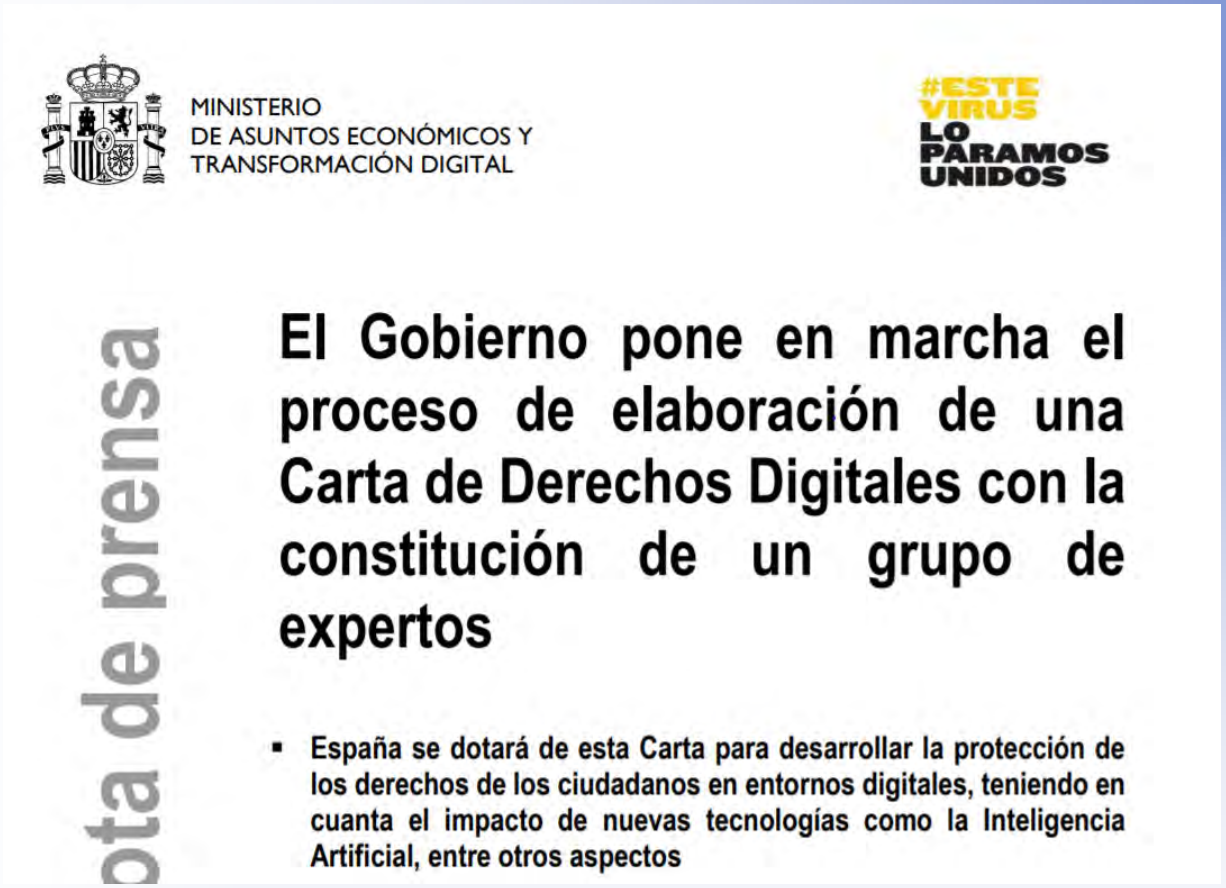
Conforme al artículo 41.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se entiende por actuación administrativa automatizada cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público. El apartado 2 del mismo artículo dispone que, en caso de actuación administrativa automatizada, deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente, así como indicarse el órgano que debe ser considerado responsable a efectos de impugnación

UNIVERSITAT DE BARCELONA

La ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación

- "Artículo 23. Inteligencia Artificial y mecanismos de toma de decisión automatizados.
- 1. En el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio.
- 2. Las administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos.
- 3. Las administraciones públicas y las empresas promoverán el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido.
- 4. Se promoverá un sello de calidad de los algoritmos."

SOFT LAW



MINISTERIO
DE ASUNTOS ECONÓMICOS Y
TRANSFORMACIÓN DIGITAL

#ESTE VIRUS LO PARAMOS UNIDOS

ota de prensa

El Gobierno pone en marcha el proceso de elaboración de una Carta de Derechos Digitales con la constitución de un grupo de expertos

- España se dotará de esta Carta para desarrollar la protección de los derechos de los ciudadanos en entornos digitales, teniendo en cuanta el impacto de nuevas tecnologías como la Inteligencia Artificial, entre otros aspectos

APORTACIÓN DE LA *RED DAIA* A LA CONSULTA PÚBLICA IMPULSADA POR LA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL PARA LA ELABORACIÓN DE UNA CARTA DE DERECHOS DIGITALES*

Contenido:

https://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1201173

UNIVERSITAT DE BARCELONA

https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

UNIVERSITAT DE BARCELONA

- XVIII
- Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas

- 6. Se promoverán los derechos de la ciudadanía en relación con la inteligencia artificial reconocidos en esta Carta en el marco de la actuación administrativa reconociéndose en todo caso los derechos a: a) **Que las decisiones y actividades en el entorno digital respeten los principios de buen gobierno y el derecho a una buena Administración digital**, así como los principios éticos que guían el diseño y los usos de la inteligencia artificial. b) **La transparencia** sobre el uso de instrumentos de inteligencia artificial y sobre su funcionamiento y alcance en cada procedimiento concreto y, en particular, acerca de los datos utilizados, su margen de error, su ámbito de aplicación y su carácter decisorio o no decisorio. La ley podrá regular las condiciones de transparencia y el acceso al código fuente, especialmente con objeto de verificar que no produce resultados discriminatorios. c) **Obtener una motivación comprensible en lenguaje natural de las decisiones que se adopten en el entorno digital, con justificación de las normas jurídicas relevantes, tecnología empleada, así como de los criterios de aplicación de las mismas al caso. El interesado tendrá derecho a que se motive o se explique la decisión administrativa cuando esta se separe del criterio propuesto por un sistema automatizado o inteligente**. d) Que la adopción de decisiones discrecionales **quede reservada a personas, salvo que normativamente se prevea la adopción de decisiones automatizadas con garantías adecuadas.** 7. Será necesaria **una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas.**

UNIVERSITAT DE BARCELONA

Reglamentos

- Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial.

- Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial (de la que existía previa previsión legal).

Principios extraidos de la regulación

- -**Principio de seguridad jurídica,** previniendo y rectificando los errores que puedan afectar al sistema.
- -**Principio de transparencia**, teniendo en cuenta la ley 19/2023 y equivalentes autonómicos, que como regla general, con excepciones que hay que justificar y aplicar proporcionadamente, prevén el derecho de acceso de los ciudadanos a la información del sistema, que es información pública. Además, como consecuencia de la publicidad activa prevista en el ordenamiento, habrá que difundir la descripción de su funcionamiento, los mecanismos de rendición de cuentas y transparencia y los datos utilizados en su configuración y aprendizaje (arte. 11.1 Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de Actuación y Funcionamiento del Sector Público por Medios Electrónicos RAFME). Esto se podrá hacer mediante el portal de transparencia y/o configurando un registro específico, como ya han hecho varias ciudades europeas y está desarrollando el Ayuntamiento de Barcelona y la Generalitat de Cataluña, que ha aprobado por su parte el acuerdo de gobierno 45/2024, de 27 de febrero, por el cual se crea la Comisión de Inteligencia Artificial y se establecen medidas en materia de inteligencia artificial, en el cual se prevé la creación del Registro de sistemas de inteligencia artificial.
- -**Principio de igualdad y no discriminación**, previniendo los sesgos del sistema, que pueden encontrarse por transmisión de los cognitivos de los programadores o en los datos utilizados.
- -**Principio de protección de datos personales**, de acuerdo con el art. 5 del RGPD.
- -**Principio de neutralidad tecnológica**, evitando la dependencia tecnológica de la Administración de las empresas que la provean con la tecnología y que permita desarrollar e implementar los adelantos tecnológicos en un ámbito de libre mercado (arte. 2 a RAFME).
- -**Principio de personalización y proactividad**, aludido por ejemplo en el Decreto catalán 76/2020, de 4 de agosto, de Administración digital, art. 4.c, cuando se refiere a los principios de la “proactividad y personalización en la prestación de servicios públicos digitales con el objetivo de situar la experiencia de las personas en el centro del diseño de servicios”.

REGULACIÓN AUTONÓMICA

- LEY 2/2025, de 2 de abril, para el desarrollo e impulso de la inteligencia artificial en Galicia, publicada en el Diario Oficial gallego el 4/4/2025
  - https://www.xunta.gal/dog/Publicados/2025/20250404/AnuncioC3B0-030425-0001_es.html

- Decreto-Ley extremeño 2/2023, de 8 de marzo de medidas urgentes de impulso a la Inteligencia Artificial (IA)

- Ley Transparencia y Buen Gobierno de Valencia 1/2022, publicidad activa

UNIVERSITAT DE BARCELONA

Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Comunitat Valenciana: SE DEBE PUBLICAR

- “l) La relación de sistemas algorítmicos o de inteligencia artificial que tengan impacto en los procedimientos administrativos o la prestación de los servicios públicos con la descripción de manera comprensible de su diseño y funcionamiento, el nivel de riesgo que implican y el punto de contacto al que poder dirigirse en cada caso, de acuerdo con los principios de transparencia y explicabilidad”

UNIVERSITAT DE BARCELONA

- **Nueva generación de leyes sobre simplificación**: Ley valenciana 6/2024, de 5 de diciembre, de Simplificación Administrativa, anteproyecto ley de Castilla-La Mancha..

- Nivel reglamentario: Cataluña...Decreto vasco 21/2012, de 21 de febrero, de Administración electrónica

BAIC BASQUE ARTIFICIAL INTELLIGENCE CENTER

UNIVERSITAT DE BARCELONA

ANTEPROYECTO DE LEY DE AGILIZACION ADMINISTRATIVA AL SERVICIO DEL CIUDADANO Y DE ATRACCIÓN DE INVERSIONES EMPRESARIALES

EM

- “La transformación digital implica la adopción de tecnologías y procesos que permiten organizar el funcionamiento de la administración abordando aspectos clave como automatización de procesos y tareas, servicios en línea, interoperabilidad de sistemas y seguridad y protección de datos. Y, principalmente, con la gestión de los datos disponibles de la digitalización, la incorporación de soluciones de inteligencia artificial, en sus diversas modalidades, que faciliten una gestión y respuesta más rápida, objetiva y eficiente a las demandas y necesidades de la ciudadanía”

UNIVERSITAT DE BARCELONA

Artículo 7. Datos e inteligencia artificial en las decisiones públicas.

1. Con carácter general, de conformidad con la estrategia global de cambio que diseñe el Gobierno de Aragón, se implementarán soluciones de inteligencia artificial, con respeto a las exigencias contempladas en el Reglamento 2024/1689, del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial de 13 de marzo de 2024, aplicadas a todas las tramitaciones y procesos que puedan proporcionar una respuesta más ágil, eficiente y transparente, sin poner en riesgo derechos fundamentales ni derechos digitales reconocidos.

2. Toda solución de inteligencia artificial deberá garantizar su enfoque centrado en la persona y su inalienable dignidad, **evitando causarle daños y persiguiendo el bien común**

7. Los interesados podrán **solicitar la supervisión e intervención humana**, así como impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial.

Artículo 42. Registro de sistemas de inteligencia artificial del Sector Público Autonómico de Aragón.

1. Se crea el Registro de sistemas de inteligencia artificial del Sector Público Autonómico de Aragón como un registro público adscrito al departamento competente en materia de administración electrónica.

UNIVERSITAT DE BARCELONA

REGULACIÓN LOCAL

B) Disposiciones y Actos

Coordinación General de la Alcaldía

102 *Resolución de 13 de enero de 2022 del Director General de la Oficina Digital por la que se aprueba la actuación administrativa automatizada de expedición de certificaciones del Padrón municipal.*

La actuación administrativa automatizada está regulada en la Ley 40/2015, del 1 de octubre, de Régimen Jurídico del Sector Público y en el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

En el ámbito municipal la actuación automatizada está regulada por la Ordenanza de Atención a la Ciudadanía y Administración Electrónica del Ayuntamiento de Madrid, de 26 de febrero de 2019 (en adelante, OACyAE), y los acuerdos de la Junta de Gobierno de la Ciudad, de 18 de noviembre de 2021, por los que se aprueban las directrices sobre actuación administrativa automatizada y la Política de Identificación y Firma Electrónicas del Ayuntamiento de Madrid.

La actuación administrativa automatizada de expedición de certificaciones del Padrón municipal se aprobó por Acuerdo de la Junta de Gobierno de la Ciudad de Madrid de 13 de febrero de 2020. Su implantación en febrero de 2020 ha permitido reducir los tiempos de respuesta a las solicitudes presentadas por los ciudadanos, así como mitigar las cargas de trabajo administrativas para su elaboración, y facilitar una respuesta inmediata, cuando los ciudadanos la solicitan a través de la sede electrónica, disponible las 24 horas al día y los 7 días de la semana.

GASETA MUNICIPAL

Ajuntament de Barcelona

23 de desembre del 2022

CSV: be51-d649-8347-151e

Altres anuncis – Normativa

PROTOCOL de Definició de metodologies de treball i protocols per a la implementació de sistemes algorítmics de 15 de desembre de Comissió de Govern.

ÍNDEX

UNIVERSITAT DE BARCELONA

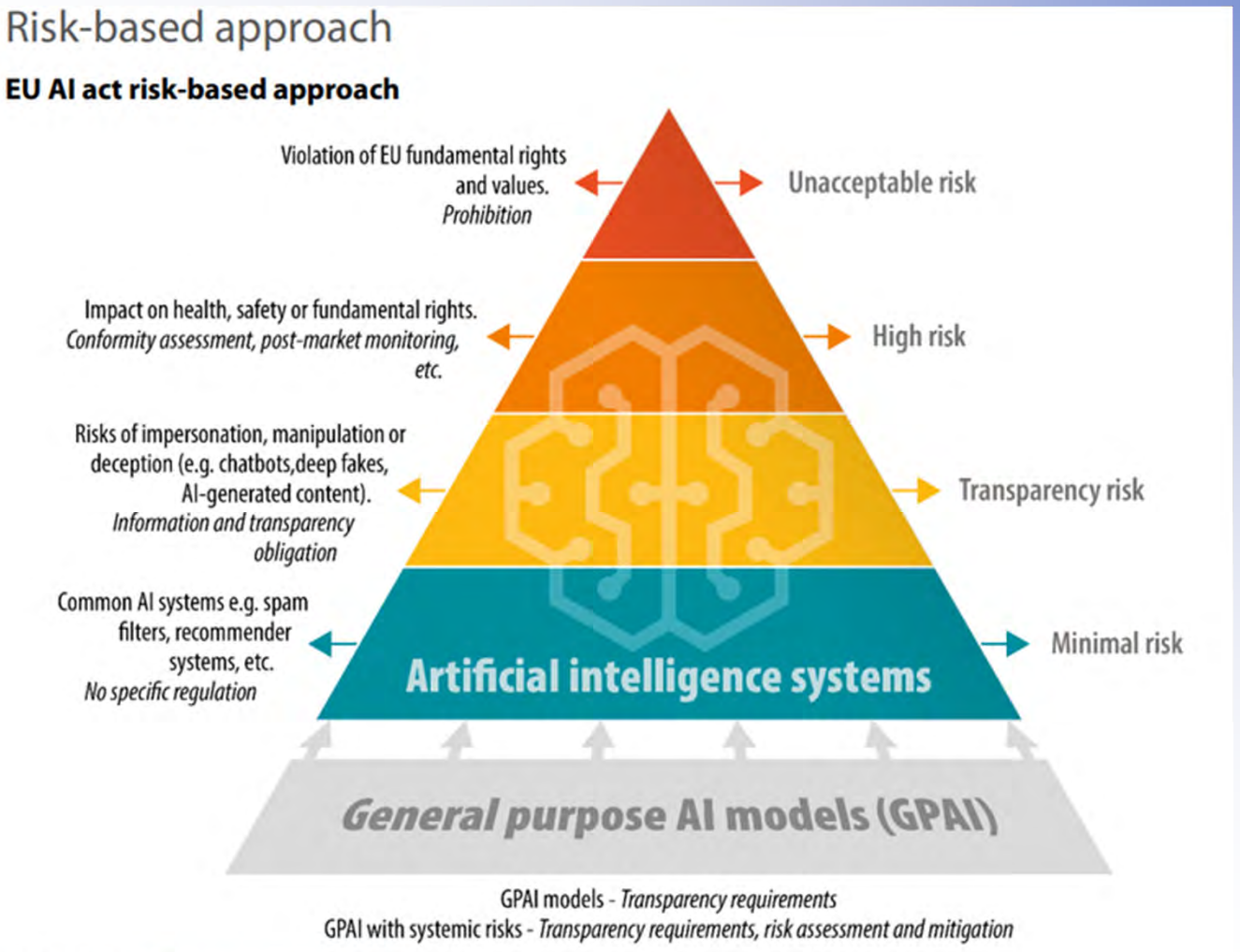
UNIÓN EUROPEA, Smusha, 2020

Concretisation of rights through legislation

Human agency and oversight	GDPR
Technical Robustness and safety	Machinery directive and sectoral safety regulation
Privacy and data governance	GDPR
Transparency	Consumer protection law & GDPR
Diversity, non-discrimination and fairness	Non-discrimination directives
Societal & environmental well-being	Environmental Regulation
Accountability	GDPR, product liability directive, procedural law

UNIVERSITAT DE BARCELONA

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (Texto pertinente a efectos del EEE) https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=OJ:L_202401689



The AI Act Explorer | Ley de Inteligencia Artificial de la UE (artificialintelligenceact.eu)

- ¿Efecto Bruselas?

UNIVERSITAT DE BARCELONA

- **Norma extensa**: 113 artículos, 13 anexos, 180 considerandos. Flexible, aplicacion progresiva entre 2025 y 2027.

- Objetivo **mejorar el funcionamiento del mercado interior** en relación con estas tecnologies y proteger derechos fundamentales.

- Definición **requisitos que tienen que cumplir los sistemas de IA para poder ser puestos al mercado o en servicio** y ser utilizados **en la Unión Europea**.

- **Marco jurídico uniforme a nivel europeo** (normas armonizadas) para evitar las divergencias que puedan obstaculizar la libre circulación, fragmentar el mercado o generar inseguridad jurídica (114 TFUE). ¿Papel para regulación estatal?

- **No regula específicamente el uso de la IA a las administraciones públicas** pero se refiere y prevé obligaciones específicas cuando utilizan sistemas de IA de alto riesgo

¿QUE ES LA INTELIGENCIA ARTIFICIAL?

UNIVERSITAT DE BARCELONA

Reglamento de la UE sobre IA:

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (Texto pertinente a efectos del EEE)

Artículo 3

Definiciones

A los efectos del presente Reglamento, se entenderá por:

1)«sistema de IA»: un sistema basado en una **máquina** que está diseñado para funcionar con distintos niveles de **autonomía** y que puede mostrar **capacidad de adaptación tras el despliegue,** y que, para objetivos explícitos o implícitos, infiere de la **información de entrada** que recibe la manera de **generar resultados** de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales;

UNIVERSITAT DE BARCELONA

Fuente: Xataca, en Del riesgo mínimo al riesgo inaceptable: así define la UE los cuatro niveles de los sistemas de IA en su nueva Ley (xataka.com)

UNIVERSITAT DE BARCELONA

RUEIA

Por eso fija:

1. **Prohibiciones** de determinadas prácticas de IA

2. **Requisitos específicos y obligaciones** para los operadores de los sistemas de IA de alto riesgo;

3. **Normas de transparencia** aplicables a determinados sistemas de IA

4. **Normas armonizadas** para la introducción al mercado de modelos de IA de uso general

5. **Normas sobre** el **seguimiento** del mercado, la **vigilancia** del mercado, la **gobernanza** y la garantía del **cumplimiento**

6. **Medidas en apoyo de** la innovación

Los sistemas de inteligencia artificial en el RÍA

Tipología de sistemas

1. Prácticas prohibidas

2. Sistemas de IA de alto riesgo

3. Sistemas de IA de riesgos específicos

4. Otros sistemas de IA

Los sistemas de inteligencia artificial en el RÍA

Sistemas de IA de alto riesgo

máquinas, juguetes, ascensores, equipos radioeléctricos, equipos de presión, equipos de embarcaciones de recreo, productos sanitarios, automoción y aviación

Doble criterio:

1. Sistemas que cumplen dos condiciones:
   - son componentes de seguridad de productos de acuerdo con los actos legislativos de armonización de la Unión identificados al anexo Y o el mismo sistema de IA es un producto y
   - el producto del cual sea componente de seguridad el sistema de IA o el mismo sistema de IA como producto se tiene que someter a una evaluación de la conformidad con un organismo de evaluación de la conformidad de terceros para su introducción al mercado o puesta en servicio de acuerdo con los actos legislativos de armonización de la Unión identificados al anexo I.

2. Sistemas incluidos en alguno de los ocho ámbitos y se encuentra dentro de las diferentes prácticas identificadas al anexo III

Los sistemas de inteligencia artificial al RÍA

Sistemas de IA de alto riesgo

1. **biometría** (identificación biométrica remota, categorización biométrica y reconocimiento de emociones);
2. **gestión y funcionamiento de infraestructuras críticas** (tráfico, agua, gas o electricidad);
3. **educación y formación profesional** (gestión del acceso o la admisión a la educación; la evaluación de los resultados de aprendizaje; o seguimiento y detección de comportamientos prohibidos por estudiantes en pruebas);
4. **ocupación**, gestión de trabajadores y acceso al autoempleo (contratación o selección de personas);
5. **acceso de las personas a servicios esenciales públicos y privados** (servicios esenciales de asistencia sanitaria, evaluación y clasificación de las llamadas de emergencia, triaje de pacientes en servicios de asistencia sanitaria urgente);
6. **garantía del cumplimiento del derecho** (evaluación del riesgo que una persona sea víctima de delitos; polígrafs);
7. **migración, asilo y control fronterizo** (como polígrafs, valoración de solicitudes de asilo, visado o permiso de residencia);
8. **administración de justicia y procesos democráticos** (ayuda la autoridad judicial en la investigación e interpretación de los hechos o la ley; resolución alternativa de litigios; sistemas utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de las personas) .

Los sistemas de inteligencia artificial al RÍA

Sistemas de IA de alto riesgo

- Excepciones

  - Sistema de IA que no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales.
  - Sistema de IA que no influya sustancialmente en el resultado de la toma de decisiones (tarea de procedimiento limitada, mejorar el resultado de una actividad humana, detectar patrones de toma de decisiones o desviaciones

→ el proveedor tendrá que documentar su evaluación antes de introducir el sistema de IA en el mercado o ponerlo al Servicio

- Adaptación: Capacitado Comisión (evaluación anual)

  - modificar o suprimir las condiciones
  - añadir o modificar

Los sistemas de inteligencia artificial al RÍA

Sistemas de IA de alto riesgo

Requisitos y obligaciones de proveedores y responsables de despliegue

1. Sistema de gestión de riesgos
   Proceso iterativo continuo durante todo el ciclo de vida. Determinación y análisis de los riesgos conocidos y previsibles que pueda plantear el sistema de IA de alto riesgo cuando se utilice de acuerdo con la finalidad prevista o cuando se dé un uso indebido razonablemente previsible. Medidas adecuadas para su gestión

2. Gobernanza y calidad de los datos
   Criterios de calidad en los conjuntos de datos de entrenamiento, validación y prueba y adoptar las medidas necesarias para que sean pertinentes y representativos, estén completos, no tengan errores y no contengan sesgos
   Adoptar prácticas adecuadas de gestión y gobernanza

3. Documentación técnica
   Demuestre el cumplimiento de los requisitos de manera clara y completa para que las autoridades competentes y los organismos notificados puedan evaluar la conformidad

Los sistemas de inteligencia artificial al RÍA

Sistemas de IA de alto riesgo

Requisitos

4. Registro automático de acontecimientos (archivo de registro).
   Registro automático de acontecimientos a lo largo del ciclo de vida del sistema para garantizar la trazabilidad de su funcionamiento y vigilancia postcomercialización

5. Transparencia
   Nivel de transparencia suficiente para interpretar y utilizar correctamente los resultados de salida
   Manual de usuario con información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible

6. Fiabilidad
   Nivel adecuado de precisión, solidez y ciberseguridad que tienen que mantener durante el ciclo de vida

7. Supervisión humana
   Vigilancia efectiva por personas para prevenir o reducir al mínimo los riesgos

UNIVERSITAT DE BARCELONA

Prácticas prohibides, art. 5 RUEIA

Generan riesgos inasumibles

- invadir de manera especialmente grave derechos y libertades de las personas
- afectar su vida privada
- provocar la sensación de estar bajo una vigilancia constante
- disuadir el ejercicio de los derechos, como por ejemplo la libertad de reunión
- generar resultados erróneos, sesgados, discriminatorios o excluyentes de determinadas personas o colectivos

1. Sistemas de IA que utilicen técnicas subliminales, manipuladoras o engañosas
2. Sistemas de IA que exploten las vulnerabilidades de personas o colectivos por su edad, discapacidad, situación social o económica
3. Sistemas de IA de puntuación ciudadana que evalúen o clasifiquen personas o colectivos en función de su comportamiento social o de sus características personales
4. Sistemas de IA de elaboración de perfiles o de evaluación para evaluar o predecir el riesgo de cometer un delito
5. Sistemas de IA que creen o amplíen bases de datos de reconocimiento facial
6. Sistemas de IA para inferir las emociones de una persona física a puestos de trabajo y centros educativos
7. Sistemas de categorización biométrica para deducir o inferir datos sensibles (raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida u orientación sexual de las personas)
8. Sistemas de identificación biométrica remota en tiempo real en espacios de acceso público para garantizar el cumplimiento del derecho

UNIVERSITAT DE BARCELONA

- OTRAS PROHIBICIONES: IA PARA ADOPTAR DECISIONES JUDICIALES TOTALMENTE AUTOMATIZADAS, ANEXO III.

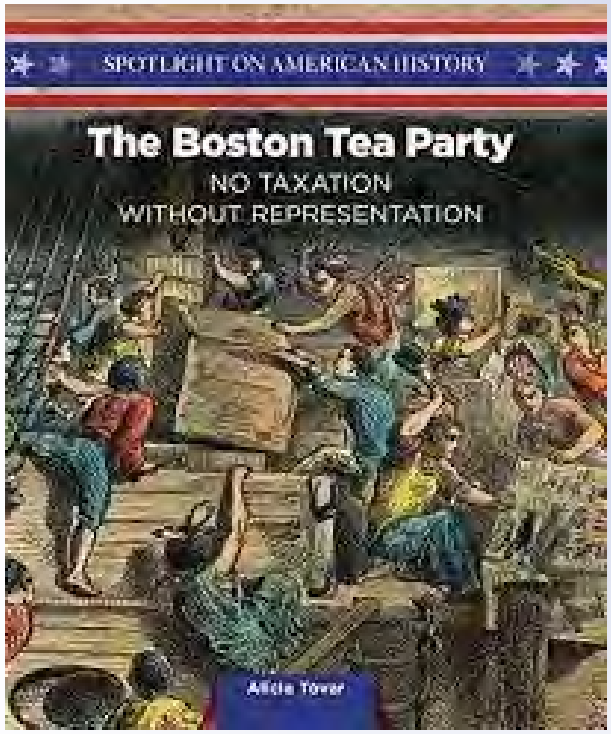
- ¿PARA ADOPTAR DECISIONES ADMINISTRATIVAS? ⟶

ESTADO SOCIAL Y DEMOCRÁTICO DE DERECHO E IA

- ESTADO DE DERECHO:
  - PRINCIPIO DE LEGALIDAD **(norma previa y reserva de ley)**
  - TUTELA DE DERECHOS (INCLUYENDO EL DERECHO A UNA BUENA ADMINISTRACIÓN)
  - RESPONSABILIDAD PATRIMONIAL

UNIVERSITAT DE BARCELONA

¿Cuándo automatitzar con IA, y con qué alcance, y cuándo no?



NO TAXATION WITHOUT REPRESENTATION…

NO AUTOMATION WITHOUT REPRESENTATION

- Regulación general, debe venir encuadrada previamente por norma con rango de ley, dados los derechos afectados (art. 18 CE)

- **Artículo 18. 4 CE "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"**

UNIVERSITAT DE BARCELONA

- LÍMITES JURÍDICOS DE LA IA BASADOS EN EL PRINCIPIO Y DERECHO A UNA BUENA ADMINISTRACIÓN RESPECTO A AUTOMATIZACIÓN TOTAL

- EL PRINCIPIO Y DERECHO A UNA BUENA ADMINISTRACIÓN: EXIGENCIAS JURÍDICAS

UNIVERSITAT DE BARCELONA

STS 4/11/2021

"Como se desprende de lo dicho por el Tribunal Supremo **el principio de buena administración tiene una base constitucional y legal indiscutible.**

Podemos distinguir dos manifestaciones del mismo,

por un lado constituye **un deber y exigencia a la propia Administración** que debe guiar su actuación bajo los parámetros referidos, entre los que se encuentra la diligencia y la actividad temporánea;

por otro, **un derecho del administrado**, que como tal puede hacerse valer ante la Administración en defensa de sus intereses y que respecto de la falta de diligencia o inactividad administrativa se refleja no ya sólo en la interdicción de la inactividad que se deriva de la legislación nacional, arts. 9 y 103 de la CE y 3 de la Ley 39/2015, -aunque expresamente no se mencione este principio de buena administración-, sino de forma expresa y categórica en el art. 41 de la CEDH…

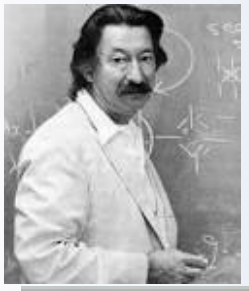
Existe, pues, con base en la normativa antes citada**, un deber administrativo a la diligencia debida, y un correlativo derecho de los ciudadanos a la proscripción de la inactividad administrativa. Es consustancial al principio de buena administración la diligencia en el actuar de la Administración y el desarrollo y resolución en tiempo razonable y proporcionado**. Cuando existe una inactividad administrativa objetiva, injustificada y desproporcionada, se está conculcando el derecho del ciudadano a la buena administración; derecho real y efectivo que debe ser garantizado y que, en su caso, debe ampararse por los Tribunales de Justicia cuando controla la referida inactivad administrativa"

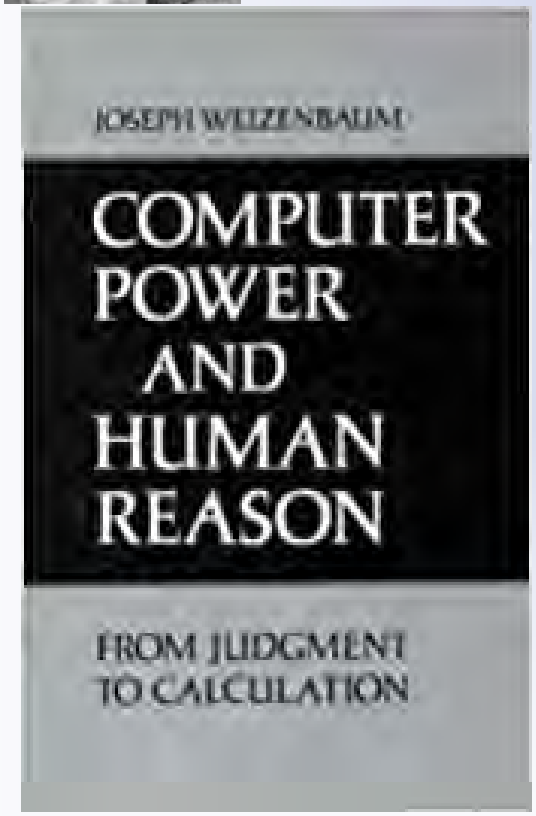
UNIVERSITAT DE BARCELONA

AI, NO INFERENCIAS ABDUCTIVAS

(12) Inducción, deducción y abducción - Lógica didáctica y sencilla ☑ - YouTube

AI, NO EMPATÍA





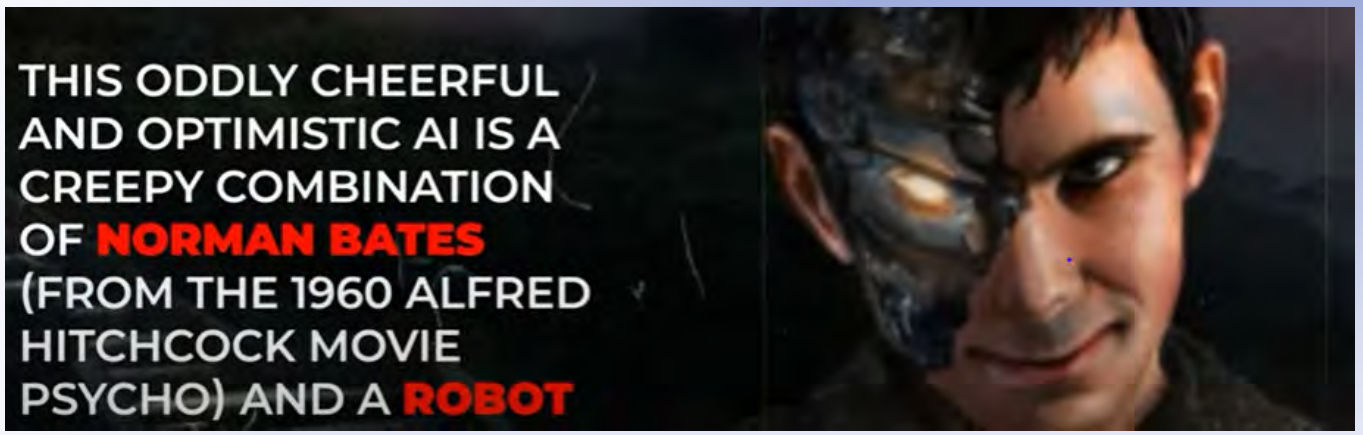
En 1976, Weizenbaum (científico del MIT) hizo un llamamiento al consenso social para que las máquinas no sustituyeran a los humanos en trabajos que se benefician de la sabiduría y la empatía, un estado que un ordenador sería incapaz de tener (pero podría imitar emociones como los psicópatas). Basándose en el trabajo de otros contemporáneos que analizaban casos concretos en los que la inteligencia artificial sería inadecuada, Weizenbaum nombró:

-representantes de atención al cliente,
-terapeutas,
-cuidadores de ancianos,
-soldados,
-jueces, -y
agentes de policía

como funciones que sólo deben desempeñar los seres humanos.

UNIVERSITAT DE BARCELONA

NO EMPATÍA=PSICOPATÍA




1
No es infalible
X realiza las preguntas
X
Aprobada si X no detectaba quién le respondía
2
No tiene la capacidad de medir el comportamiento superinteligente de las máquinas
3
Solo mide la capacidad de imitar el comportamiento humano:
Desventajas del empleo del test de Turing
Test de Turing
economipedia
Alan Turing

https://youtu.be/Xd3nJcChGGc

"Test de Voight-Kampff"

Novela *¿Sueñan los androides con ovejas eléctricas?* de Philip K. Dick, así como en su adaptación cinematográfica Blade Runner.

UNIVERSITAT DE BARCELONA

AI, PROCEDIMIENTO ADMINISTRATIVO DEBIDO Y MOTIVACIÓN

- AUDIENCIA E INFORMACIÓN PÚBLICA

- MOTIVACIÓN (Y EXPLICABILIDAD, ART. 86 RUEIA) Y CAJA NEGRA

UNIVERSITAT DE BARCELONA

AUTOMATIZACIÓN CON IA

- POTESTADES DISCRECIONALES:

SEMIAUTOMATIZACIÓN, IA COMO APOYO O ASISTENTE (CUIDADO CON SESGO DE AUTOMATIZACIÓN)

- POTESTADES REGLADAS:

ADEMÁS, AUTOMATIZACIÓN TOTAL.

UNIVERSITAT DE BARCELONA

RESERVA DE HUMANIDAD: prevista en normativa española y europea. Ej:

Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña.

- **Artículo 44. Actuación administrativa automatizada.**
- 1. Las administraciones públicas catalanas pueden realizar actuaciones automatizadas para constatar la concurrencia de los requisitos que establece el ordenamiento jurídico, declarar las consecuencias previstas, adoptar las resoluciones y comunicar o certificar los datos, actos, resoluciones o acuerdos que consten en sus sistemas de información, mediante la utilización del sistema de firma electrónica que determinen.
- **2. Sólo son susceptibles de actuación administrativa automatizada los actos que puedan adoptarse con una programación basada en criterios y parámetros objetivos**.
- 3. La actuación administrativa automatizada no afecta a la titularidad de la competencia de los órganos administrativos ni a las competencias atribuidas para la resolución de los recursos administrativos.

UNIVERSITAT DE BARCELONA

Artículo 12. Reserva de humanidad y de revisión humana

1. La Administración general de la Comunidad Autónoma de Galicia y su sector público podrán emplear sistemas de inteligencia artificial tanto en su actividad material o técnica como en la adopción de actos administrativos formalizados, tanto de trámite como resolutorios, de acuerdo con lo señalado en este artículo y de conformidad con lo establecido en la normativa europea y estatal de aplicación.
2. En caso de uso de sistemas de inteligencia artificial que sirvan de apoyo o fundamento para la adopción de actos o decisiones administrativas, se adoptarán las garantías necesarias a los efectos de mitigar cualquier sesgo por parte del órgano competente resolutorio. En ningún caso tales actuaciones en que se empleen sistemas de inteligencia artificial constituirán de por sí decisiones o actos administrativos sin validación por la persona titular del órgano competente.
3. En los supuestos de uso de sistemas de inteligencia artificial que sirvan para la adopción de actos administrativos formalizados, tanto de trámite como resolutorios, de manera automatizada sin intervención humana directa, de acuerdo con lo establecido en el artículo 76 de Ley 4/2019, de 17 de julio, deberá tratarse de actos administrativos que no requieran de una valoración subjetiva de las circunstancias concurrentes o una interpretación jurídica.
4. En caso contrario, no podrán realizarse actuaciones administrativas automatizadas a través del uso de sistemas de inteligencia, salvo que se cumplan todos los requisitos siguientes:

a) El órgano competente de la actuación administrativa automatizada aprobará previamente, siendo incorporadas en la resolución conjunta a que se refiere el artículo 76.4 de la Ley 4/2019, de 17 de julio, las instrucciones administrativas que permitan concretar los requisitos necesarios para definir de forma detallada e inequívoca los casos ordinarios a los que resulte de aplicación.

b) El órgano competente en materia de tecnologías de la información y de la comunicación, innovación y desarrollo tecnológico preparará el diseño tecnológico del sistema de inteligencia artificial en el que se basará la actuación administrativa automatizada, que respete la norma correspondiente reguladora del procedimiento y las instrucciones administrativas indicadas en el apartado anterior, que no permita la alteración no supervisada del funcionamiento del sistema o modelo y que proporcione información sencilla y fácil de entender sobre su funcionamiento para permitir a los afectados comprender y cuestionar el resultado.

5. En la regulación de los procedimientos administrativos para la adopción de decisiones administrativas automatizadas en que se empleen sistemas de inteligencia artificial se preverá el momento, modo y alcance de la intervención de personas físicas para garantizar el cumplimiento de los principios y derechos contemplados en la presente ley.

En todo caso, en los casos en que las decisiones, previsiones o recomendaciones generadas por sistemas de inteligencia artificial tengan un impacto irreversible o de difícil reversión, o impliquen actuaciones que pudieran generar riesgos para la vida o la integridad física o psicosocial de los individuos, será necesaria una validación de una persona física en el proceso decisorio, así como una decisión humana final.

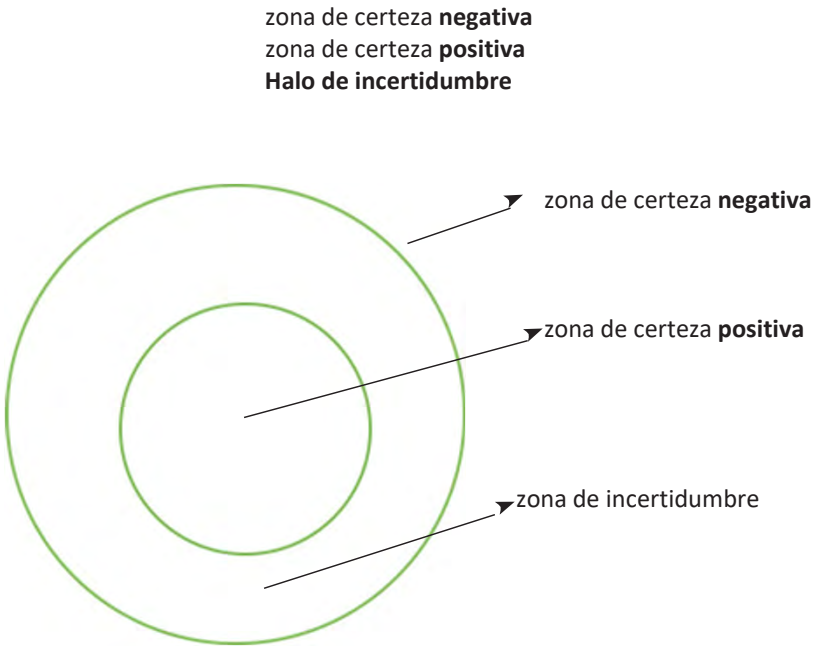
6. Sin perjuicio de los correspondientes recursos administrativos o acciones judiciales, se reconocerá el derecho a presentar sugerencias o quejas relativas al funcionamiento de los propios sistemas de inteligencia artificial empleados por la Administración autonómica y su sector público. El procedimiento o canal para la presentación de estas sugerencias o quejas será el previsto en el artículo 16 de la Ley 1/2015, de 1 de abril, de garantía de la calidad de los servicios públicos y de buena administración.

Oportunidades para la buena administración en la contratación mediante IA (Fuente: https://mymabogados.com/ia-generativa-en-contratacion-publica)

A EFECTOS DE TOTAL AUTOMATIZACIÓN, DISTINCIÓN ENTRE:

-POTESTADES ADMINISTRATIVAS REGLADAS, CON CONCEPTOS JURÍDICOS INDETERMINADOS SIN MARGEN DE APRECIACIÓN

-POTESTADES ADMINISTRATIVAS CON CONCEPTOS JURÍDICOS INDETERMINADOS CON MARGEN DE APRECIACIÓN (ZONA DE INCERTIDUMBRE) Y POTESTADES ADMINISTRATIVAS DISCRECIONALES



EJEMPLOS DE MARGEN DE APRECIACIÓN DISCRECIONAL EN CONTRATACIÓN QUE NO PUEDEN AUTOMATIZARSE TOTALMENTE (DECISIÓN RESERVADA A HUMANO):

1. FASE DE PREPARACIÓN DE CONTRATOS: LCSP "**Artículo 28. Necesidad e idoneidad del contrato y eficiencia en la contratación.**
1. Las entidades del sector público no podrán celebrar otros contratos que aquellos que sean necesarios para el cumplimiento y realización de sus fines institucionales"

2. FASE DE ADJUDICACIÓN DE CONTRATOS: LCSP "**Artículo 146. Aplicación de los criterios de adjudicación. Artículo 150. Clasificación de las ofertas y adjudicación del contrato.**

"la valoración de los criterios cuya cuantificación dependa de un juicio de valor"

"se atenderá a los criterios de adjudicación señalados en el pliego, pudiéndose solicitar para ello cuantos informes técnicos se estime pertinentes"

3. FASE DE EJECUCIÓN DE CONTRATOS: LCSP **Artículo 279. Causas de resolución**. "Son causas de resolución del contrato de concesión de obras, además de las señaladas en el artículo 211, con la excepción de las contempladas en sus letras d) y e), las siguientes:

c) El rescate de la explotación de las obras por el órgano de contratación. Se entenderá por rescate la declaración unilateral del órgano contratante, adoptada por razones de interés público, por la que dé por terminada la concesión, no obstante la buena gestión de su titular, para su gestión directa por la Administración. El rescate de la concesión requerirá además la acreditación de que dicha gestión directa es más eficaz y eficiente que la concesional"

Remunicipalización y privatización de los servicios públicos y derecho a una buena administración. Análisis teórico y jurisprudencial del rescate de concesiones

Autores: Juli Ponce Solé
Localización: Cuadernos de derecho local, ISSN 1696-0955, Número 40, 2016, págs. 68-108
Idioma: español

https://repositorio.gobiernolocal.es/xmlui/bitstream/handle/10873/1703/05_PONCE_P69_109_QDL_40.pdf?sequence=1&isAllowed=y

Importancia del procedimiento administrativo en automatización (con IA)

- Procedimiento administrativo complejo

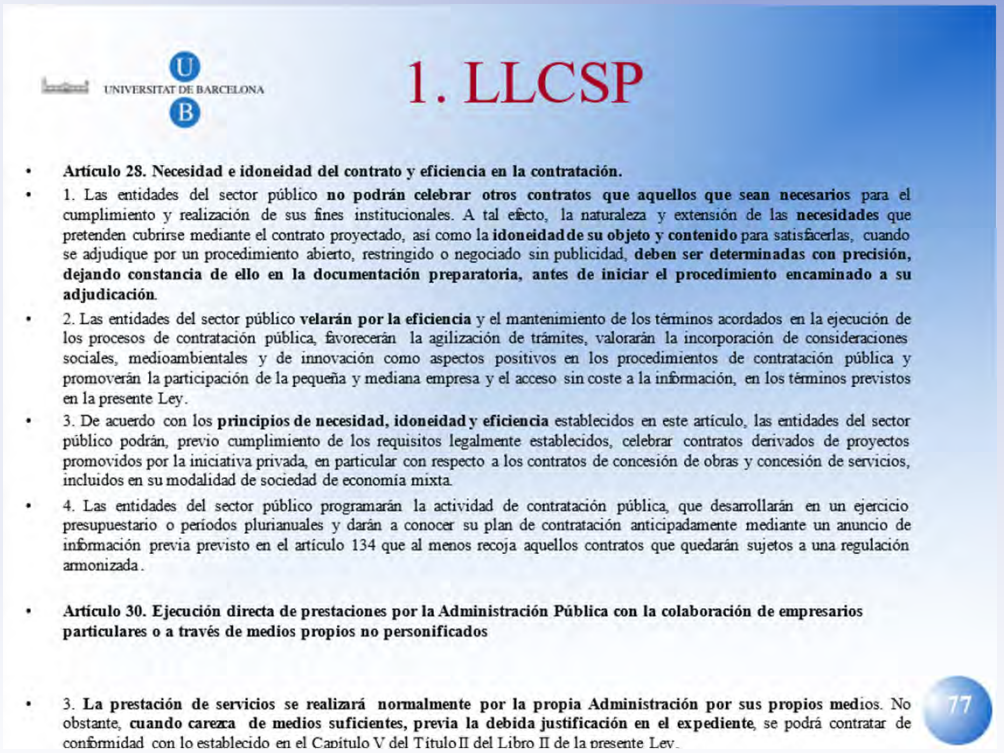
  – 1. Primer procedimiento administrativo: toma de la decisión de automatizar o no una función administrativa, con o sin IA. Necesidad de participación ciudadana. Publicidad de los elementos del sistema, incluido código fuente. NO ES UN MERO PROYECTO TÉCNICO.

  – 2. Segundo procedimiento: el específico de la toma de la decisión en el sector de qué se trate de acuerdo con las especificaciones fijadas mediante el procedimiento anterior.

UNIVERSITAT DE BARCELONA

Primer procedimiento administrativo

- -Posibilidad de uso de la IA, no obligación (¿derecho a uso de IA?: **necesidad de establecer por ley una evaluación *ex ante*** (parecida a la existente en art. 28 Ley de contratos del sector público, para contratar o no, en función de ciertos parámetros) **para decidir si se usa o no la IA, lo que va a asociado a una ponderación EN CADA CASO de costes, beneficios y riesgos (PROS Y CONTRAS)** (Coglianese).



UNIVERSITAT DE BARCELONA

Segundo procedimiento administrativo

- Se aplica la automatización previamente aprobada y diseñada.

- Da lugar a una automatización total o parcial, con la adopción, en su caso, de actos trámites o del acto definitivo, en todo caso bajo supervisión humana (RUEIA, IA de riesgo alto, art. 14...) y cumpliendo los requisitos exigidos por el ordenamiento jurídico español (elementos reglados y principios generales del Derecho)

UNIVERSITAT DE BARCELONA

CONTROL JURÍDICO USO IA POR AAPP

- NO JUDICIAL: EJ. DEFENSORES DEL PUEBLO

Declaración en Vitoria, finales de 2024

37ª reunión

9. La buena administración demanda incorporar la innovación tecnológica, con el fin de mejorar la eficiencia y la accesibilidad de los servicios públicos. La digitalización de la administración, que debe ser responsable en clave social, necesita asegurar la asistencia en el uso de herramientas electrónicas a las personas usuarias, así como la seguridad y la privacidad de los datos.
   La implantación de procedimientos electrónicos no debe menoscabar las garantías que asisten a los ciudadanos en sus relaciones con la administración, en especial la protección que merece el derecho a la corrección del error digital.
10. La buena administración necesita también aprovechar los beneficios de la inteligencia artificial para mejorar la calidad de los servicios públicos. A pesar de su significativo potencial, es también crucial identificar y corregir–los riesgos asociados a su uso para proteger los derechos y las libertades de la ciudadanía. Esto incluye garantizar la intervención humana en las decisiones, la transparencia, y evitar sesgos y discriminaciones.

UNIVERSITAT DE BARCELONA

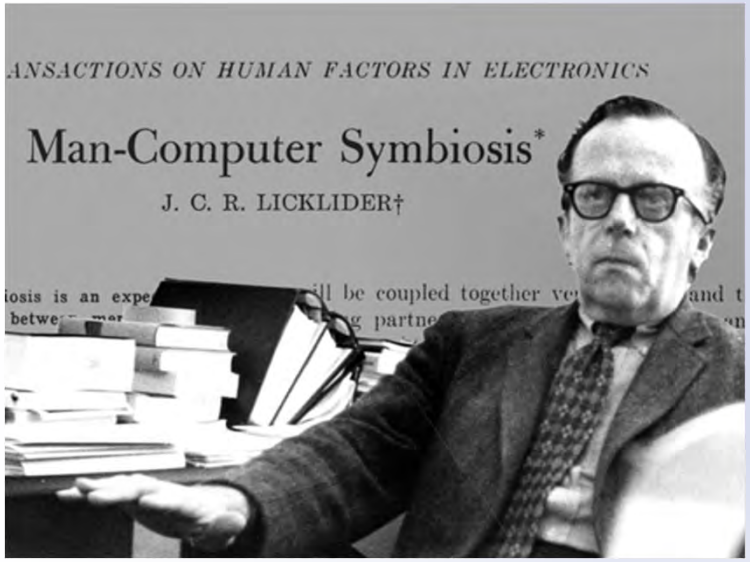
CONTROL JUDICIAL USO IA

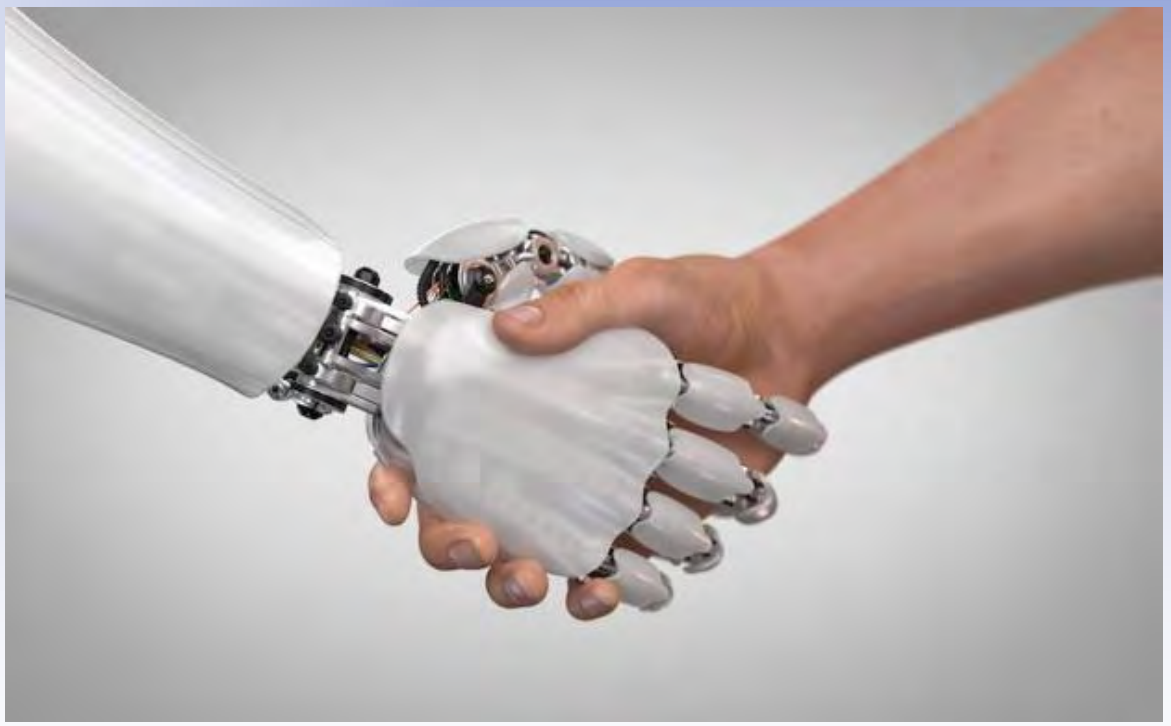
- EL EJEMPLO DEL CASO “BOSCO”, AHORA ANTE EL TRIBUNAL SUPREMO.

- CONTROL DE LA JURISDICCIÓN CONTENCIOSO-ADMINISTRATIVA: NI DEFERENCIA, NI INDIFERENCIA, NI INSUFICIENCIA.

UNIVERSITAT DE BARCELONA

BRÚJULA DE LA AUTOMATIZACIÓN EN AAPP





4. El hombre que salvó al mundo, (no confiandociegamente en los algoritmos)... S. Petrov

Muere a los 77 años Stanislav Petrov, el hombre que salvó al mundo de una guerra nuclear entre la Unión Soviética y Estados Unidos - BBC News Mundo

IA: algunos recursos abiertos en internet, para continuar

BLOG – Nudging aplicado a la Mejora de la Regulación y al Uso de Algoritmos y de Inteligencia Artificial (wordpress.com)

- **El bono social energético y el programa Bosco: sobre algoritmos, errores y código fuente. A propósito de la primera decisión judicial recaída en 2021: una mala sentencia que esperamos sea corregida pronto – Nudging aplicado a la Mejora de la Regulación y al Uso de Algoritmos y de Inteligencia Artificial (wordpress.com)**
- **De ruido, sesgos, algoritmos e inteligencia artificial – Nudging aplicado a la Mejora de la Regulación y al Uso de Algoritmos y de Inteligencia Artificial (wordpress.com)**

Beneficios y riesgos de la inteligencia artificial para el sector público y las personas en Iberoamérica: la cuestión de los sesgos – Asociación Internacional para la Gobernanza (aigob.org)

opac-retrieve-file.pl

European Review of Digital Administration & Law | Law, Digital Nudging and Manipulation: Dark Patterns, Artificial Intelligence and the Right to Good Administration (erdalreview.eu)

8 PONCE La lucha.pdf - Google Drive

SINDICATURA DE COMPTES DE CATALUNYA

La IA en l'auditoria pública

Miquel Salazar Canalda, síndic major

Abril del 2025

SINDICATURA DE COMPTES DE CATALUNYA

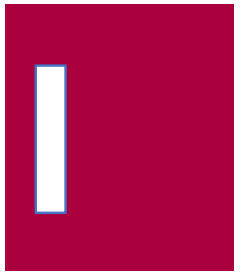
DE QUÈ PARLAREM:

1. Què fa la IA. Avantatges i reptes
2. En quins àmbits de fiscalització pot ajudar la IA:
   a. Fiscalització de l´àrea econòmica financera
   b. Fiscalització del compliment normatiu general
   c. Fiscalització de contractes
   d. Fiscalització de subvencions
3. Què està fent La Sindicatura de Comptes respecte a la IA

Principals branques de la IA utilitzables en auditoria

L'**aprenentatge automàtic (ML)** permet aprendre de les dades sense estar explícitament programades, identificant **patrons de comportament** i fent **prediccions**

Automatització robòtica de processos (RPA) utilització de programari per **automatitzar tasques repetitives** i basades en regles. Varia des d'una intervenció parcial fins a una automatització intel·ligent (amb capacitat de decisió en diverses fases dels procés)



IA en auditoria

Processament de Llenguatge natural (NLP) possibilita la comunicació entre humans i màquines permetent anàlisis de dades sobre documents no estructurats

IA discriminativa.
Ordena, classifica i prediu

IA generativa
Crea contingut nou

SINDICATURA DE COMPTES DE CATALUNYA

Què fa la IA

Cerca d'informació en format obert (articles doctrinals, sentències...)

Resums de documents complexos (informes, articles doctrinals...)

Extracte de dades de documents (contractes, escriptures...)

Disseny de macros per a Excel.

Traducció de textos

Anàlisi de ratis d'estat financers

Detectar riscos d'auditoria partint dels comptes anuals públicats

Anàlisi estadística de dades diverses, selecció de mostres, etc.

Detecció d'operacions anòmales o amb indicis de frau

Anàlisi de bases de dades massives com assentaments de diaris, factures, nòmines del personal, inventaris o registres de tot tipus

SINDICATURA DE COMPTES DE CATALUNYA

Avantatges (1/3)

L'aplicació de la IA a les auditories i fiscalitzacions suposarà els avantatges següents:

- **Economia:** realització de les diferents proves d'auditoria repetitives a un cost inferior
- **Eficàcia:** automatització en la recopilació de dades, la classificació de documents i la realització de càlculs. Així mateix, possibilitarà als auditors centrar-se en tasques de nivell estratègic, aportant un valor afegit a les tasques de direcció i anàlisi.
- **Eficiència:** realització d'anàlisis més profundes i detecció de riscos d'auditoria de manera més immediata, en un temps inferior i reduint els errors humans.

Avantatges (2/3)

- **Millora de la visió estratègica:** La utilització de la IA permetrà la millora estratègica des de dos punts de vista:
  - Ajudant a descarregar a l'auditor de les feines repetitives i permetent que es dediqui a tasques de nivell superior.
  - Millorant les anàlisis i les prediccions per optimitzar la planificació i l'execució del treball.

  Tal com va dir Donald Knuth: "cada vegada escriurem menys i validarem més".

- **Millora de la capacitat de detecció i mitigació de riscos:** Aplicant la IA a les auditories s'augmentarà la capacitat de detecció i mitigació de riscos, reduint costos d'avaluació dels controls, proporcionant una resposta immediata i generant una major fiabilitat.

SINDICATURA DE COMPTES DE CATALUNYA

Avantatges (3/3)

- **Millora del coneixement de la entitat fiscalitzada i de la seva activitat (insights):** Aquests coneixements s'obtenen a partir de l'anàlisi de dades, mineria de dades, mineria de sistemes, etc., i poden revelar patrons i tendències no evidents sense aquestes anàlisis.
- **Millora la presentació i difusió dels informes:** Proporcionar de manera ràpida resums i presentacions d'informes i elaboració de vídeos, que amb la seva publicació milloraran l'accés a la informació per part del públic no especialitzat

MILLORA EN LA QUALITAT DE LA FEINA

Reptes (1/2)

Entre els reptes que presenta la IA aplicada a l'auditoria cal destacar:

- **Fiabilitat de les dades:** Cal establir mecanismes per comprovar la veracitat i la integritat de les dades extretes utilitzant IA i evitar possibles biaixos. S'ha d'evitar el biaix de automatització (confiar cegament en la informació que proporciona la IA) i, per tant, s'haurà de supervisar sistemàticament la informació obtinguda de la IA.

- **Tractament adequat de dades: L**a utilització de la IA ha de garantir un entorn segur per garantir la confidencialitat i la disponibilitat de les dades en funció de la seva criticitat. En especial les dades de caràcter personal i aquelles que són altament sensibles. Cal tenir en compte el caràcter reservat de la informació que disposen els OCEX's.

- **Capacitació del personal: E**l personal d'auditoria ha d'estar capacitat en l'ús de metodologies basades en IA, ha de ser capaç de comprendre i explicar les troballes d'auditoria obtingudes mitjançant IA i ha d'estar contínuament actualitzat respecte als avenços en aquesta matèria.

Reptes (2/2)

- **Costos d'implementació:** Malgrat la democratització de la IA, les inversions necessàries per implementar-les poden requerir costos molt alts.
- **Disseny d'algoritmes: E**l disseny d'algoritmes vàlids per a l'auditoria pot ser complex L'auditor necessita una evidència general que requereix una varietat de fonts, una recopilació de dades molt variades i el disseny adequat de proves d'auditoria.
- **Risc de ciberseguretat: L**a implantació de la IA requerirà implementar mesures de protecció adequades i d'una forma permanent, que permetin evitar o reduir els possibles atacs als sistemes informàtics i a les dades.
- **Impacte en l'ocupació: E**s diu que, junt amb els comptables, els desenvolupadors de software i els matemàtics, els auditors són una de les ocupacions que podran veure en perill la seva continuïtat amb el desenvolupament de la IA.

SINDICATURA DE COMPTES DE CATALUNYA

En quins àmbits de fiscalització pot ajudar la IA

- Fiscalització de l'àrea econòmicofinancera
- Fiscalització del compliment normatiu general
- Fiscalització de la contractació
- Fiscalització de subvencions

Fiscalització de l'àrea economicofinancera

Possibles casos en els que la IA, mitjançant la programació dels algoritmes adequats, podria ajudar els auditors:

1. **Recopilació d'informació.** La IA podria, mitjançant l'automatització robòtica de processos (RPA), extreure i consolidar automàticament dades comptables de diferents estats i de diferents fonts, calculant ratis i facilitant la planificació.

2. **Anàlisi de riscos.** La IA pot ajudar de forma automàtica a analitzar els riscos d'auditoria i pot realitzar anàlisis predictius per preveure tendències financeres futures, basades en dades històriques o comparatives amb altres ens del sector, i ajudar a avaluar la sostenibilitat financera, la liquiditat i la solvència.

3. **Contrastació normativa.** La IA pot ajudar a verificar el compliment de les normes comptables en els registres de l'entitat.

Compliment normatiu general

Possibles casos d'ús en els que la IA podria ajudar, mitjançant la programació dels algoritmes adequats, a la fiscalització del compliment normatiu general:

1. **Planificació.** La IA pot recopilar i analitzar informació general sobre l'objecte de fiscalització i realitzar prediccions per identificar àrees de risc d'auditoria.

2. **Automatització robòtica de processos (RPA).** Mitjançant la RPA la IA podrà automatitzar tasques repetitives com, per exemple, intercanvi de fitxers entre aplicacions, revisió de llistes de verificació i generació de memoràndums o altra documentació estàndard.

3. **Anàlisi del sentiment i el to.** La IA pot identificar i classificar el to expressat en un text, per exemple, en positiu, negatiu o neutral. Això permetria analitzar el llenguatge utilitzat en documents generats en una entitat (correus electrònics, circulars, etc.) la qual cosa ajudaria a detectar possibles àrees conflictives o susceptibles de tenir algun incompliment normatiu.

Fiscalització de contractes (1/2)

Possibles casos d'ús en els que la IA podria ajudar, mitjançant la programació dels algoritmes adequats, a la fiscalització de contractes:

1. **Revisió preliminar.** La IA pot realitzar una revisió preliminar dels contractes, destacant clàusules o terminis que requereixen atenció especial o que presenten un possible risc. També pot extreure la informació clau dels contractes facilitant la seva fiscalització.

2. **Verificació de terminis.** La IA pot realitzar automàticament la verificació del compliment de terminis requerits a la llei de contractes.

3. **Anàlisi dels expedients.** Mitjançant l'ús del Processament de llenguatge natural la IA pot detectar, en el clausulat dels contractes, termes imprecisos o il·legals. També podria efectuar comparacions de plecs, contractes o altres documents de la contractació amb versions anteriors per a detectar possibles omissions de termes crítics o verificar la possible introducció de condicions diferents.

Fiscalització de contractes (2/2)

4. **Compliment de clàusules especials.** La IA pot ajudar a verificar que els contractes compleixen amb la normativa contractual i les regulacions específiques com la de protecció de dades de caràcter personal o la d'igualtat de gènere.

5. **Anàlisi dels licitadors.** Permetrà una anàlisi prèvia de possibles repartiments de quotes de mercat entre grans proveïdors, a nivell molt més ampli que l'àmbit territorial de l'OCEX.

Fiscalització de subvencions

Possibles casos d'ús en els que la IA podria ajudar, mitjançant la programació dels algoritmes adequats, a la fiscalització de subvencions:

1. **Revisió preliminar.** La IA podrà realitzar una revisió automàtica preliminar de la convocatòria, les bases, les sol·licituds i les justificacions de les subvencions, destacant els aspectes o àrees que requereixen especial atenció o presenten un possible risc.

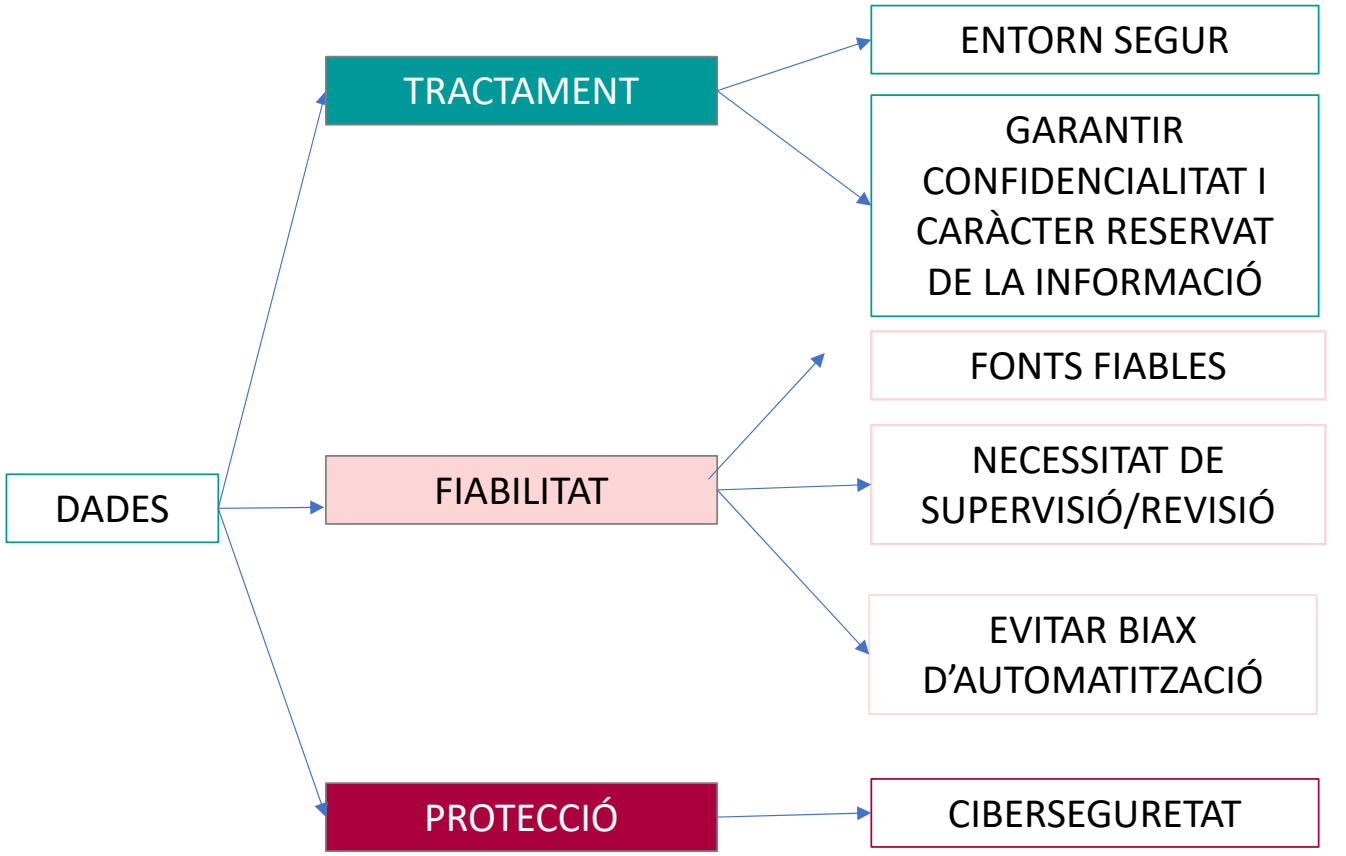
2. **Detecció d'incompliments.** La IA podrà analitzar les sol·licituds i la documentació facilitada pels beneficiaris per a detectar incompliment de les bases o la convocatòria respecte a la normativa corresponent.

3. **Detecció de patrons o comportaments.** Els algoritmes de la IA poden analitzar informació dels beneficiaris per a detectar possibles discrepàncies amb la informació continguda en altres fonts, evidenciar justificacions inadequades i detectar possibles patrons d'actuacions irregulars.

La Sindicatura de Comptes de Catalunya i la IA

Valoració institucional

RISCOS AMB EL TRACTAMENT DE DADES AMB LA UTILITZACIÓ DE LA IA



Cobrir el risc de compartir informació protegida per llei, en el núvol o online amb les eines d'IA i no tenir control sobre la protecció efectiva d'aquestes dades.

Utilitzar *informació d'alta qualitat,* evitar informació falsa o imprecisa. Utilitzar *l'excepticisme intel·ligent*. Supervisar i revisar tota la informació i evitar *el biaix d'automatització* (confiança cega en la informació que dona la IA)

S'ha de tenir la infraestructura i el programari necessari per protegir les dades de ciberatacs. (Compliment de l'ENS)

SINDICATURA DE COMPTES DE CATALUNYA

Accions

El Ple ha encomanat a una **comissió interna** formada per membres del Ple i personal auditor una sèrie d'accions a fer a curt i mitjà termini per tal d'analitzar i iniciar la seva implantació:

Estudiar i decidir quines **necessitats** poden ser cobertes per IA

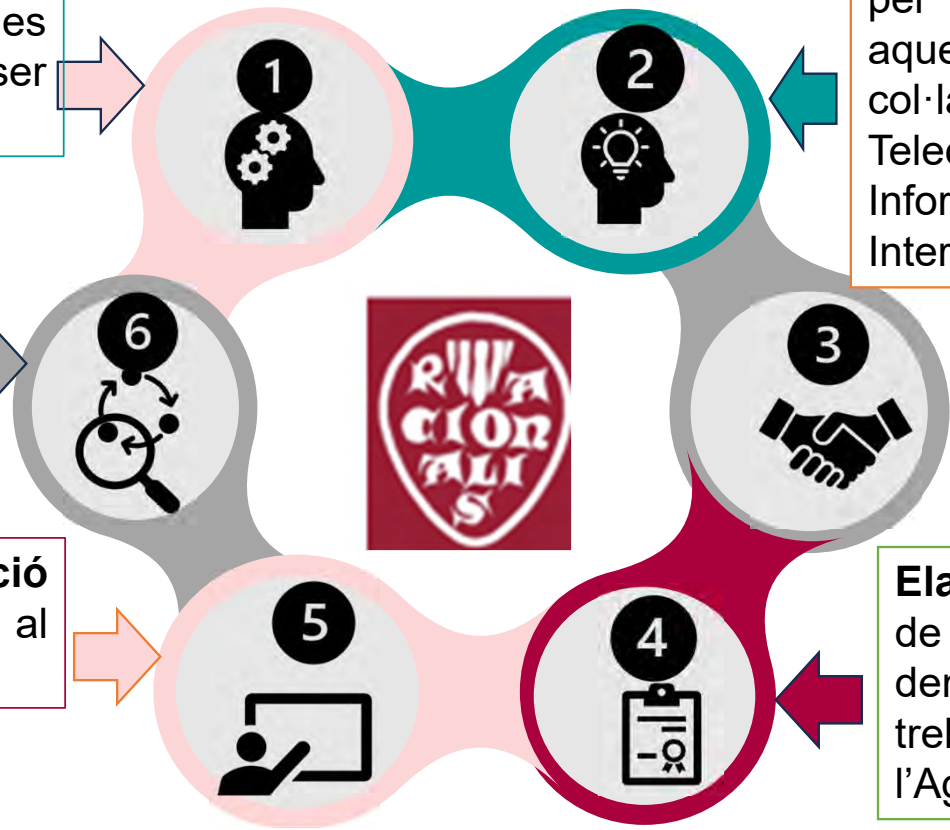
Decidir quines eines es poden utilitzar per cobrir les necessitats. Per prendre aquesta decisió es demanarà la col·laboració del Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) i de la Fundació I2CAT, Internet i Innovació Digital a Catalunya

Implantar les eines i **monitoritzar** el seu ús.

Adquirir les llicències oportunes per a ús del personal o **demanar l'elaboració d'eines ad hoc**.

Realitzar **la formació** adequada per al **personal.**

Elaborar un protocol per a la utilització de les eines d'IA per part del personal. Es demanarà la col·laboració del grup de treball de l'ENS de la Sindicatura i de l'Agència Catalana de Ciberseguretat.



SINDICATURA DE COMPTES DE CATALUNYA

SINDICATURA DE COMPTES DE CATALUNYA

"Es posible que lo que hagamos ahora con la inteligencia artificial nos parezca en el futuro excesivo o insuficiente, pero lo que nos distingue como humanos no es el éxito de lo que hacemos sino el empeño con que lo hacemos."

Daniel Innerarity (Bilbao, 1959) es filósofo.

Una teoría crítica de la inteligencia artificial, de Galaxia Gutenberg.

Aquesta feina s'ha realitzat amb la col·laboració de:

Rafael Morales i Rosales. Auditor de la Sindicatura de Comptes de Catalunya

Francesc J. Chico Martínez . Auditor supervisor de la Sindicatura de Comptes de Catalunya. CISA

Aplicación de la IA en el ámbito del control de subvenciones en la IGAE

25 de abril de 2025

Ismael García Cebada
Director de la Oficina de Informática Presupuestaria
Intervención General de la Administración del Estado
Ministerio de Hacienda

1. Contexto
2. Proyecto
3. Proceso
4. Resultados
5. Lecciones aprendidas
6. Nuevos proyectos

La Oficina de Informática Presupuestaria de la IGAE

- Presta servicio informático a la IGAE, a la Secretaría de Estado de Presupuestos y Gastos, Secretaría General de Fondos Europeos, a las Delegaciones de Economía y Hacienda

- Desarrolla y mantiene más de 200 sistemas de información, entre los que destacan el sistema contable de la AGE (SIC'3), de gestión económica (SOROLLA2), planificación de auditorías de la ONA (AUDInet), elaboración de presupuestos (PGEnet), gestión de fondos europeos (CoFFEE-MRR), …

- Entre sus funciones, junto con la ONA, desarrollo y mantenimiento de la BDNS y el Sistema Nacional de Publicidad de Subvenciones y Ayudas Públicas (www.infosubvenciones.es)

Control Financiero de Subvenciones Nacionales

- Objetivos del CFSN
  - Combatir el fraude
  - Aumentar la sensibilización entre beneficiarios y órganos concedentes
  - Buscar introducir valor añadido (frente a simple re-ejecución de procesos)
  - Maximizar las capacidades de control (descentralización)

- Respuesta: planificación anual basada en tres elementos clave
  - Subvenciones con mayor riesgo percibido
  - Visibilidad del control
  - Rentabilizar los medios disponibles

Planificación CFSN

- Análisis de riesgos sobre el universo de subvenciones para dirigir los controles
- La ONA ha desarrollado una metodología para esté análisis de riesgos
- Anualmente se aplica la metodología sobre el conjunto de subvenciones en la BDNS
- El objetivo es determinar los controles a aplicar el año siguiente

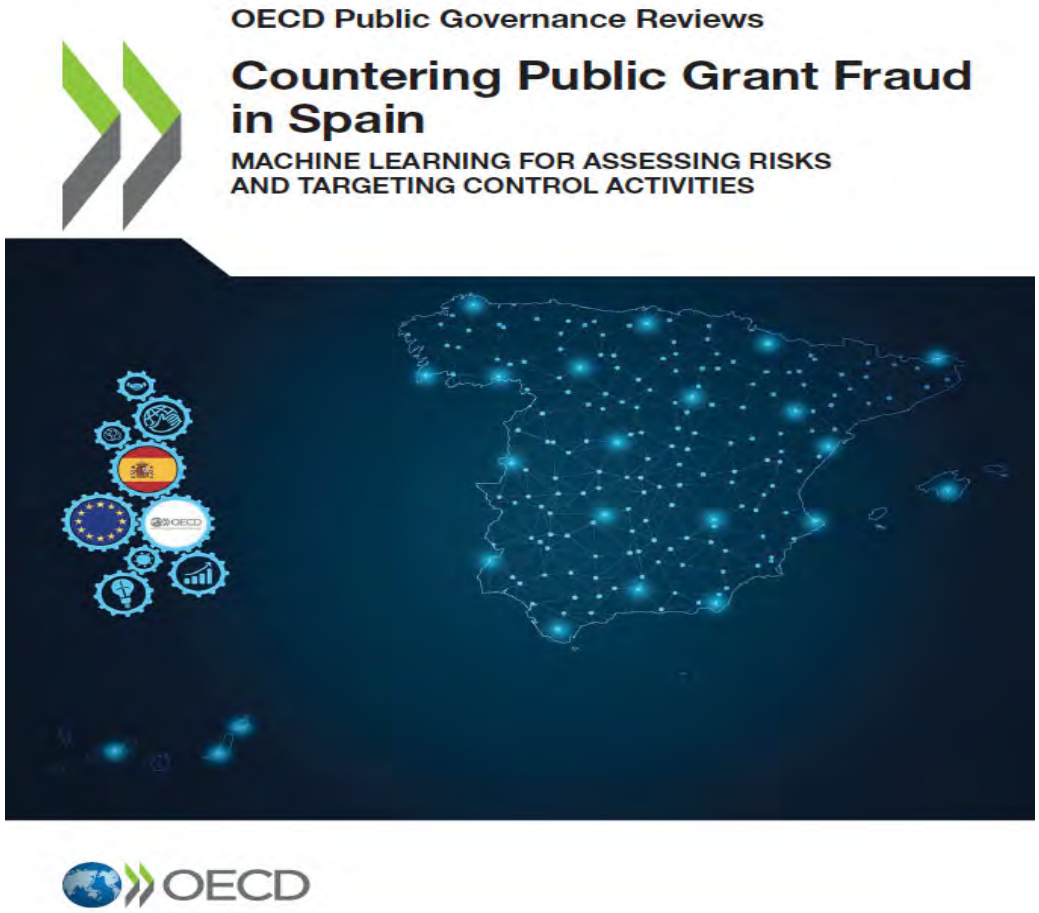
A mejorar

- Proceso complejo con tratamiento manual de gran cantidad de datos
- Se selecciona previamente una muestra del universo por criterios fijos
- Recursos limitados para la realización de controles requieren la máxima eficacia
- El aprendizaje es costoso de aplicar a la metodología

1. Contexto
2. Proyecto
3. Proceso
4. Resultados
5. Lecciones aprendidas
6. Nuevos proyectos

Proyecto conjunto con OCDE

- Programa de Reformas Estructurales de la Comisión Europea 2020
- Colaboración con la OCDE como socio ejecutor del proyecto
- Proporcionan especialistas antifraude y en técnicas de IA
- Se aprovecha el conocimiento de los equipos internos ONA y OIP



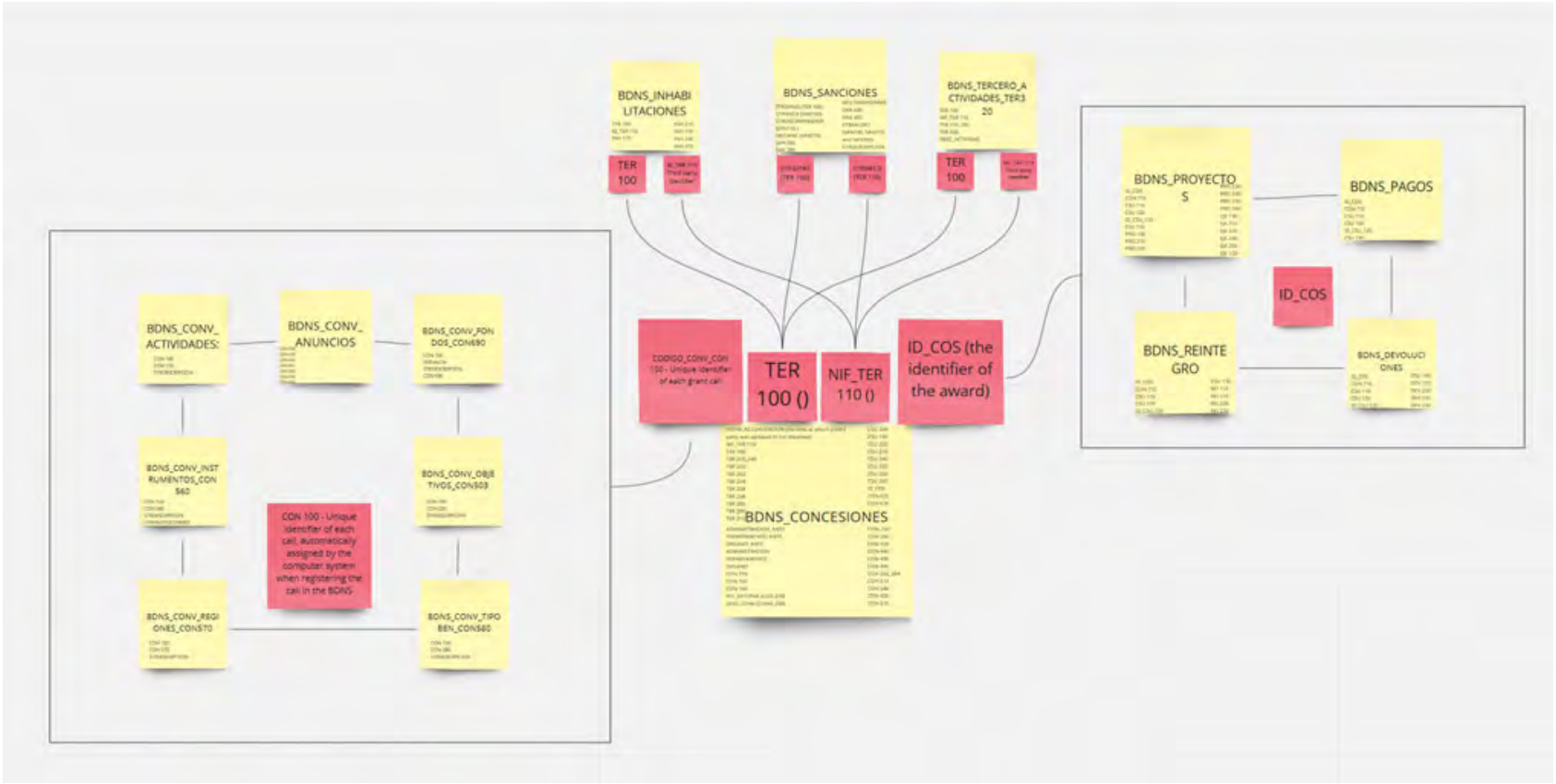
OECD (2021), *Countering Public Grant Fraud in Spain: Machine Learning for Assessing Risks and Targeting Control Activities*

OECD Public Governance Reviews

OECD Publishing, Paris,
https://doi.org/10.1787/0ea22484-en

La propuesta

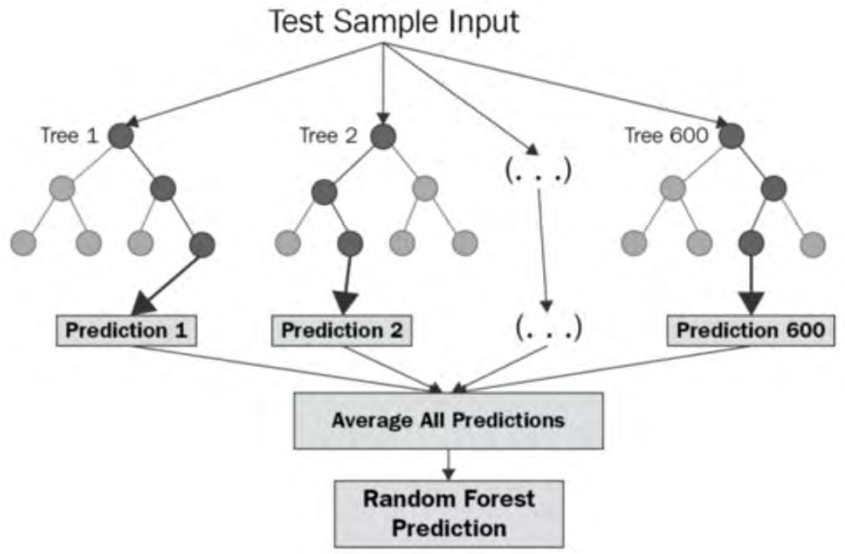
- Fuente principal de datos: BDNS incluyendo concesiones, inhabilitaciones y sanciones
- Posible incorporación posterior de otras fuentes de datos
- Metodología: Sistema de *machine learning* (aprendizaje supervisado):
- Algoritmo propuesto: *Random forest*


BDNS_INHABILITACIONES
TER 100
BDNS_SANCIONES
BDNS_TERCERO_ACTIVIDADES_TER320
TER 100
BDNS_PROYECTOS
BDNS_PAGOS
ID_COS
BDNS_REINTEGRO
BDNS_DEVOLUCIONES
BDNS_CONV_ACTIVIDADES:
BDNS_CONV_ANUNCIOS
BDNS_CONV_FONDOS_CON690
BDNS_CONV_INSTRUMENTOS_CON560
CON 100 - Unique identifier of each call, automatically assigned by the computer system when registering the call in the BDNS
BDNS_CONV_OBJETIVOS_CON503
BDNS_CONV_REGIONES_CONSTO
BDNS_CONV_TIPOBEN_CON580
CODIGO_CONV_CON150 - Unique identifier of each grant call
TER 100 ()
NIF_TER 110 ()
ID_COS (the identifier of the award)
BDNS_CONCESIONES

Aplicación del modelo random forest:

- Grupo de entrenamiento: proceso en el que se determina la relación entre las variables independientes y la variable dependiente (reintegro SI/NO) y califica la probabilidad de fraude (> ó < 50%)

- Grupo de testeo: altos de niveles de exactitud y precisión



Resultados

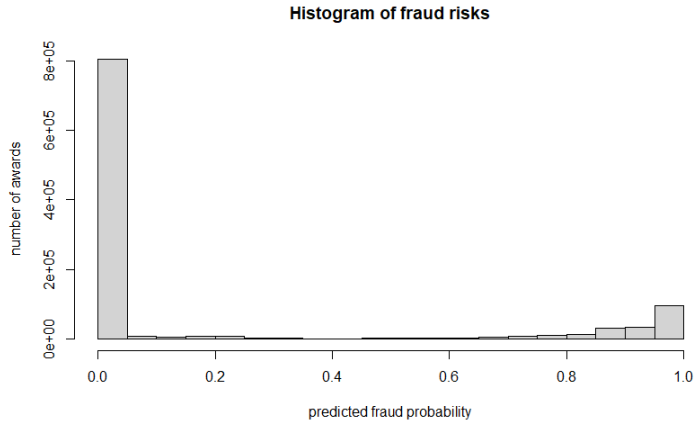
- Las cifras del test demuestran resultados muy prometedores
- Se considera que hay que ampliar criterios, incluir otras fuentes de datos y refinar el modelo progresivamente

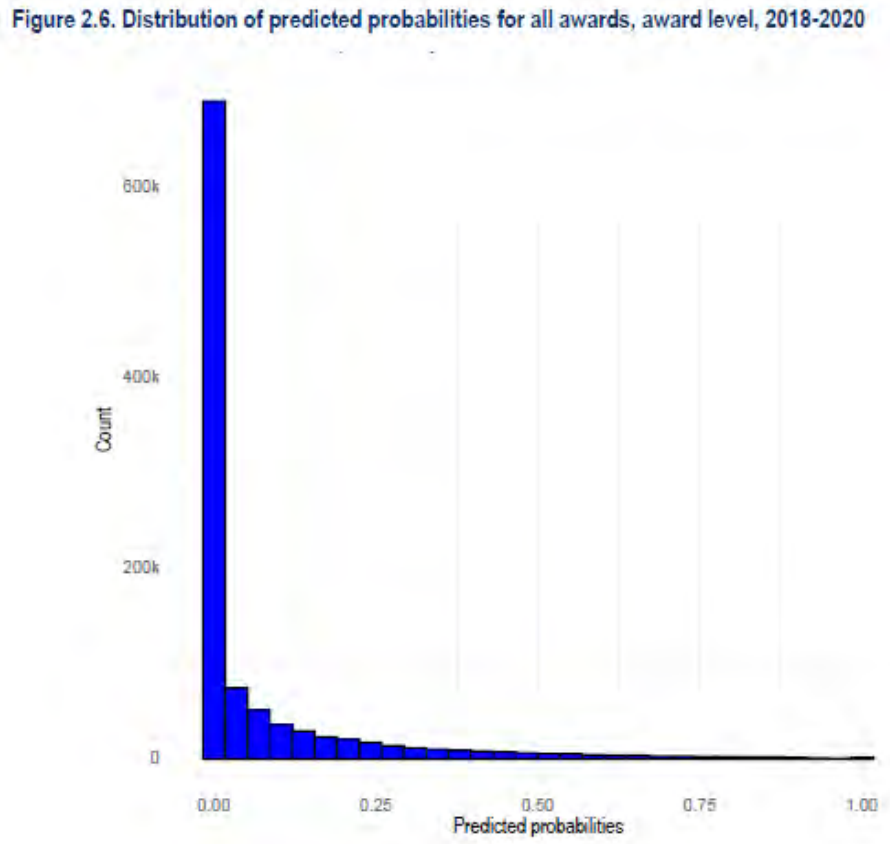
Predicted high risk/actual sanctions	NO sanctions	YES sanctions
Low risk	19,170	26
High risk	5	283

Resultados (II)

Conjunto de datos:

23 variables y
1,050,470 registros





Conclusiones del proyecto (2021)

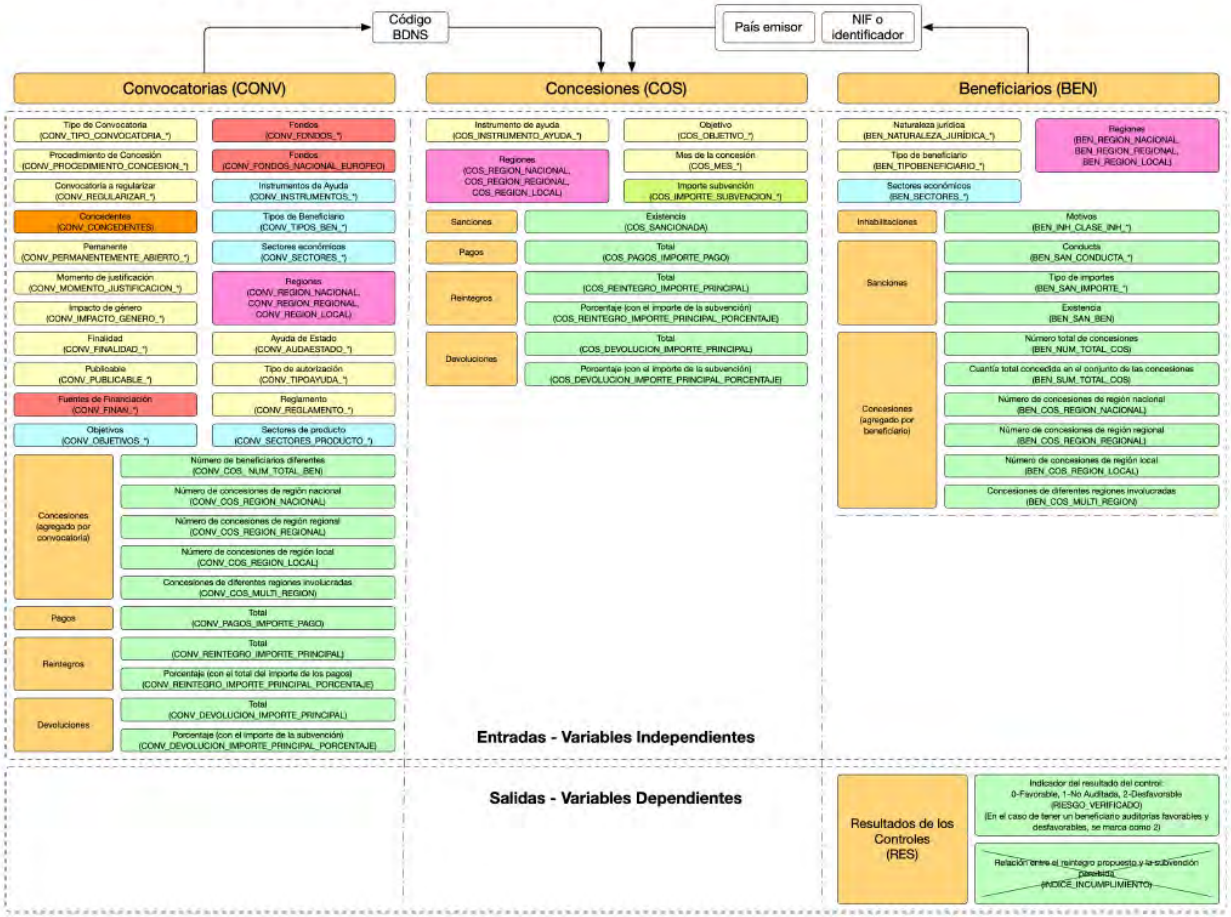
- Satisfacción de la ONA con los resultados obtenidos
- OIP ve viable continuar el proyecto con recursos propios
- Posibilidad de contratación externa para apoyo tecnológico puntual

- Decisión de utilizar los resultados en la planificación de controles:
  - De forma paralela a la metodología manual
  - Examinando los resultados y comparando con la metodología manual
  - Progresiva implantación del nuevo sistema hasta dejar el manual solo como chequeo

1. Contexto
2. Proyecto
3. Proceso
4. Resultados
5. Lecciones aprendidas
6. Nuevos proyectos

0. Punto de partida

Análisis de Riesgo: Dataset



1.Unificación

Unificación de conjuntos de datos:

- Convocatorias
- Concesiones
- Beneficiarios
- Pagos
- Inhabilitaciones
- Sanciones
- Reintegros
- Actividades terceros

Resultado: una única tabla con un registro por cada concesión. Cientos de campos.

2. Limpieza de datos

- Es necesario incrementar la calidad de los datos
- Se eliminan
  - variables con baja varianza
  - variables con elevado nivel de dato omitido
  - variables repetidas
- Se anonimizan los datos sustituyendo identificadores

- Objetivo: concentrar los análisis en variables relevantes

3. Variables binarias

- Las variables con múltiples valores no son compatibles con el análisis *random forest*
- Es necesaria su transformación en variables binarias
- Por cada variable con valor múltiple se crean un conjunto de nuevos indicadores binarios (sí o no)

4. Particionado

- Se obtienen dos conjuntos de datos
- Se particiona de forma aleatoria

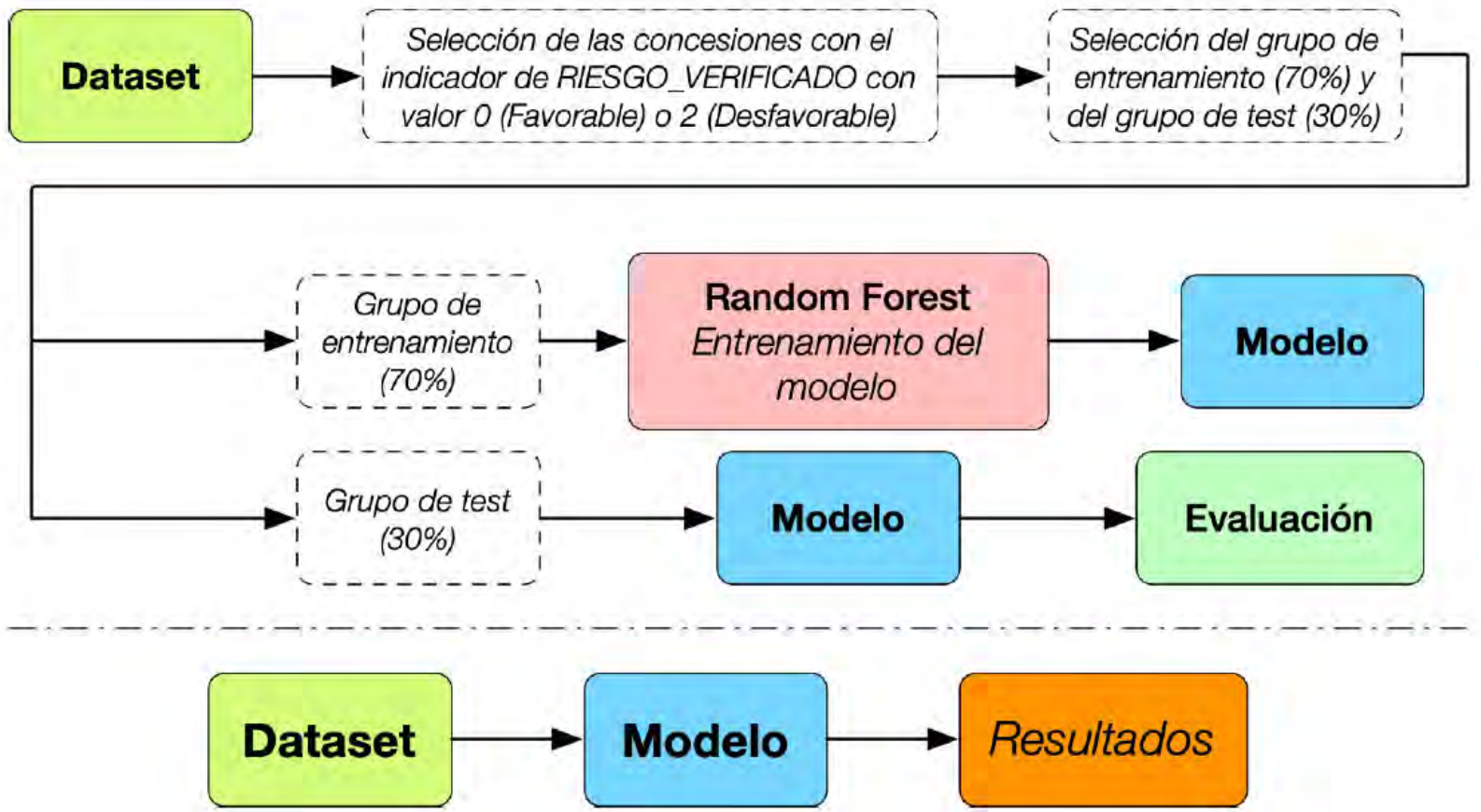
- 70% de los datos forman el conjunto de entrenamiento
- 30% de los datos forman el grupo de control
- De estos últimos se separan los datos de sanciones

- Hay que asegurar que en ambos conjuntos la proporción de concesiones sancionadas es equivalente

5. Entrenamiento

- Se genera un modelo “Random Forest”
- Se implementa con Phyton

- Se alimenta el modelo con el 70% de los datos (conjunto de entrenamiento)
- El resultado es un modelo funcional de predicción de riesgos de fraude
- Resultado binario para cada concesión: alto riesgo, bajo riesgo


Dataset
Selección de las concesiones con el indicador de RIESGO_VERIFICADO con valor 0 (Favorable) o 2 (Desfavorable)
Selección del grupo de entrenamiento (70%) y del grupo de test (30%)
Grupo de entrenamiento (70%)
Random Forest
Entrenamiento del modelo
Modelo
Grupo de test (30%)
Modelo
Evaluación
Dataset
Modelo
Resultados

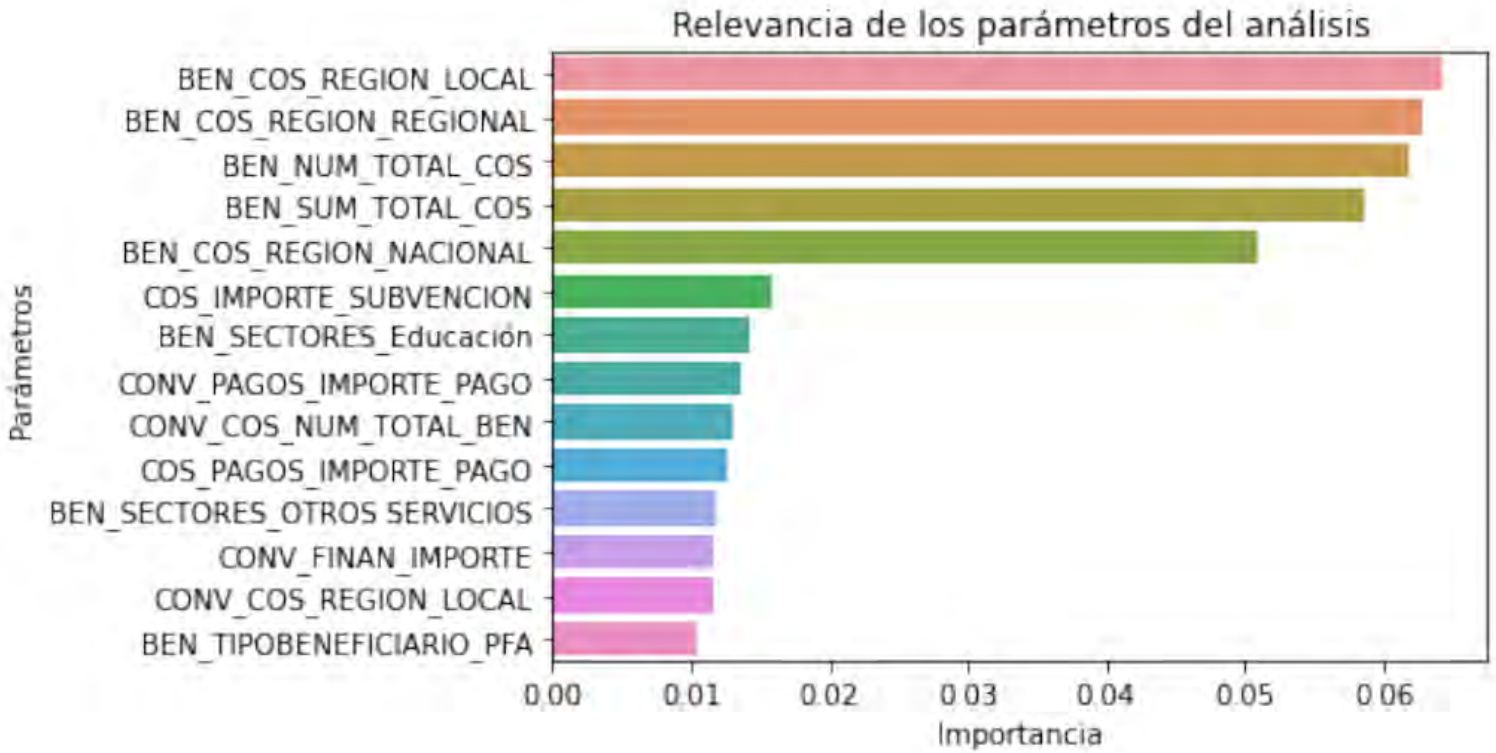
6. Prueba

- Se ponen a prueba los resultados del modelo
- Se alimenta el modelo con los datos del grupo de control, sin los datos de sanciones
- El resultado de cada concesión (alto riesgo/bajo riesgo) se compara con el resultado de los controles y sanciones
- Se evalúa la precisión del modelo:

Predicted high risk/actual sanctions	NO sanctions	YES sanctions
Low risk	19,170	26
High risk	5	283

7. Refinamiento

- Se ajustan variables y parámetros en función de la evaluación:
  - ¿Hasta qué valor se considera riesgo bajo / riesgo alto?
  - ¿Qué variables se pueden eliminar?
  - ¿A cuáles se les puede dar más relevancia?


Relevancia de los parámetros del análisis
BEN_COS_REGION_LOCAL
BEN_COS_REGION_REGIONAL
BEN_NUM_TOTAL_COS
BEN_SUM_TOTAL_COS
BEN_COS_REGION_NACIONAL
COS_IMPORTE_SUBVENCION
BEN_SECTORES_Educación
CONV_PAGOS_IMPORTE_PAGO
CONV_COS_NUM_TOTAL_BEN
COS_PAGOS_IMPORTE_PAGO
BEN_SECTORES_OTROS SERVICIOS
CONV_FINAN_IMPORTE
CONV_COS_REGION_LOCAL
BEN_TIPOBENEFICIARIO_PFA
Parámetros
0.00
0.01
0.02
0.03
0.04
0.05
0.06
Importancia

1. Contexto
2. Proyecto
3. Proceso
4. Resultados
5. Lecciones aprendidas
6. Nuevos proyectos

Resultados

- Desde 2022 se está usando el modelo para la planificación de actuaciones en CFSN

- Se combinan los resultados del modelo con actuaciones seleccionadas y no seleccionadas (aleatorias) para incrementar la eficacia del modelo en posteriores ejecuciones

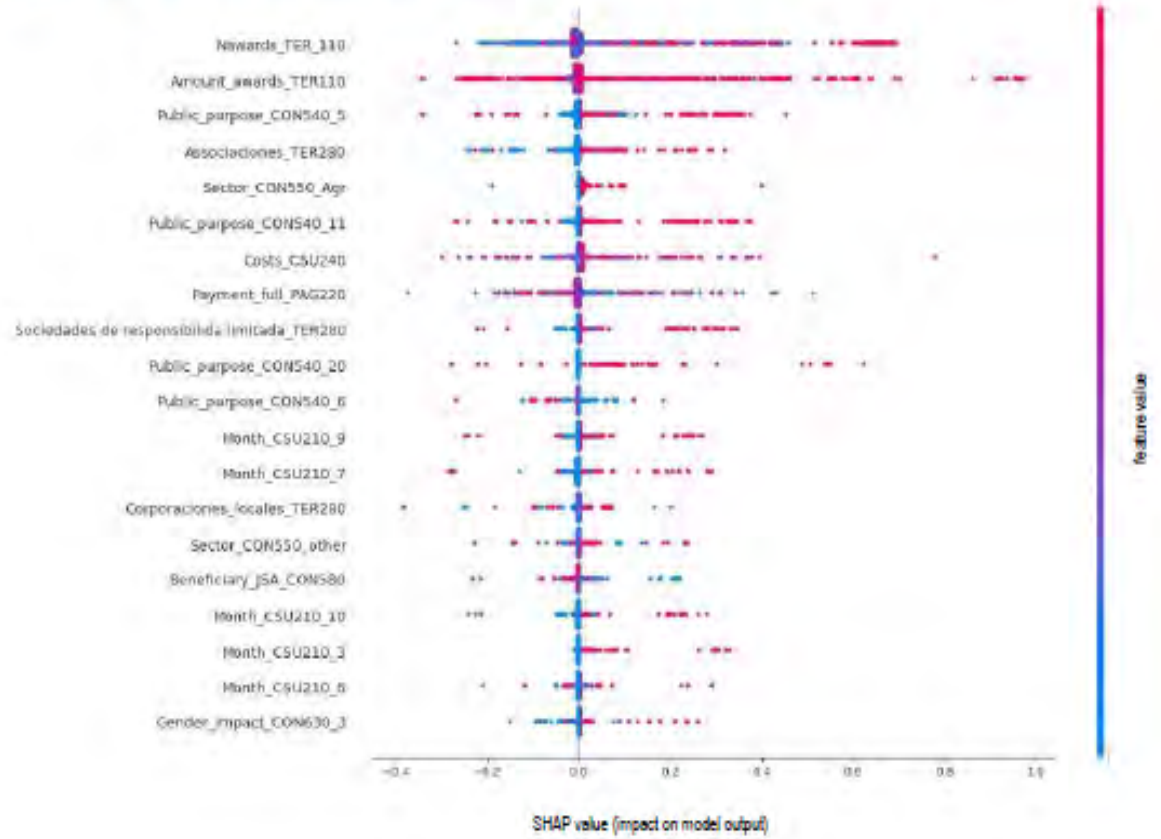
- Anualmente se realiza el proceso descrito: se entrena, se comprueba y se refina el modelo usado

Mejoras implementadas (2022 – 2025)

- Ampliación anual del número de variables y registros analizados
- Infraestructura de producción
- Normalización de direcciones: permite agregar como variable numérica el número de beneficiarios que comparten una dirección (se trata de otro proceso de IA en sí mismo)
- Trazabilidad de los resultados
- Automatización del procesado posterior para obtener una planificación

Trazabilidad

Figure 2.4. SHAP values: Variable importance and effect direction



Mejoras pendientes

- Buscar nuevos atributos que permitan enriquecer el modelo
- Incorporar nuevos esquemas de fraude que permitan su tratamiento
- Reducir posibles sesgos con los resultados observados
- Compatibilizar la selección basada en riesgos con criterios no tratables

1. Contexto
2. Proyecto
3. Proceso
4. Resultados
5. Lecciones aprendidas
6. Nuevos proyectos

Beneficios

- Se amplía el universo de datos a analizar hasta el 100%
- Se pueden refinar constantemente las variables y el modelo, en un ciclo de mejora continua
- Se reduce el tiempo dedicado al análisis
- Se evitan tareas repetitivas al personal, permitiendo centrarse en el control

Riesgos

- Es fácil introducir sesgos velados que reduzcan la objetividad del análisis
- Se puede llegar a la “auto-confirmación” del modelo
- Perdemos el control del proceso por las decisiones automatizadas
- Se pierde conocimiento del personal sobre los criterios empleados

Trazabilidad de las decisiones

- Todos los criterios usados deben quedar registrados
- Los pesos empleados deben justificarse documentalmente
- La decisión final debe quedar documentada, junto con los criterios conducentes a la misma

Soporte normativo y procedimental

- El personal implicado y en especial, los responsables, deben conocer el sistema en profundidad
- El proceso debe estar documentado, así como los procedimientos para cambios y evoluciones
- Se debe contar con las normas que den soporte a decisiones automatizadas

Controles sobre la ejecución

- Se ha comparado el resultado del sistema frente al resultado con el proceso anterior
- Se revisan los conjuntos de datos de entrada y los procesos de limpieza sobre los datos
- Se revisan periódicamente los umbrales de validez que forman parte de la configuración del sistema
- Importante introducir controles aleatorios para minimizar sesgos

1. Contexto
2. Proyecto
3. Proceso
4. Resultados
5. Lecciones aprendidas
6. Nuevos proyectos

Análisis de riesgos en expedientes de contratación

- Nuevo proyecto comenzado con la ONA
- Datos de entrada: expedientes de contratación
- Objetivo: identificación de criterios de riesgo y clasificación de los expedientes según su nivel de riesgo
- Dificultad de encontrar datos de calidad
- Dificultad de encontrar una “variable dependiente” (resultado del control)

Mejora de la calidad del dato en BDNS

- Nuevo proyecto comenzado con la ONA - BDNS
- Análisis de la documentación que acompaña al registro de la convocatoria
- Objetivo: identificación de datos en la documentación para validación de los datos introducidos en BDNS
- Utilización de IA generativa: grandes modelos de lenguaje o LLM comerciales en la nube
- Resultado inicial muy prometedor, pero económicamente no viable. Hay que explorar otras alternativas: otros modelos LLM, ejecución on-premise, …

Aplicación de IA generativa al soporte

- Dos ensayos con los sistemas BDNS y CoFFEE
- Alimentación de un sistema LLM con todos los documentos de soporte: guías, manuales de usuario, …
- Objetivo: Respuesta a consultas de soporte de los usuarios
- Dificultad de adaptar o corregir las respuestas incorrectas
- Imposibilidad de condicionar una respuesta homogénea

Preguntas
&
Gracias por su atención

Aplicación de IA en el ámbito del control de subvenciones en la IGAE

Ismael García Cebada
Director de la Oficina de Informática Presupuestaria
Intervención General de la Administración del Estado

Seminario de Gestión Económica Local
Federació de Municipis de Catalunya
25 de abril de 2025

4a sessió

16/05/25

LA IMPORTÀNCIA DE LA CIBERSEGURETAT PEL CONTROL INTERN I LA TRESORERIA DELS ENS LOCALS

Governança de la ciberseguretat, anàlisi de riscos i control intern.
Antonio Minguillón Roy, director del Gabinet Tècnic de la Sindicatura de Comptes de la Comunitat Valenciana.

Ciberseguretat en les transaccions bancàries i la gestió d'avals.
José Manuel Farfan Pérez, tresorer de la Diputació de Sevilla.

TAULA RODONA
Antonio Minguillón Roy, director del Gabinet Tècnic de la Sindicatura de Comptes de la Comunitat Valenciana.
José Manuel Farfan Pérez, tresorer de la Diputació de Sevilla.

SEMINARI
Gestió Econòmica Local 16 de maig de 2025

FMC

La importància de la ciberseguretat pel control intern i la tresoreria dels ens locals

Governança de la ciberseguretat, anàlisi de riscos i control intern.

Antonio Minguillón Roy

Auditor Director del Gabinete Técnico
de la Sindicatura de Comptes de la Comunitat Valenciana

1

La Sindicatura de Comptes de la CV y la Unidad de Auditoría de Sistemas de Información (UASI)

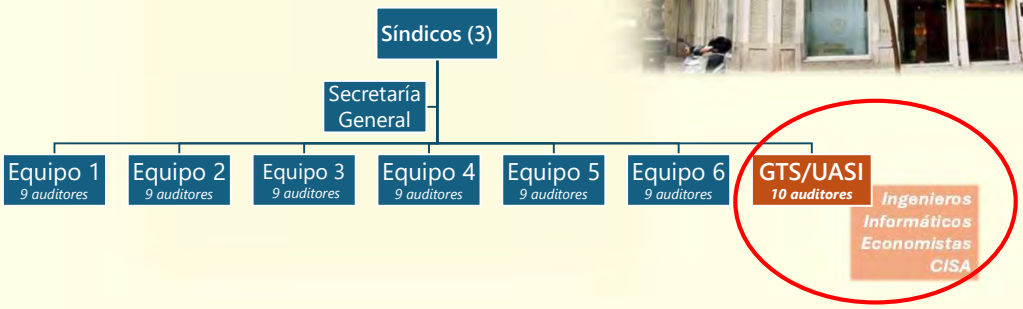
2

2

Quiénes somos

Sindicatura de Cuentas de la Comunidad Valenciana

Creada en 1986
actualmente tiene +100 empleados



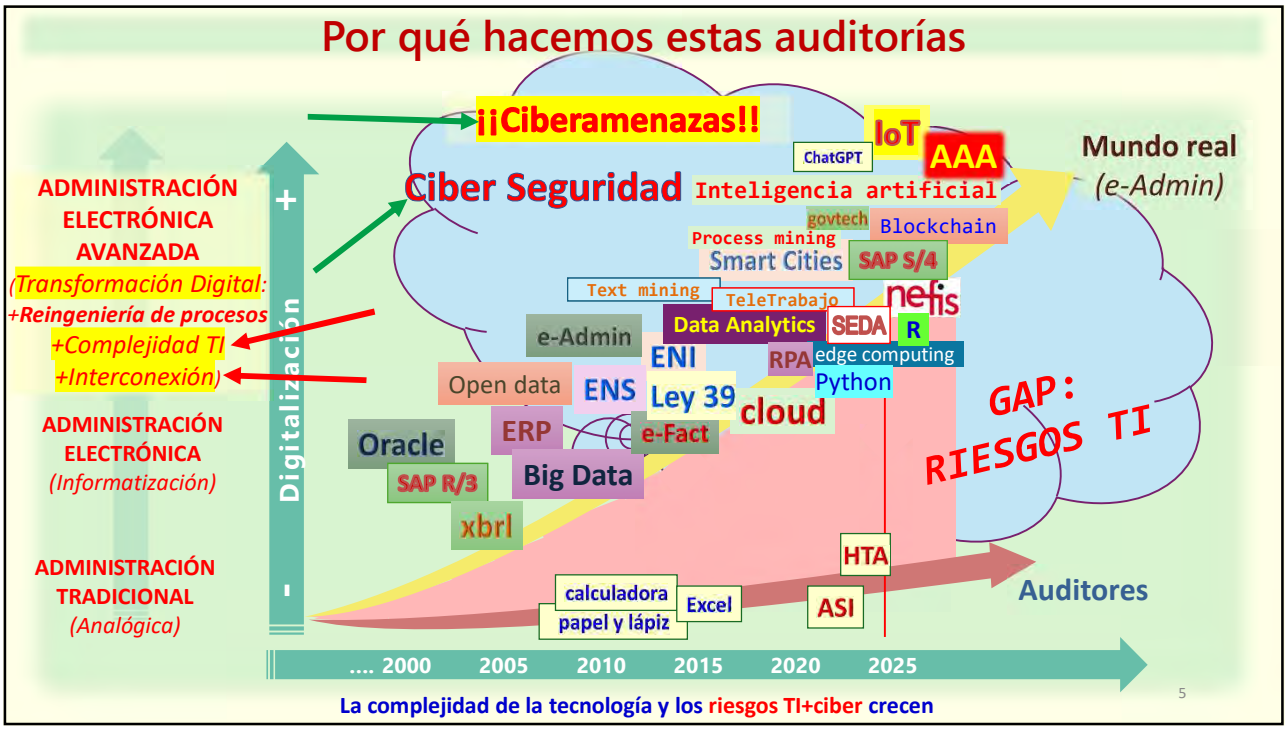
3

Qué hacemos

- Asistencia en las auditorías financieras, de cumplimiento y operativas (50%):
  - ✓ Revisión de procesos automatizados, evaluación de riesgos TI, identificación y pruebas de CGTI y CPI.
  - ✓ Pruebas masivas de datos.
- Realizamos nuestras propias auditorías:
  - ✓ Ciberseguridad *(>50 informes)*.
  - ✓ Auditorías de control interno, CGTI y CPI *(>30 informes)*.
  - ✓ Gestión de grandes proyectos TI *(3 informes)*.
- Promover el desarrollo de metodología de auditoría en entornos de Administración Electrónica Avanzada:
  - ✓ Comisión Técnica de Auditoría de la Sindicatura
  - ✓ Comisión Técnica OCEX

4

4


Por qué hacemos estas auditorías
¡¡Ciberamenazas!!
Ciber Seguridad
IoT
AAA
ChatGPT
Inteligencia artificial
Mundo real
(e-Admin)
govtech
Blockchain
Process mining
Smart Cities
SAP S/4
Text mining
TeleTrabajo
nefis
Data Analytics
SEDA
R
e-Admin
ENI
RPA
edge computing
Python
Open data
ENS
Ley 39
cloud
GAP:
RIESGOS TI
ERP
e-Fact
Oracle
SAP R/3
Big Data
xbrl
HTA
Auditores
calculadora
Excel
papel y lápiz
ASI
.... 2000
2005
2010
2015
2020
2025
ADMINISTRACIÓN ELECTRÓNICA AVANZADA
(Transformación Digital:
+Reingeniería de procesos
+Complejidad TI
+Interconexión)
ADMINISTRACIÓN ELECTRÓNICA
(Informatización)
ADMINISTRACIÓN TRADICIONAL
(Analógica)
Digitalización
+
-
La complejidad de la tecnología y los riesgos TI+ciber crecen
5

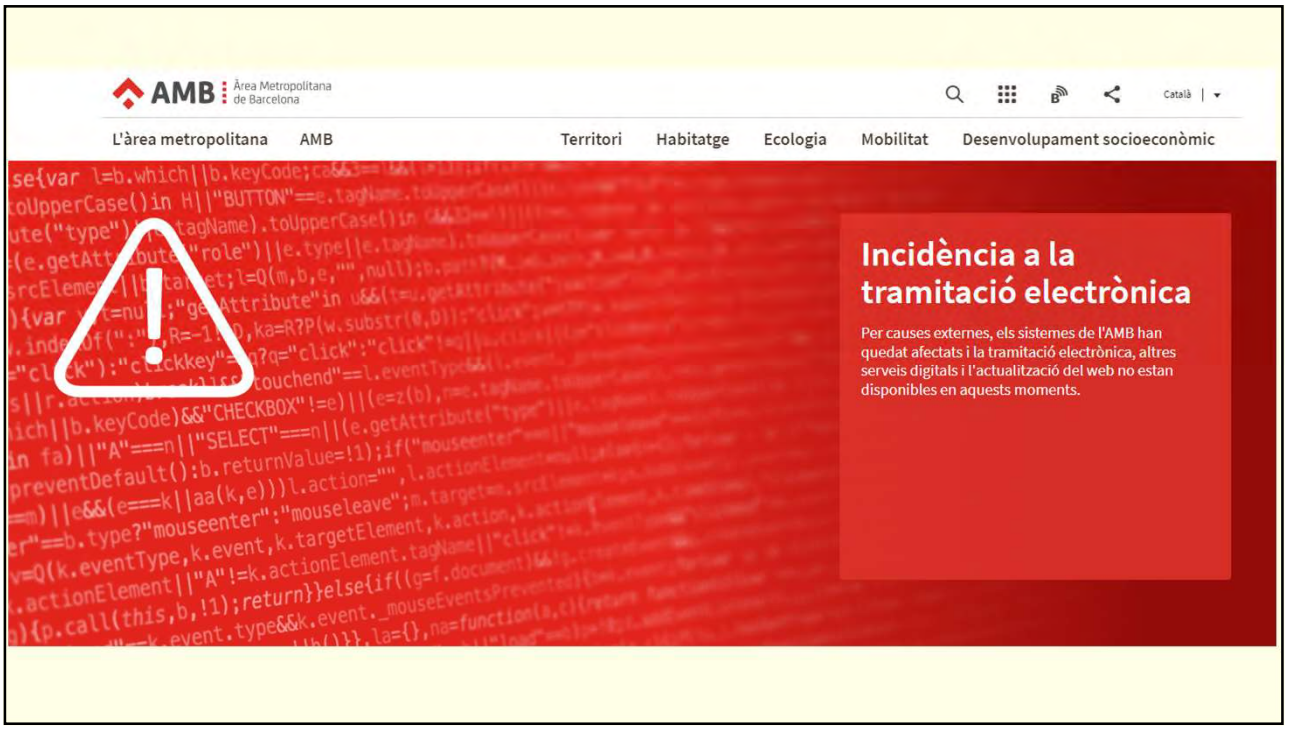
5


¿Dónde nos podemos encontrar riesgos de errores e irregularidades en la gestión de la tesorería?
Contabilidad
Gestión del gasto
Gestión del ingreso
Elaboración de Presupuestos
Tesorería
FMT
Fichero Maestro de Terceros
BANCOS
BANCOS

6

¿Por qué es tan importante la Ciberseguridad?

7



8

Los retos tecnológicos de la gestión del sector público
La ciberseguridad

El éxito de la transformación digital depende, en gran medida, de garantizar los requisitos mínimos de seguridad protegiendo la información tratada y los servicios prestados, elementos consustanciales al desarrollo de nuestra sociedad.

9

9

Qué es la ciberseguridad
(una definición sencilla)

Todos las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas

de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas

REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»)

La ciberseguridad según el ENS

La **Directiva 2016/1148 de Ciberseguridad** define la *seguridad de las redes y sistemas de información* (es decir la ciberseguridad) como la *capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la* ***disponibilidad, autenticidad, integridad*** *o* ***confidencialidad*** *de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.*

correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

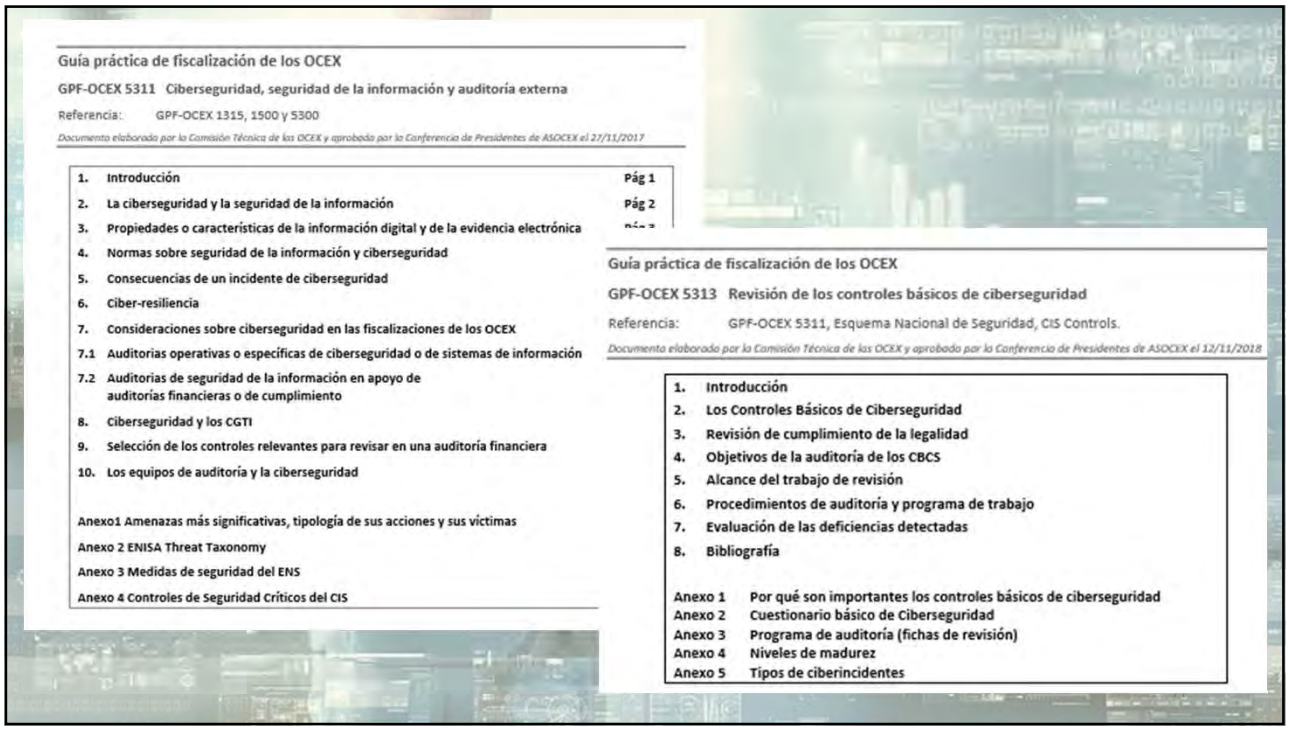
Esta definición es coincidente con la del **ENS**, que contempla además las **características fundamentales de la información** que la ciberseguridad **debe garantizar.**
Junto con la **trazabilidad** forman las **5 dimensiones de la seguridad de la información.**

Características / dimensiones de la seguridad

- La **disponibilidad** trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
  Actúa sobre la no interrupción del servicio (p.ej. Intenta evitar que la Web corporativa, perfil de contratante o algunos trámites electrónicos en la sede dejen de funcionar y no estén accesibles a través de internet.)
- La **confidencialidad** es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
  Previene la filtración de información (p.ej. Gestionar el acceso a determinado tipo de información.)
- La **integridad** es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.
  Previene manipulaciones de la información (p.ej. Disponer de documentos que han sido firmados de forma electrónica, asegurar la fecha de publicación de un documento en la sede electrónica, etc.)
- La **autenticidad** es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.
Previene manipulaciones de la información (p.ej. Disponer de documentos que han sido firmados de forma electrónica, asegurar la fecha de publicación de un documento en la sede electrónica, etc.)
- La **autenticidad** es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
  Protege el aseguramiento de la identidad (p.ej. La identidad de la persona que ha firmado un documento, quién se ha conectado a través de una red WIFI, etc.)
- La **trazabilidad** es la propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.
  - *Permite conocer posibles rastros en accesos (p.ej. sistema de registro de accesos por parte de usuario, análisis de posibles fugas de datos, intrusión a sistemas de ataques externos, etc.)*

10



11

Resultado de las auditorías de ciberseguridad en las entidades locales

Ayuntamiento	Población 2021	ORN 2021
València	789.744	956,5
Alicante/Alacant	337.304	263,8
Elche/Elx	234.205	202,9
Castelló de la Plana	172.589	178,7
Torrent	84.025	63,0
Torrevieja	82.842	108,7
Orihuela	78.940	81,1
Gandia	75.970	95,8
Paterna	71.361	63,6
Benidorm	69.118	103,5
Sagunto/Sagunt	67.043	75,3
Alcoy/Alcoi	59.128	58,5
San Vicente del Raspeig/Sant Vicent del Raspeig	58.912	41,1
Elda	52.551	42,7
Vila-real	51.130	53,8
Ayuntamientos auditados	**2.284.862**	**2.389,0**
Población de la Comunitat Valenciana	**5.058.138**	**5.288,4**
Cobertura de la auditoría	**45,2%**	**45,2%**

12

12

GPF-OCEX 5330 CGTI

Categorías de controles	Controles principales	Medidas del ENS
A. Gobernanza	A.1 Gobernanza sobre las TI	org, mp.per
	A.2 Cumplimiento normativo (CBCS 8)	
	A.3 Gobernanza de la ciberseguridad	org, mp.per
B. Gestión de cambios en aplicaciones y sistemas	B.1 Adquisición de aplicaciones y sistemas	op.pl.3 y 4
	B.2 Desarrollo de aplicaciones	mp.sw.1 y 2
	B.3 Gestión de cambios	op.exp.5, op.acc.3
C. Operaciones de los sistemas de información	C.1 Inventario de hardware y software (CBCS 1 y 2)	op.exp.1
	C.2 Gestión de vulnerabilidades (CBCS 3)	op.exp. 3 y 4
	C.3 Configuraciones seguras (CBCS 5)	op.exp.2, 3 y 4
	C.4 Registro de eventos y de la actividad de los usuarios (CBCS 6)	op.exp.8
	C.5 Servicios externos	op.ext.1 y 2 y nub.1
	C.6 Protección del entorno de TI	op.exp.6, mp.s, mp.eq
	C.7 Protección de las instalaciones e infraestructuras	mp.if
	C.8 Gestión de incidentes	op.exp.7 y 9
	C.9 Monitorización del sistema y su seguridad	op.mon
	C.10 Protección de las comunicaciones	op.pl.2, mp.com, op.ext.4
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios de administración (CBCS 4)	op.acc.
	D.2 Gestión de usuarios	
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas (CBCS 7)	mp.info.6
	E.2 Plan de continuidad	op.cont.2 y 3 op.ext.3
	E.3 Alta disponibilidad	op.cont.4

13

Controles básicos de ciberseguridad

Control		Objetivo de control	Medidas de seguridad del ENS
CBCS 1	Inventario y control de dispositivos físicos	Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.	op.exp.1
CBCS 2	Inventario y control de software autorizado y no autorizado	Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado.	op.exp.1 op.exp.2
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.	mp.sw.2 op.exp.4
CBCS 4	Uso controlado de privilegios administrativos	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.	op.acc.4 op.acc.5
CBCS 5	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	Implementar la configuración de seguridad de dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarla activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir que los atacantes exploten servicios y configuraciones vulnerables.	op.exp.2 op.exp.3
CBCS 6	Registro de la actividad de los usuarios	Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.	op.exp.8 op.exp.10
CBCS 7	Copias de seguridad de datos y sistemas	Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.	mp.info.9

14

Controles básicos de ciberseguridad

Control de legalidad		Objetivo de cumplimiento	Medidas de seguridad del ENS
CBCS 8	**Cumplimiento del ENS**	• Política de seguridad y responsabilidades • Declaración de aplicabilidad • Informe de Auditoría (nivel medio o alto) • Informe del estado de [illegible]	Org1 Art 27.4 Art.34 Art.35 Art.41
	Cumplimie LOPD/RGP		--
	Cumplimie Ley 25/201 de diciembre *(Impulso de la factura electrónica y creación del registro contable de facturas)*	• Informe de auditoría de sistemas anual del Registro Contable de Facturas	--

Gobernanza de la ciberseguridad

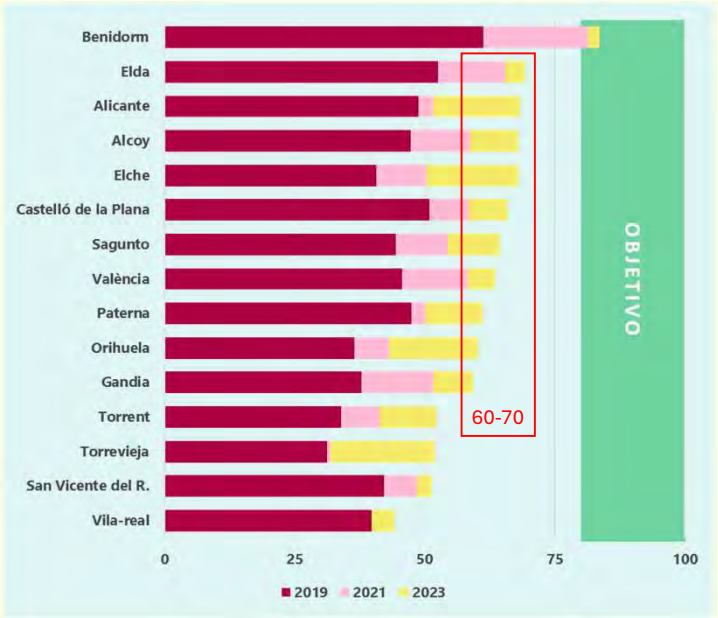
15

Metodología de evaluación: ejemplo modelo de madurez

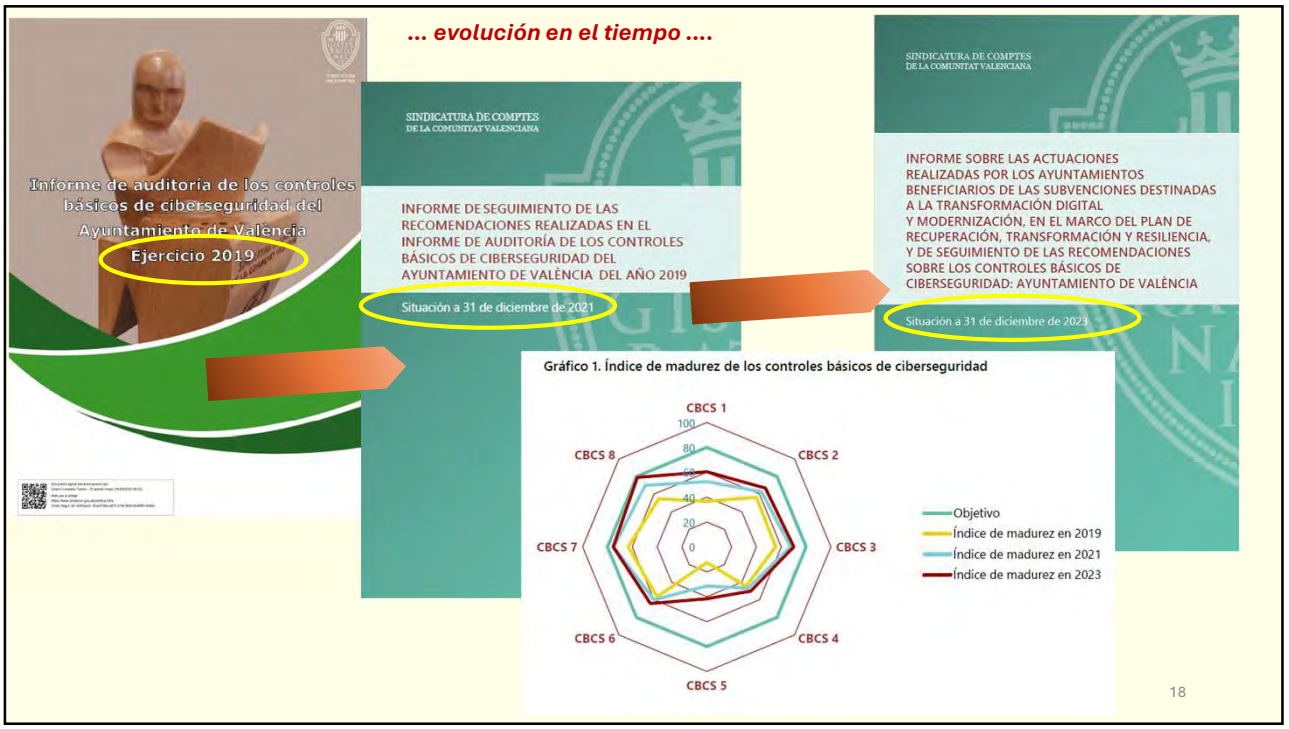
NIVEL DE MADUREZ	N/A	N0 *Inexistente*	N1 *Inicial / ad hoc*	N2 *Repetible, pero intuitivo*	N3 *Proceso definido*	N4 *Gestionado y medible*	N5 *Optimizado*
Índice de madurez	--	**0 - 10%**	**10% - 50%**	**50% - 80%**	**80% - 90%**	**90% - 100%**	**100%**
Descripción	N/A	**El CBCS no está siendo aplicado en este momento.**	**El proceso existe, pero no se gestiona.** **El enfoque general de gestión no es organizado.**	**Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas.** **No hay procedimientos escritos ni actividades formativas.**	**Los procesos están estandarizados, documentados y comunicados con acciones formativas.**	**La Dirección controla y mide el cumplimiento con los procedimientos y adopta medidas correctoras cuando se requiere.**	**Se siguen buenas prácticas en un ciclo de mejora continua.**
Ejemplo	No hay interconexión	Hay que poner un cortafuegos y no está puesto.	Ponemos el cortafuegos y nos olvidamos de él.	Revisamos el cortafuegos cuando nos sobra un rato.	Revisión del cortafuegos de forma planificada y sistemática. Existe un procedimiento	¿Es eficaz el procedimiento empleado con el cortafuegos?	Optimizamos el proceso de revisión del cortafuegos.

16

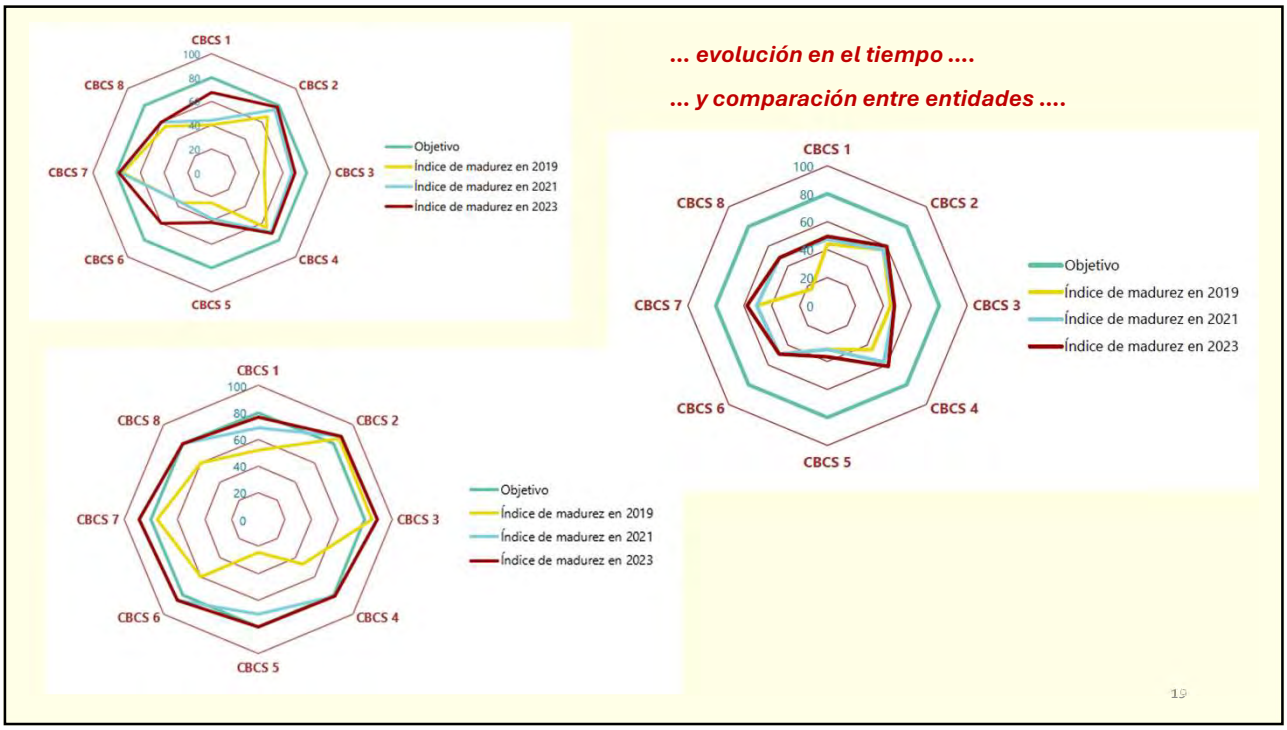
Índice de Madurez de los CBCS de los 15 mayores ayuntamientos de la CV



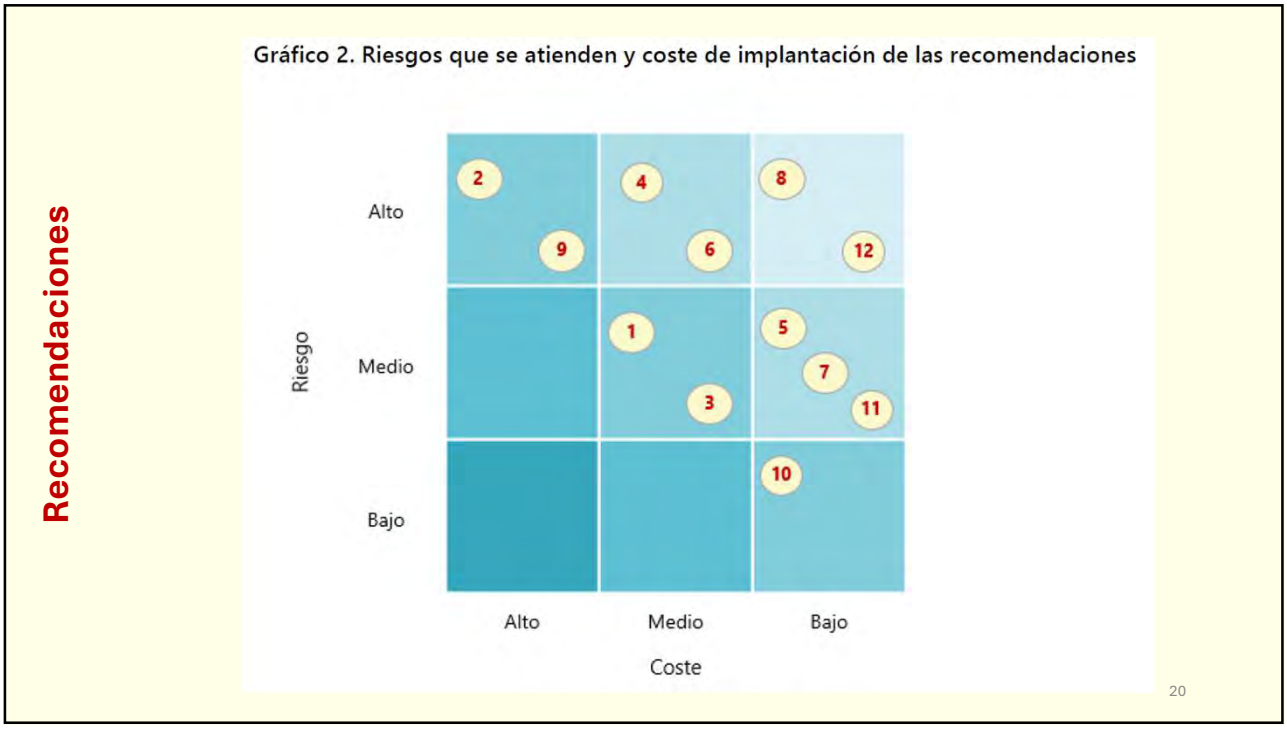
17



18


... evolución en el tiempo ....
... y comparación entre entidades ....
CBCS 1
CBCS 2
CBCS 3
CBCS 4
CBCS 5
CBCS 6
CBCS 7
CBCS 8
100
80
60
40
20
0
Objetivo
Índice de madurez en 2019
Índice de madurez en 2021
Índice de madurez en 2023
19

19


Recomendaciones
Gráfico 2. Riesgos que se atienden y coste de implantación de las recomendaciones
Riesgo
Alto
Medio
Bajo
Coste
Alto
Medio
Bajo
2
4
8
9
6
12
1
5
7
3
11
10
20

20

Análisis de resultados de las auditorías de otros OCEX

CONSEJO DE CUENTAS DE CASTILLA Y LEÓN

Ayuntamiento	Índice de madurez
Salamanca	63,2%
Burgos	54,3%
Valladolid	53,6%
Palencia	51,8%
León	37,6%
Ávila	34,5%
A	*39,4%*
B	*19,9%*
C	*17,8%*
D	*16,3%*
E	*11,4%*
F	*4,9%*
G	*3,0%*

< 20.000 habitantes

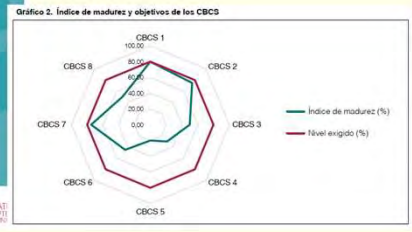
80% ens Esquema Nacional de Seguridad

21

Análisis de resultados de las auditorías de otros OCEX

SINDICATURA DE COMPTES DE CATALUNYA

Ayuntamiento	Índice de madurez
Badalona	51,4%
Mataró	53,1%
Santa Coloma	57,2%



80% ens Esquema Nacional de Seguridad

22

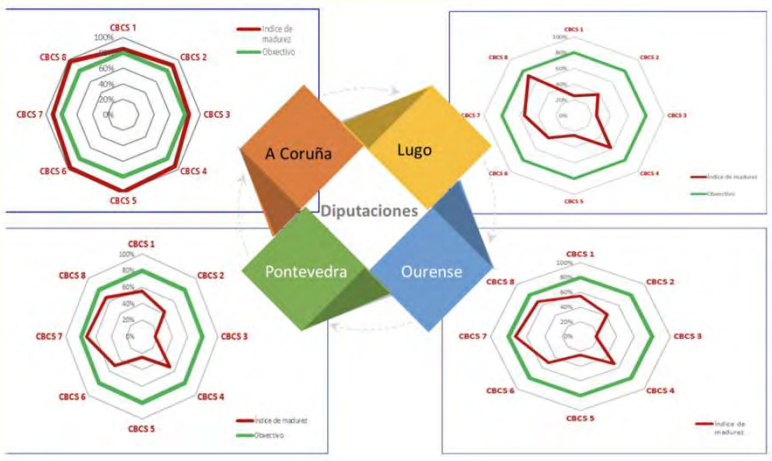
Análisis de resultados de las auditorías de otros OCEX

Consello de Contas de Galicia

80%

ens Esquema Nacional de Seguridad

Diputación	Índice de madurez
La Coruña	92%
Pontevedra	53%
Orense	48%
Lugo	42%
Ayuntamiento	**Índice de madurez**
La Coruña	56%
Orense	50%
Vigo	57%



23

CUARTA CONCLUSIÓN

Las entidades auditadas, en general, no tienen establecida una adecuada gobernanza de la ciberseguridad, tal como exigen tanto la normativa como un sistema de control interno bien establecido.

Los órganos superiores de las entidades (alcalde o alcaldesa en el caso de los ayuntamientos; presidente o presidenta en el caso de las diputaciones) son los **responsables** de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones, y su implicación, compromiso y liderazgo constituyen, posiblemente, el factor más importante para la implantación exitosa de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad. Se debe actuar de manera urgente para solventar las carencias identificadas en esta materia en cada una de las entidades, ya que afectan de manera negativa al estado de su ciberseguridad.

24

24

La Gobernanza de la Ciberseguridad

25

25

Qué es la gobernanza de ciberseguridad

Es el proceso de establecer y mantener un marco de referencia, y apoyar la estructura y los procesos de gestión para garantizar la *confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los datos*.

26

26

12.m

NIA-ES 315 Revisada: Componentes del sistema de control interno

RECORDEMOS

(i) el entorno de control;

(ii) el proceso de valoración del riesgo por la entidad;

(iii) el proceso de la entidad para el seguimiento del sistema de control interno;

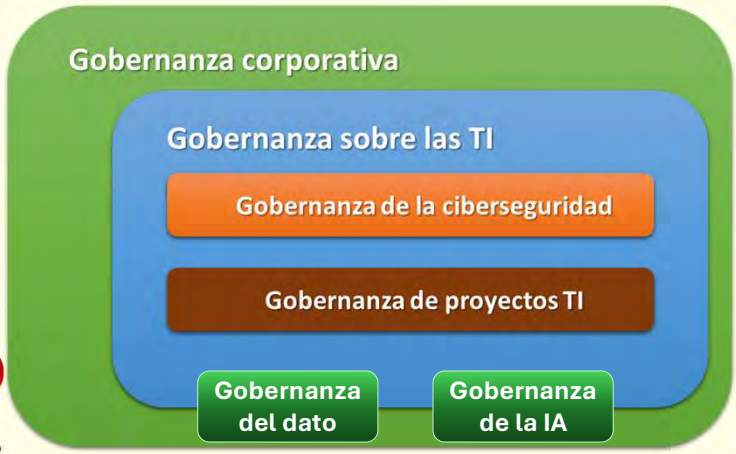
(iv) el sistema de información y comunicación; y

(v) las actividades de control.

27

La Gobernanza, primer componente de un sistema de control interno (COSO)

La Gobernanza TI es un componente esencial de la Gobernanza corporativa



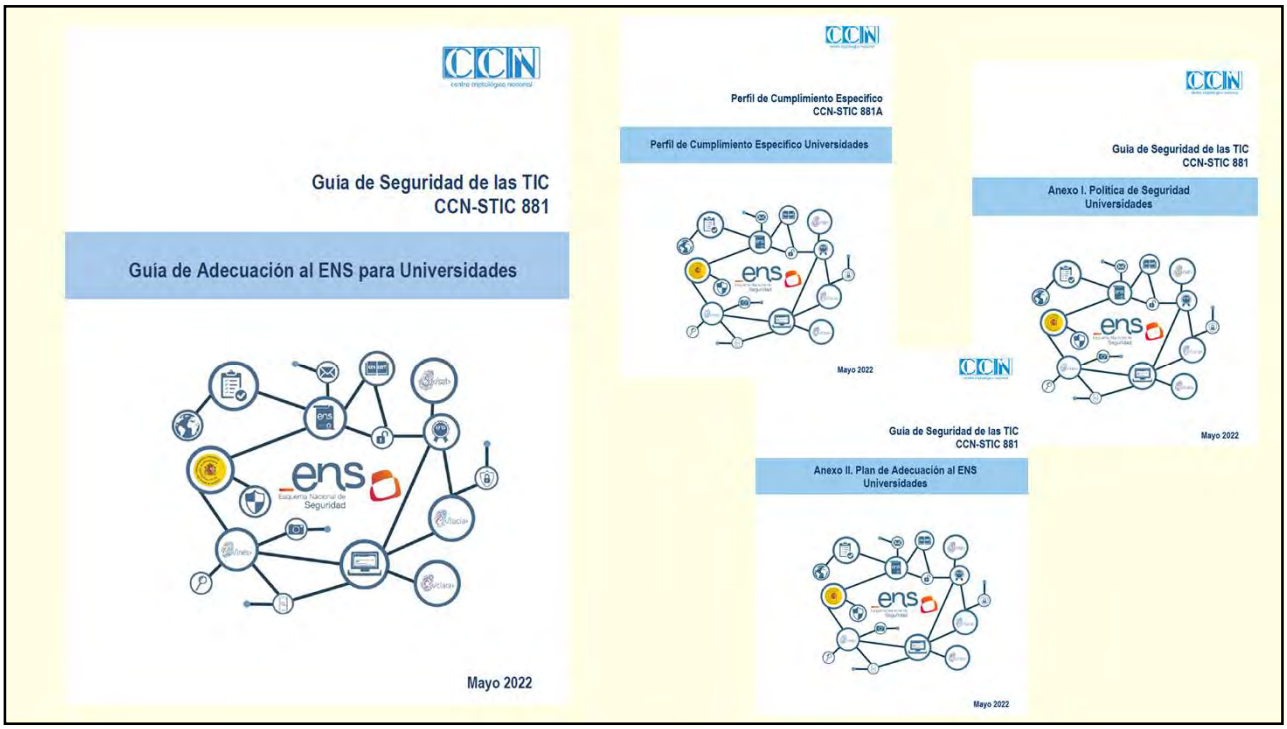
Las normas de auditoría (NIA-ES-SP) requieren que el auditor conozca este primer componente del sistema de control interno

La Gobernanza de la ciberseguridad, a su vez, es un componente esencial de la Gobernanza TI

28


APROXIMACIÓN AL MARCO DE GOBERNANZA DE LA CIBERSEGURIDAD
CCN
Año 2022
Prontuario de ciberseguridad para entidades locales
CICLO ENERO 2022
Guía de Seguridad de las TIC
CCN-STIC 883
Guía de Implantación del ENS para EELL
ens
Mayo 2020
SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA
INFORME DE SÍNTESIS DE LAS AUDITORÍAS DE CIBERSEGURIDAD DE LOS QUINCE MAYORES AYUNTAMIENTOS Y DE LAS TRES DIPUTACIONES DE LA COMUNITAT VALENCIANA
Ejercicio 2021
ÍNDICE (con hipervínculos)
1. Introducción 3
2. Objetivos, alcance y metodología de las auditorías 5
3. Conclusiones generales 10
4. Recomendaciones 17
Apéndice 1. Metodología aplicada 20
Apéndice 2. La gobernanza de la ciberseguridad 32
Apéndice 3. Situación de los controles básicos de ciberseguridad 51
Acrónimos y glosario de términos 77
CUARTA CONCLUSIÓN
Las entidades auditadas, en general, no tienen establecida una adecuada gobernanza de la ciberseguridad, tal como exigen tanto la normativa como un sistema de control interno bien establecido.

29


Guía de Seguridad de las TIC
CCN-STIC 881
Guía de Adecuación al ENS para Universidades
ens
Mayo 2022
Perfil de Cumplimiento Específico
CCN-STIC 881A
Perfil de Cumplimiento Específico Universidades
Mayo 2022
Guía de Seguridad de las TIC
CCN-STIC 881
Anexo I. Política de Seguridad Universidades
Mayo 2022
Guía de Seguridad de las TIC
CCN-STIC 881
Anexo II. Plan de Adecuación al ENS Universidades
Mayo 2022

30

Ejemplo: Modelo de gobernanza de la ciberseguridad en las universidades

CCN-STIC-881 Guía CCN-STIC 881 - Adecuación al ENS para Universidades

ÍNDICE

31

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría

Referencia: GPF-OCEX 1315 (Revisada) y GPF

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 19

1. Gobernanza y normas de auditoría
2. Por qué es importante para el auditor co entidad, incluida la gobernanza sobre las
3. Qué debe entenderse por gobierno de la
4. Qué es la gobernanza sobre las TI
5. Elementos clave de la gobernanza sobre
6. Riesgos asociados a una gobernanza sobi
7. Cómo puede el auditor evaluar si existe u
8. Bibliografía

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría

Referencia: GPF-OCEX 1315 (Revisada), GPF-OCEX 5330, GPF-OCEX 5331 y GPF-OCEX 5313

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 19/10/2023.

1. Qué es la gobernanza de la ciberseguridad
2. Por qué es importante la gobernanza de la ciberseguridad para una entidad
3. Por qué es importante la gobernanza de la ciberseguridad para el auditor
4. Responsables del establecimiento de una adecuada gobernanza de ciberseguridad
5. Elementos de la gobernanza de la ciberseguridad
6. Modelo de gobernanza
7. El comité de seguridad TIC
8. Roles en materia de seguridad de la información
9. Normativa interna de ciberseguridad
10. Otros órganos de gobierno relacionados con la gestión de la ciberseguridad
11. Posibles deficiencias en materia de gobernanza
12. Cómo puede el auditor evaluar si existe una adecuada gobernanza de la ciberseguridad
13. Bibliografía

Anexo: Programa/cuestionario para la evaluación de la gobernanza de la ciberseguridad

32

Responsabilidad de los órganos de gobierno y dirección

Los órganos de gobierno y dirección de la entidad son los responsables de preparar las cuentas anuales de conformidad con el marco de información financiera aplicable y de diseñar e implementar los controles internos necesarios para ello.

También son los responsables de contar con un proceso de gestión de riesgos con objeto de identificar riesgos, incluidos los de ciberseguridad, valorarlos e implementar y supervisar los controles internos para responder a esos riesgos.

33

33

La gobernanza de ciberseguridad: responsables

La responsabilidad sobre dicho proceso es de los órganos superiores de la Entidad, que, en el caso de las entidades locales, corresponde a su presidente y a la junta de gobierno.

Son los responsables de garantizar que el funcionamiento de la organización resulte conforme con las normas aplicables y de que existan unos adecuados controles sobre los sistemas de información y las comunicaciones.

Es más que una mera cuestión técnica, exige un liderazgo efectivo, procesos sólidos y estrategias en consonancia con los objetivos de la organización.

La responsabilidad de la ejecución de las actividades establecidas por la alta dirección corresponde a la dirección ejecutiva.

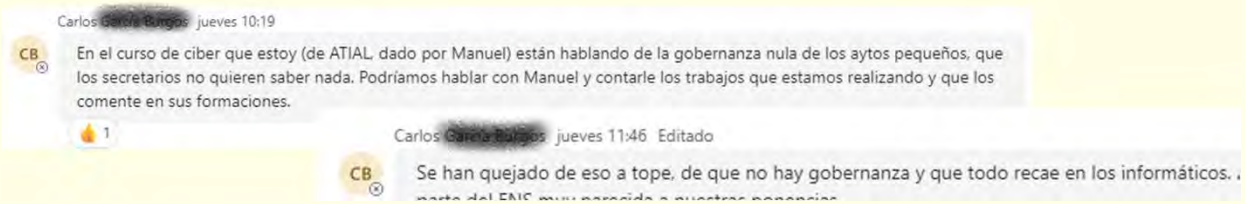
34

34

La ciberseguridad NO es “algo de los informáticos”

Sin embargo, en la práctica, de forma general, se ha asumido de manera errónea que la responsabilidad de la seguridad de la información y los servicios, materializada en el cumplimiento de ENS, recae en exclusiva sobre los responsables de las áreas TIC, incurriendo en un grave error de criterio.

Los responsables de las áreas informáticas son los responsables de la gestión de los sistemas, que es incompatible con la responsabilidad sobre la seguridad de la información.



35

Elementos de la gobernanza de ciberseguridad

- **Los órganos superiores de la entidad deben ejercer liderazgo y compromiso** con respecto a la seguridad de la información y deben velar por que sean satisfechas todas necesidades y condiciones necesarias para el establecimiento de una gobernanza adecuada.
- Debe formularse la **política de seguridad de la información (PSI), que debe ser aprobada por el por el titular del órgano competente**. Dicha PSI debe ser **difundida** entre la totalidad de los miembros de la organización.
- Debe existir un **comité de seguridad de la información** con un **funcionamiento efectivo**.
- Las entidades deben asignar **roles y responsabilidades en materia de seguridad de la información**.
- Deben existir **normas y procedimientos de seguridad formalizados y debidamente aprobados y deben ser de aplicación obligatoria en todos los sistemas de información de la entidad sin excepción.** Esta normativa interna debe diseñarse para ser aplicada, no para cumplir una formalidad.

36

36

Elementos de la gobernanza de ciberseguridad

- La entidad debe **disponer de los recursos materiales y humanos** adecuados para atender a las necesidades identificadas e implementar las medidas de seguridad necesarias. El mantenimiento actualizado y la mejora de los controles de ciberseguridad requerirá de actuaciones e inversiones, tanto en medios materiales como personales, que deben ser adecuadamente planificadas.
- Se debe establecer una **cultura en materia de ciberseguridad** que afecte a todos los niveles de la organización. Dicha cultura de ciberseguridad debe ser impulsada por la dirección en forma de planes estratégicos que definan objetivos y medidas concretas, además de incluir **planes periódicos de formación y concienciación** de los trabajadores.
- Debe existir una **planificación estratégica en materia de ciberseguridad**. La planificación estratégica de la seguridad evita una gestión reactiva basada principalmente en necesidades sobrevenidas.
- Atendiendo al **principio de proporcionalidad** deberá existir una **OT de Seguridad** y un **CoCS**.
- **Auditorías de seguridad OBLIGATORIAS.**

37

37

Elementos de la gobernanza: el comité de seguridad TIC

- **Es un elemento esencial de un SGSI.**
- **La gobernanza se articula a través de un CS-TIC, que se constituye como un órgano colegiado.**
- **Debe tener un funcionamiento regular y efectivo, no es una mera formalidad.**
- **Abarca y afecta a toda la organización.**
- **No es un comité técnico.**

38

38

Elementos de la gobernanza:
Normas y procedimientos de seguridad

La PSI de la entidad debe desarrollarse mediante:

Normas de seguridad: Uniforman el uso de aspectos concretos del sistema, indican el uso correcto y las responsabilidades de los usuarios.

Son de carácter obligatorio y describirán:

a) **el uso correcto de equipos, servicios e instalaciones;**
b) **lo que se considerará uso indebido, y**
c) **la responsabilidad del personal con respecto al cumplimiento o violación de estas normas.**

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones; como regla general, estará disponible en la intranet corporativa de la entidad a través de una dirección URL. La normativa de seguridad de cada entidad trae causa y recibe su autoridad ejecutiva de lo preceptuado en el ENS, en primera instancia, y del desarrollo normativo de la PSI de la entidad.

39

39

Elementos de la gobernanza:
Normas y procedimientos de seguridad

La PSI de la entidad debe desarrollarse mediante:

Procedimientos de seguridad: Abordan tareas concretas, indicando lo que hay que hacer, paso a paso.

Detallan de forma clara y precisa:

a) **cómo llevar a cabo las tareas habituales,**
b) **quién debe hacer cada tarea y**
c) **cómo identificar y reportar comportamientos anómalos.**

Las NyP deben estar "aterrizadas", no ser algo teórico.

Las Normas y Procedimientos de seguridad deben estar formalmente aprobadas. ¿Quién debe/puede aprobarlas?

40

40

Deficiencias frecuentes en materia de gobernanza

En materia de normativa de seguridad

- Inexistencia de PSI formalmente aprobada por la corporación, o desactualizadas o no adaptadas a la realidad de las entidades, lo que impide que los principios que deben regir las actuaciones en materia de seguridad sean conocidos por toda la corporación.
- Inexistencia de normativa y procedimientos formalizados y/o no actualizados o que no representan con fidelidad los procesos de seguridad que describen lo que puede originar el riesgo de no realización de tareas importantes.
- El contenido de los procedimientos no detalla de manera clara y precisa las tareas a realizar ni quiénes son los responsables de ejecutarlas, especificando únicamente el deber de realizar la acción, aspecto que corresponde a las normas de seguridad de rango superior, lo que genera procedimientos ineficaces.

41

41

Deficiencias frecuentes en materia de gobernanza

En relación con el comité de seguridad de la información

- Existen entidades que no disponen de comité de seguridad de la información, órgano imprescindible para coordinar la seguridad de la información en la entidad.
- En otros casos, aunque el comité de seguridad de la información está formalmente constituido, no se reúne o no lo hace la periodicidad necesaria, lo que impide hacer un seguimiento del estado de la seguridad de la información del Ayuntamiento y tomar las decisiones pertinentes de forma oportuna.
- El comité de seguridad no dispone de los miembros adecuados, estando compuesto únicamente de miembros con cargos relacionados con las TI.

  La ausencia de miembros con el más alto poder de decisión en la organización y de vocales de las áreas significativas, convierte al comité en un órgano meramente técnico e impide un gobierno eficiente y la toma de decisiones estratégicas a nivel corporativo.

42

42

Deficiencias frecuentes en materia de gobernanza

En relación con los roles de seguridad

- Existen entidades que no han asignado los roles y responsabilidades en materia de seguridad de la información.
- Existen entidades que no disponen de un delegado de protección de datos formalmente nombrado.
- Algunos de los roles se seguridad no ejercen sus funciones de manera que se garantice la necesaria independencia y la ausencia de conflicto de intereses.
- Algunos roles en materia de seguridad no disponen de la dedicación suficiente para las necesidades de la entidad. Los responsables de seguridad de manera general no ejercen sus funciones de manera exclusiva, incurriendo en una acumulación de competencias no directamente relacionadas con la seguridad de la información que impide que desarrollen sus funciones de forma efectiva.

43

43

Deficiencias frecuentes en materia de gobernanza

En relación con el liderazgo y el compromiso con la ciberseguridad

- La falta de una cultura de ciberseguridad en la entidad, materializada en acciones formativas y campañas de concienciación dirigidas a los empleados.
- Inexistencia de implicación de los máximos responsables de la organización.
- La ausencia de planes estratégicos desarrollados e impulsados por el más alto nivel de la corporación en los que se establezcan acciones, objetivos y medidas concretas para alcanzar los niveles de seguridad exigidos por la normativa.
- Falta de comunicación o inadecuada comunicación de los procedimientos de seguridad y decisiones en materia de seguridad de la información al personal de la organización.
- La falta de recursos, tanto económicos como de personal, en los departamentos TIC, indispensable para implantar las medidas de seguridad necesarias y llevar a cabo proyectos transversales que afecten a toda la organización.

44

44

La gobernanza de ciberseguridad: ejemplo de informe

El Ayuntamiento de Benidorm tiene establecida una aceptable gobernanza de la ciberseguridad y debe mantener el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información.

Los órganos superiores del Ayuntamiento (en particular el alcalde y la Junta de Gobierno) son los responsables de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones, y su implicación, compromiso y liderazgo constituyen, posiblemente, el factor más importante para la implantación exitosa de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad.

Hemos podido verificar la existencia de un adecuado nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento, junto con unos adecuados procesos de gestión. No obstante, es necesario que el comité de seguridad, como órgano colegiado, se reúna periódicamente con objeto de conocer el estado de la seguridad de la información del Ayuntamiento y tomar las decisiones convenientes. Todo ello nos permite afirmar que la gobernanza de ciberseguridad alcanza un nivel aceptable.

45

45

La gobernanza de ciberseguridad: ejemplo de informe

El Ayuntamiento de no tiene establecida una adecuada gobernanza de la ciberseguridad, situación que debe ser subsanada. Además, se debe reforzar el apoyo en forma de recursos humanos y presupuestarios dedicados a la seguridad de la información.

Los órganos superiores del Ayuntamiento (en particular el alcalde y la Junta de Gobierno) son los responsables de que existan unos controles adecuados sobre los sistemas de información y las comunicaciones, y su implicación, compromiso y liderazgo constituyen, posiblemente, el factor más importante para la implantación exitosa de un sistema de gestión de la seguridad de la información que garantice la ciberresiliencia de la entidad.

Hemos podido verificar la existencia de un insuficiente nivel de compromiso y concienciación con la ciberseguridad por parte de los órganos superiores del Ayuntamiento. Las carencias más relevantes identificadas son las siguientes:

- La falta de un marco normativo y procedimental formalmente aprobado, incluida la inexistencia de una política de seguridad de la información[2].
- La inexistencia de un comité de seguridad de la información, órgano imprescindible para coordinar la seguridad de la información en la entidad, que debe incluir representación de las áreas de la organización afectadas.
- La inexistencia, de determinados roles clave en la organización, como el responsable de seguridad de la información.

46

46

Conclusiones

95 Concluimos que la comu
(IOUE) no ha alcanzado un ni
trabajo demuestra que las IO
y, dado que suelen estar inte
privadas en los Estados mien
pueden exponer a otras a cib

III Constatamos que no siempre se aplicaban buenas prácticas esenciales de ciberseguridad, como algunos controles esenciales, y que los gastos en ciberseguridad en varias IOUE son insuficientes. En algunas IOUE tampoco existe una buena gobernanza de la ciberseguridad: en muchos casos, no existen estrategias de seguridad informática, o estas no están respaldadas por la alta dirección, las políticas de seguridad no siempre se formalizan y las evaluaciones de riesgos no abarcan todo el entorno informático. No todas las IOUE disponen de medi
ciberseguridad sujetas a una garantía independiente.

96 Constatamos que no siempre se aplicaban buenas prácticas, como algunos controles esenciales. Una buena gobernanza de ciberseguridad es esencial para la seguridad de los sistemas de información e informáticos, pero esta aún no aplica en algunas IOUE: en muchos casos, no existen estrategias y planes de seguridad informática o estos no están respaldados por la alta dirección, las políticas de seguridad no siempre se formalizan y las evaluaciones de riesgos no abarcan todo el entorno informático. El gasto en ciberseguridad es desigual, ya que algunas IOUE no gastan lo suficiente en comparación con homólogas de tamaño similar (véanse los apartados *21* a *33*, y *37* y *38*).

47

SEMINARI Gestió Econòmica Local

Federació de Municipis de Catalunya

¿Preguntas?

48

¿Cómo abordamos la revisión de riesgos y controles internos?

49

49

Responsabilidad del auditor en una auditoría financiera

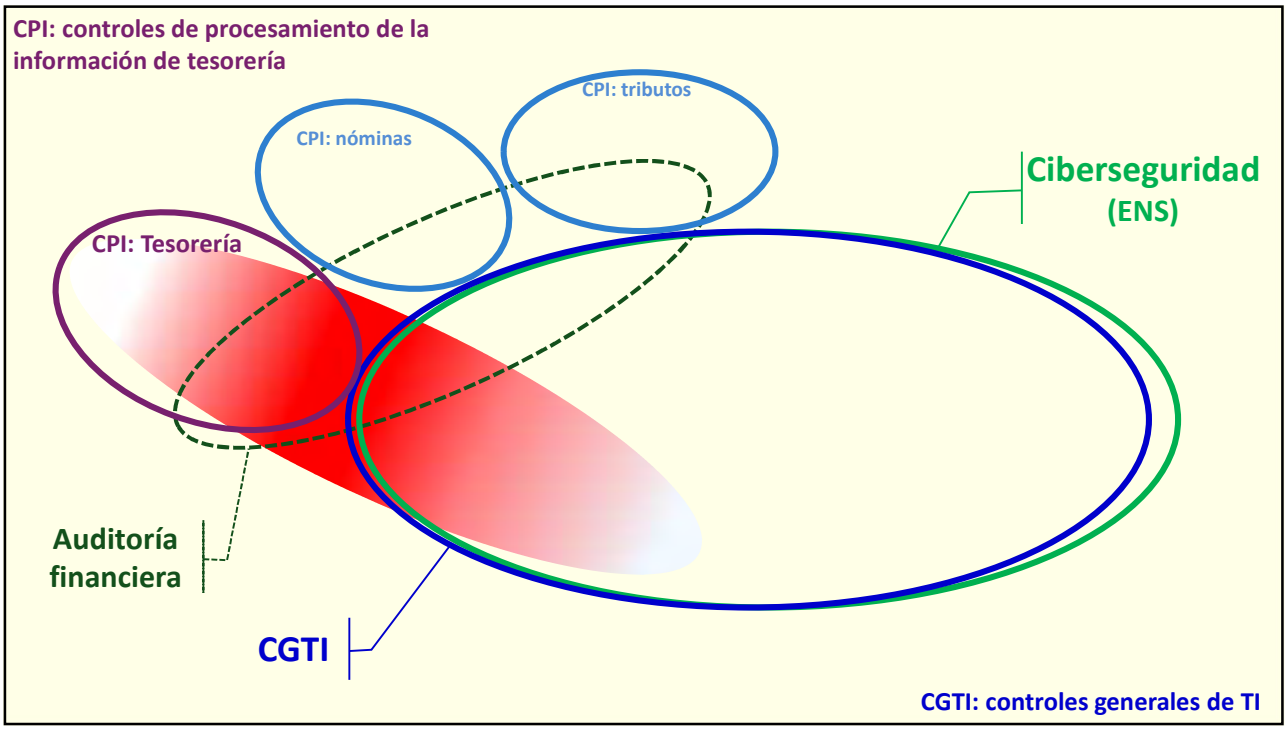
(NIA-ES 315R)

El auditor debe identificar y valorar los riesgos de incorrección material, debidos a fraude o error, tanto en los estados financieros como en las afirmaciones con la finalidad de proporcionar una base para el diseño y la implementación de procedimientos posteriores de auditoría en respuesta a los riesgos valorados de incorrección material de conformidad con la NIA-ES-SP 1330.

Entre los riesgos que debe identificar y valorar el auditor se encuentran los riesgos derivados de la utilización de las TI. (Dentro de estos, los riesgos de ciberseguridad adquieren cada vez mayor importancia y deben ser, por tanto, objeto de mayor atención por el auditor)**.**

50

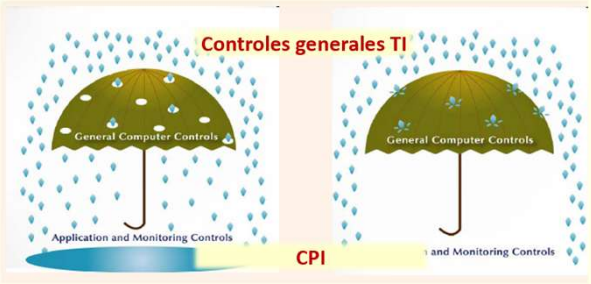
50



51

Revisión de los CGTI (*controles ciber*)

Si el auditor planea probar la eficacia operativa de un CPI automatizado,
será necesario probar la eficacia operativa de los CGTI relacionados que sustentan su funcionamiento continuo y eficaz.



Si no existieran CGTI o no fueran efectivos, no se podría confiar en los CPI y sería necesario adoptar un enfoque de auditoría basado exclusivamente en procedimientos sustantivos.

52

Categorías de controles	Controles principales	Medidas del ENS
A. Gobernanza	A.1 Gobernanza sobre las TI A.2 Cumplimiento normativo (CBCS 8) A.3 Gobernanza de la ciberseguridad	org, mp.per org, mp.per
B. Gestión de cambios en aplicaciones y sistemas	B.1 Adquisición de aplicaciones y sistemas B.2 Desarrollo de aplicaciones B.3 Gestión de cambios	op.pl.3 y 4 mp.sw.1 y 2 op.exp.5, op.acc.3
C. Operaciones de los sistemas de información	C.1 Inventario de hardware y software (CBCS 1 y 2) C.2 Gestión de vulnerabilidades (CBCS 3) C.3 Configuraciones seguras (CBCS 5) C.4 Registro de eventos y de la actividad de los usuarios (CBCS 6) C.5 Servicios externos C.6 Protección del entorno de TI C.7 Protección de las instalaciones e infraestructuras C.8 Gestión de incidentes C.9 Monitorización del sistema y su seguridad C.10 Protección de las comunicaciones	op.exp.1 op.exp. 3 y 4 op.exp.2, 3 y 4 op.exp.8 op.ext.1 y 2 y nub.1 op.exp.6, mp.s, mp.eq mp.if op.exp.7 y 9 op.mon op.pl.2, mp.com, op.ext.4
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios de administración (CBCS 4) D.2 Gestión de usuarios	op.acc.
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas (CBCS 7) E.2 Plan de continuidad E.3 Alta disponibilidad	mp.info.6 op.cont.2 y 3 op.ext.3 op.cont.4

CGTI

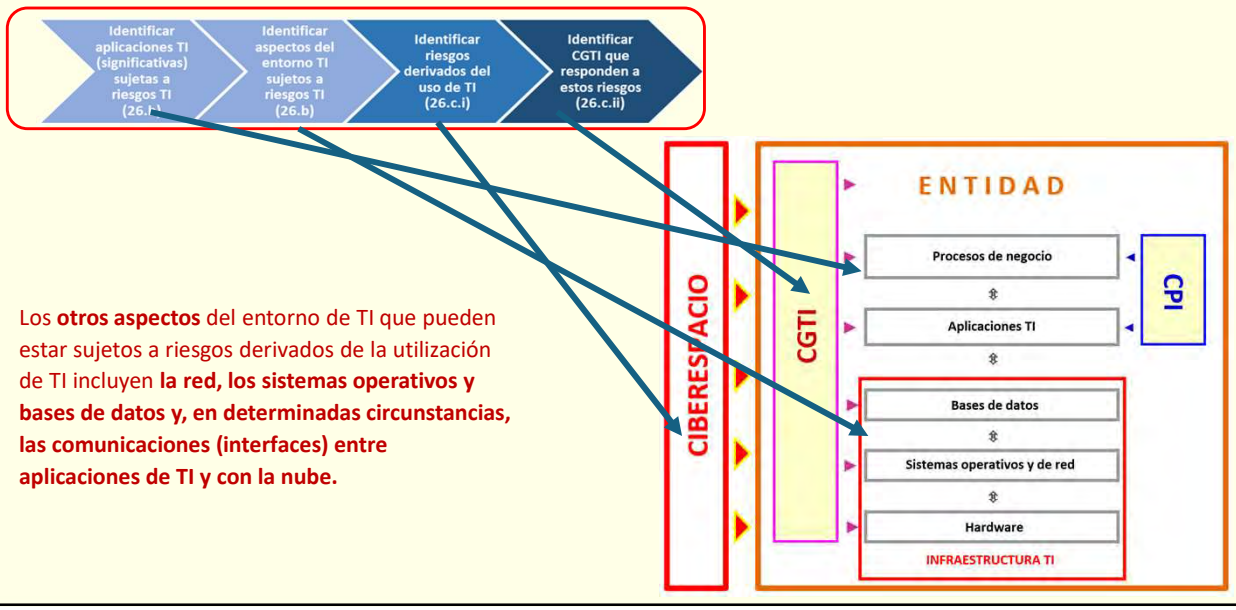
GPF-OCEX 5330

- **disponibilidad**
- **confidencialidad**
- **integridad**
- **autenticidad**
- **trazabilidad**

¡¡¡¡DANA!!!! Ransomware

53

Identificación de las aplicaciones de TI y otros aspectos del entorno de TI que están sujetos a riesgos derivados de la utilización de TI



Los **otros aspectos** del entorno de TI que pueden estar sujetos a riesgos derivados de la utilización de TI incluyen **la red, los sistemas operativos y bases de datos y, en determinadas circunstancias, las comunicaciones (interfaces) entre aplicaciones de TI y con la nube.**

54

Auditoría de la Tesorería: Riesgos y Control Interno

55

55

Guía práctica de fiscalización de los OCEX

GPF-OCEX 1957 Guía de auditoría del área de Tesorería

Referencia: GPF-OCEX 1315 Revisada, NIA-ES-SP 1330, GPF-OCEX 5330 y GPF-OCEX 5340, ISSAI-ES 400 y GPF-OCEX 4000.

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 11/12/2024.

56

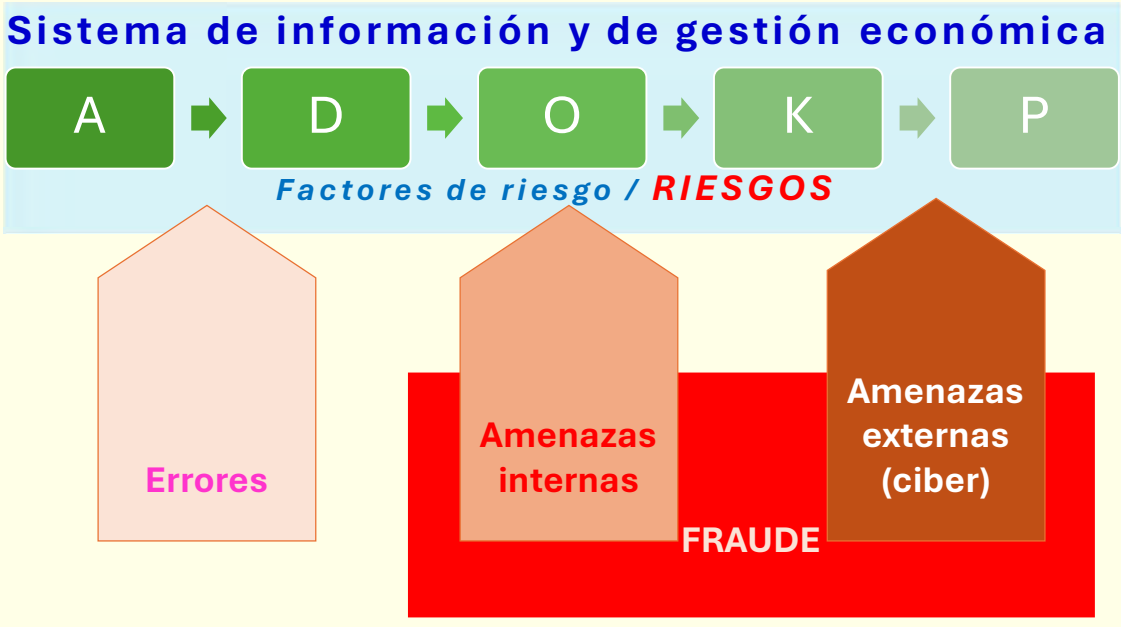
Qué hacemos: conocer el proceso de gestión

Lo primero que debemos hacer en conocer a fondo el proceso de gestión que vamos a auditar: no se puede auditar lo que se desconoce.

Toda actividad o proceso de gestión tiene vulnerabilidades y riesgos en sus distintas etapas que el auditor debe identificar y valorar

57

Qué hacemos: identificar los riesgos



58

Qué hacemos: identificar los riesgos

Utilizamos como ayuda listas predefinidas, pero no exhaustivas, que se deben adaptar y completar en cada caso

Tabla 1. Ejemplo de valoración de los riesgos inherentes en las afirmaciones

#	Riesgos inherentes	Función	Afirma-ción	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I.(PxM)
RT01	Apropiación indebida de los fondos de bancos, por ejemplo, realizando transferencias fraudulentas a cuentas ajenas.	Gestión de tesorería	E, L			
RT02	Existen cuentas bancarias no contabilizadas ni controladas.		C, L			
RT03	Existen cuentas bancarias sin movimiento en los últimos años.					
RT04	Se producen cambios de cuentas con excesiva frecuencia					
RT05	Existen personas autorizadas para disponer en cuentas sin tener competencia para ello (porque nunca la tuvieron o porque han dejado de tenerla).		E, L			
RT06	Existen firmas solidarias para disponer en cuentas, lo que representa un riesgo de disposición indebida de fondos.		E			
RT07	Los datos del FMT no son exactos.	Mantenimiento del FMT (Fichero Maestro de Terceros)	E			
RT08	Se producen altas y modificaciones no autorizadas en el FMT que pueden derivar en pagos a terceros incorrectos o fraudulentos.		E, L			
RT09	Pagos realizados por bienes o servicios no recibidos, pagos inexactos o excesivos.	Pagos	Ex, L			
RT10	Pagos realizados por personas no autorizadas o sin competencia (que acceden a la aplicación de pagos). Incluye los fraudes por suplantación de identidades en el sistema o en los correos electrónicos para el envío de órdenes de pago. Falsificación de órdenes de pago.		E, L			

59

Qué hacemos: identificar los riesgos

#	Riesgos inherentes	Función	Afirma-ción	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I.(PxM)
RT11	Realizar pagos excesivos o indebidos en cuentas extrapresupuestarias.	Pagos extrapresu-puestarios	E, L			
RT12	Modificación no autorizada de la información en la interfaz manual ERP[1]-Bancos para realizar pagos, ya que la carpeta donde se deposita transitoriamente el fichero Cuaderno 34-XML puede no estar debidamente protegida frente a accesos no autorizados.	Interfaz de pagos	L			
RT13	Pagos indebidos por modificación no autorizada de la información en la interfaz automatizada ERP-EDITRAN-Bancos para realizar pagos.		L			
RT14	Omitir o retrasar el registro de las entradas de efectivo/cobros.	Cobros	Ex			
RT15	Detraer las entradas de efectivo, una vez registradas.		E, L			
RT16	Ocultar operaciones introduciendo abonos no justificados (p. e., bonificaciones o exenciones) o anulaciones simuladas para ocultar la apropiación indebida de los cobros. Que se cancelen cuentas a cobrar como si fueran incobrables, sustrayendo los fondos o facturando por importes inferiores a los normales para disimular las cantidades sustraídas.		E, L			

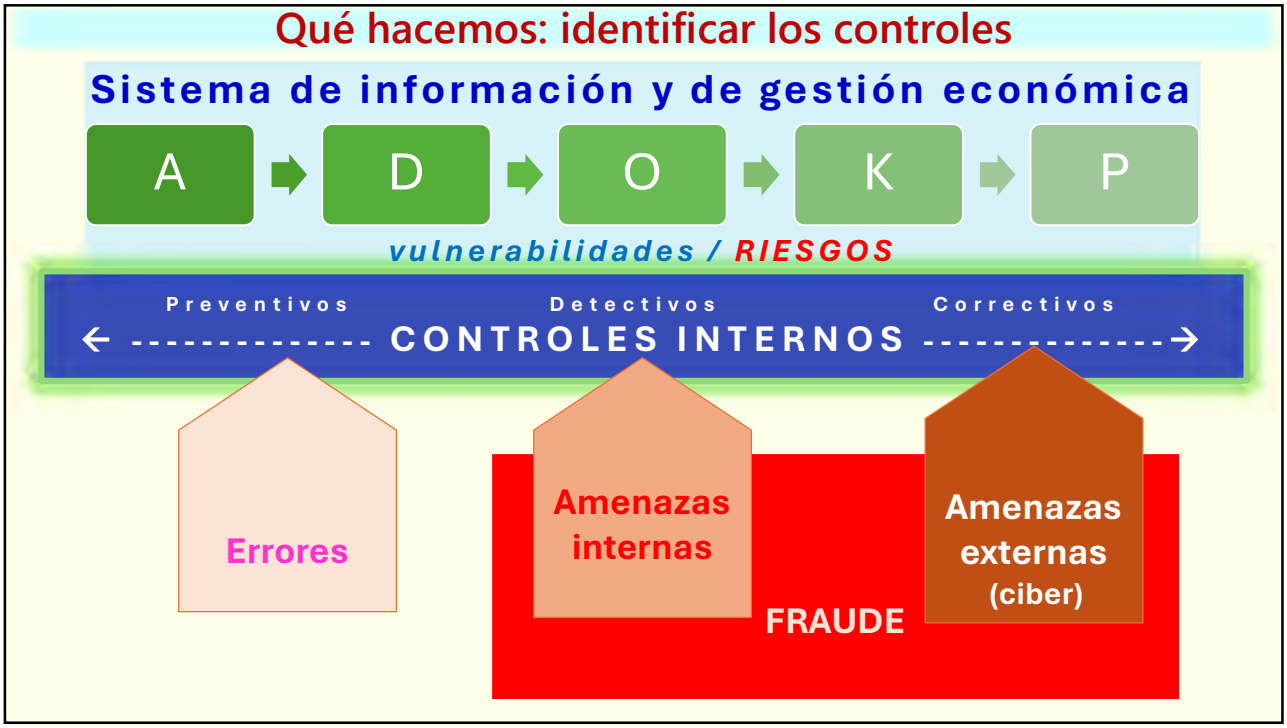
60

Qué hacemos: identificar los riesgos

#	Riesgos inherentes	Función	Afirma-ción	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I.(PxM)
RT17	Contabilización errónea o fraudulenta de saldos pendientes de cobro o pago y de movimientos bancarios	Contabilidad	Ex			
RT18	Ocultar operaciones no autorizadas o fraudulentas mediante la falsificación de conciliaciones bancarias.		Ex, L			
RT19	La interfaz de la aplicación de tesorería con la aplicación contable (en los casos que no sea la misma aplicación) no garantiza la integridad de los datos, lo que puede posibilitar la comisión de fraudes.		E Ex L			
RT20	No se registran todos las entradas y salidas de efectivo en las cajas. Se pueden detraer efectivo de forma no autorizada sin que sea detectado	Caja	E, Ex, L			
RT21	Apropiación indebida de los fondos de caja. Los saldos de efectivo no están protegidos		E, L			

61

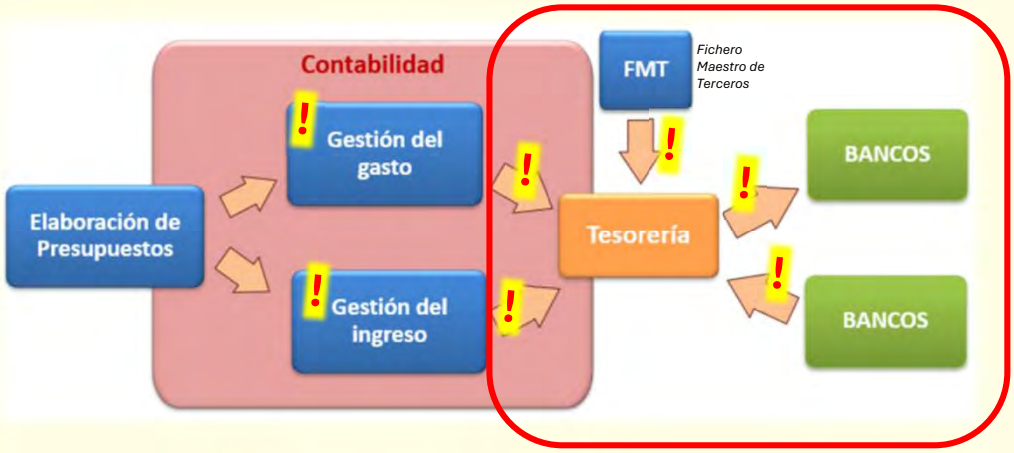
Qué hacemos: identificar los controles



62

Mapa general de procesos

Veamos con más detalle la gestión del gasto/pagos



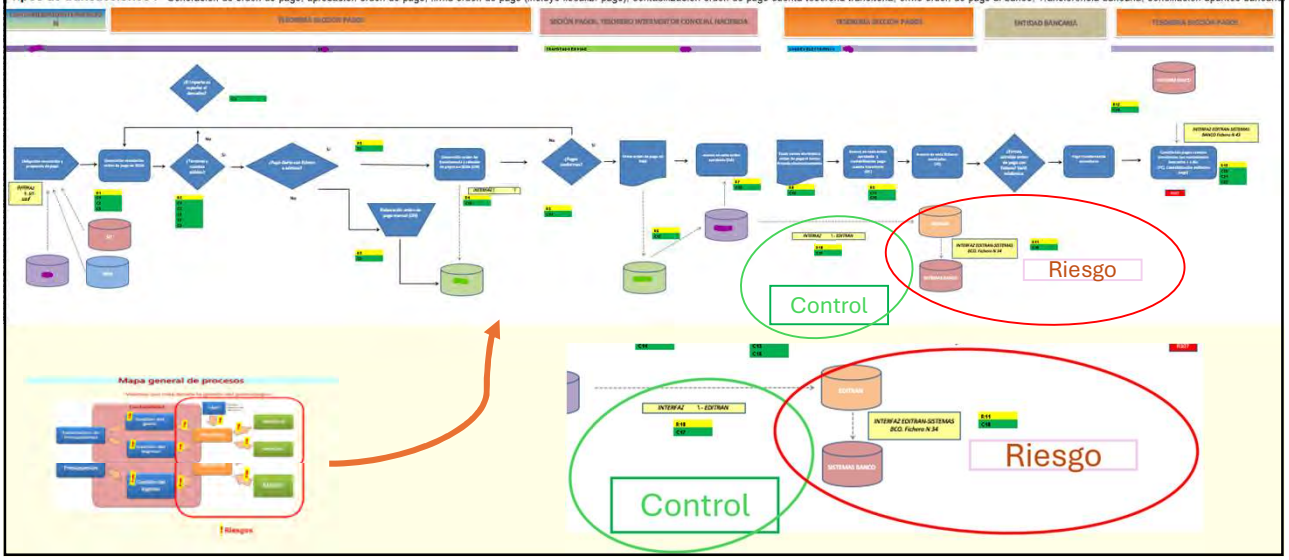
! Riesgos

63

Un ejemplo real: conocimiento del proceso de gestión

AYUNTAMIENTO DE YYYY

Proceso de gestión: GESTIÓN ECONOMICO-FINANCIERA-CONTABILIDAD
Subproceso: PROCESO DE PAGO
Aplicación: XXXX
Tipos de transacciones : Generación de orden de pago; aprobación orden de pago; firma orden de pago (incluye fiscaliz. pago); contabilización orden de pago cuenta tesorería transitoria; envío orden de pago al banco; Transferencia bancaria; conciliación apuntes bancarios



64

Un ejemplo real: riesgos y controles

R1	Inexactitud o duplicidad de los pagos realizados por la no concordancia entre orden de pago, pedido y factura.	C1 (Automático)	El sistema esta configurado para evitar duplicidades en las facturas registradas.
		C2 (Automático)	El sistema realiza de forma automatica un cruce entre orden de pago, pedido y factura, identificando y bloqueando partidas no coincidentes. Adicionalmente, el sistema bloquea pagos donde el importe total facturado supera el límite establecido en los pliegos y/o contratos.
R2	El acceso a los cambios de las caracteristicas e información de proveedores no está debidamente restringido.	C3 (Automático)	Todos los cambios maestros de proveedores (nuevos proveedores y cambios bancarios) se procesan solo después de que se hayan obtenido las aprobaciones adecuadas según la matriz de aprobación.
		C4 (Procedimiento)	Cualquier cambio en las cuentas corrientes donde se realizan pago debe estar justificado mediante un certificado de titularidad real
		C5 (Control de accesos)	Los usuarios con capacidad técnicas para realizar cambios en el maestro de proveedores se encuentran debidamente autorizados
R3	Insuficiencias de aprobación en las ordenes de pago manuales	C6 (Automático)	Validación de que la orden de pago manual se corresponde con una obligación de pago reconocida
R4	Modificación no autorizada de la información en la interfaz SICAL-GESTOR	C7 (Control de accesos)	Verificación de que el personal con acceso a la ruta donde se almacena la información que vuelca entre sistemas se encuentra debidamente autorizado
R5	Se realizan y registran desembolsos no autorizados, inexactos o fraudulentos.	C8 (Procedimiento)	Las ordenes de pago se revisan junto con la documentación de respaldo para verificar su idoneidad y precisión antes de proporcionar la aprobación.
R4	Modificación no autorizada de la información en la interfaz SICAL-GESTOR	C9 (Control de accesos)	Verificación de que el personal con acceso a la ruta donde se almacena la información que vuelca entre sistemas se encuentra debidamente autorizado

65

Un ejemplo real: riesgos y controles

R7	Modificación no autorizada en SICAL de la orden aprobada (OA)	C10 (Control de accesos)	Si existen, los usuarios con capacidad técnica para realizar cambios en las órdenes de pago se encuentran debidamente autorizados
R8	Suplantación de identidad en el correo electrónico	C11 (Emails certificados)	El correo electrónico en el que se encuentra adjunta la orden de pago se encuentra certificado para validar la identidad del remitente
R9	Contabilización errónea del pago en las cuentas transitorias	C12 (Automático)	El sistema valida que el importe contabilizado y el importe de la orden de pago es coincidente. En caso contrario, no se realiza la contabilización.
		C13 (Control de accesos)	El personal con acceso a modificar la información contable se encuentra adecuadamente
R10	Modificación no autorizada de la información en la interfaz SICAL-EDITRAN	C14 (Control de accesos)	Verificación de que el personal con acceso a la ruta donde se almacena la información que vuelca entre sistemas se encuentra debidamente autorizado
R11	Modificación no autorizada de la información en la interfaz EDITRAN - Sistemas Bancarios	C15 (Control de accesos)	Verificación de que el personal con acceso a la ruta donde se almacena la información que vuelca entre sistemas se encuentra debidamente autorizado
R12	Usuarios no autorizados con acceso a los sistemas bancarios	C16 (Control de accesos)	El acceso a los sistemas bancarios se revisa al menos trimestralmente para garantizar que esté restringido al personal adecuado.
R13	Contabilización errónea del pago en las cuentas definitivas	C17 (Automático)	El sistema valida que el importe de la N43 y el de la contabilización transitoria es coincidente. En caso contrario, no se realiza la contabilización definitiva
		C18 (Control de accesos)	El personal con acceso a modificar la información contable se encuentra adecuadamente restringido

66

Riesgos de fraude del área de tesorería *(GPF-OCEX 1957)*

6.5 Los riesgos de fraude en el área de tesorería

El área de tesorería ha sido, desde siempre, un área propensa a que se comentan fraudes e irregularidades de distinto tipo. La razón es muy sencilla, es más fácil robar dinero en efectivo o en bancos que un inmueble, por ejemplo.

Las amenazas tradicionalmente eran internas, pero con la utilización intensiva de los sistemas de información y la interconexión por internet, además de incrementarse aquellas, han aumentado de forma exponencial las amenazas externas debido a las vulnerabilidades que puede ofrecer un sistema de información mal protegido.

Tanto las amenazas internas como las externas pueden ser minimizadas con un adecuado sistema de control interno implantado de forma efectiva.

Pero, en un entorno de administración electrónica avanzado cualquier sistema de control interno debe incluir un sólido sistema de ciberdefensa basado en el ENS, es decir, **los CPI deben estar respaldados por los CGTI necesarios ya que si no cualquier sistema de control interno es tan solo un cascarón vacío**.

67

Riesgos de fraude del área de tesorería *(GPF-OCEX 1957)*

***Riesgo de fraude** manipulando el fichero maestro de terceros (FMT)*

Uno de los mecanismos más utilizados para cometer un fraude ha consistido, tradicionalmente, en la manipulación indebida de los datos relativos a los terceros a los que hay que pagar determinadas cantidades por cualquier motivo, a priori legítimo, bien sea como pago por la compra de bienes o servicios, por nóminas, subvenciones, etc. Dichos datos, incluyendo los relativos a las cuentas bancarias donde se realizan los pagos, se mantienen en un fichero que denominamos Fichero Maestro de Terceros, el cual siempre ha sido objeto de protección especial por parte de los sistemas de control interno.

Este riesgo de fraude clásico tenía como principales amenazas los usuarios internos. La utilización de sistemas de información interconectados y en particular el uso de internet ha ocasionado un aumento de las **amenazas internas y** sobre todo las externas que pueden provenir de cualquier parte del mundo, y por tanto la multiplicación de los riesgos de fraude y la exigencia de una sólida red de controles para proteger la seguridad y la integridad del FMT.

Como señala Godino y Menéndez[2], una de las funciones clave de la Tesorería, como es la tramitación de pagos, está en el punto de mira de la delincuencia organizada, la cual, aprovechándose de las vulnerabilidades de las Administraciones públicas, opera de forma fraudulenta para suplantar identidades y de este modo desviar los pagos dirigidos a los verdaderos acreedores, produciendo con ello un menoscabo en las arcas públicas al tratarse de un pago que no tiene carácter liberatorio.

68

Jueves 03.10.24
LAS PROVINCIAS

VALENCIA | 3

El Palacio de Congresos se saltó el protocolo en la estafa y no revisó el cambio de cuenta

Phishing/Man in the middle

valenciaplaza

EL PALACIO PREVÉ VARIOS FRENTES JUDICIALES | COMPROMÍS Y PSPV PIDEN RESPONSABILIDADES

Los estafadores también suplantaron al Palacio de Congresos para engañar a su proveedor

15/10/2024 - VALÈNCIA. Poco a poco se conocen más detalles sobre cómo sucedió el fraude del Palacio de Congresos, organismo municipal dependiente del **Ayuntamiento de València**. Los estafadores se hicieron pasar por un proveedor real del Palacio de Congresos para solicitar el cambio de cuenta y cobrar casi 200.000 euros en facturas de servicios efectivamente prestados por dicho proveedor. Para lo cual practicaron una segunda suplantación -y esta es la novedad-: ante el proveedor, se presentaron engañosamente como el Palacio para conseguir documentos clave que emplearon en la estafa.

Durante el fraude, unos estafadores anónimos se hicieron pasar por **representantes de un proveedor real** mediante cuentas de correo falsas para pedir el cambio de cuenta bancaria en la base de datos del Palacio y que este abonase **facturas pendientes** por servicios que el proveedor sí había prestado. La compañía gestora del Palacio procedió a la modificación aunque los protocolos señalan que es **el director financiero del Palacio** el que ha de hacer las comprobaciones previas. En este caso, estaba de baja y rebotó el primer correo de los estafadores.

69

8.2. Riesgos del desconocimiento o el no uso de DMARC

La falta de implementación de DMARC puede exponer a las organizaciones a riesgos de seguridad más elevados y a consecuencias negativas tanto operativas como estratégicas. Por tanto, adoptar DMARC es una parte importante de la estrategia de seguridad en correo electrónico para proteger los recursos y la integridad de una organización.

- **Aumento de la suplantación de identidad (spoofing),** sin DMARC, los atacantes pueden enviar correos electrónicos que aparentan ser del dominio de la organización más fácilmente. Esto puede conducir a ataques de phishing efectivos contra clientes, empleados o socios comerciales, quienes pueden ser engañados para que divulguen información confidencial o realicen acciones maliciosas, como transferencias de dinero fraudulentas.
- **Daño a la reputación del dominio y de la marca,** si los atacantes utilizan con éxito un dominio para enviar spam o malware, esto puede dañar la reputación de la marca asociada. Los clientes pueden perder confianza en la organización, y los dominios pueden ser incluidos en listas negras por servicios de correo electrónico y filtros de spam, afectando la entrega de correos legítimos.
- **Pérdida de control sobre la política de envío de correo,** al no especificar y hacer cumplir una política de envío de correos electrónicos a través de DMARC, las organizaciones pierden la oportunidad de definir y controlar quién puede enviar correos en nombre de sus dominios, lo que incrementa el riesgo de abuso.
- **Dificultad para identificar abusos y ataques** sin los informes de DMARC, las organizaciones pueden no ser conscientes de que su dominio está siendo utilizado para suplantación o de otros problemas de seguridad relacionados con el correo electrónico. Esto retrasa la capacidad de respuesta ante incidentes y reduce la efectividad de las medidas de mitigación.
- **Impacto en la confiabilidad de la comunicación,** los correos electrónicos enviados desde dominios sin una política DMARC clara pueden ser tratados con mayor sospecha por los servidores de correo receptores. Esto puede llevar a una mayor tasa de correos marcados como spam o incluso bloqueados, afectando la comunicación efectiva con clientes y socios.
- **Vulnerabilidad a ataques dirigidos,** las organizaciones sin DMARC son más vulnerables a ataques de spear phishing y otros tipos de ataques dirigidos, ya que los atacantes pueden explotar la falta de autenticación de correo electrónico para realizar ataques más convincentes y difíciles de detectar.

CCN-CERT
BP/33

Recomendaciones de seguridad en el correo electrónico, DMARC

INFORME DE BUENAS PRÁCTICAS

MAYO 2024

ccn-cert centro criptológico nacional

20 Centro Criptológico Nacional

70

Riesgos frecuentes del área de tesorería *(GPF-OCEX 1957)*

Los **fraudes** derivados de malas praxis relacionadas con los **FMT** son de muy distinto tipo:

- Fraude del CEO (se vulneran los procedimientos y se hacen pagos a IBAN distintos a los del FMT). Este fraude utiliza métodos de ingeniería social para vulnerar los procedimientos y los controles, con la finalidad de inducir pagos a proveedores y/o cuentas que no están en el FMT.
- *Phishing*. Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas. Con este método se consigue hacer cambiar el IBAN existente en el FMT de un proveedor, para pagar una deuda real a la cuenta de los defraudadores. Para culminar el fraude hay que vulnerar los procedimientos y controles.
- Ataques *Man in the middle*. Consiste en interceptar la comunicación entre un emisor y un receptor, pudiendo espiar o modificar la información con fines maliciosos.
- Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
- Suplantación. Se accede al sistema y se suplanta la identidad de un usuario autorizado para hacer cambios indebidos en el FMT.
- Modificación no autorizada de información. Ej: modificación del IBAN por un atacante empleando credenciales sustraídas de un sistema.
- Los CGTI son muy débiles o inexistentes y se puede acceder sin dificultad al FMT para hacer cambios indebidos.

71

Fraude del CEO

SUCESOS >

La EMT de Valencia sufre una rocambolesca estafa de cuatro millones de euros

Una directiva transfiere la suma a una cuenta externa tras ser víctima presuntamente del fraude del CEO

IGNACIO ZAFRA

Valencia - 27 SEPT 2019 - 18:18 | Actualizado: 28 SEPT 2019 - 13:42 CEST

La Empresa Municipal de Transportes (EMT) de Valencia ha informado este viernes de que ha sufrido una estafa rocambolesca. Su jefa de administración transfirió entre el 3 el 20 de septiembre cuatro millones de euros a una cuenta bancaria en Hong Kong creyendo que participaba en una operación confidencial de la compañía pública, cuando en realidad, según

Piratas informáticos 'hackearon' los correos de la EMT para preparar la estafa de cuatro millones de euros

La jefa de Administración, ya despedida, dio validez a la operación financiera al recibir un correo de un superior sin saber que era falso - Los expertos ven muy difícil lograr recuperar el dinero

El Supremo zanja el fraude de la EMT: la directiva tendrá que pagar por el 'agujero' de 4 millones

Pablo Plaza

18/10/2024 - VALÈNCIA. El **Tribunal Supremo** ha zanjado la disputa por la responsabilidad contable por el fraude de cuatro millones de euros de la **Empresa Municipal de Transportes (EMT)** de València. El alto tribunal ha inadmitido el recurso presentado por **Celia Zafra**, la exdirectiva de la firma pública, que es considerada tanto por la EMT como por el Tribunal de Cuentas como responsable contable de la estafa de **4,2 millones de euros**.

Esta vertiente de lo sucedido se centra en la vía contable –la penal sigue su curso en el juzgado de Instrucción número 18 de Valencia–. La Sala de lo Contencioso-administrativo del Tribunal Supremo ha **inadmitido el recurso de casación de Zafra** contra la sentencia del **Tribunal de Cuentas**, emitida en 2023.

El Tribunal de Cuentas consideró a Zafra responsable contable por una negligencia grave del robo de más de **cuatro millones de euros** y le obligó a abonar este importe. Aunque no concluyó que hubiera dolo ni que la directiva pretendiera el resultado, sí entendió que hubo falta de diligencia y que eso facilitó el fraude.

72

EL COMERCIO

El Ayuntamiento de Oviedo, víctima del 'fraude del CEO', denuncia que le han estafado 60.000 euros

Los timadores se hicieron pasar por una contratista municipal para lograr que Tesorería cambiase la cuenta en la que ingresaba los pagos

El Ayuntamiento de Oviedo EFE

GONZALO DÍAZ-RUBÍN
OVIEDO.
Martes, 13 de abril 2021, 01:13

Los tiempos adelantan que es una barbaridad. Los **estafadores**, sin dejar de lado el negocio clásico - el 'tocomocho', el 'italiano extrovertido' o el 'abrazo cariñoso'-, han ido haciéndose su propia transformación digital y el **Ayuntamiento de Oviedo** ha sido víctima de ella y de su ingenio: **más de 60.000 euros le han 'volado' a cuenta del 'fraude del CEO'**. El nombre de la estafa hace referencia a que el timador se hace pasar, vía telemática, por el consejero de una empresa con negocios con la administración y aprovecha para desviar el pago destinado a la empresa real a una cuenta bancaria propia en algún país extranjero. **A Oviedo le hicieron una versión más de andar por casa**. Los timadores, según la denuncia obrante ante la Policía Nacional, remitieron un correo electrónico en nombre del **Grupo Eulen** el pasado 22 de marzo. En el mismo, se solicitaba cambiar la cuenta en la que el Ayuntamiento le abonaba sus servicios; incluso, en el cuerpo del mensaje, se mencionaba a la contable de la empresa.

Correo electrónico

Los funcionarios no sospecharon nada. Según explicó la tesorera municipal, Reyes Aldecoa, a los agentes, **«es habitual» que las empresas utilicen el correo electrónico para comunicarse con la Tesorería**. Ese mismo día, en contestación, se recibió un segundo correo electrónico en el que el 'falso' Grupo Eulen facilitaba los nuevos datos bancarios, con ficha de acreedores y certificado de titularidad bancaria, por lo que los funcionarios procedieron a dar de baja la anterior y dar de alta la nueva. Tres días más tarde, Tesorería libró el pago mensual a Eulen por sus servicios: 60.183 euros. Lo hizo mediante cuatro transferencias desde la cuenta operativa municipal en el BBVA el mismo día 25.

El engaño solo se descubrió el día 6 de abril, cuando al utilizar los técnicos la aplicación de registro de facturas electrónicas las cuentas bancarias no encajaban. Una llamada a la empresa acabó por confirmar el engaño, por lo que la tesorera acudió a formular la correspondiente denuncia.

Los intentos por recuperar el dinero anulando las transferencias han sido infructuosos hasta el momento. Podía ser peor. Valencia transfirió cuatro millones de euros por unos coches de metro a un 'falso CEO', que acabaron perdidos en Hong Kong.

EL COMERCIO

El rastro del dinero timado al Ayuntamiento de Oviedo se pierde al ser transferido al extranjero

G. D.
OVIEDO
Miércoles

La Policía sostiene que la investigación de este tipo de estafas es «muy compleja, para cada paso hay que abrir una barrera»

Comentá

El **Ayuntamiento de Oviedo** se ha convertido, a cuenta de unos correos electrónicos, en la primera administración pública de la región en ser estafada a través del 'fraude del Ceo' y abonar más de 60.000 euros en una cuenta bancaria que no era la del proveedor. A ese dinero se le pierde la pista ya fuera del país, confirmaron ayer fuentes de la Jefatura Superior de Policía de Asturias, muy prudentes con un caso aún en investigación y el primero de este tipo en Asturias.

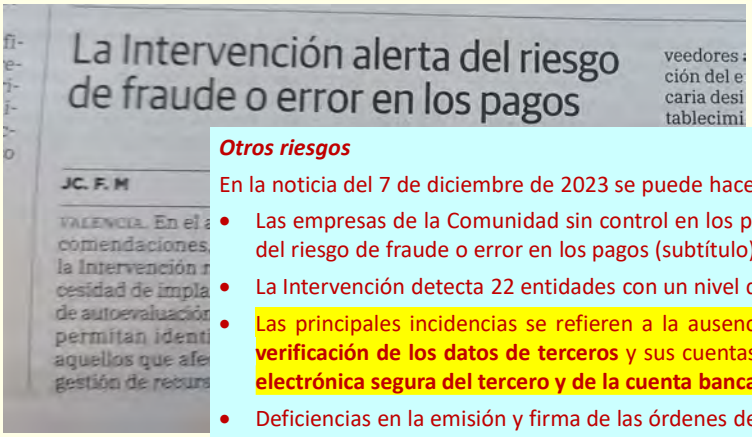
El dinero que Tesorería transfirió a la que creía que se trataba de la **nueva cuenta bancaria del Grupo Eulen** llegó a su destino e inmediatamente fue transferido al extranjero. «Son investigaciones muy complejas, para cada paso hay que abrir una barrera», explican las mismas fuentes.

La investigación parte con desventaja. Tesorería tardó más de diez días en percatarse del fraude. Recibió el 25 de marzo un correo en nombre de la contable de la contratista en el que se pedía cambiar la cuenta de pagos y un segundo correo en el que se facilitaban los nuevos datos. **A esa nueva cuenta, transfirieron los más de 60.000 euros de la mensualidad al día siguiente.** Fue el día 6 de abril, al comprobar los funcionarios la aplicación de facturas electrónicas, cuando se percataron del engaño.

Fraude del CEO

73

Riesgos frecuentes del área de tesorería *(GPF-OCEX 1957)*



La Intervención alerta del riesgo de fraude o error en los pagos

veedores
ción del e
caria desi
tablecimi

JC. F. M

VALENCIA. En el
comendaciones
la Intervención
cesidad de impla
de autoevaluación
permitan identi
aquellos que afe
gestión de tesor

Otros riesgos

En la noticia del 7 de diciembre de 2023 se puede hacer un breve catálogo básico de riesgos de fraude:

- Las empresas de la Comunidad sin control en los pagos a proveedores (titular). La Intervención alerta del riesgo de fraude o error en los pagos (subtítulo)
- La Intervención detecta 22 entidades con un nivel de riesgo alto en el área referida a los pagos.
- Las principales incidencias se refieren a la ausencia de procedimientos formalmente aprobados de **verificación de los datos de terceros** y sus cuentas bancarias, así como la **ausencia de identificación electrónica segura del tercero y de la cuenta bancaria destinataria del pago**.
- Deficiencias en la emisión y firma de las órdenes de pago.
- Se recomienda el establecimiento de medidas técnicas que posibiliten que **las conciliaciones de saldos bancarios y contable se realicen de manera informática y con periodicidad no superior a la semana**.
- Se recomienda implantar sistemas de evaluación de riesgos que permitan identificar y medir aquellos que afectan al área de gestión financiera y adaptar el sistema de control interno de forma que se evite o reduzca la probabilidad de su ocurrencia e impacto.

74

Principales controles internos del área de tesorería
(apartado 7 de la GPF-OCEX 1957)

En la **organización interna** de una entidad se deben contemplar requisitos como los siguientes:

- El departamento de tesorería debe estar separado de cualquier otro.
- El tesorero no debe realizar funciones de cuentas a cobrar y a pagar.
- Los empleados del departamento de tesorería deben tener claramente definidas sus funciones y responsabilidades.
- Debe existir una política financiera adecuada, por escrito, en cuanto a las cuentas bancarias, autorizaciones, etc.

75

Principales controles internos del área de tesorería

Los **principales controles** en el área de tesorería incluirán (relación no exhaustiva):

- Los **procedimientos** de gestión de la tesorería (cobros, pagos o transferencias, mantenimiento del fichero maestro de terceros, etc) han de constar por escrito y reflejar los límites y autorizaciones.
- Existencia de una adecuada **segregación de funciones** en todo el proceso.
- Las firmas autorizadas para disponer en bancos han de ser siempre **mancomunadas.**
- Las operaciones de disposición de fondos a través de las plataformas de las entidades financieras se regularán en los pliegos de contratación de las cuentas bancarias de forma que se requerirá la remisión de un documento electrónico firmado electrónicamente por las personas autorizadas para que la entidad financiera pueda ejecutar las órdenes de pago mediante la operativa de la banca electrónica.

  Las condiciones de los pliegos o, en su defecto, las instrucciones cursadas por escrito a las entidades financieras deben detallar las verificaciones que son responsabilidad de la entidad financiera (verificar la autenticidad de firmas de las órdenes de pago, verificar la autenticidad e integridad de los ficheros de pago, ...).

76

Principales controles internos del área de tesorería

- **Controles de acceso:**

  Solo los funcionarios de Tesorería deben tener acceso a la aplicación de gestión de tesorería o a las funcionalidades para el área de tesorería de la aplicación de contabilidad y la **asignación de permisos** a los usuarios de esa aplicación se realizará aplicando el principio de mínimo privilegio.

  Los usuarios con acceso a la aplicación o funcionalidades de tesorería se revisan periódicamente para garantizar que los privilegios estén restringidos al personal adecuado.

  Sólo los funcionarios de intervención tienen acceso a las funciones de fiscalización de ingresos y pagos.

  Sólo los funcionarios de tesorería que lo necesiten para ejercer sus funciones deben tener acceso a la banca electrónica de las cuentas de la entidad.

  Las autorizaciones de acceso y modificación del fichero maestro de terceros contemplan la segregación de funciones respecto a la gestión de ingresos y pagos (en una entidad local, por ejemplo, intervención realiza el alta y modificación de los ficheros de terceros y cuentas bancarias y los funcionarios de tesorería no tienen acceso a esos menús de la aplicación).

77

Principales controles internos del área de tesorería

- Realizar **conciliaciones bancarias** periódicamente.

  Las conciliaciones bancarias constituyen un aspecto esencial en el control interno de la tesorería. Consisten en poner de manifiesto las diferencias entre los registros contables de la entidad y los saldos del banco, según los extractos, a una fecha determinada.

  Tradicionalmente se hacían en los formularios establecidos al efecto por una persona diferente de la que realiza los registros contables y el manejo de fondos. En un entorno informatizado deben realizarse automáticamente, como mínimo semanalmente, y preferiblemente de forma diaria (en las entidades grandes desde luego).

  Deben ser revisadas y firmadas por un responsable y debidamente supervisadas.

  En un entorno de administración electrónica, la entidad realizará las conciliaciones bancarias con un alto grado de automatización. Los movimientos bancarios (ficheros norma 43[7]) diarios se recibirán al día siguiente a través del sistema EDITRAN y se cargarán de forma automatizada en el sistema contable (ERP).

  Una vez cargados estos movimientos, el ERP realiza un procedimiento de conciliación automatizado con los movimientos contables transitorios o provisionales. Cuando son coincidentes se contabilizan de forma automatizada en la cuenta contable de tesorería correspondiente.

  Si hay movimientos no coincidentes quedan registrados como movimientos transitorios pendientes de investigación hasta que definitivamente se aclaran, concilian y contabilizan.

  Las conciliaciones bancarias no deben arrastrar partidas de forma indefinida. Aunque con carácter general no puede fijarse un plazo para su aclaración, debe efectuarse de forma diligente y sin demoras no justificadas ni razonables.

78

Principales controles internos del área de tesorería

- Controles sobre los pagos:
  - El sistema realiza de forma automática un cruce entre orden de pago, pedido y factura, identificando y bloqueando partidas no coincidentes.
  - El sistema impide el registro de facturas duplicadas.
  - El sistema bloquea pagos donde el importe total facturado supera el límite establecido en los pliegos y/o contratos.
  - El sistema verifica automáticamente que una factura u obligación pendiente de pago no ha sido pagada anteriormente.
  - Las órdenes de pago se revisan junto con la documentación de respaldo para verificar su idoneidad y precisión antes de aprobarlas.
  - Una vez aprobada la orden de pago nadie está autorizado a modificarla, excepto con la firma del Tesorero e Interventor.
  - El sistema bloquea la realización de pagos no presupuestarios si el importe a pagar es mayor al ingreso no presupuestario que da origen al pago.
  - Las firmas electrónicas en las órdenes de pago garantizan la integridad.
  - El ERP **impide** (por configuración) que se puedan realizar pagos a cuentas bancarias distintas de las del FMT. **No puede realizarse ningún pago** a un IBAN que no esté registrado en el FMT para el acreedor correspondiente, en caso contrario el pago es rechazado automáticamente por el ERP.
  - Las firmas electrónicas en los correos electrónicos de remisión de las órdenes de pago garantizan la identidad del remitente.

79

Principales controles internos del área de tesorería

- Controles sobre los **cobros**:

  De haber cobros en metálico (no recomendable, con carácter general), los cobros deben ingresarse en el banco inmediatamente y no utilizarse para realizar pagos. Debe aplicarse el principio de proporcionalidad y si los cobros por caja son residuales no será preciso realizar los ingresos diariamente. Desde el punto de vista del auditor tendremos en cuenta los criterios de importancia relativa definidos en la planificación y el juicio profesional, para determinar la frecuencia recomendable en cada caso.

  Se han de usar recibos numerados correlativamente para la recepción de ingresos, y establecer un adecuado control de los recibos en blanco.

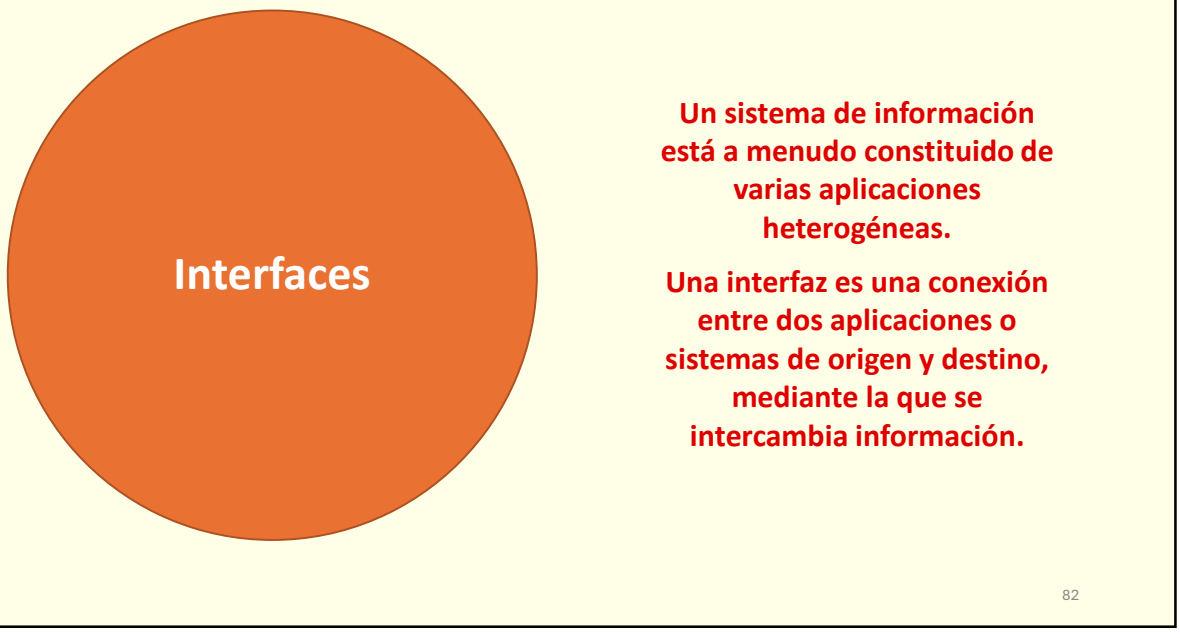
  Todas las operaciones se registran pronta y exactamente en la contabilidad o en registros auxiliares y se emiten los informes apropiados.

80

Principales controles internos del área de tesorería

- **Controles sobre el fichero maestro de terceros (FMT):**
  - Existe un procedimiento aprobado que regula la tramitación de las altas y modificaciones del FMT. Todos los cambios en el FMT se realizan según este procedimiento, que incluye una adecuada segregación de funciones y la asignación de autorizaciones y responsabilidades en las distintas etapas del proceso.
  - Cualquier cambio en los datos del IBAN donde se realizan pagos debe estar justificado mediante un certificado de titularidad real o preferentemente mediante el servicio **Iberpay** integrado con el ERP.
  - Si la cuenta que aparece en la factura electrónica no coincide con la que conste en el FMT, no se pagará la factura (nunca se debe pagar una factura a un IBAN que no conste en el FMT), se investigará, y en su caso, se requerirá al acreedor para que actualice sus datos a través del procedimiento electrónico.
  - En ocasiones los procedimientos de las entidades auditadas contemplan declaraciones responsables para acreditar la titularidad de las cuentas en el alta terceros y cuentas bancarias en el FMT. Este tipo de requisito o control, aunque es legal (art. 69 Ley 39/2015), no es un control tan robusto y fiable como los certificados o verificaciones mediante servicios web (tipo Iberpay).
  - Los cambios en el FMT (nuevos proveedores, cambios de IBAN, ...) se procesan solo después de que se hayan obtenido las aprobaciones adecuadas, de acuerdo con el principio de mínimo privilegio.
  - Los usuarios con capacidad para realizar cambios en el FMT se encuentran debidamente autorizados y restringidos de acuerdo con el principio de mínimo privilegio.

81



82

Identificar las principales interfaces

El objetivo de esta etapa de la auditoría es comprender los flujos de información y de datos entre distintas aplicaciones o sistemas, tanto electrónicos como manuales, y evaluar los **riesgos de interfaz** *(pérdida de datos por interrupción de las comunicaciones, duplicación de datos en el sistema de destino, actualización del sistema de destino con datos de un período incorrecto, etc)* y los **controles** existentes, manuales o automatizados.

83

83

Consideraciones de auditoría

Las interfaces entre aplicaciones y entre bases de datos requieren una atención especial, en particular las relacionadas con aquellas aplicaciones con impacto en las cuentas anuales.

Los ERP integrados a menudo requieren complicadas interfaces para intercambiar información con otras aplicaciones distribuidas.

A pesar de la importancia de las interfaces en el procesamiento de las transacciones, en muchos casos no se incluyen, erróneamente, en el plan de la auditoría (su mal funcionamiento puede afectar a todo el sistema y supone un riesgo a considerar).

84

84

Riesgos de las interfaces

- ✓**Pérdida de integridad de la información al pasar de una aplicación a otra, duplicidades, eliminaciones, *(por diseño erróneo, caída de las comunicaciones, fraude, etc)***
- ✓**Error humano**
- ✓**Cálculos erróneos**
- ✓**Posibilidad de accedan a los datos personas no autorizadas (confidencialidad)**
- ✓**Fraude**

85

85

Controles sobre las interfaces

Los **controles sobre las interfaces** pueden ser:

- manuales (p.e. mediante reconciliaciones manuales) o
- estar automatizados (los datos de ambos sistemas se concilian automáticamente).

- Controles sobre las **interfaces**:
  - El acceso a la ruta donde se almacena la información que vuelca entre sistemas se encuentra debidamente restringido.
  - El ERP genera automáticamente los ficheros con el detalle de las transferencias bancarias en formato XML (Cuaderno 34) y lo remite al banco mediante un servicio web o canal seguro.
  - Cuando la interfaz no es automatizada, por ejemplo, si el fichero XML (Cuaderno 34) se envía a través de la página web de la banca electrónica, las carpetas donde se depositan los ficheros de pago están debidamente protegidos.
  - Una vez generado el fichero XML, la aplicación bloquea la orden de pago correspondiente.

86

86

Procedimientos de auditoría

- ✓Pruebas de datos entre la aplicación de gestión (datos enviados) y la aplicación financiera (datos recibidos)
- ✓Recálculos de la información procesada
- ✓Revisión de las medidas de seguridad de las aplicaciones
- ✓Revisión de las medidas de seguridad de las carpetas que contienen la información generada por las interfaces

87

87

Qué decimos en los informes de auditoría

88

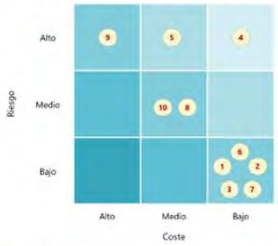
88

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

AUDITORÍA DE CIBERSEGURIDAD Y DE LOS CONTROLES GENERALES DE TECNOLOGÍAS DE LA INFORMACIÓN DEL NUEVO SISTEMA SEDA DEL AYUNTAMIENTO DE VALÈNCIA

Situación al 30 de septiembre de 2023

Gráfico 3. Riesgos que se atienden y coste de implantación de las recomendaciones



El índice de madurez de los CGTI relacionados con la ciberseguridad del sistema SEDA debe mejorar para alcanzar el objetivo establecido por el ENS.

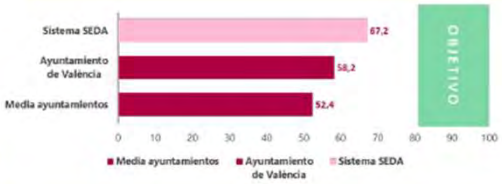
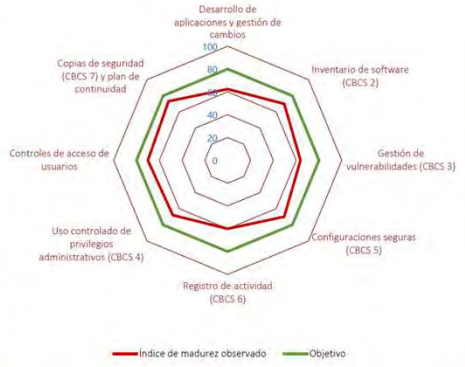


Gráfico 1. Índice de madurez, por áreas, de los controles de ciberseguridad



Cuadro 1. Índice de madurez por áreas de los controles de ciberseguridad

Áreas	Controles principales	Índice de madurez
B. Cambios en aplicaciones y sistemas	B2/B3 Desarrollo de aplicaciones y gestión de cambios	62,4%
C. Operaciones de los sistemas de información	C.1 Inventario de *software* (CBCS 2)	70,0%
	C.2 Gestión de vulnerabilidades (CBCS 3)	63,8%
	C.3 Configuraciones seguras (CBCS 5)	70,0%
	C.4 Registro de actividad (CBCS 6)	60,0%
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios administrativos (CBCS 4)	68,0%
	D2/D3/D4 Controles de acceso de usuarios	70,0%
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas (CBCS 7)	73,3%
	General	67,2%

89

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

AUDITORÍA DEL CONTROL INTERNO EN EL PROCESO PARA LA GESTIÓN DE LOS PAGOS DEL AYUNTAMIENTO DE VALÈNCIA Y DEL SISTEMA DE INFORMACIÓN SEDA

Situación al 31 de diciembre de 2023

2. CONCLUSIONES SOBRE LOS CONTROLES DE PROCESAMIENTO DE LA INFORMACIÓN DE LOS PAGOS

Como resultado de la revisión efectuada, concluimos que los controles de procesamiento de la información relacionados con la gestión de los pagos del Ayuntamiento garantizan razonablemente la completitud, exactitud, validez y legalidad de las transacciones.

Basamos nuestra conclusión en los resultados de la revisión de 21 CPI existentes en la gestión de los pagos del Ayuntamiento, tanto los automatizados en la aplicación SEDA como a través de procedimientos manuales que hemos considerado relevantes. Hemos evaluado tanto su diseño como su implementación y eficacia operativa, cuyos resultados se resumen en el siguiente cuadro:

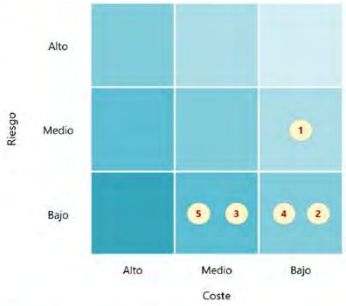
Cuadro 2. Eficacia de los CPI

Eficacia de los controles				Total controles revisados
Efectivos	Bastante efectivos	Poco efectivos	No efectivos	
13	8	0	0	21

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el siguiente gráfico se muestra la clasificación de las recomendaciones según los criterios combinados de riesgo potencial a mitigar y coste de su implantación.

Gráfico 1. Riesgos que se atienden y coste de implantación de las recomendaciones



Control 5

Los usuarios con capacidad para realizar cambios en el registro de terceros se encuentran debidamente restringidos. Solo determinados usuarios de Intervención pueden autorizar altas en el registro de terceros.

Objetivo del control

Disponer de medidas de control en el sistema que impidan el acceso de usuarios no autorizados a información crítica de terceros, mitigando el riesgo de que se produzcan modificaciones incorrectas, intencionadas o no, de dichos datos.

Situación del control

90

Cuadro 1. Índice de madurez por áreas de los controles de ciberseguridad

Áreas	Controles principales	Índice de madurez
B. Cambios en aplicaciones y sistemas	B2/B3 Desarrollo de aplicaciones y gestión de cambios	62,4%
C. Operaciones de los sistemas de información	C.1 Inventario de *software* (CBCS 2)	70,0%
	C.2 Gestión de vulnerabilidades (CBCS 3)	63,8%
	C.3 Configuraciones seguras (CBCS 5)	70,0%
	C.4 Registro de actividad (CBCS 6)	60,0%
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios administrativos (CBCS 4)	68,0%
	D2/D3/D4 Controles de acceso de usuarios	70,0%
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas (CBCS 7)	73,3%
	General	67,2%

Los controles ciber (CGTI) proporcionan seguridad respecto del buen funcionamiento de los controles internos en tesorería

Control 5

Los usuarios con capacidad para realizar cambios en el registro de terceros se encuentran debidamente restringidos. Solo determinados usuarios de Intervención pueden autorizar altas en el registro de terceros.

Objetivo del control

Disponer de medidas de control en el sistema que impidan el acceso de usuarios no autorizados a información crítica de terceros, mitigando el riesgo de que se produzcan modificaciones incorrectas, intencionadas o no, de dichos datos.

Situación del control

Efectivo

91

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE FISCALIZACIÓN DE LA EMPRESA MUNICIPAL DE TRANSPORTES DE VALÈNCIA, SAU. INGRESOS POR TRANSPORTE DE VIAJEROS Y TESORERÍA

Ejercicio 2019

7. RECOMENDACIONES

5. CONCLUSIONES SOBRE EL CONTROL INTERNO

La Sindicatura de Comptes ha observado que, durante el ejercicio 2019, existían en la EMT deficiencias significativas y debilidades materiales en el sistema de control interno que suponían elementos significativos de riesgo respecto de la integridad (completitud), exactitud y validez de las transacciones y datos en la gestión de los ingresos por transporte de viajeros y de la tesorería. El detalle de estas deficiencias es el siguiente:

- La EMT no disponía de procedimientos escritos y aprobados por los órganos de gobierno y administración de la sociedad sobre los procesos de gestión y control de las actividades de ingresos por transporte de viajeros y de tesorería, que incluyan las tareas y responsabilidades de los diferentes puestos de trabajo relacionados con dichos procesos.
- La EMT tampoco disponía de una relación de puestos de trabajo (RPT).
- No existía una adecuada segregación de funciones entre el personal del negociado de Administración en relación con el acceso al registro de terceros/facturas, la elaboración, contabilización y conciliación de las órdenes de pago y de los arqueos de caja.
- Las tareas de validación de las facturas y de revisión y aprobación de las órdenes de pago no se acreditaban adecuadamente.
- El control de los movimientos en cuentas bancarias con los datos contables no se realizaba con una periodicidad razonable, dado el volumen de transacciones de la entidad, ni se documentaba adecuadamente. Las conciliaciones bancarias se realizaban mensualmente.
- No se contaba con procedimientos escritos y aprobados por los órganos de la entidad para realizar periódicamente arqueos de las cajas de la entidad.
- No se realizaba un control efectivo sobre las personas autorizadas para la disposición de fondos en cuentas con entidades bancarias y había personas autorizadas sin los poderes aprobados por los órganos de la EMT.
- No existían controles adecuados para asegurar la integridad y autenticidad de la información del fichero XML con las órdenes de pago que se tramitan a la banca *online*.

92

SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE AUDITORÍA DE CIBERSEGURIDAD DE LA EMPRESA MUNICIPAL DE TRANSPORTES DE VALÈNCIA, SAU

Exercici 2020

Consideraciones sobre el fraude experimentado por EMT

Durante el ejercicio 2019 la EMT ha sido víctima de un tipo de estafa conocida como "fraude del CEO"[1] que ha tenido como consecuencia económica la pérdida de una cantidad superior a cuatro millones de euros.

Con objeto de dilucidar las deficiencias de gestión y seguridad que han posibilitado la perpetración de la estafa y depurar las responsabilidades sobre las mismas, se han iniciado durante 2019 y 2020 una comisión de investigación por parte del Consejo de Administración de la EMT, un proceso judicial y una investigación del Tribunal de Cuentas, trabajos actualmente en curso y cuyos resultados se encuentran pendientes de conclusión y/o publicación.

La presente auditoría no tiene como objeto incidir en este fraude y no serán revisados los hechos concretos a través de los que se ha materializado la estafa, que ya están siendo investigados por los organismos competentes y no debemos interferir en las actuaciones judiciales en curso.

No obstante, y en conformidad con el enfoque de riesgos recogido en las normas de auditoría, durante la planificación y ejecución de la auditoría sí han sido tenidas en consideración las circunstancias generales del fraude y hemos incluido en el ámbito de la revisión las áreas de interés relacionadas con los hechos, en particular el área de tesorería, dados los riesgos de posible falta de eficacia de los controles de seguridad de la información en dicha área.

Ámbito objetivo

La presente fiscalización está focalizada en la revisión de una serie de controles de seguridad de las tecnologías de la información y las comunicaciones implantados en los sistemas que soportan dos de los procesos de gestión más relevantes, relacionados con sendas áreas que están siendo auditadas por otro equipo de fiscalización de la Sindicatura. Estas áreas son la gestión de tesorería (de muy alto riesgo, tal como han acreditado las circunstancias de los últimos meses y señaladas en el apartado 1 anterior) y los ingresos por transporte de viajeros (actividad principal de la entidad). También hemos incluido dentro de nuestro alcance la contabilidad.

Dado el elevado riesgo de estas áreas, la auditoría de la ciberseguridad ha consistido en la revisión de dos grupos de controles en estas áreas:

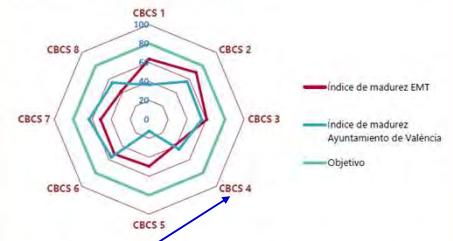
1. Revisión de los **controles básicos de ciberseguridad (CBCS).**
2. Revisión de otros **controles generales de tecnologías de la información relevantes** para la seguridad de las aplicaciones de gestión, adicionales a los CBCS.

Consideramos relevantes al conjunto de controles revisados porque su ausencia o su mal funcionamiento representaría una deficiencia significativa o una debilidad material de control interno y sobre la seguridad de los procesos señalados.

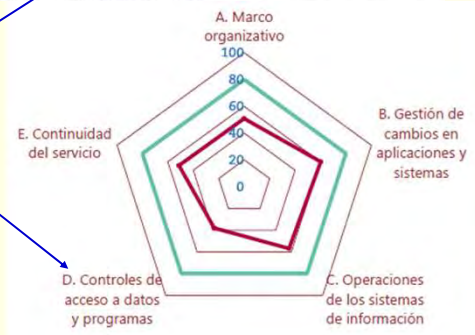
93

Áreas	Controles principales	Índice de madurez	
A. Marco organizativo	A.1 Cumplimiento de legalidad (CBCS 8)	41,7%	**50,9% (N2)**
	A.3 Formación y concienciación	60,0%	
B. Gestión de cambios en aplicaciones y sistemas	B.3 Gestión de cambios	60,2%	**60,2% (N2)**
C. Operaciones de los sistemas de información	C.1 Inventario de *hardware* (CBCS 1)	63,8%	**56,9% (N2)**
	C.1 Inventario de *software* (CBCS 2)	70,0%	
	C.2 Gestión de vulnerabilidades (CBCS 3)	60,7%	
	C.3 Configuraciones seguras (CBCS 5)	49,5%	
	C.4 Registro de la actividad de los usuarios (CBCS 6)	51,8%	
	C.5 Servicios externos	49,8%	
	C.8 Gestión de incidentes	53,1%	
D. Controles de acceso a datos y programas	D.1 Uso controlado de privilegios administrativos (CBCS 4)	38,6%	**38,1% (N1)**
	D.2 Mecanismos de identificación y autenticación	40,3%	
	D.3 Gestión de derechos de acceso	36,4%	
	D.4 Gestión de usuarios	37,3%	
E. Continuidad del servicio	E.1 Copias de seguridad de datos y sistemas (CBCS 7)	51,3%	**51,3% (N2)**
General			**51,5% (N2)**

Gráfico 3. Comparativa del índice de madurez de los controles básicos de ciberseguridad de la EMT y del Ayuntamiento de València



El índice medio de madurez de los CBCS ha sido del 53,4% en la EMT y del 47,5% en el Ayuntamiento de València; en ambos casos la situación de los controles de ciberseguridad es claramente mejorable y no puede considerarse que los sistemas de información estén debidamente protegidos.



94

4. CONCLUSIONES

Bajo índice de madurez de los controles de ciberseguridad

Se requiere mayor concienciación y más recursos dedicados a la seguridad de la información

Insuficiente gobernanza de la seguridad de la información

La EMT dispone de una *Política de seguridad de la información* (PSI), que **no ha sido aproba**

La situación de los controles de acceso privilegiado debe ser mejorada

Existen graves deficiencias en los controles relacionados con los usuarios administradores

Insuficiente grado de adecuación a la normativa de ciberseguridad

La revisión del cumplimiento de legalidad en materia relacionada con la ciberseguridad ha puesto de manifiesto un nivel insatisfactorio de adecuación a la normativa de

10

Priorización de las recomendaciones

Con objeto de que puedan establecerse acciones basadas en criterios de coste/beneficio, en el siguiente gráfico 2 se muestra la clasificación de las recomendaciones según los criterios combinados de riesgo potencial a mitigar y coste de su implantación.

Gráfico 2. Riesgos que se atienden y coste de implantación de las recomendaciones

95

Insuficiente gobernanza de la seguridad de la información

La EMT dispone de una *Política de seguridad de la información* (PSI), que **no ha sido aprobada por el Consejo de Administración**, máximo órgano de dirección de EMT, tal como requieren el ENS y la norma UNE-EN ISO/IEC 27001/27002, ni cumple con todos los requisitos establecidos en ambas normas.

La gestión de la seguridad de los sistemas de información requiere establecer una organización de la seguridad, que debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte y los mecanismos de coordinación y resolución de conflictos, designando un **Comité de Gestión de la Seguridad de la Información**, de forma que la gobernanza de la seguridad de la información esté adecuadamente estructurada.

La PSI que apruebe el Consejo de Administración debe recoger con claridad las responsabilidades sobre la gestión, administración y seguridad de los sistemas descentralizados (aquellos gestionados de manera autónoma por los departamentos), ya que la actual PSI no refleja fielmente las particularidades del modelo organizativo de la entidad. La administración de sistemas de información, que de manera general se realiza por parte del Área de Desarrollo, es asumida en determinados casos por los propios departamentos de la entidad, que administran las aplicaciones específicas que soportan los procesos críticos de sus departamentos. Esta situación no resulta recomendable, ya que dificulta la capacidad operativa del responsable de seguridad como figura que debe velar por la aplicación homogénea de medidas de seguridad en el conjunto de los sistemas de la entidad y su coherencia en un entorno de sistemas administrados por distintos departamentos. Además, existe un elevado riesgo de que los departamentos carezcan de las competencias profesionales requeridas para la administración de sistemas y de que los intereses departamentales no se encuentren alineados con los principios de la seguridad de la información aprobados por la organización.

96

La situación de los controles de acceso privilegiado debe ser mejorada

Existen graves deficiencias en los controles relacionados con los usuarios administradores de los sistemas, particularmente en aquellos gestionados de manera autónoma por los departamentos correspondientes (identificados más adelante en el informe como "sistemas descentralizados") y que proporcionan soporte a procesos críticos de negocio.

Las carencias detectadas, entre las que destacan una insuficiente aplicación del principio de mínimo privilegio y una deficiente gestión de los registros de actividad de los usuarios administradores, tienen un reducido coste de corrección y un alto impacto en el nivel general de ciberseguridad de la entidad.

Durante el trámite de alegaciones la EMT nos ha informado de la existencia de una propuesta de trabajo para la resolución de estas deficiencias. Hemos verificado la existencia de dicha propuesta y del plan de trabajo, que incluye las modificaciones necesarias en cuanto a la gestión adecuada de derechos de acceso y privilegios administrativos de los usuarios, registros de actividad y aplicación adecuada del principio de mínimo privilegio. Al emitir el presente informe esas acciones estaban en fase de implantación.

97

SEMINARI Gestió Econòmica Local

Federació de Municipis de Catalunya

¿Preguntas?

Muchas gracias por su atención

98

Guía práctica de fiscalización de los OCEX

GPF-OCEX 1957 Guía de auditoría del área de Tesorería

Referencia: GPF-OCEX 1315 Revisada, NIA-ES-SP 1330, GPF-OCEX 5330 y GPF-OCEX 5340, ISSAI-ES 400 y GPF-OCEX 4000.

Documento elaborado por la Comisión Técnica de los OCEX
y aprobado por la Conferencia de Presidentes de ASOCEX el 11/12/2024.

1. Introducción y objetivos de la guía

Las NIA-ES-SP tienen implícito un concepto fundamental: el auditor, al planificar una auditoría, debe identificar y valorar los riesgos de auditoría que pueden existir al ejecutar el trabajo y emitir su informe; teniendo en cuenta ese análisis, debe diseñar un conjunto equilibrado de procedimientos de forma que los riesgos queden reducidos a un nivel aceptable a la hora de emitir el informe de auditoría.

Este enfoque de auditoría basado en el análisis de los riesgos (o enfoque de riesgo) debe aplicarse al conjunto de la auditoría y con especial cuidado profesional en aquellas áreas más significativas o en aquellas cuyos riesgos inherentes sean típicamente altos, como es el caso de la Tesorería. La gestión de la tesorería es el resultado final de la gestión de gran cantidad de transacciones del resto de áreas de ingresos y gastos, de las actividades de inversión y de financiación, con las que está enlazada mediante múltiples interfaces automatizadas. La gestión de cobros y pagos con las entidades financieras también está automatizada y cuenta con interfaces informatizadas entre la aplicación de tesorería propia con las entidades financieras.

En estas situaciones, especialmente **en las entidades de tamaño mediano o grande, llegar a una conclusión u opinión de auditoría (favorable, con salvedades, denegada o desfavorable) sólo con pruebas sustantivas es, en la práctica, imposible**, siendo preciso confiar en los controles de procesamiento de la información, automatizados en su mayor parte o TI dependientes, implantados en la aplicaciones TI de gestión de la tesorería que ha diseñado e implantado la entidad y, por tanto, deben hacerse pruebas de auditoría sobre el diseño,

implementación y eficaz funcionamiento de los controles de procesamiento de la información (CPI) y de los controles generales de tecnologías de la información (CGTI) que los respaldan.

Esta guía es aplicable en las auditorías del área de tesorería y su **objetivo** es ayudar al auditor a:

- Adquirir un conocimiento profundo de los procedimientos/procesos de gestión establecidos por la entidad para la gestión de los cobros, pagos y el control de las cuentas de tesorería.
- Identificar y valorar los riesgos inherentes existentes en las afirmaciones relacionadas y determinar cuáles son riesgos significativos.
- Identificar, analizar y revisar el adecuado diseño, implementación y funcionamiento operativo de los CPI relevantes que abordan los riesgos inherentes significativos existentes.
- Identificar los CGTI que respaldan los CPI relevantes y revisar su adecuado diseño, implementación y funcionamiento operativo.
- Diseñar las pruebas de auditoría más adecuadas para probar la eficacia del diseño y el funcionamiento de los controles relevantes.
- Establecer los procedimientos sustantivos mínimos recomendados para la fiscalización del área de tesorería, incluyendo un contenido orientativo del programa de auditoría.
- Documentar los procedimientos ejecutados, la evidencia obtenida y las conclusiones alcanzadas.

La adecuada comprensión de esta guía **requiere el conocimiento previo de las NIA-ES-SP 1330, GPF-OCEX 1315R, 5330 y 5340**. La GPF-OCEX 5340 incluye un apartado de **definiciones** que también es aplicable a la presente guía.

2. Ámbito subjetivo de aplicación

Esta guía está diseñada para la fiscalización de cualquier entidad del sector público.

En las entidades de menor tamaño y complejidad podrá limitarse la aplicación de determinados procedimientos si a juicio del auditor resulta más eficiente y se alcanzan igualmente los objetivos de auditoría.

3. Ámbito objetivo de aplicación

La guía es aplicable a la fiscalización/auditoría del área de Tesorería. En particular las cuentas a las que son de aplicación las orientaciones de la presente guía son:

Entidades que aplican el PCG y sus adaptaciones		Entidades que aplican el PCGP y sus adaptaciones	
570, 571	Caja	570, 574	Cajas
572-575	Bancos e instituciones de crédito	571, 573, 575, 577	Entidades bancarias
576	Inversiones a CP de gran liquidez	578, 579	Otras cuentas de tesorería
		558	Pagos a justificar
		554	Cobros pendientes de aplicación
		555	Pagos pendientes de aplicación
		550	Pagos en formalización
		558	Anticipos de caja fija

Hay que tener presente que las cuentas de tesorería están íntimamente relacionadas con la mayor parte de las operaciones de ingresos, gastos, financiación, etc. de cualquier entidad, por lo que será necesario conocer dichas interrelaciones.

4. Objetivos de la auditoría del área

El **objetivo general de auditoría** del área consiste en determinar si los saldos de las cuentas de tesorería han sido adecuadamente gestionados y presentados en las cuentas anuales fiscalizadas, si estas reflejan de forma completa y exacta dichos saldos, de acuerdo con las normas contables o presupuestarias aplicables, y si la gestión se ha realizado de conformidad con la normativa aplicable.

El auditor debe diseñar y aplicar procedimientos de auditoría que sean adecuados, teniendo en cuenta las circunstancias, de forma que le permita obtener evidencia de auditoría suficiente y adecuada para poder alcanzar conclusiones razonables en las que basar su opinión. *(NIA-ES-SP 1500)*

Se debe obtener evidencia suficiente y adecuada de que los saldos de tesorería contabilizados están libres de incorrección material, debida a fraude o error. Esto significa que las afirmaciones que subyacen en los tipos de transacciones, saldos contables e información a revelar (TTSCIR) son válidas. Las afirmaciones son el elemento central para la identificación y valoración de los riesgos inherentes, identificar los controles y para seleccionar los procedimientos de auditoría más eficaces.

Las **afirmaciones** y los **objetivos detallados** de auditoría relacionados con la tesorería son:

Afirmación		Descripción/Objetivo
Existencia	E	Los saldos de tesorería (caja y bancos) existen realmente. Los cobros y pagos del periodo son reales.
Derechos y obligaciones	DO	Los saldos de tesorería (caja y bancos) son propiedad/titularidad de la entidad y no hay restricciones que limiten su disponibilidad.
Completitud	C	Los saldos de tesorería incluyen los fondos en todas las delegaciones/localidades, y todo tipo de fondos, en custodia, en tránsito, cajas fijas, etc. No se han producido omisiones. La totalidad de los cobros y pagos se han contabilizado.
Exactitud, valoración e imputación	Ex	Los saldos de tesorería están adecuadamente valorados. Los cobros y pagos son registrados prontamente en importe, periodo y cuentas correctas.
Clasificación	Cl	Los saldos de tesorería están adecuadamente clasificados en las cuentas anuales.
Presentación	P	La memoria recoge toda la información requerida sobre los saldos de tesorería.
Legalidad	L	Se han observado todas las normas legales aplicables a las transacciones de efectivo.

Por la propia naturaleza de las cuentas de tesorería, su valoración no debe constituir ningún problema, ya que normalmente están auto valoradas, por ser moneda de curso legal.

El programa detallado de auditoría debe atender a estos objetivos y adaptarse a las características de la entidad y a los riesgos de auditoría.

Desde el punto de vista del control interno, con carácter general, verificaremos si los procedimientos administrativos y las normas de control interno definidos por la dirección son adecuados para asegurar un control efectivo y si han funcionado adecuadamente en el periodo auditado.

La **conclusión global de auditoría del área** debe ser inequívoca, debe expresar la opinión profesional (basada en la evidencia obtenida tras todas las pruebas de auditoría realizadas) sobre si la cifra de tesorería que reflejan las cuentas anuales es completa, exacta, está adecuadamente contabilizada y si la gestión ha sido conforme con la normativa.

5. Obtención de conocimiento del proceso de gestión de tesorería y de la aplicación TI que lo soporta

Para poder diseñar pruebas de auditoría eficaces, que permitan alcanzar el objetivo pretendido al auditar la tesorería, es necesario conocer los procedimientos de gestión que tenga implantados la entidad fiscalizada. No se puede auditar algo cuyo funcionamiento se desconoce.

Así, de acuerdo con el apartado 25 de la GPF-OCEX 1315R (ver también el apartado 4 y 6 de la GPF-OCEX 5340) el auditor debe obtener conocimiento del sistema de información y comunicación de la entidad que sea relevante para la preparación de los estados financieros y para la gestión y contabilización de la tesorería en este caso. Para ello, debe aplicar procedimientos de valoración del riesgo a través del conocimiento de las actividades de procesamiento de la información de gestión de tesorería de la entidad, incluidos sus datos e información, los recursos que se deben utilizar en esas actividades y obtener conocimiento sobre:

(a) el modo en que la información fluye por el sistema de información, incluido el modo en que:

- las transacciones se inician y la información que sobre ellas se registra, se procesa, se corrige si es necesario, se traslada al mayor y se incluye en los estados financieros; y
- la información sobre los hechos y condiciones, distintos de las transacciones, que se captura, se procesa y se revela en los estados financieros;

(b) los registros contables, cuentas específicas de los estados financieros y otros registros de soporte relacionados con los flujos de información en el sistema de información;

(c) el proceso de información financiera utilizado para la preparación de los estados financieros de la entidad, incluida la información a revelar; y

(d) los recursos de la entidad, incluido el entorno de TI, relevantes para los apartados (a) a (c) anteriores, (la aplicación informática que soporta el proceso de gestión de tesorería y las interfaces existentes, entre otras cuestiones).

Memorándum/narrativa

Aunque en cada entidad habrá ligeras variaciones, básicamente interesa conocer y documentar el proceso de gestión de la tesorería, tanto cobros como pagos.

Para ello, se debe entrevistar a las personas responsables de las distintas tareas, elaborar una narrativa descriptiva y realizar pruebas paso a paso (ver GPF-OCEX 1511) para confirmar que el conocimiento de los procedimientos aplicados es correcto, es decir, que la descripción se corresponde con los procedimientos ejecutados en la práctica por la entidad. Debe documentarse de forma clara para facilitar la identificación de riesgos que afecten a las cuentas anuales o al cumplimiento de la legalidad y así poder centrar las pruebas de auditoría en esos riesgos.

Para facilitar la adquisición del conocimiento de los procedimientos de gestión y su documentación se puede utilizar el formulario modelo que se adjunta en el Anexo 1, o bien narrativas o memorándums alternativos a ese modelo que sean lo suficientemente claros y descriptivos.

Si la entidad dispone de **procedimientos formalizados** por escrito, la narrativa a realizar por el auditor será tanto más breve cuanto más completos y claros sean aquéllos, que serán archivados completos en el Archivo Permanente de los papeles de trabajo electrónicos y un resumen (tan extenso como se considere necesario) también en el Archivo Corriente, y serán adecuadamente referenciados. Por esta razón, dichos procedimientos deberán solicitarse al principio de la auditoría.

Descripción gráfica del proceso de gestión de la tesorería

Se recomienda vivamente complementar la narrativa con diagramas de flujo y tablas de riesgos y controles. Cuando se trata de procesos de gestión complejos como el que estamos estudiando, se empezará dibujando el mapa del proceso o flujograma general (como el del ejemplo siguiente), señalando los principales subprocesos o funciones, que posteriormente se han de describir con mayor detalle, y los departamentos implicados en cada uno de ellos. (Ver GPF-OCEX 1512).

La gestión de la tesorería se encuentra condicionada por todo el proceso de gestión presupuestaria-contable, pues muchos de los controles que afectan a la tesorería se ubican en las fases previas de este proceso (por ejemplo, para que se pueda pagar un gasto debe haber sido previamente presupuestado, autorizado, dispuesto, justificado, fiscalizado y contabilizado).

En una entidad de tamaño mediano o grande, el proceso de gestión de tesorería está soportado por una aplicación informática, que puede estar integrada o interrelacionándose con otras. Habrá que tener especial cuidado al analizar las interfaces que relacionan la aplicación de tesorería con el resto de las aplicaciones de gestión, en especial con la contable.

Para identificar y analizar las aplicaciones de gestión y las interfaces existentes será conveniente contar con la colaboración de expertos en auditoría de sistemas de información.

6. Identificación de los riesgos de incorrección material (RIM) *(Ver apartado 4.2 y 5 de la GPF-OCEX 5340)*

6.1 Identificación y valoración de los RIM en los estados financieros *(Ver apartado 5.1 de la GPF-OCEX 5340)*

Se deberá identificar y valorar los RIM en los estados financieros y/o el área de tesorería con la finalidad de (a) determinar si dichos riesgos **afectan a la valoración de riesgos en las afirmaciones** y (b) evaluar la naturaleza y extensión de su **efecto generalizado** sobre los estados financieros.

Los RIM en los estados financieros se refieren a los riesgos que se relacionan de forma generalizada con los estados financieros en su conjunto o con el área de tesorería en particular, pero que pueden afectar a muchas afirmaciones (por ejemplo, (a) si la entidad tiene un departamento de tesorería claramente infradotado afectará de forma generalizada a los componentes de los estados financieros auditados y, en especial, si el entorno de control es deficiente; otro ejemplo sería (b) si la entidad tiene establecido un sistema de gestión de la tesorería totalmente automatizado con muy poca intervención humana, pueden esperarse riesgos derivados del uso de las TI incluyendo ciberriesgos).

Si los riesgos identificados tienen un efecto generalizado en los estados financieros requerirán una respuesta global de acuerdo con la NIA-ES-SP 1330. Una posible respuesta a (a) sería incrementar las pruebas sustantivas, y a (b) planificar la intervención de un equipo de auditoría de sistemas de información. Estos riesgos también pueden afectar a las afirmaciones individuales y, por lo tanto, también pueden ayudar a determinar los procedimientos posteriores de auditoría para abordar los riesgos identificados en las afirmaciones.

La identificación de los riesgos en los estados financieros y/o el área de tesorería se ve influenciada por:

(a) El conocimiento por parte del auditor del sistema de control interno de la entidad, en particular la evaluación e identificación de deficiencias en los controles indirectos (CGTI).

(b) Susceptibilidad a la incorrección debido a factores de riesgo de fraude que afectan al riesgo inherente. (En el área de tesorería por la naturaleza líquida del activo a proteger **el riesgo de fraude mediante el uso de las TI es especialmente relevante**).

6.2 Identificación y valoración de los riesgos inherentes en las afirmaciones

Al analizar el proceso de gestión se deben identificar, en cada una de sus fases, los riesgos inherentes existentes en las afirmaciones, valorarlos, elaborar el espectro de riesgo inherente y determinar aquellos riesgos que se considerarán significativos (los que se encuentran próximos al límite superior del espectro de riesgo inherente).

Cuando se aborda el análisis de los riesgos de un determinado proceso de gestión el enfoque principal consiste en responder, tanto con carácter general, como en cada una de las fases del proceso analizados, a la pregunta:

¿**Qué puede ir mal** en el proceso de gestión de tesorería que pueda afectar significativamente a las cuentas anuales o al cumplimiento de la legalidad?

También se puede formular la pregunta así:

¿Qué podría ocurrir en esta fase que pudiera afectar negativamente en la consecución de los objetivos del proceso?

¿Representaría esto un RIM?

Se deben repetir estas preguntas en cada una de las etapas del proceso, teniendo en cuentas los factores de riesgo inherente.

La identificación de los riesgos potenciales se realiza entrevistando a usuarios y responsables del proceso de gestión auditado y analizando los distintos pasos y componentes que intervienen en el proceso (ver Anexo 1):

- El flujo de procesamiento de los datos
- Los permisos o autorizaciones
- Las interfaces (datos entrantes y salientes)
- Los datos maestros
- La segregación de funciones

Para facilitar el trabajo se pueden establecer listas previas sistematizadas y ordenadas, como la de la siguiente Tabla 1, en la que se señalan algunos de los principales riesgos inherentes que pueden existir.

Al completar la tabla siguiente, en la columna magnitud se pondrá el importe estimado de la incorrección potencial esperada. Dado que solo se deben tener en cuenta los riesgos materiales, se descartarán aquellos riesgos inherentes cuya magnitud no se acerque al nivel de materialidad que previamente hayamos definido de acuerdo con las NIA-ES-SP 1320 y GPF-OCEX 1321 (2024) para cada TTSCIR. Por ejemplo, se pueden descartar aquellos riesgos cuyo efecto estimado sea inferior a la cifra de incorrecciones claramente insignificantes (**ICI-TSI**), definida en la nueva GPF-OCEX 1321 (2024) para cada TTSCIR.

Se debe realizar o discutir este análisis en una reunión del equipo (ver GPF-OCEX 1513).

Valorar el riesgo inherente sin tener en cuenta los controles de la entidad, ayuda a evitar, por ejemplo, realizar valoraciones de riesgo inherente inadecuadamente bajas basadas en supuestos o en la **confianza excesiva** de que los controles funcionan de manera eficaz, sin haber evaluado el diseño y probado la eficacia operativa de dichos controles.

La siguiente tabla es un ejemplo orientativo, no es exhaustiva.

Tabla 1. Ejemplo de valoración de los riesgos inherentes en las afirmaciones

#	Riesgos inherentes	Función	Afirma-ción	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I.(PxM)
RT01	Apropiación indebida de los fondos de bancos, por ejemplo, realizando transferencias fraudulentas a cuentas ajenas.	**Gestión de tesorería**	E, L			
RT02	Existen cuentas bancarias no contabilizadas ni controladas.		C, L			
RT03	Existen cuentas bancarias sin movimiento en los últimos años.					

#	Riesgos inherentes	Función	Afirma-ción	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I.(PxM)
RT04	Se producen cambios de cuentas con excesiva frecuencia					
RT05	Existen personas autorizadas para disponer en cuentas sin tener competencia para ello (porque nunca la tuvieron o porque han dejado de tenerla).		E, L			
RT06	Existen firmas solidarias para disponer en cuentas, lo que representa un riesgo de disposición indebida de fondos.		E			
RT07	Los datos del FMT no son exactos.	**Mantenimiento del FMT (Fichero Maestro de Terceros)**	E			
RT08	Se producen altas y modificaciones no autorizadas en el FMT que pueden derivar en pagos a terceros incorrectos o fraudulentos.		E, L			
RT09	Pagos realizados por bienes o servicios no recibidos, pagos inexactos o excesivos.	**Pagos**	Ex, L			
RT10	Pagos realizados por personas no autorizadas o sin competencia (que acceden a la aplicación de pagos). Incluye los fraudes por suplantación de identidades en el sistema o en los correos electrónicos para el envío de órdenes de pago. Falsificación de órdenes de pago.		E, L			
RT11	Realizar pagos excesivos o indebidos en cuentas extrapresupuestarias.	**Pagos extrapresu-puestarios**	E, L			
RT12	Modificación no autorizada de la información en la interfaz manual ERP[1]-Bancos para realizar pagos, ya que la carpeta donde se deposita transitoriamente el fichero Cuaderno 34-XML puede no estar debidamente protegida frente a accesos no autorizados.	**Interfaz de pagos**	L			
RT13	Pagos indebidos por modificación no autorizada de la información en la interfaz automatizada ERP-EDITRAN-Bancos para realizar pagos.		L			
RT14	Omitir o retrasar el registro de las entradas de efectivo/cobros.	**Cobros**	Ex			
RT15	Detraer las entradas de efectivo, una vez registradas.		E, L			
RT16	Ocultar operaciones introduciendo abonos no justificados (p. e., bonificaciones o exenciones) o anulaciones simuladas para ocultar la apropiación indebida de los cobros. Que se cancelen cuentas a cobrar como si fueran incobrables, sustrayendo los fondos o facturando por importes inferiores a los normales para disimular las cantidades sustraídas.		E, L			

[1] ERP: Enterprice Resource Planing. Es el software utilizado por la organización para gestionar sus actividades empresariales diarias como pueden ser, entre otras, la tesorería

#	Riesgos inherentes	Función	Afirma-ción	Probabilidad (1 a 10)	Magnitud (1 a 10)	Valoración del R.I.(PxM)
RT17	Contabilización errónea o fraudulenta de saldos pendientes de cobro o pago y de movimientos bancarios	**Contabilidad**	Ex			
RT18	Ocultar operaciones no autorizadas o fraudulentas mediante la falsificación de conciliaciones bancarias.		Ex, L			
RT19	La interfaz de la aplicación de tesorería con la aplicación contable (en los casos que no sea la misma aplicación) no garantiza la integridad de los datos, lo que puede posibilitar la comisión de fraudes.		E Ex L			
RT20	No se registran todos las entradas y salidas de efectivo en las cajas. Se pueden detraer efectivo de forma no autorizada sin que sea detectado	**Caja**	E, Ex, L			
RT21	Apropiación indebida de los fondos de caja. Los saldos de efectivo no están protegidos		E, L			

Aunque no son objeto de estudio en esta guía no debe pasarse por alto también los riesgos relacionados con los avales contraídos y las fianzas (con relación a su custodia, conciliación entre contabilidad y documentación de los constituidos y cancelados, sobre si se cumple la normativa, riesgos en gestión de avales en formato digital, etc).

6.3 Determinar los riesgos significativos en el espectro de riego inherente *(Ver apartado 5.6 de la GPF-OCEX 5340)*

Una vez completada una tabla como la Tabla 1, una forma fácil de calcular el espectro de riesgo inherente consistirá en ordenarla según el valor, de mayor a menor, de la columna "**Valoración del R.I.**".

Serán riesgos significativos los que estén ubicados en la parte alta de la tabla. El límite para distinguir cuales son riesgos significativos y cuáles no, será una cuestión de juicio profesional y dependerá de las circunstancias.

6.4 Determinar los riesgos para los que los procedimientos sustantivos por sí solos no proporcionan evidencia de auditoría suficiente y adecuada *(Ver apartado 5.7 de la GPF-OCEX 5340)*

El auditor también debe determinar qué riesgos no pueden ser abordados únicamente con procedimientos sustantivos, que no pueden proporcionar evidencia de auditoría suficiente y adecuada con respecto a alguno de esos riesgos significativos en las afirmaciones y, por tanto, se requiere la aplicación de pruebas de controles.

Este puede ser el caso en aquellas circunstancias en las que una cantidad significativa de la información de la entidad se inicia, registra, procesa o notifica solo de manera electrónica, como en un ERP que implica un alto grado de integración a través de sus aplicaciones de TI. Un ejemplo claro de esto sería la auditoría de una entidad mediana o grande, en la que el proceso de gestión de tesorería está **muy automatizado** con escasa o nula intervención manual y **la evidencia de auditoría únicamente está disponible en formato electrónico** y su suficiencia y adecuación dependen de la eficacia de los controles sobre su exactitud y completitud *(en un gran ayuntamiento, con cientos de miles de movimientos de tesorería, revisar las conciliaciones bancarias manualmente probablemente no permitirá reducir el riesgo de auditoría a un nivel aceptable y será preciso valorar el riesgo de control y revisar los CPI y los CGTI relacionados).*

La posibilidad de que la información se inicie o altere de manera incorrecta y de que este hecho no se detecte puede ser mayor si los correspondientes controles no están funcionando de manera eficaz. En estas circunstancias, la única forma de obtener evidencia de auditoría suficiente y adecuada es comprobar la eficacia operativa de los controles existentes.

Un aspecto relevante a considerar es la posible existencia de procedimientos administrativos automatizados en los que no interviene un funcionario persona física en la tramitación y resolución del procedimiento. En estos casos, si las transacciones son significativas y se han valorado con un nivel elevado de riesgo inherente se deberá verificar si se han cumplido todos los requisitos y aprobaciones en el establecimiento del procedimiento automatizado y que los controles implantados funcionan correctamente.

6.5 Los riesgos de fraude en el área de tesorería

El área de tesorería ha sido siempre un área propensa a que se cometan fraudes e irregularidades de distinto tipo. La razón es muy sencilla, es más fácil robar dinero en efectivo o en bancos que un inmueble, por ejemplo.

Las amenazas tradicionalmente eran internas, pero con la utilización intensiva de los sistemas de información y la interconexión por internet, además de incrementarse aquellas, han aumentado de forma exponencial las amenazas externas debido a las vulnerabilidades que puede ofrecer un sistema de información mal protegido.

Tanto las amenazas internas como las externas pueden ser minimizadas con un adecuado sistema de control interno implantado de forma efectiva.

Pero, en un entorno de administración electrónica avanzado cualquier sistema de control interno debe incluir un sólido sistema de ciberdefensa basado en el ENS, es decir, **los CPI deben estar respaldados por los CGTI necesarios ya que si no cualquier sistema de control interno es tan solo un cascarón vacío**.

Riesgo de fraude manipulando el fichero maestro de terceros (FMT)

Uno de los mecanismos más utilizados para cometer un fraude ha consistido, tradicionalmente, en la manipulación indebida de los datos relativos a los terceros a los que hay que pagar determinadas cantidades por cualquier motivo, a priori legítimo, bien sea como pago por la compra de bienes o servicios, por nóminas, subvenciones, etc. Dichos datos, incluyendo los relativos a las cuentas bancarias donde se realizan los pagos, se mantienen en un fichero que denominamos Fichero Maestro de Terceros, el cual siempre ha sido objeto de protección especial por parte de los sistemas de control interno.

Este riesgo de fraude clásico tenía como principales amenazas los usuarios internos. La utilización de sistemas de información interconectados y en particular el uso de internet ha ocasionado un aumento de las **amenazas internas y** sobre todo las **externas** que pueden provenir de cualquier parte del mundo, y por tanto la multiplicación de los riesgos de fraude y la exigencia de una sólida red de controles para proteger la seguridad y la integridad del FMT.

Como señala Godino y Menéndez[2], una de las funciones clave de la Tesorería, como es la tramitación de pagos, está en el punto de mira de la delincuencia organizada, la cual, aprovechándose de las vulnerabilidades de las Administraciones públicas, opera de forma fraudulenta para suplantar identidades y de este modo desviar los pagos dirigidos a los verdaderos acreedores, produciendo con ello un menoscabo en las arcas públicas al tratarse de un pago que no tiene carácter liberatorio.

Ver más información en el Anexo 1A.

Ciberriesgos

Los fraudes derivados de malas praxis relacionadas con la seguridad de los sistemas de información son de muy distinto tipo:

- Fraude del CEO (se vulneran los procedimientos y se hacen pagos a IBAN distintos a los del FMT). Este fraude utiliza métodos de ingeniería social para vulnerar los procedimientos y los controles, con la finalidad de inducir pagos a proveedores y/o cuentas que no están en el FMT[3].
- *Phishing*. Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas. Con este método se consigue hacer cambiar el IBAN existente en el FMT de un proveedor, para pagar una deuda real a la cuenta de los defraudadores. Para culminar el fraude hay que vulnerar los procedimientos y controles[4].
- Ataques *Man in the middle*. Consiste en interceptar la comunicación entre un emisor y un receptor, pudiendo espiar o modificar la información con fines maliciosos.

[2] **Seguridad y eficacia en los pagos. El fraude bancario. Cómo minimizar los riesgos y evitar responsabilidades derivadas**. Rosario Godino López y Marina Menéndez Miralbés, Revista de Estudios Locales nº 271. Este artículo analiza en profundidad toda la problemática relacionada con los FMT y por eso es recomendable su lectura.

[3] El caso más mediático fue el perpetrado hace unos pocos años a una empresa municipal de transporte urbano en el que defraudaron 4,5 millones de euros que no se han recuperado.

[4] La implantación del protocolo DMARC en los correos electrónicos mitiga este riesgo. Ver nota al pie nº 10.

- Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
- Suplantación de identidad (por métodos distintos al *phishing*). Se accede al sistema y se suplanta la identidad de un usuario autorizado para hacer cambios indebidos en el FMT o para hace pagos no autorizados.[5]
- Modificación no autorizada de información. Ej: modificación del IBAN por un atacante empleando credenciales sustraídas de un sistema.
- Los CGTI son muy débiles o inexistentes y se puede acceder sin dificultad al FMT u otros procesos y/o registros para hacer cambios indebidos. (Ver apartado 10).

6.6 Otros riesgos

Una fuente de información interesante, que periódicamente proporciona información sobre fraudes cometidos, son las noticias de prensa. Tomando una noticia del 7 de diciembre de 2023 sobre un informe emitido por la Intervención General de una comunidad autónoma se puede hacer un breve catálogo básico de riesgos de fraude (omitimos las entidades fiscalizadas, pero según esa noticia afectan en distinto grado al 90% de las entidades auditadas y un 46% tienen un nivel de riesgo alto en el área de pagos), según aquella:

- Las empresas de la Comunidad sin control en los pagos a proveedores (titular).
- La Intervención alerta del riesgo de fraude o error en los pagos (subtítulo)
- La Intervención detecta 22 entidades con un nivel de riesgo alto en el área referida a los pagos.
- Las principales incidencias se refieren a la ausencia de procedimientos formalmente aprobados de **verificación de los datos de terceros** y sus cuentas bancarias, así como la **ausencia de identificación electrónica segura del tercero y de la cuenta bancaria destinataria del pago**.
- Deficiencias en la emisión y firma de las órdenes de pago.
- Se recomienda el establecimiento de medidas técnicas que posibiliten que **las conciliaciones de saldos bancarios y contable se realicen de manera informática y con periodicidad no superior a la semana**.
- Se recomienda implantar sistemas de evaluación de riesgos que permitan identificar y medir aquellos que afectan al área de gestión financiera y adaptar el sistema de control interno de forma que se evite o reduzca la probabilidad de su ocurrencia e impacto.

7. Identificación de los controles de procesamiento de la información relevantes

7.1 Qué son los CPI relevantes

Tras la narrativa, el dibujo de los flujogramas y la identificación de los riesgos y controles existentes, estos se recogerán en unas tablas que relacionen los riesgos significativos identificados (los que están en la parte superior del espectro de riesgo inherente tal como se ha visto antes) con los CPI. Un ejemplo posible es la Tabla 2 siguiente.

Además de identificar los riesgos inherentes del proceso de gestión, en las interfaces y en los datos maestros, debe adquirirse una comprensión preliminar de los CPI (manuales o automatizados) que mitiguen dichos riesgos.

[5] José Manuel Farfán Pérez en el artículo **Gestión de pagos en la Administración Local: ciberseguridad y validación de cuentas**, en "El Blog de espublico",señala que la directiva PSD2 ha aumentado la seguridad en las transacciones, pero a la vez se está produciendo un fenómeno de **incremento de la ciberdelincuencia en los procesos anteriores al pago, a través de la suplantación de identidad en los procesos de acreditación de terceros**. Las malas prácticas han posibilitado una creciente proliferación de fraudes de suplantación de identidad y los pagos a un tercero no acreedor.

En esta fase, el auditor identificará los **CPI**, que son controles aplicados durante el procesamiento de la información en el sistema de información de la entidad y **responden directamente a los riesgos para la integridad de la información, es decir, la completitud, exactitud y validez de las transacciones y otra información[6].** A estos objetivos, en el sector público hay que añadir el de **legalidad**.

Teniendo en cuenta la complejidad de los procesos y de las aplicaciones de gestión en los actuales entornos de gestión de tesorería, es importante centrarse en lo esencial, por ello la identificación de los riesgos significativos y de los CPI implantados para mitigarlos constituye la base para una auditoría eficaz. Solo se revisarán aquellos CPI que tengan relevancia a efectos de la auditoría, circunstancia que deberá ser definida por el auditor a partir de los riesgos significativos identificados.

Serán CPI relevantes los controles que el auditor debe identificar, cuyo diseño debe evaluar y cuya implementación debe verificar. Según la GPF-OCEX 1315R (25 y A151) y la GPF-OCEX 5340 (apartado 5.7) son:

- **Controles que responden a riesgos que se consideran significativos**. El conocimiento obtenido acerca del enfoque de la dirección para responder a esos riesgos puede proporcionar una base para el diseño y aplicación de procedimientos sustantivos que respondan a riesgos significativos. Generalmente incluyen políticas, procedimientos, prácticas y una estructura organizativa que son esenciales para que la dirección pueda reducir los riesgos significativos y alcanzar el objetivo de control relacionado.

  Se requerirá el conocimiento de:

  - Espectro de riesgo inherente.
  - Controles que la entidad ha diseñado e implementado para los riesgos significativos derivados de cuestiones no rutinarias o que requieran la aplicación de juicio, como por ejemplo la revisión de hipótesis por la alta dirección o por expertos, documentación de las estimaciones contables o la aprobación por los responsables de la entidad.
  - Controles que la dirección ha diseñado, implementado y mantenido para prevenir y detectar el fraude.

- **Controles sobre asientos en el diario**, incluidos aquellos asientos que no son estándar y que se utilizan para registrar transacciones o ajustes no recurrentes o inusuales.

  La identificación de asientos no estándar en el diario, en los sistemas de mayores manuales requerirá la inspección de los mayores, diarios y documentación soporte. Si se utilizan procesos automatizados para la llevanza de los libros, el uso de técnicas de auditoría automatizadas facilitará esta identificación.

- **Controles cuya eficacia operativa se tiene previsto comprobar para determinar la naturaleza, el momento de realización y la extensión de los procedimientos sustantivos**. La evaluación estos controles proporciona al auditor la base para el diseño de pruebas de controles de conformidad con la NIA-ES-SP 1330.

- **Controles que responden a riesgos para los cuales los procedimientos sustantivos por si solos no proporcionan evidencia de auditoría suficiente y adecuada.**

- **Otros controles** que el auditor considere adecuado identificar, como:

  - Controles que responden a riesgos valorados como más alto dentro del espectro de riesgo inherente pero que no han sido considerados riesgos significativos.
  - Controles relacionados con conciliaciones de registros detallados con el mayor.
  - En el caso de utilizar una organización de servicios, controles complementarios de la entidad usuaria. Si se utilizan servicios de computación en la nube se tendrá en consideración la GPF-OCEX 1403.

En la revisión de estos controles se analizará si respaldan más de un objetivo de control y si hacen frente directamente a los riesgos significativos. En su evaluación se tendrá también en cuenta que los controles preventivos son, por regla general, más eficientes que los detectivos y que los controles automatizados son más fiables que los controles manuales. Cuando múltiples controles alcancen individualmente el mismo objetivo, no es necesario identificar cada uno de los controles relacionados con dicho objetivo.

[6] Apartado A148 de la NIA-ES 315R/GPF-OCEX 1315R.

Los controles que responden a los riesgos de incorrección material en las afirmaciones, individualmente o combinados entre ellos, son indispensables para la reducción de los riesgos a un nivel aceptable. Son los que permiten reducir los riesgos de incorrección material (RIM) a un nivel aceptablemente bajo.

Los CPI relevantes constituyen el elemento fundamental del sistema de control y deben ser, pues, objeto de comprobación prioritaria; los otros controles tienen menos importancia para el auditor.

Todo el trabajo de auditoría posterior debe centrarse en estos controles, ya que todo trabajo que se realice sobre los otros controles existentes no aporta satisfacción o utilidad adicional de auditoría, y será un trabajo ineficiente.

Para documentar la valoración del riesgo de control se puede cumplimentar una tabla como la siguiente relacionando riesgos inherentes significativos para las afirmaciones identificados con los CPI relevantes.

Tabla 2. Riesgos inherentes significativos en las afirmaciones y CPI relevantes

TTSCIR	Afirmación	Riesgos (inherentes) significativos	CPI relevantes
Para cada saldo contable	Existencia		
	Derechos y obligaciones		
	Completitud		
	Exactitud, valoración e imputación		
	Clasificación		
	Presentación		

Si hay varios controles que tienen el mismo objetivo, el auditor deberá entender cada uno de ellos y seleccionar como controles relevantes aquellos que considere que alcanzan más eficazmente su objetivo y teniendo en cuenta el coste/eficacia que puede suponer su comprobación.

Se debe analizar si el equilibrio entre controles manuales/automatizados y entre preventivos/correctivos es adecuado. Una excesiva confianza en controles manuales en un entorno informatizado puede ser un indicador de debilidad del control interno.

El auditor debe evitar depositar un exceso de confianza en los controles automatizados en un entorno de administración electrónica mediante una adecuada revisión de su diseño, implantación y eficacia operativa.

7.2 Principales controles internos del área de tesorería

La entidad auditada debe mantener un adecuado control interno sobre el dinero en efectivo dado que la mayoría de las transacciones finalizan en movimientos de caja y bancos, y la falta de controles puede incentivar actividades fraudulentas.

En la **organización interna** de una entidad se deben contemplar requisitos como los siguientes:

- El departamento de tesorería debe estar separado de cualquier otro.
- El tesorero no debe realizar funciones de cuentas a cobrar y a pagar.
- Los empleados del departamento de tesorería deben tener claramente definidas sus funciones y responsabilidades.
- Debe existir una política financiera adecuada, por escrito, en cuanto a las cuentas bancarias, autorizaciones, etc.

Los **principales controles** en el área de tesorería incluirán (relación no exhaustiva):

- Los **procedimientos** de gestión de la tesorería (cobros, pagos o transferencias, mantenimiento del fichero maestro de terceros, etc) han de constar por escrito y reflejar los límites y autorizaciones.
- Existencia de una adecuada **segregación de funciones** en todo el proceso.
- Las firmas autorizadas para disponer en bancos han de ser siempre **mancomunadas**.
- Las operaciones de disposición de fondos a través de las plataformas de las entidades financieras se regularán en los pliegos de contratación de las cuentas bancarias de forma que se requerirá la remisión de un documento electrónico firmado electrónicamente por las personas autorizadas para que la entidad financiera pueda ejecutar las órdenes de pago mediante la operativa de la banca electrónica.

  Las condiciones de los pliegos o, en su defecto, las instrucciones cursadas por escrito a las entidades financieras deben detallar las verificaciones que son responsabilidad de la entidad financiera (verificar la autenticidad de firmas de las órdenes de pago, verificar la autenticidad e integridad de los ficheros de pago, …).
- **Controles de acceso**:
  - Solo los funcionarios de Tesorería deben tener acceso a la aplicación de gestión de tesorería o a las funcionalidades para el área de tesorería de la aplicación de contabilidad y la asignación de permisos a los usuarios de esa aplicación se realizará aplicando el principio de mínimo privilegio.
  - Los usuarios con acceso a la aplicación o funcionalidades de tesorería se revisan periódicamente para garantizar que los privilegios estén restringidos al personal adecuado.
  - Sólo los funcionarios de intervención tienen acceso a las funciones de fiscalización de ingresos y pagos.
  - Sólo los funcionarios de tesorería que lo necesiten para ejercer sus funciones deben tener acceso a la banca electrónica de las cuentas de la entidad.
  - Las autorizaciones de acceso y modificación del fichero maestro de terceros contemplan la segregación de funciones respecto a la gestión de ingresos y pagos (en una entidad local, por ejemplo, intervención realiza el alta y modificación de los ficheros de terceros y cuentas bancarias y los funcionarios de tesorería no tienen acceso a esos menús de la aplicación).
- Controles sobre los **cobros**:
  - De haber cobros en metálico (no recomendable, con carácter general), los cobros deben ingresarse en el banco inmediatamente, en cuentas distintas a las que se emplean para realizar pagos. Debe aplicarse el principio de proporcionalidad y si los cobros por caja son residuales no será preciso realizar los ingresos diariamente. Desde el punto de vista del auditor tendremos en cuenta los criterios de importancia relativa definidos en la planificación y el juicio profesional, para determinar la frecuencia recomendable en cada caso.
  - Se han de usar recibos numerados correlativamente para la recepción de ingresos, y establecer un adecuado control de los recibos en blanco.
  - Todas las operaciones se registran pronta y exactamente en la contabilidad o en registros auxiliares y se emiten los informes apropiados.
- Realizar **conciliaciones bancarias** periódicamente.

  Las conciliaciones bancarias constituyen un aspecto esencial en el control interno de la tesorería. Consisten en poner de manifiesto las diferencias entre los registros contables de la entidad y los saldos del banco, según los extractos, a una fecha determinada.

  Tradicionalmente se hacían en los formularios establecidos al efecto por una persona diferente de la que realiza los registros contables y el manejo de fondos. En un entorno informatizado deben realizarse automáticamente, como mínimo semanalmente, y preferiblemente de forma diaria (en las entidades grandes desde luego).

  Deben ser revisadas y firmadas por un responsable y debidamente supervisadas.

En un entorno de administración electrónica, la entidad realizará las conciliaciones bancarias con un alto grado de automatización. Los movimientos bancarios (ficheros norma 43[7]) diarios se recibirán al día siguiente a través del sistema EDITRAN y se cargarán de forma automatizada en el sistema contable (ERP).

Una vez cargados estos movimientos, el ERP realiza un procedimiento de conciliación automatizado con los movimientos contables transitorios o provisionales. Cuando son coincidentes se contabilizan de forma automatizada en la cuenta contable de tesorería correspondiente.

Si hay movimientos no coincidentes quedan registrados como movimientos transitorios pendientes de investigación hasta que definitivamente se aclaran, concilian y contabilizan.

Las conciliaciones bancarias no deben arrastrar partidas de forma indefinida. Aunque con carácter general no puede fijarse un plazo para su aclaración, debe efectuarse de forma diligente y sin demoras no justificadas ni razonables.

- Controles sobre los **pagos**:
  - El sistema realiza de forma automática un cruce entre orden de pago, pedido y factura, identificando y bloqueando partidas no coincidentes.
  - El sistema impide el registro de facturas duplicadas.
  - El sistema bloquea pagos donde el importe total facturado supera el límite establecido en los pliegos y/o contratos.
  - El sistema verifica automáticamente que una factura u obligación pendiente de pago no ha sido pagada anteriormente.
  - Las órdenes de pago se revisan junto con la documentación de respaldo para verificar su idoneidad y precisión antes de aprobarlas.
  - Una vez aprobada la orden de pago nadie está autorizado a modificarla, excepto con la firma del Tesorero e Interventor.
  - El sistema bloquea la realización de pagos no presupuestarios si el importe a pagar es mayor al ingreso no presupuestario que da origen al pago.
  - Las firmas electrónicas en las órdenes de pago garantizan la integridad.
  - El ERP **impide** (por configuración) que se puedan realizar pagos a cuentas bancarias distintas de las del FMT. **No puede realizarse ningún pago** a un IBAN que no esté registrado en el FMT para el acreedor correspondiente, en caso contrario el pago es rechazado automáticamente por el ERP.
  - Las firmas electrónicas en los correos electrónicos de remisión de las órdenes de pago garantizan la identidad del remitente. Se aplica el protocolo DMARC (ver nota al pie nº 11 en el Anexo 1B).

[7] La norma 43 es un estándar bancario que regula y normaliza la transmisión de extractos bancarios de cuentas corrientes. Fue desarrollado por las entidades de crédito españolas a través de sus respectivas asociaciones, con especial participación de la Asociación Española de Banca (AEB). Sirve, en mayor medida, para facilitar un proceso contable tan crítico e importante como es la conciliación bancaria, es decir, el contraste de la información de las cuentas bancarias de una empresa con su contabilidad, a fin de detectar cargos o abonos pendientes y, en general, conocer el estado real de su tesorería.

Las entidades bancarias suelen enviar de manera diaria estos ficheros a las empresas que tengan contratado este servicio a través de redes P2P, generalmente a primera hora de la mañana. Una vez recibido, los sistemas empresariales integran todos estos movimientos en sus sistemas y ejecutan la conciliación bancaria de manera automática. Adicionalmente, las entidades permiten la descarga manual de esta norma.

Desde el punto de vista técnico, el cuaderno 43 (norma 43) es un fichero que tiene una estructura definida donde están reflejados todos y cada uno de los movimientos (cargos y abonos) de las cuentas bancarias de una empresa durante un intervalo de tiempo determinado. A pesar de que cada entidad puede estructurar este fichero de forma diferente, en la mayoría de los casos consta de varios tipos de registros: saldo inicial, movimientos y saldo final.

- Controles sobre las **interfaces**:
  - El acceso a la ruta donde se almacena la información que vuelca entre sistemas se encuentra debidamente restringido.
  - El ERP genera automáticamente los ficheros con el detalle de las transferencias bancarias en formato XML (Cuaderno 34) y lo remite al banco mediante un servicio web o canal seguro.
  - Cuando la interfaz no es automatizada, por ejemplo, si el fichero XML (Cuaderno 34) se envía a través de la página web de la banca electrónica, las carpetas donde se depositan los ficheros de pago están debidamente protegidos.
  - Una vez generado el fichero XML, la aplicación bloquea la orden de pago correspondiente.
- Controles sobre la **caja**
  - Existen procedimientos por escrito y aprobados para la gestión de las cajas de efectivo.
  - Se realiza un arqueo diario de los saldos de cada una de las cajas de efectivo llevando el control de entradas y salidas desde el saldo anterior. El arqueo es presenciado por un responsable que supervisa al cajero. El arqueo debe firmarse por ambos. En algunas ocasiones debe ser sorpresivo.
  - Existe una aplicación para registrar los ingresos por los precios públicos. Los usuarios de la aplicación pueden registrar, pero no borrar los apuntes de cobro. Los ingresos se traspasan automatizadamente a la contabilidad.
  - Sólo gestionan las cajas las personas que tienen asignadas estas tareas. Existe segregación de funciones respecto a contabilización y cobro.
  - El efectivo en caja está sometidos a eficaces procedimientos de custodia y protección física.
  - Debe haber protección contra los incendios, robos, etc. Existen cajas fuertes para proteger el efectivo.
- **Controles contables:**
  - La contabilización es automática.
  - Todos los asientos de tesorería no automatizados están restringidos y son supervisados.
  - El personal con acceso a modificar la información contable se encuentra adecuadamente restringido mediante la asignación de permisos de acceso a los menús de contabilización (mosaicos) en el ERP solo a los usuarios que lo requieren en base a las tareas asignadas. Las autorizaciones han sido proporcionadas en base a la aplicación del principio de mínimo privilegio, mitigando el riesgo de que se produzcan accesos no autorizados y se realicen contabilizaciones erróneas.
  - Todas las operaciones se acumulan, clasifican y resumen correctamente en las cuentas; los saldos contables se concilian periódicamente con los de los extractos bancarios.
- **Controles sobre el fichero maestro de terceros (FMT)**:
  - Existe un procedimiento aprobado que regula la tramitación de las altas y modificaciones del FMT. Todos los cambios en el FMT se realizan según este procedimiento, que incluye una adecuada segregación de funciones y la asignación de autorizaciones y responsabilidades en las distintas etapas del proceso.
  - Cualquier cambio en los datos del IBAN donde se realizan pagos debe estar justificado mediante un certificado de titularidad real o preferentemente mediante el servicio **Iberpay** integrado con el ERP.
  - Si la cuenta que aparece en la factura electrónica no coincide con la que conste en el FMT, no se pagará (nunca se debe pagar una factura a un IBAN que no conste en el FMT), se investigará, y en su caso, se requerirá al acreedor para que actualice sus datos a través del procedimiento electrónico.
  - En ocasiones los procedimientos de las entidades auditadas contemplan declaraciones responsables para acreditar la titularidad de las cuentas en el alta terceros y cuentas bancarias en el FMT. Este tipo de requisito o control, aunque es legal (art. 69 Ley 39/2015), no es un control tan robusto y fiable como los certificados o verificaciones mediante servicios web (tipo Iberpay).

- Los cambios en el FMT (nuevos proveedores, cambios de IBAN, ...) se procesan solo después de que se hayan obtenido las aprobaciones adecuadas, de acuerdo con el principio de mínimo privilegio.
- Los usuarios con capacidad para realizar cambios en el FMT se encuentran debidamente autorizados y restringidos de acuerdo con el principio de mínimo privilegio.
- Analizar si existe una adecuada SdF para llevar a cabo las altas y cambios del FMT y su aprobación. Tendremos en consideración el tamaño de la entidad y las disponibilidades de personal.
- Los controles de acceso al ERP (módulo FMT) están bien configurados.
- Los CGTI *D.1 Uso controlado de privilegios de administración* y *D.2 Gestión de usuarios* funcionan eficazmente, bajo el principio de mínimo privilegio.

Ver más información sobre estos controles sobre el FMT en el Anexo 1A.

- En un entorno de administración electrónica avanzada, **el establecimiento de unos sólidos CGTI para garantizar estos CPI es absolutamente crítico,** ya que la mayor parte de los CPI anteriores son dependientes del buen funcionamiento de los CGTI.

8. Evaluación del diseño e implementación (D+I) de los CPI relevantes

Para cada uno de los controles (CPI+CGTI) identificados **que sean relevantes o significativos** el auditor debe:

a) **Evaluar si el control está diseñado (D) eficazmente** para responder al RIM en las afirmaciones (CPI) o si está diseñado eficazmente para sustentar el funcionamiento de otros controles (CGTI). Implica que el auditor considere si el control, de manera individual o en combinación con otros controles, es capaz de prevenir de modo eficaz, o de detectar y corregir, incorrecciones materiales (es decir, permite alcanzar el objetivo de control) o si es capaz de sustentar el funcionamiento de otros controles.

b) **Determinar si el control ha sido implementado (I)** estableciendo que el control existe y que la entidad lo está utilizando.

Para cada CPI que se identifique como relevante, el auditor debe aplicar procedimientos de valoración del riesgo (PVR) para **analizar la efectividad de su diseño para realizar la actividad de control y su implementación**, considerando el riesgo TI y los objetivos de la auditoría. Si se concluye que el diseño e implementación es eficaz se aplicarán procedimientos posteriores de auditoría para **verificar, mediante una prueba de control, si está en funcionamiento durante todo el periodo auditado**.

Para más información, ver el apartado 8 de la GPF-OCEX 5340.

9. Valoración del riesgo de control

Si bien el auditor siempre está obligado a valorar el riesgo inherente de los riesgos identificados a nivel de afirmación, **solo se exige valorar el riesgo de control si se tiene previsto probar la eficacia operativa de los controles o cuando los procedimientos sustantivos por sí solos no proporcionan suficiente evidencia de auditoría a nivel de afirmación**.

Si el auditor no tiene previsto comprobar la eficacia operativa de los controles, su valoración del RIM será la misma que la valoración del riesgo inherente. En estos casos, en los que se tiene previsto adoptar un enfoque fundamentalmente sustantivo de la auditoría, una vez que se haya obtenido el conocimiento de los componentes del sistema de control interno que se exige en los apartados 21 a 27 de la NIA-ES 315R/GPF-OCEX 1315R, no será necesario realizar procedimientos adicionales.

Existe un vínculo estrecho entre el trabajo realizado para obtener un conocimiento de los componentes del sistema de control interno de la entidad, su D+I, y la valoración del riesgo de control. El conocimiento por parte del auditor del sistema de control interno de la entidad informa sus expectativas sobre la eficacia operativa de los controles y si el auditor planea probar la eficacia operativa de los controles, ese conocimiento le ayudará en el diseño y la realización de procedimientos de auditoría posteriores de acuerdo con la NIA-ES-SP 1330.

Cualquier plan para probar la eficacia operativa de los controles se basa en la expectativa de que los controles funcionan eficazmente, y esto será la base de la valoración del riesgo de control por el auditor.

Para más información, ver el apartado 9 de la GPF-OCEX 5340.

10. Revisión y evaluación de los CGTI: factores de riesgo a considerar

La eficacia de los CPI automatizados **depende en gran medida** del buen funcionamiento de los controles generales de tecnologías de la información (CGTI). Por tanto, la revisión de los CPI y la decisión de depositar confianza en ellos debe hacerse tras una evaluación previa de los CGTI, según los procedimientos descritos en el apartado 10 de la GPF-OCEX 5340 y en la GPF-OCEX 5330.

El equipo de expertos en auditoría de sistemas de información al realizar la revisión de los CGTI deberá tener presente la GPF-OCEX 5330. A modo de ejemplo, se indican los siguientes riesgos derivados de la utilización de las TI, que están entre los más habituales en relación con la gestión de la tesorería.

Entorno de control

Un entorno de control efectivo es fundamental para asegurar que la información sobre la tesorería y el tratamiento de la información relacionada sean exactos y completos, y que se mantenga la integridad y confidencialidad de la información.

Ejemplo:

Deficiencia de control observada	Riesgo	Recomendación
Durante la realización de la fiscalización se ha observado una serie de incumplimientos en los procedimientos de gestión y de control interno que ponen en cuestión la eficacia del sistema de control interno de la entidad y afectan a la fiabilidad de la información económico-financiera recogida en las cuentas anuales. Un elemento esencial en cualquier sistema de control interno es el denominado tono directivo. Es la forma en que la alta dirección expresa sus convicciones respecto de la importancia del control interno y determina en gran medida su eficacia.	**Alto** Debido a las circunstancias indicadas no se puede tener la seguridad de que todos los pagos se hayan tramitado de acuerdo con los procedimientos aprobados, hayan tenido entrada en el sistema administrativo contable y estén adecuadamente recogidos en las cuentas anuales.	Recomendamos que los órganos de dirección establezcan, formalicen, comuniquen, mantengan operativos y exijan su cumplimiento, los procedimientos administrativos de gestión que requiera la actividad de la entidad y un sistema de control interno que garanticen el cumplimiento de los principios de buena administración.

Un elemento clave del entorno de control es la existencia de una adecuada gobernanza de la ciberseguridad (véase GPF-OCEX 5314).

Gestión de cambios

Es importante que existan unos controles efectivos a fin de asegurar que los cambios en las aplicaciones sean autorizados y debidamente comprobados antes de introducirlos en el sistema de producción.

El procedimiento de gestión de cambios tiene como finalidad evitar que se introduzcan cambios en la programación sin la autorización apropiada, que pudiera posibilitar posteriormente modificaciones no autorizadas en la información sobre los cobros y pagos o los movimientos bancarios. Contemplará entre otras cuestiones que:

- Todas las solicitudes de cambios a introducir en las aplicaciones de gestión de tesorería, así como cualquier cambio en la estructura de la base de datos deberán ser revisados y aprobados por el responsable funcional antes de ser implementados.
- Todos los cambios deben probarse y autorizarse antes de ser introducidos en el entorno de producción.
- Debe existir SdF a fin de limitar la capacidad del personal para realizar cambios que afecten tanto a la base de datos de producción como a la configuración de la aplicación de gestión de tesorería.

  Si una aplicación se ha desarrollado en la entidad y un equipo de desarrolladores internos tiene acceso a modificar la aplicación, el riesgo será alto, por lo que deben establecerse controles internos como la segregación de funciones y controles de supervisión.

  Sin embargo, en una aplicación comercial cualquier cambio en el código fuente necesitará la intervención del fabricante y unos procedimientos adicionales.

Debido a la criticidad del sistema informático de gestión de tesorería y a los aspectos fundamentales de sus operaciones, el mantenimiento y las actualizaciones de las aplicaciones deben ser incorporados a los procedimientos de gestión de cambios.

Ejemplo:

Deficiencia de control observada	Riesgo	Recomendación
Se han identificado debilidades en la asignación de la responsabilidad que otorga máximo nivel de privilegios en la aplicación de gestión tesorería. En concreto, se han identificado un total de 30 usuarios, de los que la mayoría corresponden a personal que realiza labores de desarrollo, con acceso a la aplicación y datos de producción. El acceso a producción para labores de desarrollo no debe permitirse, y menos aún, realizarse de forma generalizada.	**Alto** El personal con capacidades de desarrollo podría introducir modificaciones no autorizadas a los datos y programas que están en el entorno de producción, ya sea de forma accidental o deliberada, representando un riesgo alto de incorrecciones materiales significativas en las cuentas anuales, incluyendo el riesgo de fraude.	Recomendamos que se implante un entorno de pruebas, aislado del de producción, que permita realizar de forma adecuada las labores de desarrollo, evitando de esta forma los accesos innecesarios a producción. Recomendamos que se apruebe formalmente un procedimiento para la gestión continua de cambios, que especifique los siguientes requisitos: - Registro de todas las solicitudes de cambio, incluidas las urgentes y las originadas desde el equipo técnico o desde los responsables funcionales del servicio. - Evaluación de las solicitudes teniendo en cuenta los riesgos de seguridad. - Autorización de los cambios por parte del personal responsable, previamente a su pase a producción. - Realización de pruebas, con carácter previo a la implantación del cambio y aceptación por parte del usuario final y de los responsables funcionales. - Planificación de la puesta en funcionamiento del cambio. - Mejorar la gestión documental del proceso e incluir toda la información necesaria.

Controles de acceso y gestión de usuarios

Los riesgos en esta área están asociados con accesos indebidos a los sistemas, a los datos y a la información financiera o contable.

Una gestión eficaz de los controles de acceso de los usuarios proporciona garantía, mediante la aplicación del principio de mínimo privilegio, de que las aplicaciones de tesorería y contabilidad están adecuadamente protegidas para evitar el uso no autorizado, divulgación, modificación o pérdida de información o la sustracción de fondos.

La gestión de usuarios es un componente crítico para el establecimiento de una efectiva segregación de funciones.

Los parámetros críticos que pueden incidir en los accesos a las aplicaciones y bases de datos son:

Número de usuarios activos

El número de usuarios con acceso a una aplicación tiene un impacto directo en el riesgo de accesos o de transacciones no autorizadas (cuantos más usuarios mayor riesgo). Una aplicación con tres usuarios será considerada probablemente de bajo riesgo en este aspecto, sin embargo, una aplicación con 5.000 usuarios tendrá un nivel alto de riesgo porque existirán más probabilidades de errores humanos al conceder accesos y privilegios, de que existan accesos que presenten conflictos frente a lo que se considera una adecuada segregación de funciones o por una monitorización inadecuada de los accesos.

Solamente deben estar activos los usuarios estrictamente necesarios para desarrollar las funciones.

Privilegios elevados

El acceso o la modificación de los privilegios de acceso debe ser aprobado y documentado, bajo el principio de mínimo privilegio y de necesidad de saber.

El acceso al sistema se basará en una estructura de roles de usuario.

Número de administradores

Como ocurre con el número de usuarios, el número de administradores de la aplicación tiene un impacto directo y proporcional con la valoración del riesgo. El acceso de administrador o acceso "privilegiado" debe estar limitado estrictamente a las necesidades de la entidad.

Acceso directo a la base de datos (BD) subyacente

Este es otro parámetro crítico, ya que puede dejar puertas traseras para acceder directamente a la BD sin necesidad utilizar la aplicación. Este acceso "privilegiado" debe estar limitado estrictamente a las necesidades de la entidad.

Autenticación

Los usuarios del sistema de gestión de tesorería deberán ser identificados de forma única. Los usuarios tendrán un identificador individual de acceso y no deberán compartir contraseñas. Es muy importante evaluar los mecanismos de autenticación implantados en una aplicación de gestión para determinar la lista de personas con acceso a la misma.

Veamos algunos ejemplos:

Deficiencia de control observada	Riesgo	Recomendación
Hemos observado que las directivas de contraseñas no son todo lo robustas que sería conveniente de acuerdo con las mejores prácticas en la materia. La deficiencia de control, que afecta a todos los niveles del sistema de información, nos ha permitido constatar intervalos de caducidad elevados, desbloqueo automático de cuenta en caso de superar los intentos de acceso fallido prefijados, periodo de tiempo elevado en el cierre de sesión por inactividad, no activación de requerimientos de complejidad de las contraseñas, elevado número de usuarios cuya contraseña no caduca, así como usuarios que no requieren de contraseña para acceder al sistema.	**Alto** Las deficiencias detectadas debilitan la efectividad del control de acceso en los distintos niveles de los sistemas de información representando un riesgo sobre la integridad y confidencialidad de los datos de la Entidad.	Implementar una política de contraseñas robustas, de acuerdo con las mejores prácticas en esta materia y adaptarlas a los parámetros generalmente aceptados (complejidad mínima, cambio de contraseñas cada 3 a 6 meses, historial de contraseñas mínimo de 5, bloqueos ante intentos fallidos, etc.) en todos los niveles del sistema de información de la Entidad (SAP, Oracle, HPUX, Directorio activo). Implantar el DFA.
Los permisos de administración del entorno SAP no se habían restringido suficientemente, existiendo un elevado número de usuarios con capacidad total sobre el sistema (perfil SAP_ALL). En el análisis efectuado se han detectado usuarios de gestión, proveedores externos, y usuarios que han causado baja en la Entidad, que disponen de permisos de administración. El perfil SAP_ALL básicamente consta de todas las autorizaciones posibles en SAP con lo cual, el usuario que tenga este perfil asignado puede realizar cualquier actividad sobre el sistema (tanto a nivel de sistema como a nivel de negocio, por ejemplo, crear usuarios, eliminar o modificar bases de datos, borrar o modificar registros, crear y autorizar órdenes de compra, etc.)	**Alto** La ausencia de control sobre los permisos de administrador de SAP otorgados a los usuarios durante el ejercicio representaba un alto riesgo por la posibilidad de acceso total a los datos, a la gestión económica y a la manipulación de los sistemas de información de la Entidad, con el perjuicio que podría ocasionarle. En dichos usuarios no existe el control basado en la segregación de funciones incompatibles.	Se recomienda mejorar la gestión de los usuarios administradores del entorno SAP. El perfil SAP_ALL debería ser asignado a un grupo muy reducido de usuarios, un máximo de dos o tres administradores de sistemas. Además, dicha asignación debería ir acompañada de unas políticas de seguridad adecuadas, como por ejemplo cambio periódico de contraseñas, registros de auditoría y revisiones periódicas de estas. Además, dicho perfil no debería ser asignado en ningún caso a: - Usuarios de negocio - Usuarios desarrolladores - Usuarios externos
Se han identificado 24 cuentas de usuario genéricas (lo que supone un 20% sobre el total de cuentas de usuario activas) cuyo uso no está justificado o bien no se conoce quién y para qué se utilizan.	**Alto** La utilización de cuentas genéricas impide mantener la trazabilidad de las acciones realizadas.	Realizar una revisión detallada de los usuarios existentes en la aplicación de gestión de Tesorería, con el fin de identificar las cuentas genéricas y conocer su uso. Estas cuentas deben ser sustituidas por cuentas nominativas, que permitan identificar al usuario responsable de las acciones realizadas con ellas.

Deficiencia de control observada	Riesgo	Recomendación
No existe un procedimiento para las altas, bajas y modificaciones de los usuarios y sus permisos en las aplicaciones ni para la revisión periódica de dichos permisos. Existen usuarios que llevan inactivos varios meses o que no han accedido nunca.	**Medio** Esta situación implica un riesgo medio de accesos indebidos y de actuaciones no autorizadas.	Formalizar un procedimiento de gestión de usuarios y de permisos, que contemple los procesos y la implicación de los responsables de los diferentes departamentos en las altas, en los cambios de puesto de trabajo y en las bajas de los usuarios de dominio y de las aplicaciones. También debe incluir la revisión periódica de los usuarios autorizados y sus privilegios en los sistemas y aplicaciones, de forma que se garantice que cada usuario dispone de las capacidades mínimas necesarias para desempeñar sus tareas y ninguna más. Debe conservarse la documentación acreditativa de las revisiones realizadas, los resultados y las acciones llevadas a cabo.

Continuidad del servicio

El mantenimiento de cualquier sistema requiere la adopción de unas medidas para el caso de que ocurra una interrupción en el funcionamiento del sistema. Se debe comprobar que las entidades cuentan con los procedimientos necesarios para recuperarse de tal interrupción:

- Se debe disponer de una estrategia documentada para la gestión de las copias de seguridad periódicas, tanto de los datos como de los programas.
- Deben realizarse pruebas de restauración programadas.
- Hay que definir los plazos de retención y los requisitos de almacenamiento para la información.

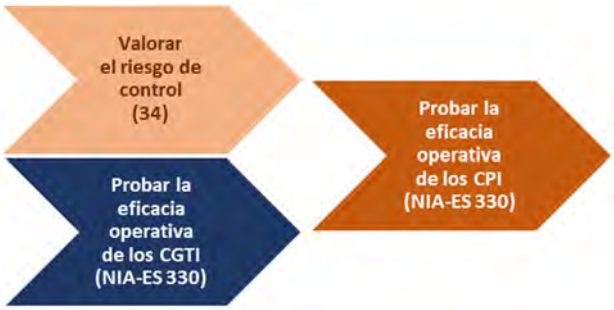
En el caso de que las aplicaciones informáticas de gestión de tesorería o parte de los sistemas de información utilizados se hayan contratado en modo Cloud (SaaS, PaaS o IaaS) deberán considerase las especificidades de los controles de TI en este entorno.

Incluimos a continuación algunos ejemplos:

Deficiencia de control observada	Riesgo	Recomendación
Aunque se dispone de una arquitectura de alta disponibilidad para los servidores de aplicación basada en la existencia de clústeres de servidores, todos los equipos se ubican en un mismo CPD.	En caso de ocurrir un desastre que afecte al CPD, existe el riesgo **alto** de que se pierdan, de forma irreversible, los sistemas de producción junto con las configuraciones de los sistemas y la lógica de las aplicaciones. La reconstrucción de esta pérdida podría prolongarse durante meses.	Analizar los requisitos relacionados con la continuidad del servicio y la disponibilidad de la información y desarrollar un plan de recuperación ante desastres, que permita continuar la actividad de la entidad en los tiempos y con los requisitos marcados en caso de ocurrencia de una contingencia grave que afecte a los sistemas principales.
No se ha definido un plan de continuidad de la actividad que permita la recuperación de los procesos de gestión críticos en un tiempo limitado y fijado con anterioridad, tras la ocurrencia de una contingencia que afecte a los sistemas de producción.	Existe un riesgo **alto**, en caso de un evento que afecte a los procesos de gestión críticos y los sistemas de información que los soportan, de que no se recuperen las actividades y los datos en los plazos y condiciones requeridas para el logro de los objetivos del Ayuntamiento.	Elaborar y aprobar un **Plan de Continuidad de la Actividad** corporativo, que incluya el análisis sobre elementos críticos de negocio existente, la estrategia de continuidad, los planes particulares de contingencia de los sistemas del Ayuntamiento y la ejecución planificada de pruebas periódicas del plan.
La copia de seguridad de datos y programas se guarda en una caja fuerte ignífuga en el Centro de Proceso de Datos (CPD). En caso de desastre, la copia de datos y programas puede correr la misma suerte que el CPD.	Esta situación implicaría un riesgo **alto** de pérdida de datos y programas. Además, esto es una obligación legal para los datos de carácter personal de nivel alto.	Contemplar el traslado y almacenamiento fuera del CPD principal de las copias de seguridad que se realicen de datos y programas.

11. Revisión de la eficacia operativa de los CPI relevantes

Una vez verificada la razonabilidad del D+I de los CPI y la eficacia operativa de los CGTI relacionados, que posibilitan el adecuado funcionamiento de aquellos, se debe verificar el adecuado funcionamiento operativo de los CPI relevantes en los que se va a confiar.



Para ello la NIA-ES-SP 1330 (apartado 8) establece que **el auditor diseñará y realizará pruebas de controles con el fin de obtener evidencia de auditoría suficiente y adecuada sobre la eficacia operativa de los controles relevantes si:**

(a) la valoración de los riesgos de incorrección material en las afirmaciones realizada por el auditor comporta la expectativa de que los controles estén operando eficazmente (es decir, para la determinación de la naturaleza, momento de realización y extensión de los procedimientos sustantivos, el auditor tiene previsto confiar en la eficacia operativa de los controles); o

(b) los procedimientos sustantivos por sí mismos no pueden proporcionar evidencia de auditoría suficiente y adecuada en las afirmaciones.

Además, el apartado 9 de la misma NIA se señala que en el diseño y aplicación de pruebas de controles, **el auditor obtendrá evidencia de auditoría más convincente cuanto más confíe en la eficacia de un control.**

La obtención de evidencia de auditoría sobre la implementación de un **control manual** en un determinado momento **no proporciona evidencia** de auditoría sobre la eficacia operativa del control en otros momentos del periodo que comprende la auditoría.

En el caso de **CPI automatizados**, el auditor comprobará su eficacia operativa tras la identificación y comprobación de CGTI que aseguran el funcionamiento congruente del CPI automatizado (por ejemplo, auditando los controles de acceso y los controles de gestión de cambios) en vez de aplicar pruebas de eficacia operativa directamente sobre los CPI automatizados[8].

Aunque la realización de pruebas sobre la eficacia operativa de los controles no es lo mismo que la obtención de conocimiento y la evaluación de su diseño e implementación, muchas veces, en entornos de administración electrónica, se utilizan los mismos tipos de procedimientos de auditoría para alcanzar ambos objetivos simultáneamente. En consecuencia, **es posible que el auditor decida que resulta eficiente probar la eficacia operativa de los controles al mismo tiempo que se evalúa su diseño y se determina si han sido implementados.** *(NIA-ES-SP 1330, A21)*

Para más información ver el apartado 11 de la GPF-OCEX 5340.

12. Segregación de funciones (SdF)

Al revisar el proceso de gestión de la tesorería, un aspecto fundamental es el estudio de la segregación de funciones, que constituye uno de los principios más importantes del control interno.

Significa que las funciones se distribuyen entre las personas de forma que nadie pueda controlar todas las fases del proceso de una transacción de modo tal que puedan pasar inadvertidas incorrecciones debidas a errores o fraudes. Teóricamente, el flujo de las actividades debería proyectarse de tal forma que el trabajo de una persona sea independiente del de otra o sirva para comprobación de este último.

Debido a que, de todos los activos, el efectivo es el más susceptible de apropiación indebida, es especialmente

[8] Apartado A180 de la NIA-ES 315R/GPF-OCEX 1315R.

importante que se segreguen las funciones para que ninguna persona controle todas las etapas de gestión de la tesorería.

En la práctica, este principio de SdF ha de conciliarse con consideraciones tales como el volumen, la complejidad y la materialidad de los distintos tipos de operaciones y la secuencia de pasos necesarios para procesarlas. Los aspectos a considerar variarán ampliamente de una entidad a otra. En las entidades de mayor tamaño, las posibilidades de desagregación del trabajo en el proceso de gestión son mayores.

Un aspecto que ha de tenerse siempre en cuenta es el coste de mantenimiento de los controles en relación con el riesgo de las pérdidas por error o fraude que podrían producirse en ausencia de aquéllos. A veces no es posible establecer una adecuada segregación de tareas, sobre todo en entidades de pequeño tamaño, ya que no se dispone de personal suficiente para su implantación, pero en estos casos deben establecerse otro tipo de **controles compensatorios**[9].

Si no es adecuada la segregación de funciones se debe explicar por qué y hasta qué punto puede afectar al riesgo de auditoría. Se deben concretar los riesgos que puede provocar la falta de segregación e indagar si existen controles compensatorios que mitiguen esos riesgos.

Entre los mecanismos de control disponibles para ayudar a la hora de llevar a cabo controles alternativos a una segregación de funciones eficaz se incluyen:

- Pistas de auditoría/trazabilidad.
- Conciliaciones.
- Informes sobre anomalías.
- Supervisión.

En los actuales sistemas altamente automatizados, en los que los usuarios tienen acceso potencialmente a todas las funciones del sistema, el análisis de la segregación de funciones adquiere una importancia especial y debe hacerse una detallada revisión de los riesgos existentes. Dada su complejidad y "no visibilidad" ese análisis muchas veces **solo será posible realizarlo** con la colaboración de personal especializado en auditoría de sistemas de información utilizando herramientas y técnicas automatizadas (HTA).

En el cuadro siguiente se recogen las principales situaciones de conflicto de segregación de funciones en el proceso de gestión de tesorería, que pueden entrañar riesgos de errores o irregularidades, y por tanto riesgos de auditoría. Este cuadro solo es un ejemplo de posibles situaciones conflictivas por lo que debe adaptarse a la realidad en cada entidad, analizando como está estructurado el proceso de gestión, ya que las funciones principales y, en consecuencia, sus conflictos, dependen de cada caso específico.

El procedimiento de auditoría lógico consistiría en describir los procedimientos de gestión de cobros y pagos, documentar las respuestas, la evidencia obtenida sobre los posibles conflictos de segregación de funciones y sus consecuencias en nuestra evaluación del control interno y valoración del riesgo.

El auditor deberá hacerse las siguientes preguntas y consideraciones:

#	Función	Consideraciones de control / Preguntas de auditoría	Controles posibles/ Recomendaciones
1	Tesorería	El empleado que formula las peticiones para abrir cuentas bancarias ¿puede autorizar dichas peticiones en el banco?	Existe un procedimiento aprobado para la apertura de cuentas bancarias que contempla la autorización de dos o más personas, incluyendo la que tiene la competencia para la contratación de este tipo de servicios.
2	Tesorería	¿Existen procedimientos aprobados para verificar que están controladas y registradas todas las cuentas bancarias a nombre de la entidad?	Existe un procedimiento aprobado que contempla la revisión periódica de las cuentas de la Entidad, e incluye la solicitud a la entidad bancaria para que envíe confirmación de las nuevas cuentas al departamento de tesorería, así como a un miembro del personal de la alta dirección distinto del autorizado.

[9] Un control compensatorio es aquel que reduce el riesgo de una debilidad, real o potencial, no eliminada por un control directo.

#	Función	Consideraciones de control / Preguntas de auditoría	Controles posibles/ Recomendaciones
			El personal encargado de la gestión y tramitación de la apertura de cuentas bancarias no puede contabilizar transacciones bancarias ni preparar las conciliaciones.
3	Tesorería	¿Las responsabilidades por la entrada y salida de efectivo están segregadas de todas las demás funciones conexas? *La SdF entre el registro de cobros y pagos, por una parte, y su contabilización, por otra, permite una revisión independiente de las operaciones de caja y para mantener la integridad de las cuentas de control del mayor general.*	Los empleados con responsabilidad por las entradas y salidas de efectivo deben ser independientes de las correspondientes funciones de gestión y contabilidad (como expedición, facturación, notas de abono, cuentas por cobrar, compras, cuentas por pagar y nómina).
4	Tesorería	¿La responsabilidad de los cobros en efectivo está segregada de la correspondiente a los pagos en efectivo? *La mezcla de las actividades de cobros y pagos puede dar oportunidad de ocultar apropiaciones indebidas de cobros mediante la manipulación del proceso o del registro de los pagos. P.e., puede desviarse el importe recibido de una cuenta a cobrar sin afectar el saldo de la cuenta de caja si la anotación del ingreso desviado se compensa con la anotación de un desembolso simulado por el mismo importe.*	Ningún empleado puede simultanear dichas tareas.
5	Conciliaciones bancarias	El empleado responsable de preparar las conciliaciones bancarias ¿realiza también alguna de las siguientes tareas? • Recibir las entradas de caja/cobros por caja • Preparar los depósitos de caja • Preparar o autorizar transferencias • Ejecutar o autorizar transferencias bancarias • Revisar y aprobar la conciliación bancaria • Contabilizar operaciones bancarias	La persona que prepara las conciliaciones no debe encargarse de registrar los cobros o pagos, ni contabilizar operaciones de tesorería. *Las malversaciones de efectivo pueden ocultarse falseando las conciliaciones.* *Si la responsabilidad por la preparación y aprobación de las conciliaciones se asigna a personas independientes de las actividades de proceso y registro de tesorería, no sólo hay menos oportunidad de realizar manipulaciones, sino que también se instrumenta un medio para descubrir los errores en el proceso o registro tanto de cobros y pagos.*
6	Conciliaciones bancarias	¿Son supervisadas las conciliaciones bancarias?	Las conciliaciones deben ser revisadas y aprobadas por una persona distinta de la que las ha preparado.
7	Cobros	¿El empleado responsable de cobros en efectivo también lleva a cabo alguna de las siguientes funciones?: • Contabilizar los cobros • Registrar o autorizar saneamientos o ajustes en las cuentas de deudores en contabilidad • Conciliar las cuentas bancarias	El empleado responsable de recibir el efectivo no debe tener acceso a registrar o autorizar operaciones en contabilidad. La persona que recibe el dinero en efectivo o que prepara su depósito en bancos no debería ser responsable de registrar las transacciones en metálico ni tampoco preparar las conciliaciones bancarias. *Se deben implantar procedimientos para minimizar los cobros en efectivo. Si se realizan deben ser supervisados por persona distinta de quien los realiza.* *Deben realizarse arqueos diarios o semanales de los cobros y pagos en efectivo que deben firmarse por la persona que gestiona los fondos y por la que lo revisa.*
8	Mantenimiento del Fichero Maestro de	El empleado responsable del mantenimiento del FMT (p. ej. añadir, borrar o cambiar/modificar las	El empleado con responsabilidad para modificar/introducir cambios en el FMT no debe ser responsable de introducir las facturas de acreedores en

#	Función	Consideraciones de control / Preguntas de auditoría	Controles posibles/ Recomendaciones
	Terceros (FMT)	cuentas bancarias de acreedores) ¿realiza también alguna de las siguientes tareas/funciones?: • Contabilizar o modificar los asientos y/o documentos de contabilización de las obligaciones o de los pagos. • Aprobar las facturas de acreedores • Realizar o autorizar transferencias	el sistema contable ni tampoco tener capacidad para efectuar y autorizar pagos.
9	Mantenimiento del FMT	Los cambios en el FMT (p.ej. cambios en las direcciones o nombres de terceros y altas en el FMT), ¿son revisados y aprobados por un supervisor de quien los introduce?	Las altas o modificaciones del FMT deben ser revisadas o fiscalizadas previamente a estar disponibles para su uso en el sistema contable. Se emite un informe sobre los cambios en el FMT que es revisado por un empleado que no tenga acceso o responsabilidad para realizar esas funciones.
10	Pagos	Los empleados responsables de aprobar las facturas y los pagos ¿pueden también contabilizar en proveedores? *Si quienes tramitan o aprueban los pagos controlan también su contabilización, hay mayor oportunidad de que se efectúen pagos no autorizados o respaldados por documentos simulados y de que se registren luego las operaciones en cuentas no sujetas a un control riguroso.*	Los empleados responsables de autorizar las facturas y pagos a los acreedores no deberían encargarse de contabilizar las facturas.
11	Pagos	¿La disposición de fondos es mancomunada? ¿Es la transferencia el medio normal de pago	Las disposiciones de fondos de cuentas bancarias se realizan de forma mancomunada y el medio normal de pago es la transferencia bancaria.
12	Pagos	La persona responsable de autorizar transferencias bancarias ¿realiza también alguna de las siguientes funciones? • Preparar las transferencias • Preparar las conciliaciones bancarias • Revisar y aprobar las conciliaciones bancarias • Contabilizar facturas de proveedores • Introducir cambios en el FMT • Aprobar las facturas y los documentos OK • Gestión de compras y proveedores	La preparación y la aprobación de transferencias bancarias deberían ser realizados por dos empleados distintos. El empleado responsable de autorizar las transferencias a los proveedores no debe tener competencia para introducir cambios en el FMT, contabilizar las facturas de proveedores ni tampoco participar en el proceso de conciliación bancaria. Se revisan los pagos a realizar por personal diferente del de tesorería previamente a la realización del pago. Los pagos realizados son verificados a posteriori por personas diferentes de los que los tramitan.

Si los controles no son eficaces, el auditor deberá realizar procedimientos sustantivos para detectar si se han producido casos de conflicto de SdF. Con HTA podrán realizarse comprobaciones sobre el 100% de las transacciones, de otra forma deberá efectuarse la prueba en base a muestreo.

13. Análisis de las interfaces y de los controles sobre ellas *(Ver Anexo 1 de la GPF-OCEX 5340)*

Las interfaces son programas que sirven para transferir datos de una aplicación a otra. Las entidades pueden utilizar sistemas de gestión de tesorería distintos de los sistemas contables y aplicaciones de gestión de otros procesos que comparten la información mediante interfaces.

Las interfaces hacia y desde el sistema de cobros/pagos/tesorería presentan un área de riesgos significativos para el mantenimiento de la integridad de los datos.

Por ejemplo, un caso común es aquel en que una entidad envía a los bancos, mediante una interfaz, los datos de las transferencias (pagos) a realizar. Esa interfaz externa (mediante la que se remite a las entidades financieras el fichero de pagos en formato XML) es un foco de riesgo de fraude de apropiación indebida si no está

debidamente protegida frente a accesos indebidos (El acceso a los ficheros bancarios para pagos debe estar restringido al personal que lo necesite de acuerdo con sus funciones).

Además de la interfaz de pagos con el banco, se debe prestar atención a las que interactúan con otras aplicaciones, como la de contabilidad o la de recaudación, etc.

Las interfaces pueden estar automatizadas o ser manuales. En ambos casos existe el riesgo de **pérdida o manipulación** de la información, de forma que los datos de la aplicación de origen no coincidan con los que llegan a la aplicación de destino.

Debemos, por tanto:

a) Identificar las interfaces existentes que puedan afectar significativamente a las cuentas anuales y suponer un riesgo de auditoría.

b) Identificar y evaluar los controles que tenga establecidos la entidad para garantizar la exactitud e integridad de los datos traspasados.

c) Diseñar y ejecutar las pruebas de auditoría que se estimen pertinentes sobre las interfaces para garantizar la exactitud e integridad de los datos.

14. Revisión del cumplimiento legal

El objetivo de la fiscalización de cumplimiento consiste en verificar que la organización y gestión de la tesorería es conforme y se realiza de acuerdo con la normativa aplicable.

Los programas de auditoría recogerán las principales comprobaciones a realizar para asegurar que se ha cumplido, razonablemente, con la normativa.

Es aplicable la guía GPF-OCEX 4320.

15. Importancia relativa

Son aplicables la NIA-ES-SP 1320, la GPF-OCEX 1321, sobre la importancia relativa en las auditorías financieras y la GPF-OCEX 4320 sobre la importancia relativa en las fiscalizaciones de cumplimiento de la legalidad.

Sobre la importancia relativa de las deficiencias de control a efectos de la auditoría ver apartado 14 de la GPF-OCEX 5340.

16. Procedimientos y programas de auditoría

La naturaleza, momento de realización y extensión de los procedimientos de auditoría se determinan de acuerdo con las circunstancias de cada trabajo y deben basarse en el conocimiento de la actividad que realiza el ente auditado, de su organización, de los riesgos valorados, así como en la evaluación del control interno y de la importancia relativa de los saldos en las cuentas anuales.

Los procedimientos de auditoría son las respuestas a los riesgos valorados y por tanto deben ser deben ser proporcionales a esos riesgos. Así las áreas de riesgo más alto deben recibir mayor atención y esfuerzo de auditoría.

Los programas de auditoría deben ser adaptados a cada entidad en base a la valoración del riesgo de incorreciones materiales, e incluirán:

- Pruebas de controles (si procede).
- Procedimientos sustantivos (incluyendo procedimientos analíticos y pruebas en detalle).

En las **pruebas de controles** el auditor debe decidir qué controles son relevantes y diseñar y ejecutar pruebas sobre los mismos.

Tras realizar estas pruebas, si se han detectado deficiencias de control:

- Se debe evaluar la gravedad de dichas deficiencias.
- Modificar la valoración preliminar del riesgo.
- Documentar las implicaciones de las deficiencias de control.

Si no se han detectado deficiencias de control, se debe:

- Determinar que la valoración preliminar del riesgo como bajo es adecuada.
- Determinar el grado de evidencia que proporcionan los controles sobre la corrección de los saldos.
- Determinar los procedimientos sustantivos a ejecutar.

Algunos de los principales **procedimientos sustantivos** son:

- Obtener confirmaciones bancarias.
- Realizar arqueos de caja (cuando sea significativa) y conciliar con la contabilidad.

En el Anexo 2 se incluye, a modo de ejemplo, un programa de auditoría que debe ser adaptado a las circunstancias de cada fiscalización.

Pruebas masivas de datos

La utilización de aplicaciones informáticas para la gestión de la tesorería y su contabilización permite realizar pruebas masivas de datos para verificar su adecuada gestión. A continuación, se detalla a modo de ejemplo los tipos de pruebas de datos que pueden realizarse a partir de las tablas de las bases de datos de las aplicaciones de gestión de tesorería y contabilidad:

- Verificar la integridad de la información facilitada: verificaciones de totales de registros, suma de valores numéricos, numeración de registros, razonabilidad de fechas e importes, …
- Analizar los usuarios autorizados para acceder a la aplicación de gestión de tesorería o perfiles de tesorería de la aplicación de contabilidad. Seleccionar usuarios administradores (todos o una muestra, en función del número) para comprobar que están autorizados.
- Verificar el correcto funcionamiento de la interfaz entre la aplicación de tesorería y la de contabilidad.
- Revisar las conciliaciones bancarias.
- Revisar las interfaces de pagos. Verificar que la aplicación genera correctamente los ficheros de pagos xml (C34).
- Verificar, en su caso, la interfaz de entrada automatizada de los movimientos de las cuentas bancarias en contabilidad (C43).

Las pruebas de tratamiento masivo de datos se efectuarán de acuerdo con la GPF-OCEX 5370, Guía para la realización de pruebas de datos.

17. Colaboración de expertos en auditoría de sistemas de información

Para la realización de algunos de los procedimientos de auditoría descritos en esta guía, **los auditores necesitarán, probablemente, conocimientos especializados** proporcionados por auditores de TI para ayudarlos a obtener suficiente evidencia de auditoría adecuada a medida que aumenta la complejidad del entorno de TI. **El OCEX debe garantizar que los miembros del equipo de fiscalización y, en su caso, los expertos externos que formen parte del equipo colectivamente tengan la competencia y las capacidades adecuadas para realizar la fiscalización**.

18. Evaluación de las deficiencias de control interno detectadas

Ver apartado 12 de la GPF-OCEX 5340.

19. Recomendaciones

Ver GPF-OCEX 1735 y apartado 15 de la GPF-OCEX 5340.

20. Documentación del trabajo

Ver NIA-ES-SP 1230, GPF-OCEX 1231 y apartado 16 de la GPF-OCEX 5340.

Documentación del conocimiento del proceso de gestión de tesorería

El auditor debe describir y documentar el conocimiento del proceso de gestión de tesorería de la Entidad.

Para ello puede utilizar este modelo, en el que dicho proceso se descompone en las principales actividades, cada una de las cuales debe **incluir como mínimo**, la siguiente información, independientemente de que se realice manualmente o de forma automatizada:

- **Qué** transacciones y operaciones se realizan en el proceso: Contratación y baja de cuentas bancarias, ingresos, pagos, órdenes de pago, registro contable de los ingresos y pagos, fiscalización formal y material del pago, conciliaciones, registro de terceros, fiscalización alta terceros, …
- **Quién** ejecuta el proceso
- **Cómo y cuándo** se ejecuta
- **Qué sistemas informáticos, documentos fuente y registros contables** están involucrados
- **Cómo se subsanan** las transacciones o procesos incorrectos

La descripción realizada en este memorándum debe acompañarse del correspondiente diagrama de flujo, ya que ambos se complementan.

Si la entidad dispone de procedimientos formalizados por escrito, la narrativa a realizar por el auditor será tanto más breve cuanto más completos y claros sean aquéllos, que serán archivados y referenciados.

Las funciones/los subprocesos detallados más adelante son ejemplos y deben modificarse todo lo que sea necesario para adaptarse a las circunstancias de cada entidad fiscalizada.

Los párrafos sombreados en amarillo incluyen información adicional y ejemplos que se puede considerar al hacer la descripción del proceso, pero que se debe eliminar del documento final, ya que solo tiene valor informativo para el auditor que está documentando el proceso.

##########

Entidad: _____

Fecha CCAA: _____

Resumen realizado por (Técnico/fecha): _____

Revisado por (Auditor/fecha): _____

Persona/s entrevistada/s: _____

1. Aspectos generales y organizativos

Se debe indagar y preguntar a los responsables de la gestión de tesorería cuestiones como:

- Solicitar/obtener el organigrama de la entidad que incluya el departamento de tesorería. ¿Está aprobado?

  Si no existe, realizar uno en base a la información obtenida tras cumplimentar este anexo 1.

- ¿El departamento de tesorería es independiente de cualquier otro de la entidad?

  Sí / No

- ¿Hay normas o procedimientos escritos sobre la gestión de la tesorería?

  Sí (adjuntar) / No

- ¿Están claramente definidas las responsabilidades de cada empleado? ¿Estas funciones y responsabilidades están expuestas por escrito?

  Sí / No

- ¿Son suficientes los efectivos existentes para cubrir las necesidades del servicio?
- ¿Existen medios para asegurar que el personal cuenta con los conocimientos y/o formación necesarios para realizar su trabajo? ¿Se realizan actuaciones de formación para mantener/actualizar estos conocimientos? ¿Con qué frecuencia?
- ¿Existe la debida segregación de funciones dentro de este departamento? (Ver apartado 12 de la guía).

  Sí / No
- El personal de tesorería realiza, en algún caso, funciones de:

  ¿Registro de cuentas a cobrar?
  ¿Decisión sobre descuentos, bonificaciones, etc…, en ingresos?
  ¿Preparación de documentos de pago y nóminas?
  ¿Registro contable de caja o bancos?
  ¿Preparación de facturas de venta y registro contable de las mismas?
  ¿Conciliaciones bancarias?
- ¿Existe una política sobre el manejo de fondos clara y definida?

  Sí / No
- ¿Tiene la entidad problemas de cash-flow de tesorería para hacer frente puntualmente a sus obligaciones de pago?
- ¿Utiliza la entidad programas de gestión de tesorería de forma efectiva?
- La entidad utiliza las siguientes aplicaciones informáticas:

  Gestión de tesorería:

  Contabilidad: SAP / SicalWin / Desarrollo propio /….
- ¿Utiliza la entidad algún servicio de gestión de tesorería ofrecido por las entidades financieras? ¿De qué tipo? ¿Banca electrónica? ¿quién tiene acceso a la banca electrónica, con qué funcionalidades? Detallar.
- ¿Ha realizado la entidad algún cambio significativo en sus procedimientos de tesorería en el último año?

  ¿Y en el sistema informático?

  ¿Y en la normativa?

  ¿Y en el personal clave?
- ¿Realiza el departamento de control interno revisiones periódicas?
- ¿Se ha realizado algún tipo de actuación de control por otro órgano?
  Si sí, solicitar informe de resultados.
- ¿Tiene el equipo de auditoría algún motivo para sospechar que la dirección puede tener algún interés en manipular los saldos de tesorería?

2. Flujograma general (resumido) y detallado

- Solicitar y/o elaborar. Poner referencia a su archivo.

3. Gestión de la tesorería

En las EELL revisar las bases de ejecución del presupuesto.

El auditor debe describir:

a) Las operaciones de gestión de tesorería se inician de la siguiente forma:

b) Las operaciones de gestión de tesorería se autorizan de la siguiente forma:

c) Las operaciones de gestión de tesorería se registran de la siguiente forma:

d) Las operaciones de gestión de tesorería se procesan y se reportan en los estados financieros de la siguiente forma:

4. Bancos

Objetivo de control: Todos los saldos en cuentas bancarias están sometidos a eficaces procedimientos de control

La apertura de cuentas solo puede realizarse por personas con poder suficiente.

¿Están debidamente autorizadas las cuentas bancarias y las personas que firman las disposiciones?

¿Es **mancomunada** la disposición de efectivo?

Sí / No

¿Qué personas están autorizadas para disponer de las cuentas bancarias?

¿Se avisa a los bancos cuando un firmante autorizado deja de serlo?

Se deben implantar procedimientos para notificar inmediatamente a los bancos cada vez que una persona autorizada para disponer de fondos deje de formar parte de la empresa.

¿Se tiene constancia de la recepción de dicho aviso?

Solicitar el inventario de cuentas al tesorero/responsable de tesorería y hacer un resumen de las cuentas bancarias utilizadas:

Denominación de la cuenta	Finalidad de la cuenta	Tipo de cuenta	Entidad financiera	Número de cuenta	Libre disposición/ Con restricciones	Saldo a 31/12/24	Firmas autorizadas durante 2024	Altas de firmas en 2024	Bajas de firmas en 2024	Tipo de disposición (solidaria, mancomunada)

5. Conciliaciones bancarias

Objetivo de control: Todas las operaciones se acumulan, clasifican y resumen correctamente en las cuentas; los saldos de contabilidad se concilian con los de los extractos bancarios.

Las conciliaciones bancarias, incluso cuando las realizan personas independientes de las funciones relacionadas con el efectivo, no siempre ponen de manifiesto la existencia de operaciones irregulares; sin embargo, reducen la oportunidad de ocultarlas.

¿Se concilian periódicamente las cuentas bancarias?

Sí / No

¿Con qué periodicidad?

Diaria/Semanal/Mensual

¿Son automáticas o manuales?

¿Quién las realiza y quién las revisa?

Los procedimientos manuales para realizar las conciliaciones bancarias de todas las cuentas, ¿incluyen?:

a) La recepción de los extractos bancarios directamente por la persona encargada de las conciliaciones.

b) La comparación de las fechas e importes de los depósitos en bancos, tal y como se indican en el extracto, con el libro mayor.

   No deben existir diferencias que pudieran indicar que los fondos han sido utilizados para otros fines durante el periodo previo a su depósito en el banco.

c) La investigación de las transferencias interbancarias, para comprobar si ambas partes de la transacción han sido debidamente contabilizadas.

   Hay que verificar si las transferencias han sido registradas en el mismo período contable en los dos bancos.

d) La revisión de las conciliaciones bancarias por una persona responsable.

   La mera realización de una prueba aritmética entre el saldo según libros y el extracto es insuficiente. Se debe realizar un cuidadoso examen de todas las partidas de la reconciliación y se debe obtener una explicación satisfactoria para todas ellas.

Si son manuales ¿se realizan y revisan o aprueban por personal ajeno al departamento de tesorería?

Sí / No

¿O están automatizados? Describir el procedimiento.

¿Son adecuados los procedimientos de conciliación de las cuentas bancarias?

6. Caja

Objetivo de control: El efectivo en caja está sometido a eficaces procedimientos de custodia y a protección física

Consideraciones previas: La amplitud del conocimiento de los procedimientos, su descripción y la del control interno relacionado será proporcional a su significatividad. Si es poco significativo se reducirán los procedimientos para su conocimiento y su posterior revisión.

La entidad debe estar atenta a todo aumento del movimiento de los fondos de efectivo, ya que esto puede ser indicio de que se están utilizando en operaciones que deberían ser tramitadas a través de los procedimientos normales de pago. Un modo de reducir dicha actividad a un mínimo consiste en poner un límite al importe de los pagos realizados con fondos de la caja fija.

Los fondos de caja fija y otros fondos de maniobra deben ser administrados por el sistema de fondo fijo y por una persona que no desarrolle otras funciones relacionadas con el efectivo. Deben prepararse los justificantes o recibos de manera que hagan imposibles las alteraciones y los cheques de reposición de fondos deben extenderse a favor de la persona responsable de la custodia de los fondos.

No podrán pagarse en efectivo las operaciones, en las que alguna de las partes intervinientes actúe en calidad de empresario o profesional, con un importe igual o superior a 1.000 euros. (Artículo 18 de la Ley 11/2021 de 9 de julio).

¿Se realizan cobros o pagos por caja?

Sí / No

¿Cuál es el volumen gestionado por las cajas de efectivo al año? ¿Es significativo?

Identificar el número de cajas que dispone la entidad y quién es el responsable que autoriza su apertura

¿Existe algún límite de fondos en caja?

Describir los mecanismos de custodia de efectivo

¿Se realizan arqueos periódicos?

Deben realizarse arqueos de caja periódicos, sin previo aviso, por parte de una persona independiente de todas las demás funciones relacionadas con el efectivo.

¿Quién los realiza?

¿Son adecuados los controles sobre los fondos de efectivo?

¿Es adecuada la protección física de los fondos de efectivo? ¿Se utiliza una caja fuerte para la custodia de los fondos de efectivo?

La adecuación de la protección física de los fondos de efectivo depende del grado de riesgo de pérdida por causa de incendio, negligencia o robo. La protección física puede comprender el uso de cubículos especiales para los cajeros, de cajas acorazadas con doble combinación, de sistemas de depósito de seguridad y de cajas ignífugas. También dependerá del volumen de los movimientos de fondos por caja.

¿Se usa el sistema de fondo fijo para todas las cajas?

El sistema de fondo fijo simplifica el control sobre los importes en caja, fijando el importe total por el cual el cajero es siempre responsable.

Uno de los principios del sistema es que el fondo sea reembolsado tan sólo bajo presentación de los justificantes de caja debidamente aprobados y por la suma de tales justificantes.

¿Se encuentra cada fondo fijo o cada caja bajo la responsabilidad de una persona únicamente?

Se trata de ver si la responsabilidad por cada fondo está total y claramente asignada a un individuo.

¿Está establecido el importe máximo de los pagos que pueden hacerse de cada fondo?

Los procedimientos deben hacer que todos los desembolsos importantes atraigan la atención de las personas responsables de su revisión y aprobación antes de que el pago sea realizado.

El fondo en efectivo tiene por objeto atender los pagos urgentes y de poco importe. Las prevenciones que se toman para los pagos por transferencia no se toman generalmente para los pagos efectuados por caja. Es aconsejable limitar los importes que pueden pagarse por caja bajo la exclusiva responsabilidad del cajero.

Los desembolsos por caja ¿están documentados por justificantes debidamente aprobados?

¿Se obliga, en todos los casos, a firmar los recibos a la persona que recibe el dinero?

Se debe tener especial cuidado cuando los comprobantes no están respaldados por una factura u otro documento indicativo del importe, preparado independientemente del comprobante.

¿Aprueban la reposición del fondo personas ajenas a su custodia, después de un examen minucioso de los comprobantes?

Quien firma un pago debe estar seguro de que el importe responde a unos cargos adecuados y que anteriormente no fueron pagados.

¿Se cancelan de forma efectiva los comprobantes a fin de evitar la repetición de su uso?

Los auditores internos u otros empleados responsables ¿practican arqueos de caja por sorpresa?

El fondo de caja debe siempre estar compuesto por efectivo o por comprobantes de los desembolsos efectuados. El fondo no debe utilizarse para anticipos no autorizados o desembolsos similares que constituyen un uso impropio de los fondos de la empresa (anticipos de fecha antigua).

7. Cobros

Objetivo de control: Todos los cobros se identifican correctamente, se obtienen los totales de control y se ingresan íntegros y rápidamente en bancos

¿Son adecuados los procedimientos para procesar e ingresar los pagos realizados por los clientes/ usuarios/ contribuyentes?

Todas las entradas de efectivo deberán ingresarse intactas y rápidamente.

Un control práctico y eficaz sobre las entradas de efectivo consiste en utilizar únicamente las transferencias bancarias o ingresos en cuentas restringidas como medio de cobro.

¿Son adecuados los procedimientos fijados para las entradas de efectivo?

Si el personal de algún departamento recibe efectivo directamente, puede ser necesario el uso de impresos de recibo prenumerados, de cajas registradoras con totales inalterables u otros procedimientos de control, dependiendo del volumen y del tipo de las operaciones implicadas.

Todas las entradas, junto con la documentación apropiada, deberán ser enviadas íntegras a la persona responsable de efectuar los ingresos en bancos. Una copia de la lista-resumen o del informe de los cobros deberá enviarse al departamento de contabilidad para su subsiguiente cotejo con los ingresos bancarios y su contabilización.

¿Qué tipos de ingresos diferentes obtiene la entidad?

¿En qué cuentas bancarias se depositan los ingresos a través de banco? ¿Existen cuentas restringidas de ingresos?

¿Se producen ingresos por caja? (En caso afirmativo describir el procedimiento hasta su ingreso en una cuenta bancaria).

¿Existen sistemas de cobro a través de tarjeta de crédito, domiciliaciones de recibos u otros similares? En caso afirmativo, identificar el circuito de cobros y la conciliación de los ingresos con las liquidaciones efectuadas por la entidad.

¿Qué aplicaciones de gestión de ingresos y cobros emplea la entidad?

El auditor debe describir:

a) Departamento/servicio que realiza esta función:

b) El proceso se inicia y desarrolla de la siguiente forma:

c) Persona responsable entrevistada:

d) Consideraciones sobre la Segregación de funciones

8. Pagos

Objetivo de control: ***Todos los pagos se preparan basándose en la documentación adecuada y aprobada; se comparan con los datos justificativos, se aprueban, y se ordenan según las normas establecidas***

Ver Anexo 1B.

¿Los pagos se realizan únicamente mediante transferencias bancarias?

¿Son adecuados los procedimientos de autorización de los pagos?

La ordenación de los pagos puede suponer la aprobación definitiva en el proceso de gastos. Si se realiza correctamente por personas conscientes y competentes, esta tarea es un control importante de las operaciones antes del desembolso.

En las entidades pequeñas, en las cuales el número limitado de empleados reduce las oportunidades de segregación de funciones (SdF), la aprobación final de los pagos por el director puede ser el único sustituto eficaz de los controles que se consiguen en las organizaciones mayores a través de la SdF.

Para que la aprobación final sea eficaz, se debe facilitar al ordenante de la transferencia documentación justificativa suficiente para:

(1) comprobar la necesidad del gasto realizado,

(2) determinar si la operación fue correctamente iniciada por un empleado autorizado,

(3) satisfacerse de que todas las fases del proceso de la operación se han llevado a cabo de acuerdo con la normativa / los procedimientos establecidos, y

(4) revisar si la imputación contable se ha realizado correctamente.

Si los firmantes de transferencias no dan importancia a la función de aprobación final, no sólo se produce una pérdida de control de las operaciones normales del negocio, sino que se puede abrir el camino para la realización de operaciones no autorizadas.

Los pagos se realizarán utilizando una aplicación de banca electrónica en una terminal segura. Se considerarán **controles** relevantes:

- El archivo (ISO 20022 XML) conteniendo los datos para realizar la transferencia bancaria se almacena en una carpeta segura de la red corporativa y se transmite de forma segura.
- La orden bancaria de pago debe requerir, al menos, dos firmas mancomunadas. Verificar si se utilizan firmas electrónicas que impiden o dificultan la falsificación de las órdenes de pago.

Un control manual importante es la conciliación entre el documento de transferencia bancaria y el resumen de los pagos por la persona que va a autorizar el pago.

Si las órdenes de pago se envían por correo electrónico a la entidad financiera se debe añadir la firma electrónica de la persona que envía al correo para evitar ataques de "man in the middle" que puedan falsificar los datos de los pagos. En caso de que no pueda implementarse este control se deberían establecer controles alternativos, como un procedimiento que garantice que la entidad bancaria comprueba telefónicamente el origen de los pagos enviados superiores a un determinado importe.

Analizar si están correctamente definidas las responsabilidades y verificaciones a realizar por la entidad financiera en el proceso de pago (requerir firma mancomunada, autenticar firmas autorizadas, requerir firma electrónica, reconciliación de totales e identificación de los ficheros de pago, …).

El auditor debe describir:

a) Departamento/servicio que realiza esta función:

b) El proceso de pago se inicia y realiza de la siguiente forma:

c) El proceso de pago es autorizado de la siguiente forma:

d) Las órdenes de pago se envían de la siguiente forma:

e) La entidad financiera realiza las siguientes verificaciones en cada envío de orden de pago:

f) Los pagos son contabilizados de la siguiente forma:

g) Los registros de pagos son reconciliados con los extractos bancarios y saldos de las cuentas de mayor de la siguiente forma:

h) Persona responsable entrevistada:

i) Consideraciones sobre la Segregación de funciones:

9. Pagos a justificar (PJ) y anticipos de caja fija (ACF)

¿Se han detectado incumplimientos legales en la expedición de órdenes de PJ y de ACF (inexistencia de Acuerdo/Resolución, superación de cantidades máximas, gastos imputables a conceptos presupuestarios no autorizados, etc.)?

¿Existe una adecuada calidad de las cuentas justificativas, que eviten una inadecuada utilización de los fondos?

¿Se produce una utilización abusiva del sistema de anticipos de caja fija, pagos a justificar o procedimientos equivalentes, con respecto al procedimiento ordinario de pago (pagos en firme)?

10. Contabilidad

Objetivo de control: Todas las operaciones se registran pronta y exactamente en contabilidad o en registros auxiliares y se emiten los informes apropiados

¿Aseguran los procedimientos empleados que los cobros y los pagos se registran prontamente?

La demora en la contabilización de las cantidades cobradas o de los pagos dará lugar a que los saldos de efectivo sean mayores o menores de lo que debían ser al final del período contable.

¿Si la aplicación contable es distinta de la de gestión de la tesorería, la interfaz entre ambas tiene controles que garanticen la integridad de la información traspasada?

¿Son adecuados los procedimientos para la autorización y el registro de las transferencias interbancarias?

Todas las transferencias deben ser ejecutadas por las personas autorizadas o, en el caso de las transferencias automáticas (p. e., desde el banco depositario al banco en que la empresa tiene centralizadas sus operaciones) habrán de ser amparadas por las normas y procedimientos establecidos.

Las técnicas contables utilizadas para registrar las transferencias interbancarias deben garantizar que tanto los reintegros como los ingresos se registran correcta y prontamente en el mismo período y en las dos cuentas afectadas por la transferencia.

11. Mantenimiento del fichero maestro de terceros (FMT): Alta o modificación de datos de terceros y de cuentas bancarias

Ver Anexo 1A

Describir el procedimiento para dar de alta a un tercero, indicando la documentación que se solicita al tercero para confirmar la titularidad de la cuenta. (Véase a continuación un ejemplo). Debe averiguarse:

¿La entidad mantiene un registro de terceros (FMT)?

¿El registro es informatizado?

¿Validan el IBAN con Iberpay?

¿Está conectado con la contabilidad?

¿Quiénes son los autorizados para introducir o modificar los datos de un tercero?

¿Con qué periodicidad se comprueban los datos de los terceros con los que opera la entidad?

12. Observaciones significativas, riesgos significativos, hallazgos y conclusiones

Los procedimientos que hemos realizado para adquirir nuestro conocimiento del proceso han sido los siguientes: *(poner en cada caso lo que corresponda)*

- Hemos revisado los procedimientos de la entidad archivados en el AP.
- Nos hemos entrevistado el __/__/202_ con la persona responsable _____.
- Hemos realizado una prueba paso a paso en (Ref).
- Hemos realizado un flujograma archivado en (Ref).
- Otros procedimientos: ____
- Deficiencias de control detectadas: _____
- Recomendaciones realizadas: ____

Anexo 1 A Consideraciones sobre el fichero maestro de terceros (FMT)

Los ficheros maestros contienen los datos permanentes utilizados por múltiples aplicaciones y participan en la correcta ejecución del procesamiento de datos realizados por las aplicaciones.

Para que cualquier acreedor pueda recibir un pago, es un requisito que figure en el **fichero maestro de terceros (FMT)** acreedores de la Entidad con sus datos identificativos, incluyendo la cuenta bancaria (**IBAN**) a la que se realizarán los pagos.

El mantenimiento de su integridad es un elemento crítico para la correcta ejecución de la aplicación de gestión de la tesorería y para controlar que solo se realicen pagos a terceros autorizados en sus cuentas bancarias verificadas.

Es necesario que la entidad tenga un procedimiento escrito, detallado, completo, claro y debidamente aprobado que abarque todas sus fases y deje claras las funciones y responsabilidades de todos los intervinientes.

1.1 Procedimiento electrónico alta o modificación de terceros

De acuerdo con el artículo 14.2 de la Ley 39/2015 de PACAP **el procedimiento ordinario de comunicación será electrónico**. En este procedimiento, los terceros deben acceder a la Sede Electrónica de la Entidad, dónde deben identificarse electrónicamente por cualquiera de los medios admitidos por el sistema Cl@ve del Gobierno Español (Cl@ave móvil, Certificado electrónico/DNI, Cl@ve PIN, o Cl@ve permanente) e iniciar el procedimiento.

Cuando se accede para realizar el trámite como representante, si no se está dado de alta en el registro electrónico de representantes, se debe aportar la documentación justificativa que acredite la representación.

Una vez dentro del trámite, los datos identificativos de la persona que accede se rellenan automáticamente y se deben añadir otros datos personales o de la cuenta bancaria que se quiere dar de alta o modificar. Se admiten cuentas de los países adheridos al sistema SEPA de cuentas bancarias europeas y también de fuera de este sistema bancario.

Se exige que la cuenta bancaria a añadir al registro sea de titularidad de la persona que realiza la solicitud o a quien se representa. Para acreditarlo, se exige un certificado de la entidad bancaria de titularidad de la cuenta, que deberá estar firmado digitalmente o con CSV (conjunto de dígitos que identifica de forma única los documentos electrónicos).

Las declaraciones responsables previstas en el artículo 69 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, utilizadas como justificantes de la titularidad de la cuenta bancaria, aunque son un procedimiento legalmente previsto, no constituyen un control robusto a efectos de garantizar efectivamente la titularidad de la cuenta bancaria. En los apartados siguientes se describen procedimientos automatizados para verificar esta titularidad con garantías adecuadas.

Una vez presentada la documentación y grabada directamente la información por el interesado se fiscaliza en Intervención, que, previamente al alta del tercero, revisa que toda la información es correcta y está debidamente acreditada. En este momento todos los datos de la solicitud se cargan automáticamente en el FMT.

1.2 Procedimiento presencial de alta o modificación de terceros no obligados a comunicarse electrónicamente

En el procedimiento presencial de alta o modificación de terceros no obligados a comunicarse electrónicamente los solicitantes deben de personarse en el Registro general del Ayuntamiento o en cualquiera de las oficinas habilitadas para ello.

En estas sedes se debe presentar la solicitud mediante un formulario que se puede descargar de la Web del Ayuntamiento, en la que consignan sus datos personales y de la cuenta bancaria a registrar.

Los requisitos documentales para acreditar la titularidad de la cuenta bancaria son los mismos que en el trámite electrónico. Sin embargo, en esta forma de tramitación se debe presentar también, en todo caso, acreditación de la identidad persona solicitante y/o de la persona representada mediante la aportación de su documento de identificación fiscal completo.

La documentación presentada en papel se digitaliza para continuar el resto de la tramitación de forma electrónica.

El resto de los requisitos son los mismos que en el trámite electrónico.

1.3 Verificación del IBAN hasta el 9 de octubre de 2025

Un aspecto importante en el mantenimiento del FMT es la verificación de la concordancia del titular real del IBAN con el acreedor o tercero que consta en el FMT. La certificación de la entidad financiera da una cierta seguridad, pero se han cometido fraudes en los que se ha falsificado esa certificación. Recientemente se ha implantado el servicio de verificación **IBERPAY** que da solución a esta problemática.

¿Qué es el servicio de titularidad de cuentas Iberpay?
Fuente: https://www.iberpay.com/es/servicios/sectoriales/titularidad-de-cuentas/

El servicio de titularidad de cuentas es un servicio sectorial, digital y de alto valor añadido, prestado por Iberpay, que permite la verificación instantánea de la titularidad de las cuentas bancarias españolas en tiempo real y 24x7.

Desarrollado por Iberpay, este servicio cuenta con la participación de todas las entidades del sistema bancario español, lo que permite confirmar la titularidad de más de 80 millones de cuentas de pago (el 99% de las cuentas bancarias españolas).

Titularidad de cuentas es un servicio digital que ayuda a **reducir el fraude en los pagos** de cuenta a cuenta y a **reducir errores** en las transacciones comerciales, los pagos y los cobros. Además, facilita que la propia operativa bancaria se vea significativamente mejorada, dado que el banco reduce la operativa fraudulenta y errónea que recibe de sus clientes, evita excepciones y procesos manuales, y mejora el proceso automático “end-to-end” de los pagos.

Las claves del servicio:

- Confirmación de la titularidad de cualquier cuenta de pago, CIF/NIF contra el código IBAN de una cuenta, a través de un **servicio digital, instantáneo y 24x7**.
- **Evita fraude**: verifica la cuenta del beneficiario en tiempo real, por ejemplo, antes de enviar pagos o cobros, o en el proceso de onboarding digital de clientes.
- **Reduce errores:** anualmente, se registran +5 millones de devoluciones y más de 0,38 millones de rechazos de operaciones de pago.
- **Certifica la titularidad**: sustituye al certificado de titularidad bancaria de forma digital.
- **Información fidedigna,** más actualizada, en tiempo real.
- **Universalidad y sin fricción**: +80 millones de cuentas verificables en España (≈ todas), sin fricción y en menos de tres segundos.
- Comercialización y acceso al servicio **a través de los bancos**.

¿Cómo funciona el servicio Iberpay?

Paso 1-**Inicio de la solicitud:** el proceso comienza cuando un cliente bancario solicita a su entidad la confirmación de la titularidad de una cuenta.

Paso 2-**Solicitud de verificación:** la entidad inicia la solicitud con los detalles de titularidad de una cuenta que se desea verificar.

Paso 3-**Verificación en tiempo real:** Iberpay utiliza su tecnología en tiempo real para remitir dicha solicitud a la entidad confirmante de cuyo cliente se desea confirmar la titularidad.

Paso 4-**Confirmación de la titularidad:** la entidad confirma si los datos proporcionados son correctos y proporciona una respuesta inmediata sobre la autenticidad de la cuenta.

Paso 5-**Resultados de la verificación**: los resultados de la verificación se envían de vuelta a la entidad solicitante. Este proceso tarda menos de un segundo.

Paso 6-**Uso en transacciones o procesos comerciales**: con la información de la titularidad confirmada en tiempo real, la empresa o cliente puede proceder con confianza en sus operaciones financieras o comerciales, evitando fraudes y errores relacionados con la titularidad de la cuenta.

Iberpay se integra en el ERP de la entidad auditada y se comunica automáticamente vía servicios web con las entidades financieras por lo que al autorizar el alta del IBAN en el FMT, Tesorería puede hacer, con carácter previo, esta comprobación de forma automatizada.

1.4 Verificación del IBAN/beneficiario después del 9 de octubre de 2025

El 9 de octubre de 2025 entrará en vigor el **Artículo 5 quater** del Reglamento (UE) nº 260/2012, de 14 de marzo de 2012, por el que se establecen requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros, según la redacción dada por el Reglamento (UE) 2024/886 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de marzo de 2024.

El Reglamento (UE) 2024/886 señala que la seguridad de las transferencias en euros, tanto inmediatas como no inmediatas, es fundamental para aumentar la confianza de los usuarios de servicios de pago para enviar y recibir transferencias y garantizar su uso. Con arreglo a la Directiva (UE) 2015/2366, **el único factor determinante de la correcta ejecución de la operación con respecto al beneficiario es el identificador único (IBAN)**, definido en dicha Directiva, y **los proveedores de servicios de pago (las entidades financieras) no están obligados a verificar el nombre del beneficiario**. **Los proveedores de servicios de pago deben tener implantadas medidas sólidas y actualizadas de detección y prevención del fraude, diseñadas para evitar que se envíe una transferencia a un beneficiario no deseado como consecuencia de un fraude o error**, dado que el ordenante podría no poder recuperar los fondos antes de que se abonen en la cuenta del beneficiario.

Los proveedores de servicios de pago deben ofrecer un servicio de garantía de la verificación del beneficiario al que el ordenante tenga la intención de enviar una transferencia (**servicio de garantía de la verificación**). Para evitar fricciones o retrasos indebidos en el tratamiento de la operación, el proveedor de servicios de pago del ordenante debe prestar dicho servicio inmediatamente después de que este facilite la información pertinente sobre el beneficiario y antes de que se le ofrezca la posibilidad de autorizar la transferencia.

Algunos atributos del nombre del beneficiario a cuya cuenta el ordenante desea realizar una transferencia, como la presencia de signos diacríticos o diferentes transliteraciones posibles de nombres en otros alfabetos, diferencias entre los nombres de uso habitual y los nombres indicados en los documentos oficiales, podrían dar lugar a una situación en la que el nombre del beneficiario facilitado por el ordenante y el nombre asociado al identificador de la cuenta de pago que se especifica en el punto 1, letra a), del anexo del Reglamento (UE) n.o 260/2012 (identificador de la cuenta de pago), que fue facilitado por el ordenante, no coinciden de forma exacta, pero sí casi exacta. En tales casos, para evitar una fricción indebida en el tratamiento de las transferencias en euros y facilitar la decisión del ordenante sobre si proceder o no a la operación prevista, el proveedor de servicios de pago debe indicar al ordenante el nombre del beneficiario asociado al identificador de la cuenta de pago facilitado por el ordenante.

Autorizar una transferencia en la que no se haya verificado el beneficiario puede dar lugar a la transferencia de fondos a un beneficiario no intencionado. **Los proveedores de servicios de pago no deben ser considerados responsables de la ejecución de una operación enviada a un beneficiario no intencionado** por causa de un identificador único incorrecto, tal como se establece en el artículo 88 de la Directiva (UE) 2015/2366, en la medida en que los proveedores de servicios de pago **hayan prestado correctamente el servicio que garantice la verificación**. No obstante, **cuando los proveedores de servicios de pago no presten correctamente dicho servicio y esto dé lugar a una operación de pago ejecutada de manera defectuosa, dichos proveedores de servicios de pago deberán reembolsar sin demora el importe transferido al ordenante** y, cuando proceda, restablecer el saldo de la cuenta de pago en la cual se haya efectuado el adeudo a la situación en la que habría estado si no hubiera tenido lugar la operación de pago. Los proveedores de servicios de pago deben informar a los usuarios

de servicios de pago de las consecuencias que la decisión de estos últimos de desatender una notificación facilitada con arreglo al presente Reglamento modificativo tenga con respecto a la responsabilidad y los derechos al reembolso de los usuarios de los servicios de pago.

1.5 Controles sobre los datos maestros de terceros

Para combatir la ciberdelincuencia en el sistema de pagos, fundamentalmente son necesarias dos cosas:

a) Que exista un sistema de control interno bien establecido, **con procedimientos de gestión de la tesorería escritos debidamente aprobados y comunicados** que incluyan:

- la gestión de pagos,
- el mantenimiento del FMT, describiendo con detalle el procedimiento de alta y modificación de datos de terceros y de cuentas bancarias,
- las personas autorizadas para cada operación, por ejemplo, para realizar el alta y modificación del FMT y para aprobar los cambios,
- los cambios en el FMT (nuevos proveedores, cambios de datos bancarios, ...) se procesan solo después de que se hayan obtenido las aprobaciones adecuadas, de acuerdo con el principio de mínimo privilegio.
- una adecuada segregación de funciones,
- las altas y variaciones de datos **solo** se pueden hacer de forma electrónica a través de la sede electrónica (excepto para los no obligados legalmente),
- cualquier cambio en los datos del IBAN donde se realizan pagos debe estar justificado mediante un certificado de titularidad real o **preferentemente** mediante el servicio Iberpay integrado con el ERP,
- las declaraciones juradas de titularidad de cuenta corriente no se deben utilizar por los riesgos de falsedad documental,
- si el IBAN que aparece en la factura electrónica no coincide con el que consta en el FMT, no se pagará la factura a aquel IBAN sin verificarlo a través de Iberpay (hasta el 9/10/2025). Solo se pagará al que conste en el FMT, previa aclaración de la cuestión.
- En ocasiones los procedimientos de las entidades auditadas contemplan declaraciones responsables para acreditar la titularidad de las cuentas en el alta terceros y cuentas bancarias en el FMT. Este tipo de requisito o control, aunque es legal (art. 69 Ley 39/2015), no es un control tan robusto y fiable como los certificados o verificaciones con servicios *web* (tipo Iberpay) y representará un mayor riesgo.
- A partir del 9/10/2025 se actualizarán los procedimientos de comprobación del IBAN según se ha comentado en el apartado 1.4 anterior.

b) Establecer una **adecuada ciberseguridad** y controles generales de tecnologías de la información (CGTI) de acuerdo con el Esquema Nacional de Seguridad (ENS) que respalden los controles de procesamiento de la información, ya que de otra forma no serán fiables. Los controles sobre los FMT son especialmente dependientes de los CGTI y estos deben contemplar:

- la protección perimetral de la red,
- controles de acceso al ERP (módulo FMT) bien configurados. Se revisará que los CGTI *D.1 Uso controlado de privilegios de administración* y *D.2 Gestión de usuarios* funcionan eficazmente, bajo el principio de mínimo privilegio que establece el ENS.
- se mantiene un fichero histórico con todos los cambios en los datos maestros, incluyendo quién los realizó.

Los principales ***objetivos de control*** relativos a los datos maestros son los siguientes:

- Las altas y modificaciones deben ser realizadas por personas autorizadas, de forma exacta y completa.
- Las altas y modificaciones deben ser registradas y archivadas de forma que se mantenga la pista de auditoría (*logs*).

Anexo 1 B Consideraciones y ejemplos sobre los procedimientos de pago

1. Requisitos técnicos establecido en el Reglamento nº260/2012 del Parlamento Europeo y del Consejo de 14 de marzo de 2012 por el que se establecen requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros.

El artículo 5.1 establece que los proveedores de servicios de pago efectuarán transferencias y adeudos domiciliados con arreglo a los siguientes requisitos:

a) Deberán utilizar el identificador de cuenta de pago, el número IBAN.

b) Deberán utilizar los formatos de mensaje establecidos en la norma ISO 20022 XML.

El Reglamento señala que la «norma ISO 20022 XML» es la norma para la elaboración de mensajes financieros electrónicos, según lo definido por la ISO, relativa a la representación física de las operaciones de pago en sintaxis XML, de acuerdo con las disposiciones mercantiles y las directrices de aplicación de los regímenes de operaciones de pago comunes a toda la Unión comprendidas en el ámbito del presente Reglamento.

En resumen, las órdenes de pago emitidas por las entidades públicas a las entidades financieras o proveedores de servicios de pago (PSP) en la terminología del Reglamento debe emitirse con el formato de la norma ISO 20022 XML.

2. Normas del SEPA[10]

Qué significa SEPA

SEPA son las siglas en inglés de Single Euro Payments Area, es decir, Zona Única de Pagos en Euros. Se trata de una iniciativa por la que se establece una verdadera zona integrada de pagos europeos en euros en los que dichos pagos están sujetos a un conjunto uniforme de estándares, normas y condiciones.

La transferencia SEPA es un instrumento de pago básico para efectuar abonos en euros, sin límite de importe, entre cuentas bancarias de clientes en el ámbito de la SEPA, de forma totalmente electrónica y automatizada.

Mensajes ISO 20022 XML de iniciación de pagos

El gráfico siguiente muestra el ámbito que cubren los mensajes ISO 20022 para iniciación de pagos.

En la publicación "Órdenes en formato ISO 20022 para emisión de transferencias y cheques en euros" de la AEB se especifican los aspectos técnicos del mensaje de pagos que se debe enviar a las entidades financieras. En la práctica podemos encontrarnos con que la entidad denomina a estos documentos como ***Cuaderno 34-XML o ISO 20022 XML***. En esta guía usamos la primera.

El Cuaderno 34-XML para la presentación de transferencias, cheques, pagarés y pagos domiciliados, es el fichero de pagos en formato xml, con el que el cliente ordenante presenta las órdenes en formato estándar ISO 20022 XML para la emisión de transferencias en euros y en divisas, y cheques, pagarés y pagos domiciliados en euros.

[10] Fuente: Órdenes en formato ISO 20022 para emisión de transferencias y cheques en euros, noviembre 2023, AEB. (https://s2.aebanca.es/wp-content/uploads/2023/11/folleto.-rdenes-en-formato-iso-20022-para-emisin-de-transferencias-y-cheques-en-euros-noviembre-2023-v102.pdf).

El lenguaje XML (Extensible Mark-up Language) es un metalenguaje de etiquetas creado para el intercambio de información estructurada entre diferentes plataformas que permite definir un formato por medio de esquemas xsd, los cuales determinan qué elementos puede contener un documento XML, cómo están organizados, y qué atributos y de qué tipo son los que pueden tener dichos elementos. Mediante el uso del esquema pain.001.001.03.xsd se puede, además, verificar la validez de la forma y contenido de la información intercambiada.

3. Ejemplos de Gestión de los pagos a acreedores desde cuentas operativas (ni ACF ni PJ) en una entidad local.

El procedimiento de gestión de pagos a acreedores de la entidad parte de los documentos contables que acreditan un saldo a pagar al acreedor derivado de la tramitación de gastos, presupuestarios o no presupuestarios.

Cuando se va a realizar un pago, de acuerdo con el plan de tesorería aprobado, la Tesorería municipal inicia el proceso en la aplicación CONTABLE/TESORERÍA seleccionando los acreedores cuya ordenación de pagos se va a realizar. La prioridad de los acreedores a incluir en la simulación se establece en el plan de tesorería aprobado.

Los pagos se hacen normalmente mediante transferencia bancaria y pueden ser de varios tipos según su circuito de tramitación, los más habituales son:

- Tipo A. Transferencias masivas. Se cursa una orden de pago a la entidad financiera por un importe global que se genera en la aplicación CONTABLE/TESORERÍA. El detalle individualizado de los pagos a realizar se incluye en un fichero con formato estándar bancario (Cuaderno 34-XML) que se envía a la entidad financiera mediante un circuito seguro de transmisión de ficheros.
- Tipo B. Transferencias masivas específicas: pago de nóminas, retenciones judiciales y pensiones alimenticias. Generalmente se realizan una vez al mes. El procedimiento de tramitación es el mismo que en el tipo A.
- Tipo C. Transferencia manual con documento cobratorio. En este caso el oficio de orden de pago al banco se elabora en la aplicación CONTABLE/TESORERÍA, pero va acompañado de un documento cobratorio. Requiere la apertura de un expediente para la obtención del documento (pagos de IVA, IRPF, SS, pago a juzgados, …).

Canales de transmisión de los ficheros entre el ayuntamiento y la entidad financiera. Los ayuntamientos podrán enviar sus ficheros (Cuaderno 34-XML) a través de los siguientes canales:

- Transmisión a través de la página web de la entidad financiera.
- Transmisión Host to Host (protocolos Editran, XCom, Swiftnet). Estos protocolos de transmisión son utilizados principalmente por entidades con un gran volumen de pagos.
- Transmisión desde la oficina gestora. El ayuntamiento deberá entregar el fichero mediante el soporte convenido con la oficina gestora, usualmente un pendrive USB conteniendo el fichero a procesar. Este procedimiento **NO** es recomendable.

Procedimiento ordinario: Transmisión Host to Host

Los documentos generados en la aplicación CONTABLE/TESORERÍA se envían al portafirmas del gestor de expedientes de la entidad de manera automática y siguen las fases que se detallan a continuación.

a) Tramitación del proceso de firma del documento de orden de pago al banco y del documento de oficio de propuesta de ordenación en el portafirmas.

   Los firmantes van recibiendo, por el orden establecido en el portafirmas en el flujo del procedimiento, una notificación para revisar los documentos y firmar electrónicamente para aprobar o rechazar el pago. Además de las tres personas que deben de firmar la orden de pago, también revisa y firma los pagos a realizar el jefe del servicio de Tesorería. En este punto, los firmantes pueden revisar uno a uno los documentos que se van a firmar y los perceptores y cuentas bancarias a las que se va a realizar el pago.

   Una vez se ha aprobado el pago por todos los firmantes, ya estarán disponibles los documentos firmados para su envío.

   La disposición de fondos de las cuentas operativas del Ayuntamiento es mancomunada y requiere siempre la firma de tres de los autorizados para la disposición de fondos: Tesorero, Interventor y Concejal, o sus sustitutos.

La fiscalización formal y material del pago prevista en la normativa aplicable a las Entidades Locales se realiza en esta fase de la tramitación.

b) Contabilización de la relación de los pagos ordenados

En este punto se genera el documento contable de pago presupuestario o no presupuestario, y el fichero en formato bancario Cuaderno 34-XML a remitir a la entidad financiera.

Los apuntes contables de pago se realizan en una cuenta contable de tesorería "transitoria" hasta que se "concilien" con los movimientos reales en banco enviados por la entidad financiera al día siguiente (cuaderno 43), momento en que contabilizan en la cuenta contable de tesorería definitiva.

Este fichero (Cuaderno 34-XML) se almacena en una carpeta del sistema CONTABLE/TESORERÍA a la que **sólo** tiene acceso el propio sistema CONTABLE/TESORERÍA para procesos automatizados o los administradores del sistema.

c) Envío de ficheros al banco

El responsable de pagos remite mediante correo electrónico (con los protocolos SPF, DKIM y DMARC[11]) la orden de pago firmada electrónicamente a la entidad financiera seleccionada que va a realizar el pago.

Adicionalmente, y de forma **automatizada** se envía mediante el sistema EDITRAN el fichero de pagos Cuaderno 34-XML a la entidad financiera. Este envío se realiza a través de la aplicación CONTABLE/TESORERÍA, mediante una interfaz automatizada entre ambos sistemas. **No** se admite su envío por email o fax, ya que no cumple los requisitos de la PSD2.

d) Recepción de la orden de pago y del fichero de pagos por la entidad financiera

La entidad financiera recibe la orden de pago por correo electrónico y debe verificar que está firmada electrónica y mancomunadamente por las tres personas con autorización para disponer fondos.

También verifica que el importe de la orden de pago coincide con el importe total del fichero de pagos enviado a través de EDITRAN.

Procedimiento extraordinario: Transmisión a través de la página web de la entidad financiera

El procedimiento es similar al anterior, pero el fichero de pagos generado (Cuaderno 34-XML) se almacena en una carpeta del sistema a la que tienen acceso N personas (las N personas autorizadas deben ser las mínimas necesarias), incluyendo el personal de tesorería. El fichero Cuaderno 34-XML se carga manualmente en la página web de la entidad financiera. El resto del procedimiento es similar al anterior.

El riesgo principal aquí es la protección de la integridad del Cuaderno 34-XML frente a accesos no autorizados a la carpeta en la que se guarda.

[11] El Centro Criptológico Nacional publicó en mayo de 2024 el informe de buenas prácticas **"BP/33: Recomendaciones de Seguridad en el correo electrónico, DMARC"**. En este documento se explica el concepto de DMARC (*Domain-based Message Authentification Reporting and Conformance*), que es un protocolo de validación de correo electrónico diseñado para proteger los dominios de correo electrónico de la suplantación de identidad, la integridad de la información y otras formas de abuso en el correo electrónico, como el fraude y el phishing.

Se examinan las repercusiones que se desencadenan al aplicar DMARC, detallando cómo esta medida puede influir en la identificación y prevención de intentos de suplantación de identidad (phishing) y otros ciberataques relacionados con el correo electrónico. Se presentan ejemplos concretos de situaciones que pueden surgir al implementar DMARC y se proporciona información esencial para comprender cómo esta herramienta contribuye a garantizar la integridad y autenticidad de los mensajes electrónicos.

Antes de DMARC, ya existían SPF (*Sender Policy Framework*) y DKIM (*DomainKeys Identified Mail*), que son métodos para verificar si los correos electrónicos provienen de fuentes legítimas. Sin embargo, estos métodos tenían limitaciones, especialmente en cómo se trataban los mensajes que fallaban en estas verificaciones. DMARC utiliza las tecnologías de SPF y DKIM antes mencionadas para verificar que los mensajes de correo electrónico procedentes de un dominio sean auténticos y no hayan sido alterados en tránsito.

Programa de auditoría:

Al diseñar los programas se seleccionarán aquellas pruebas que respondan mejor a los riesgos significativos identificados y se adaptarán a las circunstancias de la entidad. El ejemplo siguiente es un programa ejemplo meramente orientativo, para la auditoría de un ayuntamiento, que debe adaptarse a las circunstancias de cada auditoría y de cada tipo de entidad.
Cada OCEX podrá sustituir este programa por los que tenga establecidos como estándar.

Hoja sumaria

Trabajo a realizar:

1. Preparar una hoja sumaria del área y obtener los saldos individuales a 31 de diciembre, de las distintas cuentas comprobando que coinciden con la contabilidad.

   Será la información que debe figurar en la nota __ del modelo de la memoria. Cruzar el total con el epígrafe correspondiente del balance (subgrupo 57).

   Mostrar también los movimientos de cobros y pagos de todas las cuentas para visualizar el volumen de actividad de cada cuenta.

2. Cajas.

   Cruzar las existencias de fondos líquidos de cada caja con las actas de arqueo que deben venir unidas a las cuentas anuales de la entidad.

3. Cuentas bancarias.

   Cruzar los saldos a favor de la entidad en cada cuenta de entidades bancarias con las notas o certificaciones que deben venir unidas a las cuentas anuales de la entidad.

   En caso de haberse solicitado a la entidad un certificado de cuentas bancarias, cruzar los datos con el certificado obtenido.

   Cuando no coincida saldo contable y bancario cruzar saldos con la correspondiente conciliación bancaria.

4. Solicitar una comunicación comprensiva de todas las cuentas bancarias de la entidad con las que han operado durante el ejercicio y solicitar los contratos firmados vigentes con las entidades financieras y analizar entre otros aspectos, los siguientes para cada cuenta bancaria:

   - ✓ Entidad bancaria.
   - ✓ Número de cuenta y tipo.
   - ✓ Título de la cuenta.
   - ✓ Naturaleza de la cuenta (si se trata de una cuenta de provisión de fondos, restringida de recaudación, restringida de pagos, etc.).
   - ✓ Autorización para la apertura.
   - ✓ Fecha de apertura, de última prórroga y, en su caso, de cancelación.
   - ✓ Describir el tipo de restricciones de la cuenta.
   - ✓ Tipo de interés aplicable a saldos deudores y acreedores, periodicidad con la que se liquidan y plazos de ingreso.
   - ✓ Régimen de firmas y personas autorizadas para disponer de los fondos, así como la comunicación a la entidad bancaria de las posibles modificaciones existentes. Indicar en su caso, la situación en que una firma autorizada se ha mantenido con posterioridad a que el titular dejase de desempeñar el cargo que determinó dicha autorización de firma.
   - ✓ Obtener el importe total de cobros y pagos gestionados a través de cada cuenta bancaria.

Información complementaria:

Art. 194 a 199 del TR LRHL

Art 5 del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional

Conocer y comprender los procedimientos de gestión de tesorería y el control interno

Trabajo a realizar:

5. Solicitar si existen procedimientos de gestión de tesorería y revisarlos.
   Solicitar las bases de ejecución del presupuesto.
6. Completar el cuestionario "*Anexo 1 Documentación del conocimiento del proceso de gestión de tesorería"* de la GPF-OCEX 1957.

   Considerar al menos los siguientes aspectos:

   a. Estructura organizativa del departamento de Tesorería.
   b. La forma habitual de ingresos y pagos.
   c. La segregación de funciones.
   d. El puesto de tesorero.
   e. Identificar las aplicaciones informáticas utilizadas en la contabilización y gestión de la tesorería. Señalar quiénes tienen acceso a las aplicaciones de gestión de tesorería o a las opciones de tesorería de la aplicación de contabilidad.
   f. Obtener información sobre el procedimiento para dar de alta terceros y sus cuentas bancarias en las aplicaciones y quienes son los encargados de tramitarlos y aprobarlos (no duplicar si ya se ha hecho el trabajo en otras áreas).
   g. Averiguar si es posible cambiar el tercero y/o cuenta bancaria en un documento de obligación reconocida ya contabilizado. Si es posible, averiguar quién puede hacerlo (no duplicar si ya se ha hecho el trabajo en otras áreas).
   h. Obtener información sobre la carpeta en la que se depositan los ficheros bancarios de pagos y si está restringido el acceso a las personas que lo necesitan exclusivamente.
   i. Comprobar que la Tesorería sirve al principio de unidad de caja, mediante la centralización de todos los fondos y valores generados por operaciones presupuestarias y extrapresupuestarias.
   j. Comprobar si las existencias de efectivo en caja están reglamentariamente limitadas y, en este caso, si se ajustan a dichas limitaciones.
   k. Realizar un flujograma general del procedimiento, y de los subprocesos más relevantes.
7. Analizar conflictos de segregación de funciones.
8. Si hay informes de auditoría de años anteriores, revisarlos y hacer el seguimiento de las deficiencias y de las recomendaciones. Concluir sobre el estado actual e impacto en la presente fiscalización.
9. En las entidades más grandes, considerar la conveniencia de solicitar la ayuda de los expertos en auditoría de sistemas de información.
10. Realizar un resumen de los **principales riesgos inherentes identificados** en el proceso de gestión, valorar los riesgos inherentes y elaborar el espectro de riesgo inherente (si no se ha elaborado al planificar la auditoría de las cuentas anuales). Determinar qué riesgos son significativos.
11. Revisar la valoración del riesgo para esta área.
12. Identificar los CPI relevantes relacionados con el proceso de gestión y los CGTI que los soportan.
13. Identificar y revisar, en su caso, las interfaces de la aplicación con la que se gestiona la tesorería con otras relevantes (contabilidad si no es la misma, ingresos, generación y envío de ficheros a las entidades financieras, …).
14. Se debe realizar o discutir este análisis en una reunión del equipo (ver GPF-OCEX 1513).
15. Documentar el trabajo según el Anexo 1 de la GPF-OCEX 1957.
16. Concluir y señalar la valoración del riesgo para esta área.

    Hacer un resumen de las incidencias detectadas y proponer las sugerencias y recomendaciones que se consideren oportunas para mejorar el control interno y comentarlas con la dirección de la entidad.

Información complementaria:

Revisar los controles generales de TI

***NOTA**: Este paso de programa se cumplimentará por el auditor de sistemas cuando esté prevista su colaboración.*

En las fiscalizaciones recurrentes más importantes, cuando esté previsto en el plan anual o en función de las circunstancias se considere necesario ampliar el alcance de la revisión del proceso y aplicación de gestión de tesorería se deberá recabar la colaboración del auditor de sistemas.

En los ayuntamientos pequeños probablemente no sea fácil cumplimentar este paso.

17. Solicitar la colaboración de expertos en auditoría de sistemas.
18. Ver el trabajo hecho por el equipo de fiscalización en el paso de programa: ***Conocer y comprender los procedimientos de gestión***, y comentarlo entre el auditor y el auditor de sistemas. Completar la revisión del proceso/aplicación de gestión realizada por el equipo de fiscalización.
19. Realizar las pruebas de eficacia del diseño y de eficacia operativa (pruebas de controles).
20. Concluir sobre la situación de los CGTI, su impacto en los CPI y si tiene efecto en la opinión de auditoría.

Información complementaria:

Plan de disposición de fondos/de tesorería

Trabajo a realizar:

21. Comprobar que la entidad ha elaborado el Plan de disposición de fondos exigido por la normativa y revisar el control realizado por el interventor y si existen reparos.

Información complementaria:

El artículo 187 del Texto Refundido de la Ley Reguladora de las Haciendas Locales (TRLRHL), establece: «La expedición de las órdenes de pago habrá de acomodarse al **plan de disposición de fondos** de la tesorería que se establezca por el presidente que, en todo caso, deberá recoger la prioridad de los gastos de personal y de las obligaciones contraídas en ejercicios anteriores». El Plan de Disposición de Fondos es un instrumento necesario para la gestión de la tesorería; y constituye la herramienta para regular la liquidez del sistema financiero local.

El interventor en virtud del artículo 214 del TRLRHL, debe fiscalizarlo formulando reparo en su caso.

Por otra parte, la DA 4ª de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera indica: «Las Administraciones Públicas deberán disponer de **planes de tesorería** que pongan de manifiesto su capacidad para atender el pago de los vencimientos de deudas financieras con especial previsión de los pagos de intereses y capital de la deuda pública». En vigor durante 2012.

Si bien en vigor a partir del 1 de enero de 2013, el contenido mínimo del **Plan de Tesorería** aparece recogido en el apartado 8 art. 16 de la Orden HAP/2105/2012, de 1 de octubre (BOE del 5), por el que se desarrollan las obligaciones de suministro de información previstas en la Ley Orgánica de Estabilidad Presupuestaria y Sostenibilidad Financiera, que establece que, antes del último día del mes siguiente a cada trimestre se deberán presentar «las actualizaciones de su Plan de tesorería y detalle de las operaciones de deuda viva». Esta remisión al Ministerio de Hacienda y Administraciones Públicas la debe hacer el Interventor del Ayuntamiento:

"8. Las actualizaciones de su Plan de tesorería y detalle de las operaciones de deuda viva que contendrá al menos información relativa a:

a) Calendario y presupuesto de Tesorería que contenga sus cobros y pagos mensuales por rúbricas incluyendo la previsión de su mínimo mensual de tesorería.
b) Previsión mensual de ingresos.
c) Saldo de deuda viva.
d) Impacto de las medidas de ahorro y medidas de ingresos previstas y calendario previsto de impacto en presupuesto.
e) Vencimientos mensuales de deuda a corto y largo plazo.
f) Calendario y cuantías de necesidades de endeudamiento.
g) Evolución del saldo de las obligaciones reconocidas pendientes de pago tanto del ejercicio corriente como de los años anteriores.
h) Perfil de vencimientos de la deuda de los próximos diez años.

Cajas (570-574)

Trabajo a realizar:

22. Obtener una relación de Cajas existentes en la Entidad y sus responsables y comprobar:
    a. Que las actas de arqueo unidas a la cuenta general están adecuadamente cumplimentadas y formalizadas. *(Firmadas por el ordenador de pagos (Alcalde), por el responsable administrativo de la gestión financiera (Tesorero) y por el órgano de control interno (Interventor)).*
    b. que las existencias reales con los datos contables a dicha fecha. Investigar las posibles diferencias.
    c. que la existencia en efectivo más la documentación justificativa de pagos realizados que se encuentren pendientes de registrar en el momento de efectuar el arqueo no superan las cuantías máximas de existencias en efectivo autorizadas
23. Realizar un **arqueo sorpresivo** sobre las existencias en las diferentes cajas de la entidad.

    El recuento de los fondos y demás justificantes deberá realizarlo el Cajero pagador en presencia del funcionario de la Intervención o del Tesorero.

    Detallar los resultados de los arqueos en documentos firmados tanto por personal del equipo como de los responsables de la entidad (tesorero) que deben estar presentes durante el arqueo.
24. Revisar los movimientos de efectivo para detectar y analizar partidas poco usuales o extraordinarias.
25. Concluir sobre la razonabilidad de los saldos de caja.

Información complementaria:

Los riesgos más destacados que se pretenden analizar en este apartado son:

Riesgos de incumplimiento:

- Existencia de cajas indebidamente constituidas incumpliendo la normativa aplicable.
- Inadecuada utilización de los fondos.

Riesgos de ineficacia e ineficiencia:

- Inexistencia de una relación completa de Cajas pagadoras, Subcajas, Habilitaciones y unidades administrativas adscritas al organismo/entidad que gestionen fondos de tesorería, así como la falta de información sobre los pagos gestionados por cada una de ellas, impidiendo llevar el control sobre las cajas y el seguimiento de su actividad.
- Ausencia de controles de caja a través de conciliaciones periódicas, circularizaciones periódicas, etc.
- Ausencia de restricciones en el uso de dinero efectivo mediante segregación de funciones, firmas mancomunadas, etc.

El trabajo realizado debe permitir concluir sobre:

- La adecuación normativa de las cajas pagadoras, subcajas, habilitaciones, etc. que gestionan el efectivo existente en el Organismo/Entidad. El cumplimiento de la normativa vigente en cuanto a nombramiento de Cajeros, creación, mantenimiento de existencias en efectivo, etc.
- El cumplimiento de la normativa vigente respecto al control de las cajas de efectivo mediante la realización de arqueos (la no superación de las cuantías máximas de efectivo autorizadas, las posibles diferencias con los registros en libros, etc.).

Cuentas en entidades bancarias (571-573-575-577)

Trabajo a realizar:

26. Comprobar que todas las cuentas han sido aperturadas cumpliendo la normativa aplicable.

    Analizar la relación de cuentas bancarias proporcionada por el auditado.

    Sin perjuicio de otros aspectos que el auditor considere relevantes, verificar que las cuentas bancarias cumplen con los requerimientos legales para su creación, mantenimiento y, en su caso, extinción.

Circularización

27. Solicitar a la entidad la preparación de las cartas de confirmación de saldos bancarios. (*la información a solicitar a los bancos dependerá del alcance de la fiscalización, por lo que los anexos a remitir deberán ser adaptados*).

    La entidad debe preparar las cartas de circularización, conforme a los modelos facilitados al efecto por el auditor, de <u>todas</u> las entidades bancarias en las que hay o haya habido alguna cuenta bancaria durante el ejercicio auditado.

Una vez firmada por la entidad, el auditor las envía.

La carta debe decir claramente que la respuesta ha de enviarse directamente al auditor.

Se pretende que:

i. El banco conteste detallando todas y cada una de las cuentas que la entidad tiene o ha tenido abiertas en el período auditado, especificando su saldo a 31 de diciembre del ejercicio auditado, haciendo constar en su caso si hay alguna restricción al uso de alguno.

ii. Que el banco informe sobre posibles pasivos (muy importante) si hay préstamos o anticipos.

iii. Total, de las letras: descontadas y pendientes de cobro, enviadas en gestión de cobro y pendientes impagadas en poder del banco.

iv. Pormenores sobre toda clase de valores a favor de la entidad auditada que hayan estado en poder del banco, en custodia o en depósito.

v. Cualquier otra información relativa a la entidad auditada con el banco.

vi. Personas que figuran con autorización en el banco para la firma de cheques, letras, endosos, etc., indicando cuántas de ellas son indispensables y combinaciones de las mismas.

28. Añadir el papel de trabajo de control de circularización, actualizándolo convenientemente.

Realizar las siguientes comprobaciones:

- ✓ Número de las cuentas.
- ✓ Naturaleza de las cuentas.
- ✓ Tipo de interés.
- ✓ Firmas autorizadas.
- ✓ Que el saldo, según la información obtenida mediante la circularización coincide con el reflejado en el correspondiente registro contable.
- ✓ Deudas existentes.
- ✓ El número de tarjetas de crédito o débito disponibles.

Analizar los datos proporcionados por las entidades financieras**:** Sin perjuicio de otros aspectos que el auditor considere relevantes, analizar la fiabilidad e integridad de los datos proporcionados por el ente auditado, una vez analizados los registros de las entidades financieras. Si los datos proporcionados fueran poco fiables, incompletos, incorrectos o no íntegros, explicar las razones.

29. En los casos de no respuesta a la primera petición tras un periodo determinado (dos semanas, por ejemplo), remitir la segunda petición.

30. En los casos de no respuesta a la segunda petición, solicitar al personal responsable de la entidad local que se ponga en contacto con la entidad bancaria para que nos conteste de forma inmediata.

31. Revisar las respuestas de las entidades bancarias.

Cruzar los saldos confirmados por los bancos con las conciliaciones bancarias (que deben estar unidas a la cuenta general) en los supuestos que no coincidan con los saldos contables, o con la hoja sumaria de tesorería en los supuestos de coincidencia.

Verificar que las firmas confirmadas y la forma de disposición de los fondos son correctas.

Cruzar toda la información confirmada por los bancos con la información contable de la entidad, para las áreas objeto del alcance de la fiscalización.

Conciliaciones bancarias

32. Verificar que las conciliaciones bancarias, a la fecha de cierre contable, están adecuadamente realizadas y revisadas. Comprobar:

- La exactitud matemática de las conciliaciones.
- Cotejar saldos con extractos bancarios/contestaciones y con contabilidad.
- Analizar con documentación soporte las partidas en conciliación que sean significativas o sospechosas.
- Concluir sobre la razonabilidad de cada una de las conciliaciones.
- Comentar el resultado de la prueba y proponer los ajustes, reclasificaciones o recomendaciones que resulten oportunos.

Otros

33. Verificar si existen cuentas restringidas de ingresos o de gastos, y en caso afirmativo comprobar que sus saldos al cierre están incluidos en el balance.
34. **Analizar los cobros, pagos y saldos de las operaciones con mayores riesgos**: Sin perjuicio de otros aspectos que el auditor considere relevantes, verificar aquellas operaciones como posibles descubiertos en cuentas, la adecuada justificación de las operaciones en el exterior, las realizadas por un agente mediador o equivalente, etc.
35. **Analizar las operaciones extrapresupuestarias**: Sin perjuicio de otros aspectos que el auditor considere relevantes, verificar las operaciones extrapresupuestarias, con objeto de detectar entradas y salidas de fondos no justificadas, verificar la existencia de operaciones anómalas por la atipicidad del importe, la existencia de salidas/entradas de mismo importe, etc.
36. En el caso de **cuentas sin movimientos** durante el periodo auditado, analizar el saldo el último día del período auditado, los días sin movimiento, las causas de su mantenimiento, así como los posibles gastos y rentabilidades asociados a las mismas.
37. **Analizar los movimientos de una muestra de cuentas**: Sin perjuicio de otros aspectos que el auditor considere relevantes, analizar la situación de las cuentas sin movimientos, los motivos de esa falta de movimientos, así como los posibles gastos generados por las mismas.
38. **Corte de operaciones**: consiste en obtener los extractos bancarios de unos días anteriores y posteriores a la fecha de referencia (Cierre) y verificar el movimiento habido en los saldos de la cuenta y su correcta imputación al período correspondiente.
39. Concluir.

Información complementaria:

Los riesgos más destacados que se pretenden analizar en este apartado son:

Riesgos de incumplimiento:

- Incumplimiento de los requisitos legales de apertura, mantenimiento o cierre de las cuentas bancarias.
- Incumplimientos legales en la gestión del pago de los expedientes de gasto, de las nóminas y de los fondos en el exterior.
- Uso inadecuado de los fondos existentes por falta de mecanismos de control.

Riesgos de ineficacia e ineficiencia:

- Inexistencia de una relación íntegra de todas las cuentas bancarias abiertas por la entidad, lo que puede impedir el adecuado control por parte del organismo/entidad de las cuentas bancarias y su estado.
- Inexistencia de registros actualizados sobre la totalidad de cobros y pagos realizados, lo que puede derivar en un inadecuado uso de los fondos.

El trabajo realizado debe permitir concluir sobre:

- El cumplimiento de los requerimientos legales para la creación, mantenimiento y, en su caso, extinción de las cuentas bancarias abiertas por la entidad.
- El volumen de actividad de la Caja pagadora a través de los saldos totales de cobros y pagos.
- El grado de integridad y fiabilidad de la información proporcionada por el gestor, con respecto a la información suministrada por las entidades financieras a través de las circularizaciones realizadas.
- El cumplimiento de la normativa aplicable con respecto a la rentabilidad y/o costes generados por las cuentas corrientes abiertas en las entidades financieras.
- Si los cobros y pagos registrados en las cuentas bancarias están adecuadamente justificados y contabilizados.

Revisión de las conciliaciones bancarias que ha realizado la entidad:

La conciliación consiste en cuadrar, a la fecha del cierre, el saldo según los libros de contabilidad de la entidad con el saldo del extracto o confirmación directa del banco. Además de verificar la exactitud aritmética de la conciliación, desde el punto de vista de la auditoría, hay que analizar con detenimiento las partidas de la misma, verificando su naturaleza, antigüedad e importe. Una partida que aparezca constantemente (años) en la conciliación puede ser indicio de alguna irregularidad.

Otras cuentas de tesorería

Trabajo a realizar:

40. 578 Movimientos internos de tesorería. (Utilización opcional). Verificar que presenta saldo cero al cierre del ejercicio. Revisar si han tenido lugar operaciones significativas durante el ejercicio y comprobar para una muestra su adecuado tratamiento contable.
41. 579. Formalización. Ídem que el punto anterior.
42. 554 y 555 Cobros y pagos pendientes de aplicación. Analizar el saldo al cierre y movimientos del año si son significativos. Comprobar para una muestra significativa si su utilización es la adecuada.
43. Concluir.

Información complementaria:

Pagos a justificar (558)

Trabajo a realizar:

44. *Comprobar si las **bases de ejecución** contienen las normas reguladoras de la expedición de órdenes de pago a justificar y que éstas han sido informadas por el interventor, conforme a lo establecido en el artículo 190.2 del* TRLRHL y en el artículo 72.2 del RD 500/1990. También podrá incluirse la regulación de este procedimiento especial de pagos en los reglamentos o normas generales de ejecución presupuestaria de la Entidad.
45. Obtener del sistema de información contable, las órdenes de pago a justificar contabilizadas al debe de la cuenta 558.5 "Libramientos *para provisiones de fondos" y **seleccionar una muestra** representativa de los mismos que incluya pagos efectuados y pendientes de justificación, pagos efectuados, justificados y contabilizados y pagos pendientes de efectuar, a 31 de diciembre del ejercicio fiscalizado.*
46. *Verificar la adecuada **contabilización** de los libramientos seleccionados, conforme a lo dispuesto en la regla 33 de la ICAL. En caso de que la Entidad aplique el modelo básico, comprobar que los registros extracontables* permiten un adecuado seguimiento y control.
47. Ver*ificar la **adecuación a la legalidad** de la muestra de pagos seleccionada, mediante la verificación de los siguientes aspectos, previstos en los artículos 69 a 71 del RD 500/1990 y a lo dispuesto en la normativa interna del ayuntamiento:*
    a) *Existe una propuesta motivada formulada por el responsable del gasto.*
    b) *La orden de pago a justificar ha sido aprobada por el órgano competente para autorizar el gasto.*
    c) *La expedición de la orden a justificar se acomoda al plan de disposición de fondos de la tesorería, establecido por el alcalde.*
    d) *El plazo máximo de tres meses para su justificación.*
    e) *El reintegro de los importes librados y no pagados o no justificados en el plazo legal.*
    f) *No se han expedido nuevas órdenes de pagos a justificar a perceptores que no hubieran justificado órdenes anteriores por los mismos conceptos.*
    g) *Que los pagos efectuados se han aplicado a la finalidad autorizada.*
    h) *Que los justificantes reúnen los requisitos formales previstos reglamentariamente.*
    i) *Aquellos otros extremos contemplados en la normativa del ayuntamiento.*
48. *Concluir.*

Información complementaria:

Se debe efectuar la imputación presupuestaria en el momento de la expedición y pago de la orden librada a justificar, lo que origina un cargo y un abono en la cuenta 5585. Conforme se van efectuando los pagos al acreedor último se carga la cuenta 5580, la cual se abona a la justificación de los gastos. Si el reintegro del sobrante tiene lugar en un ejercicio posterior debe contabilizarse como un ingreso presupuestario, si es en el mismo ejercicio será un menor gasto presupuestario. A 31 de diciembre todos los gastos realizados por el perceptor, pendientes de justificación, se abonarán a la cuenta 5586. En las entidades que apliquen la Instrucción del modelo básico no se realizan los cargos y abonos detallados en las cuentas de contabilidad financiera.

Anticipos de caja fija (558)

Trabajo a realizar:

49. Comprobar que las bases de ejecución contienen las normas reguladoras de los anticipos de caja fija y que éstas han sido informadas por el interventor, conforme a lo establecido en el artículo 75 del RD 500/1990. También podrá incluirse la regulación de este procedimiento especial de pagos en reglamentos o normas generales de ejecución presupuestaria aprobados por el Pleno.
50. Comprobar que las provisiones de fondos en concepto de caja fija se atienen a lo establecido en los artículos 73 y siguientes del RD 500/90, así como su adecuada contabilización, conforme a la regla 36 de la ICAL.
51. Obtener del sistema de información contable, los pagos efectuados a los acreedores finales con abono a las cuentas restringidas de tesorería de caja fija y cargo a la cuenta 558.1 "Provisiones de fondos para anticipos de caja fija pendientes de justificación" y seleccionar una muestra.
52. Verificar la adecuación a la legalidad de la muestra de pagos seleccionada, conforme a lo establecido en los artículos 73 y siguientes del RD 500/1990 y a lo dispuesto en la normativa interna del ayuntamiento, y su adecuada contabilización (regla 36 ICAL).
53. Operaciones pendientes de aplicar a presupuesto a 31 de diciembre. Comprobar su contabilización en la cuenta 413.
54. Concluir.

Información complementaria:

Los riesgos más habituales en este apartado son:

Riesgos de incumplimiento:

- Incumplimientos legales en la expedición de órdenes de PJ y de ACF (inexistencia de Acuerdo/ Resolución, superación de cantidades máximas, gastos imputables a conceptos presupuestarios no autorizados, etc.).

Riesgos de ineficacia e ineficiencia:

- Falta de calidad de las cuentas justificativas, pudiendo originar una inadecuada utilización de los fondos.
- Utilización abusiva del sistema de anticipos de caja fija, pagos a justificar o procedimientos equivalentes, con respecto al procedimiento ordinario de pago (pagos en firme).
- Procedimientos especiales de pago equivalentes diseñados que establezcan procedimientos ineficientes o desactualizados.
- Existencia de errores o incongruencias en la información contenida en los EST debidos a una mala gestión de la información y documentación que los soporta.

El trabajo realizado debe permitir concluir sobre:

- El cumplimiento de la normativa vigente en los procedimientos especiales de pago (normas que los establezcan, naturaleza de los gastos, órgano competente, tipos de pagos, etc.).
- Idoneidad y eficiencia de la gestión de los procedimientos especiales de pago (saldos de cajas de efectivo y/o cuentas, reintegros, pagos sin justificación, cuentas justificativas fuera de plazo, cuentas justificativas favorables, cuentas sin defectos, incidencias en el pago etc.).
- El cumplimiento de las obligaciones contables (llevanza de los libros y registros contables, cuentas justificativas y documentación que las acompaña, etc.).

9. Estado de Flujos de Efectivo.

Trabajo a realizar:

55. Verificar que las agrupaciones del EFE se estructuran como se indica a continuación:

    i. Flujos de efectivo de las actividades de gestión: son los que constituyen su principal fuente de generación de efectivo y, fundamentalmente los ocasionados por las transacciones que intervienen en la determinación del resultado de gestión ordinaria de la entidad. Se incluyen también los que no deban clasificarse en ninguna de las dos categorías siguientes, de inversión o de financiación.

    ii. Flujos de efectivo de las actividades de inversión: son los pagos que tienen su origen en la adquisición de elementos del inmovilizado no financiero y de inversiones financieras, tanto de corto como de largo plazo, no consideradas activos líquidos equivalentes a efectivo, así como los cobros procedentes de su enajenación o de

su amortización al vencimiento. Forman parte de estos flujos los cobros derivados de la venta de activos en estado de venta.

iii. Flujos de efectivo de las actividades de financiación: comprenden los cobros procedentes de la adquisición por terceros de títulos valores emitidos por la entidad o de recursos concedidos por entidades financieras o terceros, en forma de préstamos u otros instrumentos de financiación y, los correspondientes a aportaciones al patrimonio de la entidad o entidades propietarias. También comprenden los pagos realizados por amortización o devolución de los anteriores instrumentos de financiación y por reparto de resultados a la entidad o entidades propietarias.

iv. Flujos de efectivo pendientes de clasificación: recogen los cobros y pagos cuyo origen se desconoce en el momento de elaborar el estado de flujos de efectivo.

v. Efecto de las variaciones de los tipos de cambio: recoge, con el fin de permitir la conciliación entre las existencias de efectivo al principio y al final del período, el efecto de la variación de los tipos de cambio, sobre el efectivo y otros activos líquidos equivalentes que figuraran denominados en moneda extranjera. El valor en euros de estos últimos será el que corresponda al tipo de cambio de 31 de diciembre.

56. Verificar que en la elaboración del EFE la entidad pública ha tenido en cuenta las disposiciones previstas en el apartado 1 sobre "Normas de elaboración de las cuentas anuales" de la tercera parte del PGCP.

57. Verificar que el saldo de "efectivo y activos líquidos equivalentes al efectivo al final del ejercicio" del estado de flujos de efectivo coincide con los importes reflejados en el epígrafe de "Tesorería" del Balance de Situación.

Información complementaria:

Información de la memoria

58. Verificar la concordancia de la información en Memoria con la ofrecida por los registros contables, así como, si la memoria muestra la información exigida en el PGCP.

59. Verificar que el Estado del remanente de tesorería, incluido en el punto 24.6 de la memoria, se ha elaborado a partir de los saldos de las cuentas del PGCP a que se hace referencia en el cuadro del citado punto.

El remanente de tesorería total se obtendrá por la suma de los fondos líquidos más los derechos pendientes de cobro deduciendo las obligaciones pendientes de pago y agregando las partidas pendientes de aplicación de conformidad con los criterios que se establecen en la memoria.

Información complementaria:

Conclusión del área

60. Concluir sobre si se han alcanzado razonablemente los objetivos del área.

61. Redactar un resumen de los aspectos más importantes del área de tesorería, el trabajo realizado y las incidencias observadas.

62. Comentar las incidencias con los responsables y anotar sus comentarios y nuestra consideración.

63. Referenciar el análisis de las incidencias a las fichas correspondientes de AS1. Indicar para cada incidencia si es de carácter financiero o de legalidad, así como su consideración de salvedad, o a comentar solo en el interior del informe o recomendación de control interno a comentar en el interior del informe y en su caso en el apartado de recomendaciones.

64. Redactar la parte del proyecto de informe del área con el formato aplicable.

Información complementaria:

Al finalizar la fiscalización de esta área se deberá concluir sobre si, tras el trabajo realizado y el análisis de las evidencias obtenidas, se considera que se han alcanzado razonablemente los objetivos de auditoría y no se ha detectado ninguna incorrección de carácter significativo. En caso contrario se describirán las incorrecciones detectadas.

Guía práctica de fiscalización de los OCEX

GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría

Referencia: GPF-OCEX 1315 (Revisada), GPF-OCEX 5330, GPF-OCEX 5331 y GPF-OCEX 5313

Documento elaborado por la Comisión Técnica de los OCEX y
aprobado por la Conferencia de Presidentes de ASOCEX el 19/10/2023.

1. Qué es la gobernanza de la ciberseguridad

Con la implantación de la administración electrónica avanzada los actuales sistemas de información son más complejos y están más interconectados que nunca. En este entorno interconectado aumentan los riesgos de ciberseguridad, su probabilidad y las consecuencias perturbadoras sobre los servicios prestados por los entes públicos. Como certeramente indica la reciente publicación *Cybersecurity Program Audit Guide* de la US Government Accountability Office, "*las amenazas de ciberseguridad continúan aumentando a medida que aumenta la conectividad de los sistemas y las técnicas de ataque crecen en sofisticación*".

El *Código de buen gobierno de la ciberseguridad*[1] señala que "***La ciberseguridad se ha convertido en el pilar estratégico sobre el que poder asentar la revolución digital que han experimentado todos los sectores de la sociedad, incluyendo Administraciones públicas, empresas y ciudadanía. Solo sobre la base de la ciberseguridad es posible continuar avanzando de forma segura en dicha transformación***." En términos muy similares se manifiesta el Centro Criptológico Nacional (CCN) en su publicación *Aproximación al marco de gobernanza de la ciberseguridad*, en la que se afirma que el éxito de la transformación digital depende, en gran medida, de garantizar los requisitos mínimos de seguridad protegiendo la información tratada y los servicios prestados, elementos consustanciales al desarrollo de nuestra sociedad.

Por esta razón, **es imperativo que los responsables de los entes públicos gestionen dichos riesgos e implanten una sólida gobernanza de la ciberseguridad como elemento fundamental para establecer una ciberdefensa eficaz.**

Se entenderá por gobernanza de la seguridad de la información y las comunicaciones o de ciberseguridad (términos que utilizamos de forma indistinta) **el conjunto de responsabilidades y actividades que tienen como objetivo proporcionar una dirección estratégica en esta materia, garantizar que se logren los objetivos, verificar que el riesgo se gestione adecuadamente y comprobar que se utilicen los recursos de la entidad de una forma responsable**.[2]

---

[1] Publicado en junio de 2023 por el Foro Nacional de Ciberseguridad.

[2] Véase el glosario de la Information Systems Audit and Control Association (ISACA).

La gobernanza es el proceso de establecer y mantener un marco de referencia, y apoyar la estructura y los procesos de gestión para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los datos.

Es más que una mera cuestión técnica, por lo que exige un liderazgo efectivo, procesos sólidos y estrategias en consonancia con los objetivos de la organización[3]. Este liderazgo debe ser ejercido por la alta dirección/órganos superiores de la entidad. Su compromiso con la seguridad es el factor clave que habilita el establecimiento de un marco de gobernanza efectivo en las organizaciones.

2. Por qué es importante la gobernanza de la ciberseguridad para una entidad

La gestión de la ciberseguridad, como tarea clave para la prevención proactiva, requiere del establecimiento de un marco de gobernanza, en el que se designen a los organismos o unidades responsables de dicha gestión y se definan claramente sus competencias en este ámbito, que deberán ser conocidas por toda la organización.[4]

La importancia de la gobernanza en la gestión de la ciberseguridad ha sido objeto de diversos documentos y guías del Centro Criptológico Nacional (CCN), entre los que destacan la *Aproximación al Marco de Gobernanza de la Ciberseguridad. Año 2022*, la *Guía de Seguridad de las TIC CCN-STIC 201 Organización y Gestión para la Seguridad de las TIC* y la *Guía de Seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones*.

La existencia de un conjunto eficaz de procesos de gestión de la ciberseguridad y de responsabilidades definidas proporciona a las entidades múltiples ventajas con respecto a las entidades sin un marco de gobernanza adecuadamente definido, independientemente de la existencia de recursos técnicos y de las medidas de seguridad aplicadas.

Algunas de las ventajas que la existencia de un marco efectivo de gobernanza proporciona a las entidades serían:

- Posibilita la alineación de las actividades relativas a la seguridad de la información con los objetivos estratégicos de la entidad.
- Facilita la coordinación entre distintas áreas de la organización y los implicados en materia de seguridad de la información.
- Posibilita que el conjunto de actividades realizadas y medidas de seguridad aplicadas constituyan un Sistema de Gestión de la Seguridad de la Información que trasciende las iniciativas individuales.
- Establece las responsabilidades del personal implicado, necesarias para garantizar que se cumplen los objetivos y se alcanza el nivel de seguridad requerido.
- Establece procesos que impiden que la eficacia de las actividades de seguridad dependa de roles concretos de la organización o solo de iniciativas personales, sino de un sistema bien establecido.
- Ayuda a fomentar una cultura en materia de ciberseguridad en las organizaciones.

Por el contrario, aquellas entidades que no disponen de un marco de gobernanza adecuadamente definido e implantado tienen una alta probabilidad de experimentar las siguientes carencias:

- El principal riesgo consiste en que la entidad sea vulnerable frente a ciberataques por carecer de un sistema de controles coherente y aceptado por toda la organización.
- Probable uso ineficiente de los recursos, dado que, independientemente de la idoneidad de dichos recursos con respecto a las necesidades identificadas, no existen mecanismos que aseguren que estos son utilizados de manera adecuada para responder a necesidades alineadas con los objetivos estratégicos.
- No asegura la existencia de mecanismos de coordinación interna entre las distintas áreas de la organización y los responsables de la seguridad, lo que impide garantizar que las necesidades sean adecuadamente identificadas en tiempo y forma. Además, posibilita que existan áreas que, de manera

[3] Véase el apartado 66 de Análisis N.º 02/2019: Desafíos de una política eficaz de ciberseguridad en la UE del Tribunal de Cuentas Europeo.

[4] Aproximación al marco de gobernanza de la ciberseguridad, CCN 2022.

inadecuada, realicen una gestión no coordinada de la seguridad al margen las políticas y normas de seguridad de la organización.

- No se asegura que el conjunto de medidas y procesos de seguridad implantados constituyan un Sistema de Gestión de la Seguridad de la Información, integrado y coherente, lo que implica un riesgo de que no existan mecanismos de control que velen por la eficacia de dichas medidas y procesos.
- En caso de no haberse definido responsabilidades al nivel directivo adecuado, existe un riesgo de que las necesidades con respecto a la seguridad de la información identificadas por sus responsables no sean debidamente atendidas por la organización.
- No se asegura que existan mecanismos que independicen las medidas y procesos de seguridad de las personas encargadas de gestionarlas, de modo que existe un riesgo de que ante determinadas ausencias, las medidas de seguridad no sean aplicadas.

Por lo tanto, podemos concluir que **una gobernanza adecuadamente establecida proporciona a las entidades mecanismos que garantizan que la seguridad es entendida como un sistema integrado, continuado y proactivo, con procesos de gestión que velan por la eficacia de las medidas y procesos de seguridad**. La inexistencia de este marco de gobernanza, independientemente de los esfuerzos y recursos dedicados a la seguridad, impide asegurar su eficacia e idoneidad.

3. Por qué es importante la gobernanza de la ciberseguridad para el auditor

En la *GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría* se señalan las razones por la que tiene gran relevancia en una auditoría financiera analizar la situación de la gobernanza sobre las tecnologías de la información (TI) y de la gobernanza de la ciberseguridad al revisar el componente "Entorno de control" del sistema de control interno de la entidad auditada, de acuerdo con los requerimientos de la NIA-ES 315 Revisada / GPF-OCEX 1315 Revisada.

Las ciberamenazas representan hoy en día uno de los principales riesgos al que deben hacer frente las organizaciones públicas, por ello, los auditores públicos deben vigilar que estas despliegan unos adecuados controles de ciberseguridad cuya organización y estructuración parte del establecimiento de una sólida gobernanza de la ciberseguridad.

Pero además de la importancia de la gobernanza en la revisión del control interno, el auditor público tiene la obligación de revisar el cumplimiento de la legalidad en la gestión de los entes que audita. Las disposiciones legales y reglamentarias que puedan tener un efecto directo o indirecto en los estados financieros de la entidad incluyen normas sobre seguridad de la información y sobre protección de datos de carácter personal.

La consideración del cumplimiento por la entidad de las disposiciones legales y reglamentarias, de conformidad con la NIA 250 (Revisada), puede incluir la obtención de conocimiento de los procesos de TI de la entidad y de los controles de TI que la entidad ha implementado en virtud de disposiciones legales o reglamentarias. (*Anexo 5, párrafo 20, NIA-ES 315 Revisada)*

Para cumplir los requisitos de la *NIA-ES-SP 1250 Consideración de las Disposiciones Legales y Reglamentarias en la Auditoría de Estados Financieros*, un auditor puede, por ejemplo, considerar:

- Cumplimiento con el Esquema Nacional de Seguridad (ENS). Son cumplimientos relevantes relacionados con la gobernanza de la ciberseguridad, al menos, los siguientes:
  - De acuerdo con el ENS, debe formularse la **política de seguridad de la información (PSI)** que debe ser aprobada por el titular del órgano superior de la entidad. Dicha PSI debe ser difundida entre la totalidad de los miembros de la organización, así como, en su caso, a proveedores y terceros.
  - Deben haberse designado los **roles y responsabilidades en materia de seguridad de la información**. Los órganos superiores de la entidad deben nombrar al responsable de la información (que puede tratarse de una persona o un órgano colegiado), al responsable del servicio (que puede ser el mismo que el anterior), al responsable de la seguridad y al responsable del sistema. El procedimiento de nombramiento formal de los responsables mencionados debe constar en la política de seguridad de la información de la entidad.
  - Debe haberse implementado un **comité de seguridad TIC**.

- Debe haberse realizado una **auditoría de seguridad** al menos hace dos años.

- Cumplimiento con la normativa de protección de datos de carácter personal. Son cumplimientos relevantes, al menos, los siguientes:
  - El nombramiento de **delegado de protección de datos** (DPD) y notificación a la Agencia de Protección de Datos, como exige la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
  - Elaboración de un **registro de actividades del tratamiento**.
  - Realización de un **análisis de riesgos** sobre los tratamientos de datos personales.
  - Realización de una **auditoría** en materia de protección de datos.

Ambas normas son muy importantes y su incumplimiento puede tener consecuencias relevantes en términos de vulnerabilidad frente a ataques a los sistemas de información o de vulneración de datos personales. Por esta razón **debe exigirse su cumplimiento con carácter generalizado**.

Será de aplicación la *GPF-OCEX 4320 Guía sobre la importancia relativa en las fiscalizaciones de cumplimiento de la legalidad*.

En los informes de auditoría financiera su incumplimiento deberá ser reportado en el apartado *Otros requerimientos legales y reglamentarios*[5].

4. Responsables del establecimiento de una adecuada gobernanza de ciberseguridad

Aunque las responsabilidades relacionadas con la gobernanza se encuentran distribuidas entre distintos agentes implicados, con diferentes niveles de responsabilidad y atribuciones, la responsabilidad de establecer una adecuada gobernanza de la ciberseguridad, que empieza con la aprobación de las políticas de seguridad de la información, de acuerdo con artículo 12 del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad, es del órgano competente de la entidad (normalmente el órgano de gobierno o el titular del órgano superior correspondiente).

En las entidades locales, esta responsabilidad principal recae en su presidente/a. Son los responsables de garantizar que el funcionamiento de la organización resulta conforme con las normas aplicables y de que existan unos adecuados controles sobre los sistemas de información y las comunicaciones. En las comunidades autónomas la responsabilidad principal recae en el órgano de gobierno autonómico. Son los máximos responsables de la implantación del ENS.

La implicación de los órganos superiores es, tal vez, el factor más importante para la implantación con éxito de un sistema de gestión de la seguridad de la información o de ciberseguridad[6].

Sin embargo, en la práctica, de forma general, se ha asumido de manera **errónea** que la responsabilidad de la seguridad de la información y los servicios, materializada en el cumplimiento de ENS, recae en exclusiva sobre los responsables de las áreas informáticas y tecnológicas, incurriendo en un grave error de criterio que menoscaba la ciberresiliencia de las instituciones.

Los responsables de las áreas TI ya asumen la responsabilidad de la gestión de los sistemas, que es incompatible con la responsabilidad sobre la seguridad de la información (artículo 11 del ENS).

La responsabilidad de la ejecución de las actividades establecidas por los responsables del gobierno de la entidad corresponde a la dirección. Ver a este respecto el apartado 3 de la *GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría*.

[5] Véase la GPF-OCEX 1730 Preparación de informes de auditoría sobre los estados financieros.

[6] Guía de iniciación a actividad profesional implantación de sistemas de gestión de la seguridad de la información (SGSI) según la norma ISO 27001, Colegio Oficial de Ingenieros de Telecomunicación.

5. Elementos de la gobernanza de la ciberseguridad

Para lograr implantar un sistema de prevención proactiva de ciberseguridad, las organizaciones deben establecer un marco de gobernanza, en el que se designe a los responsables en la materia y sus funciones, y describir los procesos de gestión relacionados con la ciberseguridad[7].

De acuerdo con este marco hay una serie de elementos que, o bien son componentes esenciales de la gobernanza o son condiciones imprescindibles para su buen funcionamiento.

La relación de estos elementos esenciales es la siguiente:

- **Los órganos superiores de la entidad deben ejercer liderazgo y compromiso** con respecto a la seguridad de la información y deben velar por que sean satisfechas todas necesidades y condiciones necesarias para el establecimiento de una gobernanza adecuada.
- Debe formularse la **política de seguridad de la información (PSI), que debe ser aprobada por el titular del órgano superior correspondiente**. Dicha PSI debe ser difundida entre la totalidad de los miembros de la organización.
- Debe existir un **comité de seguridad de la información** con un funcionamiento efectivo.
- Las entidades deben asignar **roles y responsabilidades en materia de seguridad de la información**.
- Deben existir **normas y procedimientos de seguridad formalizados y debidamente aprobados y deben ser de aplicación obligatoria en todos los sistemas de información de la entidad sin excepción.** Esta normativa interna debe diseñarse para ser aplicada, no para cumplir una formalidad legal.
- La entidad debe **disponer de los recursos materiales y humanos** adecuados para atender a las necesidades identificadas e implementar las medidas de seguridad necesarias. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa[8]. La ciberseguridad requiere de una constante y adecuada dotación de recursos asignados a su mantenimiento y mejora.
- Debe existir una **planificación estratégica en materia de ciberseguridad**, que proporcione un marco de actuación a medio plazo que asegure la atención a las necesidades prioritarias con respecto a la seguridad, y se encuentre alineada con la estrategia corporativa. La planificación estratégica de la seguridad evita una gestión reactiva basada principalmente en necesidades sobrevenidas.
- El conjunto de procesos implantados para la gestión de la seguridad debe constituir un **Sistema de Gestión de la Seguridad de la Información (SGSI)**, que trate la seguridad de manera integrada, continuada y proactiva, y que abarque todas las fases del proceso de seguridad: conocer, evaluar y tratar los riesgos y establecer las medidas de seguridad necesarias.
- Se debe establecer una **cultura en materia de ciberseguridad.** Todo el personal de la organización necesita poseer suficientes conocimientos en materia de ciberseguridad para enfrentarse y mitigar el riesgo al que esté expuesto. Dicha cultura de ciberseguridad debe ser impulsada por la dirección en forma de planes estratégicos que definan objetivos y medidas concretas, además de incluir **planes periódicos de formación y concienciación** de los trabajadores.

Aunque la ausencia de alguno de estos elementos no implica necesariamente la falta de efectividad de las medidas de seguridad que se encuentren implantadas en las entidades, la carencia de una correcta organización de la ciberseguridad impedirá asegurar que la efectividad se mantendrá a lo largo del tiempo, independientemente de las circunstancias y condicionantes existentes, lo que **incrementará los ciberriesgos**.

[7] Aproximación al marco de gobernanza de la ciberseguridad, CCN 2022.

[8] Exposición de motivos del Real Decreto 311/2022.

Las entidades deben organizar sus estructuras de gobernanza atendiendo al **principio de proporcionalidad**, al que se alude varias veces en el Real Decreto 311/2022 que aprueba el ENS, teniendo en cuenta su propia complejidad, tamaño, riesgos a los que esté sometida, recursos con los que cuenta y el resto de las circunstancias aplicables.[9]

6. Modelo de gobernanza

La gestión de la seguridad de los sistemas de información exige establecer una organización interna de la seguridad. Tal organización debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.

Cada entidad deberá establecer y aprobar su propio modelo de gobernanza de acuerdo con su estructura, dimensión y recursos disponibles, atendiendo al principio de proporcionalidad y deberá recogerlo en su Política de Seguridad de la Información.

En las guías del CCN se propone un modelo de gobernanza de la seguridad que facilita la toma de decisiones interna y articula la colaboración entre ellas. Está destinado a la gestión de los procesos relacionados con el Esquema Nacional de Seguridad y basado en bloques de responsabilidad. Habrá que adaptar este modelo a las posibilidades reales de decisión, gestión y operación de la seguridad de cada entidad.

Según el modelo, la gobernanza de la seguridad se articula a través de un Comité de Seguridad TIC, se gestiona a través de una Oficina de Seguridad TIC, y se implementa mediante Centros de Operaciones de Ciberseguridad (COCS) en colaboración con el departamento de TI. El COCS, realiza una vigilancia continua de los sistemas bajo su responsabilidad, junto a otros roles, y colabora con el departamento de TI, para asegurar la correcta operación e implementación de la seguridad.

A modo de ejemplo se representa gráficamente la estructura básica de ciberseguridad, propuesta en una reciente guía del CCN:

Fuente: Guía CCN-STIC 881

[9] De acuerdo con el "Principio 1: Proporcionalidad" del Código de buen gobierno de ciberseguridad.

7. El comité de seguridad TIC

La gobernanza de la seguridad de la información en una organización se articula a través de un comité de seguridad TIC[10] o comité de seguridad de la información, que se constituye como un órgano colegiado[11], algunos de cuyos miembros ostentarán roles especializados dentro de la organización de la seguridad. Es la máxima autoridad en la organización respecto a las decisiones de seguridad que afecten a los sistemas que manejan información o prestan algún servicio.

El comité de seguridad TIC es el órgano especializado y permanente de una organización para la ciberseguridad y estará integrado por aquellas personas de la organización con responsabilidad en la toma de decisión en materia de seguridad y privacidad de la información, así como por aquellas designadas en representación de otros órganos o comités. Podrá integrar a vocales de otras áreas de la entidad que sean relevantes para la finalidad del comité, tales como la persona designada como Delegado de Protección de Datos o del Departamento Jurídico o de Recursos Humanos, entre otras.[12]

De acuerdo con lo dispuesto en el ENS, con los criterios generales expuestos en las guías del CCN consideramos que al definir la composición del comité de seguridad TIC y en su funcionamiento se deben tener en cuenta las siguientes consideraciones:

- **No es un comité meramente técnico**, sino que debe integrar vocales de cualquier área significativa necesaria para llevar a cabo sus objetivos.
- Debe ser un **órgano con poder de decisión ágil de toma de decisiones**. Un comité sin poder de decisión, o sin capacidad de influir en quien deba tomarlas, puede resultar inefectivo. Por este motivo se requiere que el órgano cuente con integrantes del nivel más alto de las organizaciones, además de contar con el apoyo necesario para implantar cuantas decisiones y acuerdos se tomen en las reuniones.
- Debe **reunirse periódicamente** con objeto de conocer el estado de la seguridad de la información de la entidad y tomar las decisiones pertinentes de forma oportuna.

  En algunas de las entidades se observa una baja o nula actividad del comité, pese a estar constituido formalmente, lo cual es equivalente a su no existencia. En entidades de gran tamaño y dada la complejidad que presentan sus sistemas de información, el comité debería reunirse al menos trimestralmente.[13]
- **El personal con roles asignados en materia de seguridad de la información o protección de datos deben disponer del suficiente tiempo de dedicación a la seguridad** para desempeñar sus funciones de manera efectiva.
- **El comité de seguridad TIC debe ejercer sus competencias sobre todos los sistemas de la entidad sin excepciones, incluidos aquellos que por su naturaleza son gestionados directamente por los servicios que explotan dichos sistemas.**

  Hay una peculiaridad en el caso de los ayuntamientos que se debe mencionar. En estos casos, en general, los departamentos de policía municipal gestionan de forma casi totalmente independiente sus propios sistemas de información, no integrándose en muchos casos en el marco general de ciberseguridad del ayuntamiento. No es tarea de los OCEX definir cómo deben estar organizados en un ayuntamiento u otra entidad sus sistemas de información, ni si los sistemas policiales y otros sistemas críticos deben estar totalmente integrados con los sistemas corporativos (que normalmente es la solución idónea) o es mejor que estén totalmente separados (lo cual entraña ciertos riesgos innecesarios). Esta es una decisión organizativa de la corporación.

[10] Guía de seguridad de las TIC, CCN-STIC 201. Organización y gestión para la seguridad de las TIC, CCN, enero de 2021.

[11] Regulado por lo dispuesto en la Sección 3ª del Capítulo II del Título Preliminar, de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

[12] Apartado 5.1 de "Aproximación al Marco de Gobernanza de la Ciberseguridad. Año 2022", CCN.

[13] El Código de buen gobierno de la ciberseguridad recomienda que se reúna al menos dos veces al año, pero lo consideramos totalmente insuficiente.

No obstante, cualquiera que fuere la fórmula elegida para organizar los sistemas de información de una entidad, **su marco de ciberseguridad debe ser único**. Esto quiere decir que puede haber un único responsable de seguridad de la información con responsabilidades en el conjunto de sistemas de información de la entidad. O puede haber un responsable de la seguridad de la información de los sistemas de información policiales y/o sistemas críticos, pero en este caso deberán estar integrados también en el CSI para que sean copartícipes y corresponsables de las decisiones que se adopten.

Componentes

La guía CCN-STIC 201 indica que será cada administración la que establezca la composición de su comité de seguridad TIC en función de sus competencias, estructura y circunstancias. No obstante, las guías del CCN[14] establecen una serie de orientaciones sobre su composición y las responsabilidades de sus miembros, que deberían ser, al menos, los siguientes:

- **El presidente** del comité.

  En el caso de una entidad local debería ser el concejal o diputado responsable en materia TIC.

  En el caso de las universidades el CCN recomienda que sea el rector o una persona en la que delegue.

- El **secretario** del comité. En la Guía de seguridad de las TIC CCN-STIC-881, se propone que sea el secretario general de la entidad o una persona en la que delegue.

  Consideramos imprescindible la participación en el comité de seguridad TIC de los/as secretarios/as generales de las entidades, o alguien de su equipo, dado que sobre ellos recae la responsabilidad sobre la ejecución de muchas decisiones del comité.

  Al secretario le corresponderá:

  - Convocar las reuniones del Comité de Seguridad de la Información.
  - Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
  - Elaborar el acta de las reuniones.
  - Es responsable de la ejecución directa o delegada de las decisiones del Comité.

- Responsable de seguridad de la información (**RSEG**).
- Responsable de la información.
- Responsable del sistema.
- Responsable de seguridad física.

  Este rol asume la responsabilidad sobre la seguridad física de la organización[15].

- Delegado de protección de datos (**DPD**), que participará con voz, pero sin voto, para no condicionar sus decisiones futuras y garantizar su independencia y ausencia de conflicto de intereses.

  Este rol es **incompatible** con el de responsable de seguridad.

- Responsable del cumplimiento legal.

El comité puede constituirse con miembros fijos y otros opcionales, por lo que además de los expuestos, podrá invitarse a intervenir en las reuniones cuantas personas sean necesarias de acuerdo con los asuntos a tratar.

La composición del comité de seguridad TIC debe constar en la PSI y sus miembros designados de acuerdo con el procedimiento en ella establecido.

[14] La Guía de seguridad de las TIC CCN-STIC-881 Guía de Adecuación al ENS para Universidades, de mayo de 2022 es muy específica sobre los componentes del CSI para el caso de las universidades, aunque muchos criterios son de aplicación general.

[15] CCN-STIC 201.

8. Roles en materia de seguridad de la información

El ENS (artículo 13.2) establece que la PSI deberá identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

a) El **responsable de la información** determinará los requisitos de la información tratada.

b) El **responsable del servicio** determinará los requisitos de los servicios prestados.

c) El **responsable de la seguridad de la información** (RSEG) determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

d) El **responsable del sistema**, que se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo

El procedimiento de nombramiento formal de estos responsables debe constar en la política de seguridad de la información de la entidad.

Las características de los roles y sus responsabilidades en materia de ciberseguridad se detallan en la *Guía de Seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones*, además de ser una cuestión abordada por diversos documentos y guías del Centro Criptológico Nacional.

Para una correcta organización de la seguridad de la información debe tenerse en cuenta que:

- **Los roles en materia de seguridad deben estar formalmente establecidos.**
- **Los roles establecidos ejercerán sus funciones de manera efectiva.** La mera designación de roles para cumplir con la normativa no es suficiente.

  Las organizaciones deben garantizar que las personas designadas **tengan la disponibilidad de tiempo necesaria para realizar sus tareas** de manera efectiva.
- **Los roles estarán correctamente asignados, sin existir incompatibilidades con otras competencias.**

El responsable de seguridad de la información

El responsable de seguridad de la información (RSEG) puede ser un cargo unipersonal del nivel directivo de la organización o un órgano colegiado. No requiere desarrollar funciones de carácter técnico, su función es básicamente supervisora del cumplimiento efectivo de las decisiones del comité de seguridad TIC y de la normativa de seguridad. No obstante, de acuerdo con el *Código de buen gobierno de la ciberseguridad*, esta figura será una persona con el conocimiento, experiencia y competencias adecuadas para desarrollar la función y contará **con la suficiente capacidad de decisión e influencia en la organización**.

De acuerdo con el artículo 11.2 y 13.3 del Real Decreto 311/2022, la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos, no debiendo existir dependencia jerárquica entre ambos. Es decir, **ambos roles deben ser independientes.**

La *Guía de Seguridad de las TIC CCN-STIC 801 Esquema Nacional de Seguridad Responsabilidades y Funciones*, establece "*…que la figura del Responsable de la Seguridad debe estar situada en una posición que le permita tener un acceso directo a los niveles directivos de la organización.*" Y además indica que "*…En el caso de entidades locales (Diputaciones, Cabildos o Ayuntamientos), debería depender del Secretario General, ...*"[16]

[16] De acuerdo con la guía CCN-STIC 201, el responsable de seguridad debería ser el secretario del Comité de Seguridad de la Información, pero no se ha seguido este mismo criterio en la guía CCN-STIC 881.

9. Normativa interna de ciberseguridad

Política de seguridad de la información *(medida de seguridad org.1)*

La política de seguridad de la información (PSI) es un documento de alto nivel que define, de acuerdo con el artículo 12 del ENS (2022), **el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta**. Constituye la expresión formal del compromiso y liderazgo de la alta dirección con la seguridad.

Se aprobará de conformidad con lo dispuesto en el artículo 12 del ENS, y se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

[*org.1.1*] Los objetivos o misión de la organización.

[*org.1.2*] El marco legal y regulatorio en el que se desarrollarán las actividades.

[*org.1.3*] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

[*org.1.4*] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.

[*org.1.5*] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

El ENS indica los principios básicos y los requisitos mínimos de la PSI. Además, existen algunos aspectos que las organizaciones deben tener en cuenta, como son:

- Debe ser elaborada por el comité de seguridad TIC y aprobada por el presidente del ente local o el órgano superior de la entidad.
- Debe ser un documento breve, dejando detalles técnicos para las normas que la desarrollan.
- Debe ser revisada y actualizada periódicamente.
- Debe ser accesible (publicada y dada a conocer) a los empleados y colaboradores de la organización.

Un sistema de gestión continuada de la seguridad de la información requiere que la PSI se complete con *normativa interna*, desarrollada en documentos más precisos que materialicen los requisitos de la PSI (uso correcto de equipos, servicios, instalaciones, usos indebidos, responsabilidades del personal); y un conjunto de *procedimientos de seguridad* que describan, paso a paso, cómo deben realizarse tareas concretas (documentos que detallan cómo se realizan las tareas habituales, responsables, reporte de comportamientos anómalos).

Esta normativa interna **debe diseñarse para ser aplicada**, no para cumplir una mera formalidad. El contenido del conjunto de políticas, normas y procedimientos aprobados debe ser una representación fidedigna y precisa del sistema de seguridad implantado por el ente local. La aprobación de un marco normativo que no represente la realidad del ente deviene en un uso estéril de recursos por su carencia de efectividad y en una falsa percepción de cumplimiento que puede conllevar el abandono de otras medidas más adecuadas.

Cada entidad debe establecer y aprobar su propia organización de seguridad, de acuerdo con su naturaleza, estructura, dimensión y recursos disponibles, que deberá estar recogida en su Política de Seguridad de la Información[17].

Es importante tener en cuenta que, independientemente del modelo organizativo existente en una entidad, toda la normativa de ciberseguridad afectará, sin excepción, **a todos los departamentos y sistemas de información**. La organización de la seguridad sea la que sea, debe estar definida en la PSI aprobada por el órgano superior e incluirá todos los sistemas de información sin ninguna excepción.

[17] CCN-STIC-801, Esquema Nacional de Seguridad, Responsabilidades y funciones

Normativa de seguridad *(medida de seguridad org.2)*

Se dispondrá de una serie de documentos que describan:

[*org.2.1*] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.

[*org.2.2*] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Esta normativa deberá ser aprobada por quien se disponga en la PSI. Es de carácter obligatorio y deberá estar a disposición de todos los miembros de la organización (publicada en la intranet corporativa).

Es importante diferenciar entre norma y procedimiento. Una norma indica "qué debe hacerse". Los procedimientos detallan las acciones a realizar, es decir, el "cómo debe hacerse" y, cuando procede, quienes deben hacerlo.

Procedimientos de seguridad *(medida de seguridad org.3)*

Las entidades deben disponer de un conjunto de procedimientos aprobados que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

[*org.3.1*] Cómo llevar a cabo las tareas habituales.

[*org.3.2*] Quién debe hacer cada tarea.

[*org.3.3*] Cómo identificar y reportar comportamientos anómalos.

[*org.3.4*] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere.

Los procedimientos deberán ser aprobados por quien se disponga en la PSI.

10. Otros órganos relacionados con la gestión de la ciberseguridad

Las organizaciones, dependiendo de su tamaño y complejidad, pueden disponer, además del comité de seguridad TIC, de diversos órganos de gobierno relacionados con la gestión de la ciberseguridad, que pueden administrar funciones a distintos niveles, incluyendo el operativo, el ejecutivo/supervisión o el de gobierno. Algunos de estos órganos pueden ser:

- El comité de seguridad corporativa.
- El comité de gobernanza sobre las TI.
- La oficina de seguridad TIC.
- El centro de operaciones de seguridad.
- El equipo de respuesta a incidentes de seguridad.
- El comité de gestión de crisis.

La existencia de estos órganos responde, en general, a las exigencias de la normativa básica de aplicación, el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos. No obstante, puede ser de también de aplicación otra legislación sectorial y específica, como la de Ley de Protección de Infraestructuras Críticas (Ley PIC8/2011), que establecen sus propios requisitos de seguridad adicionales, incluyendo medidas organizativas.

Aunque la existencia de estos órganos puede no ser obligatoria en todas las circunstancias, dependiendo de la legislación que sea de aplicación en cada caso, sí resulta **imprescindible que**, en caso de existir, el **conjunto de estos órganos coordine adecuadamente sus actividades y existan mecanismos de comunicación y colaboración** entre los mismos.

Comité de seguridad corporativa

La seguridad de la información es una más de las áreas de seguridad de una organización. En organizaciones de tamaño significativo suele existir un Comité de Seguridad Corporativa (con su propio Secretario, al que suele denominarse Responsable de la Seguridad Corporativa). El responsable de la seguridad de la información será un miembro de este Comité, junto con otros responsables de seguridad de otras áreas o departamentos.[18]

Comité de gobernanza sobre las TI

Debería tener algún miembro común con el comité de seguridad TIC (como por ejemplo el responsable del sistema y el responsable de seguridad) de forma que sus actividades sean coherentes. Ver la guía *GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría*.

Oficina de seguridad TIC

Dentro de la estructura de gobernanza de la ciberseguridad, como elemento operativo, se podrá constituir una Oficina de seguridad TIC, cuyas competencias estarán relacionadas con las siguientes áreas de trabajo:

- Adecuación al ENS, marco normativo y análisis y gestión de riesgos.
- Seguridad en las interconexiones y conectividad.
- Vigilancia y determinación de superficie de exposición.
- Monitorización y gestión de incidentes.
- Observatorio digital y cibervigilancia.
- Otras funciones conexas o concordantes.

Para su composición se propone:

- El Director de la Oficina de seguridad TIC, nombrado por el comité de seguridad TIC, que actuará como enlace con el mismo, que será el responsable de seguridad (RSEG), o la persona en quien delegue.
- Secretario de la Oficina de Seguridad TIC, nombrado por el Comité de Seguridad TIC, a propuesta de los miembros de la Oficina de Seguridad.
- Todos aquellos administradores especialistas de seguridad (AES) que el responsable de seguridad determine que sean necesarios.

Las funciones de la Oficina de Seguridad TIC serán, entre otras que les puedan ser encomendadas por el comité de seguridad TIC[19]:

a) Gestión y operativa de la seguridad del proyecto de adecuación, implantación y gestión de la conformidad en el ENS, análisis y gestión de riesgos, explotación, normativa y mantenimiento.

b) Redacción y presentación de propuestas al comité de seguridad TIC. Elaborará los aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al comité.

c) Promover la mejora continua del SGSI.

Centros de operaciones de ciberseguridad (COCS)

De acuerdo con la guía CCN-STIC 201, la gobernanza de la seguridad en una organización se articula a través de un comité de seguridad TIC y se implementa mediante centros de operaciones de ciberseguridad que velan por la operación y correcta implementación de la seguridad mediante una vigilancia continua de los sistemas bajo su responsabilidad.

Bajo la responsabilidad y dirección del responsable de seguridad, el centro de operaciones de ciberseguridad presta sus servicios, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, especialmente los que manejan información clasificada, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

[18] Guía CCN-STIC 801.

[19] Ver un mayor detalle en CCN STIC-881.

En definitiva, los centros de operaciones de ciberseguridad articularán la respuesta a los incidentes de seguridad, sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración con competencias y de la función de coordinación de los CSIRT de referencia y del CCN-CERT, como coordinador nacional.

Asimismo, en función de la naturaleza y dimensiones de la organización, el COCS puede ser interno o estar externalizado, en cuyo caso actuará remotamente a través de canales establecidos en coordinación con el responsable de seguridad.

El COCS puede llevar a cabo las siguientes funciones:

- Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.
- Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.
- Operaciones de seguridad sobre los dispositivos de defensa.
- Podrá constituir un Equipo de Respuesta a Incidentes de Seguridad.
- Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.
- Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación/parcheado) de aplicaciones y servicios.
- Análisis forense digital y de seguridad.
- Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

El equipo de respuesta a incidentes de seguridad

Este equipo se encarga de gestionar los incidentes de seguridad bajo las directrices marcadas por el comité de seguridad TIC y funcionales del RSEG y posibles alertas recibidas del COCS.

Está compuesto por un equipo con capacidades de atención inmediata denominado primer nivel de atención y por un grupo de especialistas para aquellos incidentes no resueltos por el primer nivel que requieran un mayor grado de especialización.

Comité de gestión de crisis

Un ciberincidente grave provocará una crisis y esto implica la necesidad de tomar decisiones bajo mucha presión, en poco tiempo y con información probablemente incompleta.

Con independencia del tipo de ciberincidente que cause la crisis, se hace patente la componente de gestión que implica su resolución. Para ello, la organización afectada necesita haberse dotado de las capacidades y estructuras de gestión (comités/equipos) adecuadas que le han de permitir abordarla con garantías de éxito.

En resumen, la capacidad de gestionar una situación de crisis depende en gran medida de las estructuras o comités que se hayan establecido antes de que ocurra el desastre causado por un ciberincidente que sea un suceso de baja probabilidad y alto impacto.

El comité de crisis es el órgano encargado de la gestión de la crisis a alto nivel dentro de la organización, con una visión estratégica. Se encargará de tomar las decisiones y coordinar las acciones necesarias para la resolución de los incidentes que hayan sido calificados como crisis dentro de la entidad, determinando y/o validando las estrategias de análisis, de contención y mitigación que permitan recuperar las operaciones en el menor tiempo posible, minimizando los impactos sobre las partes interesadas.

11. Posibles deficiencias en materia de gobernanza

Entre otras se pueden citar las siguientes[20]:

En materia de normativa de seguridad

- Inexistencia de PSI formalmente aprobada por la corporación, o desactualizadas o no adaptadas a la realidad de las entidades, lo que impide que los principios que deben regir las actuaciones en materia de seguridad sean conocidos por toda la corporación.
- Inexistencia de normativa y procedimientos formalizados, lo que puede originar el riesgo de no realización de tareas importantes por no estar asignadas a responsables, dependiendo su ejecución de la buena voluntad de quienes los llevan a cabo.
- El contenido de los procedimientos no detalla de manera clara y precisa las tareas a realizar ni quiénes son los responsables de ejecutarlas, especificando únicamente el deber de realizar la acción, aspecto que corresponde a las normas de seguridad de rango superior, lo que genera procedimientos ineficaces.
- Existencia de procedimientos escritos que, aunque están definidos de manera correcta, han sido realizados por consultoras externas y tienen poca o nula adaptación al entorno de la entidad, dado que no reflejaban la realidad de las acciones llevadas a cabo en la práctica.
- Los procedimientos existentes, incluidos aquellos formalmente aprobados, no se encuentran actualizados y no representan con fidelidad los procesos de seguridad que describen.

En relación con el comité de seguridad TIC

- Existen entidades que no disponen de comité de seguridad de la información, órgano imprescindible para coordinar la seguridad de la información en la entidad.
- En otros casos, aunque el comité de seguridad de la información está formalmente constituido, no se reúne o no lo hace la periodicidad necesaria, lo que impide hacer un seguimiento del estado de la seguridad de la información del Ayuntamiento y tomar las decisiones pertinentes de forma oportuna.
- El comité de seguridad no dispone de los miembros adecuados, estando compuesto únicamente de miembros con cargos relacionados con los sistemas de información y la seguridad. La ausencia de miembros con el más alto poder de decisión en la organización y de vocales de las áreas significativas, convierte al comité en un órgano meramente técnico e impide un gobierno eficiente y la toma de decisiones estratégicas a nivel corporativo.

En relación con los roles de seguridad

- Existen entidades que no han asignado los roles y responsabilidades en materia de seguridad de la información.
- Existen entidades que no disponen de un delegado de protección de datos formalmente nombrado.
- Algunos de los roles se seguridad no ejercen sus funciones de manera que se garantice la necesaria independencia y la ausencia de conflicto de intereses.
- Algunos roles en materia de seguridad no disponen de la dedicación suficiente para las necesidades de la entidad. Los responsables de seguridad de manera general no ejercen sus funciones de manera exclusiva, incurriendo en una acumulación de competencias no directamente relacionadas con la seguridad de la información que impide que desarrollen sus funciones de forma efectiva.

En relación con el liderazgo y el compromiso con la ciberseguridad

- La falta de una cultura de ciberseguridad en la entidad, materializada en acciones formativas y campañas de concienciación dirigidas a los empleados.
- Inexistencia de implicación de los máximos responsables de la organización.

[20] Se ha tomado como referencia los más de 40 informes sobre ciberseguridad publicados por la Sindicatura de Cuentas de la Comunidad Valenciana en los que se señalan numerosas deficiencias en materia de gobernanza de la ciberseguridad.

- La carencia de planes estratégicos desarrollados e impulsados por el más alto nivel de la corporación en los que se establezcan acciones, objetivos y medidas concretas para alcanzar los niveles de seguridad exigidos por la normativa.
- Falta de comunicación o inadecuada comunicación de los procedimientos de seguridad y decisiones en materia de seguridad de la información al personal de la organización.
- La falta de recursos, tanto económicos como de personal, en los departamentos TIC, indispensable para implantar las medidas de seguridad necesarias y llevar a cabo proyectos transversales que afecten a toda la organización.

12. Cómo puede el auditor evaluar si existe una adecuada gobernanza de la ciberseguridad

Se podrá utilizar el programa de auditoría/cuestionario del Anexo, que tiene la siguiente estructura, y que deberá ser adaptada en cada caso:

1. *Políticas, normas y procedimientos sobre seguridad de la información (apartado 9 de la guía)*
2. *Comité de seguridad TIC, roles y responsabilidades*
3. *Compromiso de la dirección y de la alta dirección*
4. *Gestión de riesgos*
5. *Cumplimiento legal: ENS y protección de los datos personales*
6. *Recursos del departamento TIC y de seguridad*

13. Bibliografía

ASOCEX

- GPF-OCEX 1315 Identificación y valoración del riesgo de incorrección material (Revisada).
- GPF-OCEX 1316 Guía de implementación por primera vez de la GPF-OCEX 1315 Identificación y valoración del riesgo de incorrección material (Revisada).
- GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa.
- GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad.
- GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica.
- GPF-OCEX 5331 Gobernanza corporativa, gobernanza sobre las TI y su auditoría

CENTRO CRIPTOLÓGICO NACIONAL (CCN)

- Guía de seguridad de las TIC CCN-STIC-801, Esquema Nacional de Seguridad, Responsabilidades y funciones, CCN, 2019.
- Guía de seguridad de las TIC CCN-STIC 201. Organización y gestión para la seguridad de las TIC, CCN, 2021.
- Guía de seguridad de las TIC CCN-STIC-881 Guía de Adecuación al ENS para Universidades, CCN 2022.
- Aproximación al marco de gobernanza de la ciberseguridad, CCN, 2022.

OTROS

- Código de buen gobierno de la ciberseguridad, Foro Nacional de Ciberseguridad, junio de 2023.
- Sindicatura de Cuentas de la Comunidad Valenciana, Informe de síntesis de las auditorías de ciberseguridad de los quince mayores ayuntamientos y de las tres diputaciones de la Comunitat Valenciana, publicado en mayo de 2023.
- Guía de iniciación a actividad profesional implantación de sistemas de gestión de la seguridad de la información (SGSI) según la norma ISO 27001, Colegio Oficial de Ingenieros de Telecomunicación, 2012.
- Cybersecurity Program Audit Guide, US Government Accountability Office, septiembre de 2023.

INSTRUCCIONES:

El presente programa/cuestionario tiene por finalidad realizar una evaluación sobre el **nivel de la gobernanza de la seguridad de la información** en la entidad.

Las contestaciones al cuestionario se referirán a la situación a fecha _____ del año _____ y podrán ser comentadas y verificadas por el equipo de auditoría en el curso del trabajo.

El cuestionario incluye preguntas relativas a diversos temas y se encuentran fundamentadas en normativa de obligado cumplimiento y metodologías de gestión de seguridad de la información de reconocido prestigio, particularmente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad.**
- Guía de Seguridad de las TIC **CCN-STIC 801**. Esquema Nacional de Seguridad Responsabilidades y Funciones.

La metodología y criterios de auditoría utilizados se encuentran recogidos en la GPF-OCEX 5314.

La remisión del cuestionario cumplimentado, así como de la documentación que en caso necesario deba ser adjuntada al mismo, se realizará **únicamente por medios seguros**, dada la sensibilidad de la información tratada. Se remitirá …. ***(especificar método)***

Para cualquier duda, no dude en ponerse en contacto con los miembros del equipo de fiscalización (Correo electrónico: _____).

Le rogamos nos facilite el cuestionario cumplimentado en el plazo de _____ días.

CUMPLIMENTADO POR:

Nombre:

Cargo:

Fecha:

1. Políticas, normas y procedimientos sobre seguridad de la información

Respecto a las Política de Seguridad de la Información-PSI (Org.1)

Objetivo de auditoría: comprobar si la entidad tiene políticas sobre la seguridad de los sistemas de información (PSI) adecuadas, están aprobadas y actualizadas. Si la PSI está estructurada de forma que incluya, con claridad, al menos el contenido que señala el ENS.

Cuestionario:

1.1 ¿Dispone la entidad de una PSI aprobada?

Aportar documento formal conteniendo la PSI y documentación acreditativa de su aprobación.

En caso negativo, indicar se la entidad se ha adherido a la PSI de la que depende o está vinculada.

Aportar evidencia de su publicación, y de su difusión interna.

Indicar fecha de aprobación de la primera versión de la PSI

Indicar fecha de aprobación de la versión vigente de la PSI

Comprobaciones:

- Revisar las PSI para verificar si están aprobadas por el órgano superior correspondiente y publicadas, si están actualizadas, si tienen el contenido requerido por el ENS y si reflejan las necesidades de la entidad.
- Revisar el historial de control de cambios de las PSI para determinar que se actualizan periódicamente alineándolos con los objetivos de la entidad y los requisitos normativos.
- Si se define la estructura del comité de seguridad TIC, junto a otros comités técnicos o grupos de trabajo que puedan llegar a definirse (OTS, COCS…), detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
- Si se determinan en la PSI los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación: al menos, responsable de la información, responsable del servicio, responsable de seguridad y responsable del sistema.
- Se determinan los diferentes niveles de normativa de desarrollo de las PSI y los órganos competentes para aprobar las normas a cada nivel.

Respecto a la normativa de seguridad (Org.2)

Objetivo de auditoría: comprobar si la entidad dispone de normativa interna donde se determine el uso correcto de equipos, servicios e instalaciones, así como lo que se considera uso indebido.

Cuestionario:

1.2 ¿Dispone la organización de normas y procedimientos de seguridad TIC debidamente aprobados que se adapten a la realidad y necesidades de la entidad?

- Aportar una relación de las normas aprobadas, indicando nombre, fecha de aprobación y órgano que la aprobó.
- Evidencia de su aceptación por empleados y colaboradores.

Comprobaciones:

- Revisar si las normas y procedimientos existen, están debidamente aprobadas, si se han comunicado adecuadamente a las partes interesadas y son accesibles.
- Revisar si las normas y procedimientos están adaptadas a las necesidades de la entidad o son puramente teóricas.
- Revisar el historial de control de cambios de normas y procedimientos para determinar que se actualizan periódicamente alineándolos con los objetivos de la entidad y los requisitos normativos.

Respecto a los procedimientos de seguridad (Org.3)

Objetivo de auditoría: comprobar si la entidad dispone de un conjunto de procedimientos documentados que determinan cómo realizar las tareas habituales y quiénes son sus responsables.

Cuestionario:

1.3 ¿Dispone la organización de normas y procedimientos de seguridad TIC debidamente aprobados que se adapten a la realidad y necesidades de la entidad?

- Aportar una relación de los procedimientos aprobados, indicando nombre, fecha de aprobación y órgano que la aprobó.

Comprobaciones:

- Revisar si las normas y procedimientos existen, están debidamente aprobadas, si se han comunicado adecuadamente a las partes interesadas y son accesibles.
- Revisar si las normas y procedimientos están adaptadas a las necesidades de la entidad o son puramente teóricas.
- Revisar el historial de control de cambios de normas y procedimientos para determinar que se actualizan periódicamente alineándolos con los objetivos de la entidad y los requisitos normativos.

2. Comité de seguridad TIC, roles y responsabilidades

Objetivo de auditoría: Evaluar si las estructuras de gobierno de la ciberseguridad (comité de seguridad de las TIC y los distintos roles exigidos por la normativa) y sus responsabilidades están claramente definidas, si la entidad ha realizado los nombramientos en materia de seguridad de la información de acuerdo con lo previsto en las PSI y si las personas designadas disponen del tiempo necesario para llevar a cabo sus tareas de manera efectiva.

Cuestionario:

2.1 ¿Se ha constituido formalmente el Comité de Seguridad TIC?

- Aportar documentación acreditativa de la constitución.
- Aportar documento/s de nombramiento / asignación de roles y responsabilidades.

2.2 ¿Tiene el Comité de Seguridad TIC una actividad continuada y efectiva?

- Periodicidad de las reuniones: _____
- Aportar las actas de las reuniones celebradas en el año fiscalizado y el anterior.

2.3 ¿Existen otros órganos destinados a la gestión de la seguridad de la información?:

Oficina de seguridad TIC	SI/NO
Órgano de Auditoría Técnica (OAT)	SI/NO
Centro de Operaciones de ciberseguridad (COCS)	SI/NO

- Aportar documentación acreditativa de la constitución y funcionamiento de dichos órganos.

2.4 ¿Se han nombrado los roles en materia de seguridad de la información?

Responsable de la información	SI/NO
Responsable del servicio	SI/NO
Responsable de la seguridad de la información (RSEG)	SI/NO
Responsable del sistema	SI/NO

- Aportar documentación acreditativa de los nombramientos.

2.5 ¿Dispone el RSEG de dedicación suficiente a la gestión de la seguridad de la organización como para desempeñar sus funciones de manera adecuada?

¿Es conocida su responsabilidad por el resto de la organización?

Comprobaciones:

- Revisar las PSI para determinar si las funciones y responsabilidades del CIS y los distintos roles de la seguridad de la información han sido claramente definidas y comunicadas.
- Determinar si el CSI está integrado por los roles requeridos por el ENS y cumple con buenas prácticas.
- Revisar las actas de las reuniones para ver si el CSI está desempeñando de forma efectiva sus funciones (verificar la periodicidad de sus reuniones) y las responsabilidades definidas.
- Revisar si la corporación ha designado los roles y responsabilidades en materia de seguridad correctamente.
- Revisar si las personas con roles asignados ejercen de manera efectiva y disponen del tiempo necesario para realizar las tareas atribuidas.
- ¿Se dispone de un acta del Comité de Seguridad TIC donde se designen sus miembros, o las altas y bajas que se puedan llegar a producir?

3. Compromiso de la dirección y de la alta dirección

Objetivo de auditoría: evaluar las acciones relacionadas con la implicación de los miembros de la dirección y la alta dirección. Los miembros de la dirección y la alta dirección deben participar de forma activa en el establecimiento de políticas y objetivos estratégicos de la entidad, la gestión de riesgos y en la aplicación de medidas para mitigarlos. Debe existir un liderazgo reconocible.

Cuestionario:

3.1 ¿Dispone la entidad de un Plan Estratégico TIC o documento equivalente que abarque el periodo auditado?

- Aportar plan estratégico o documento equivalente.

3.2 ¿Los responsables de la gobernanza del Plan Estratégico TIC mantienen reuniones periódicas de revisión/seguimiento de cumplimiento del plan anterior?

- Aportar actas de las reuniones de revisión/seguimiento del plan anterior, indicadores de cumplimiento de los objetivos.

3.3 ¿Dispone la entidad de un Plan Estratégico de Seguridad o documento equivalente que abarque el periodo auditado?

- Aportar plan estratégico o documento equivalente.

3.4 ¿Los responsables de la gobernanza del Plan Estratégico de Seguridad mantienen reuniones periódicas de revisión/seguimiento de cumplimiento de dicho plan?

- Aportar actas de las reuniones de revisión/seguimiento del plan anterior, indicadores de cumplimiento de los objetivos.

3.5 ¿El Comité de seguridad TIC incluye miembros de la dirección/alta dirección?

- ¿Participan de manera activa en sus reuniones?

3.6 ¿Realiza la alta dirección de la entidad acciones que promuevan la concienciación sobre la ciberseguridad y la difusión de la política de seguridad?

- Describir brevemente las actividades o formaciones llevadas a cabo en el último año.

3.7 ¿Existe un plan de formación y concienciación en materia de ciberseguridad?

- Describir brevemente las actividades o formaciones llevadas a cabo en el último año.
- Aportar plan de formación/concienciación y acreditación de su ejecución.

3.8 ¿Facilita la alta dirección los recursos necesarios para el buen funcionamiento del sistema de gestión de la seguridad de la información (SGSI) y según las necesidades identificadas?

- Proporcione una relación de informes de necesidad, o documento equivalente, remitidos a la dirección o la alta dirección e indique cuáles de los mismos han sido atendidos adecuadamente por la organización.

Procedimientos de auditoría:

- Analizar la información recibida y evaluar las acciones relacionadas con la implicación de los miembros de la dirección y la alta dirección y su participación activa en el establecimiento en la definición e implementación de políticas y objetivos estratégicos de la entidad, la gestión de riesgos y en la aplicación de medidas para mitigarlos.
- Identificar si existe un liderazgo reconocible.

4. Gestión de riesgos

Objetivo de auditoría: evaluar si la entidad ha realizado y documentado un análisis sobre los riesgos que afectan a sus sistemas de información y los ha clasificado por niveles de seguridad (alto, medio o bajo) de acuerdo con los requisitos del ENS (art. 40 y 41).

Cuestionario:

4.1 ¿Existe un sistema para la gestión de riesgos TI/ciberseguridad

- Aportar documentación sobre el análisis de riesgos realizado

4.2 ¿Participa activamente la dirección/alta dirección en la gestión de riesgos, la definición de los criterios de aceptación del riesgo, de los niveles aceptables de riesgo y en la articulación de medidas para mitigarlos?

- ¿Cómo se materializa esa participación?

Procedimientos de auditoría:

- Revisar la documentación del análisis de riesgos. Verificar que incluye los sistemas de información críticos de la entidad y que está actualizado.

5. Cumplimiento legal

Esquema Nacional de Seguridad

Objetivo de auditoría: evaluar si existe un adecuado nivel de cumplimiento legal respecto al Esquema Nacional de Seguridad.

Cuestionario:

5.1 Además de las cuestiones incluidas en los apartados anteriores, informar y aportar la documentación justificativa sobre:

- Si la Entidad ha formalizado un documento con la **declaración de aplicabilidad**, que recoge las medidas de seguridad que son de aplicación en función del nivel y categoría del sistema, que además ha sido firmada por el responsable de seguridad.

  Aportar la declaración de aplicabilidad.

- Si la entidad ha realizado la **auditoría de cumplimiento del ENS** para los sistemas de categoría Media y Alta o autoevaluación para nivel básico.

  En caso afirmativo, indicar la empresa que ha realizado la auditoría y aportar el informe de auditoría y/o autoevaluación.

  Indicar si se ha realizado en el periodo revisado algún otro tipo de auditoría de seguridad.

- Los resultados de la auditoría y/o de la autoevaluación han sido revisados por el responsable de seguridad y las conclusiones presentadas al responsable del sistema para que adopte las medidas correctoras adecuadas.
- Si la entidad no ha realizado informe de auditoría ENS (niveles medio y alto) ni autoevaluación (nivel básico) verificar si se ha realizado un Plan de adecuación al ENS.
- La entidad facilita los datos necesarios para el **Informe del Estado de la Seguridad** a través de la herramienta INES, cumpliendo así la Instrucción Técnica de Seguridad aprobada por resolución de 7 de octubre de 2016.

  Aportar el Informe INES
- La entidad ha publicado en su sede electrónica las **declaraciones de conformidad** y los distintivos de seguridad correspondientes, según los resultados de la autoevaluación o auditoría.

Procedimientos de auditoría:

- Revisar la declaración de aplicabilidad y verificar que las medidas de seguridad se corresponden con los niveles de seguridad de los sistemas de información aprobados.
- Verificar que se ha elaborado y comunicado en informe sobre seguridad de la información para el ejercicio auditado (informe INES. Art. 32 ENS: Instrucción técnica de seguridad, Resolución de 7 de octubre de 2016 de la Secretaría de estado de las Administraciones Públicas).
- Verificar que se han realizado los informes de auditoría de seguridad requeridos por el ENS (Art. 31).

Protección de datos de carácter personal

Objetivo de auditoría: Evaluar si se da cumplimiento a los requisitos mínimos del RGPD y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales.

Cuestionario:

5.2 ¿Existe un adecuado nivel de cumplimiento respecto al cumplimiento legal en materia de **protección de datos de carácter personal**?

- La entidad ha designado un Delegado de Protección de Datos (DPD) y su nombramiento ha sido comunicado a la AEPD.

  Aportar documento acreditativo del nombramiento y de la notificación a la AEPD.
- La entidad dispone del registro de actividades de tratamiento (RAT) con la información requerida por el RGPD

  Aportar RAT.
- La entidad ha realizado análisis de riesgo de los tratamientos de datos personales y evaluaciones de impacto para aquellos de riesgo alto.

  Aportar registro de los análisis de riesgo realizados en materia de protección de datos y evaluaciones de impacto.
- La entidad evalúa periódicamente la eficacia de las medidas técnicas y organizativas implantadas

  Aportar informes de auditoría para dar cumplimiento al requisito anterior.

Procedimientos de auditoría

- Verificar si se ha nombrado un delegado de protección de datos y se ha comunicado a la AEPD (art. 37 RGPD).
- Verificar si se ha elaborado y publicado en la web de la entidad el RAT (Art. 30 RGPD y 31 LOPDGDD)
- Verificar si se han realizado análisis de riesgos y evaluaciones de impacto sobre los datos personales tratados por la entidad (Art. 32 y 35 RGPD)
- Verificar que se han realizado auditorías sobre la protección de los datos personales en base al principio de responsabilidad proactiva del RGPD (art 32 RGPD)

6. Recursos del departamento TIC y de seguridad

Objetivo de auditoría: comprobar si la organización asigna al departamento TIC y a la seguridad los recursos humanos y materiales necesarios para llevar a cabo tareas de seguridad, y si estos son adecuados al tamaño de la entidad.

Cuestionario:

6.1 ¿Dispone la entidad de los recursos humanos necesarios para cumplir adecuadamente con obligaciones con respecto a la seguridad de la información?

Informar sobre:

	Año anterior	**Año fiscalizado**
Número total de funcionarios/empleados al cierre del ejercicio.		
Número de funcionarios/empleados tiempo completo (o equivalente) pertenecientes en al departamento de TIC al cierre del ejercicio.		
Número de funcionarios/empleados tiempo completo (o equivalente) dedicadas a la seguridad TIC. Señalar si están incluidas o no en los datos anteriores.		
Número de personas contratadas a proveedores a tiempo completo que prestan servicio o asistencia al departamento TIC, NO dedicadas a la seguridad TIC.		
Número de personas contratadas a proveedores a tiempo completo que prestan servicio o asistencia al departamento TI dedicadas a la seguridad TIC.		

6.2 ¿Realiza la entidad las inversiones necesarias en proyectos o servicios para cumplir adecuadamente con obligaciones con respecto a la seguridad de la información?

Informar sobre:

(Con datos en miles de euros)	**Año N**	**Año N+1**
Obligaciones reconocidas netas (ORN) totales de la entidad		
ORN capítulo 1 del departamento TIC		
ORN capítulo 2 del departamento TIC		
ORN capítulo 6 del departamento TIC		
ORN capítulo 1 del departamento TIC -SOLO SEGURIDAD		
ORN capítulo 2 del departamento TIC -SOLO SEGURIDAD		
ORN capítulo 6 del departamento TIC -SOLO SEGURIDAD		

Procedimientos de auditoría

- Analizar el número de personal a tiempo completo (o equivalente) pertenecientes en al departamento/área/negociado de gestión de las TIC de la entidad, identificando cuántas de ellas se dedican a la SSI.

- Se revisará la dotación presupuestaria de los Capítulos 1, 2 y 6 del departamento TIC y a la SSI.
- Se revisará el total de ORN de los Capítulos 1, 2 y 6 del presupuesto.

7. Otros aspectos

Incluya a continuación información sobre otros proyectos o medidas implantadas o carencias identificadas que considere que deben ser contempladas para la evaluación de la gobernanza de la ciberseguridad.

GESTION DEL AVAL ELECTRONICO

José Manuel Farfán Pérez
Tesorero General
Diputación de Sevilla y OPAEF

INDICE

1. Introducción.

Tal como establece el Banco de España, los avales, fianzas y garantías son tres términos que reflejan una misma realidad: el negocio jurídico de garantía.

La garantía es cualquier medio jurídico que asegura el cumplimiento de una obligación por parte del deudor, evitando el perjuicio que su incumplimiento ocasione al acreedor, reforzando la posición y seguridad de este último.

En sentido estricto la garantía es un nuevo derecho, distinto al principal o garantizado, que se identifica y agota en la finalidad de garantizar el contenido del contrato principal garantizado, siendo esencial al mismo la idea de accesoriedad.

En este sentido, la «garantía» representa la denominación más amplia y genérica, por ello el «aval» es la garantía cambiaría por antonomasia, al tiempo que ha servido igualmente para denominar las garantías prestadas a favor de la Administración Pública, o las creadas por leyes especiales. Por su parte, la «fianza» constituye la denominación legal clásica de la garantía en el ordenamiento jurídico privado, civil y mercantil.

El aval (como modalidad más común de garantía), surgió en el ámbito cambiario, y ha pasado a concretarse en pólizas mercantiles y de ahí se ha extendido a las garantías emitidas por entidades de crédito. Surgió en el derecho mercantil como garantía accesoria a la letra de cambio y se viene aplicando en la fijación de las garantías emitidas ante las administraciones públicas y en las creadas por leyes especiales. El aval viene recogido en la Ley 19/1985 Cambiaria y del Cheque, como regulación básica

El aval electrónico y sus peculiaridades es el objeto de este artículo. Pero más concretamente nos ceñiremos al proceso de gestión de este, entendiendo por tal: la constitución, custodia, cancelación/devolución y ejecución en su caso.

2. Acreditación y usos del aval.

No toda Entidad Financiera puede emitir un aval, la acreditación de la constitución de la garantía será por: entidad bancaria, caja de ahorros, cooperativa de crédito, establecimiento financiero de crédito o sociedad de garantía recíproca autorizada para operar en el Reino de España, para lo cual se debe comprobar que se halle incluido en el registro del Banco de España y además ese aval debe ser inscrito en el registro especial de avales, este último es un registro propio de cada entidad financiera. Para simplificar los acreditados le denominaremos Entidad Financiera.

Una vez obtenida la autorización y tras su constitución e inscripción en el Registro Mercantil, los establecimientos financieros de crédito deberán, antes de iniciar sus actividades, quedar inscritos en el Registro especial de establecimientos financieros de crédito que se creará en el Banco de

España. Las inscripciones en este Registro especial Registro Especial de Establecimientos Financieros de Crédito es obligatoria, así como las bajas de este y se publicarán en el «Boletín Oficial del Estado».

De este Registro Especial de Avales de cada entidad de crédito, su obligatoriedad viene impuesta por la Circular del Banco de España 4/2017 de 27 de noviembre. Si necesitamos copias debemos pedírselas a cada entidad, a sus servicios centrales, pues tienen obligación de conservarlas. Actualmente la mayoría de estas permiten el acceso en tiempo real a estos avales, así como al histórico por terceros.

Para verificar la autorización a operar del Banco de España y su inclusión en el Registro podemos acceder al Banco de España, a la Consulta del registro oficial de entidades que de forma online permite consultar diversos datos (denominación, domicilio, fecha de alta y baja, código, etc.) de las entidades registradas en el Banco de España: bancos, cajas de ahorros, cooperativas de crédito, sucursales en España de entidades de crédito extranjeras, oficinas de representación en España de entidades de crédito extranjeras, entidades de crédito extranjeras que prestan servicios en España sin establecimiento y filiales de éstas que prestan servicios en España sin establecimiento.

El registro de Entidades normativamente se regula en el RD 309/2020, de 11 de febrero, sobre el régimen jurídico de los establecimientos de financieros de crédito y por el que se modifica el Reglamento financieros de crédito y por el que se modifica el Reglamento del Registro Mercantil, aprobado por el RD 1784/1996, de 19 de junio, y el RD 84/2015, de 13 de febrero, por el que se desarrolla la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito, así como por el requisito de “autorizados para operar en España”, previsto en el artículo 108 de la LCSP para la constitución de avales por alguno de los bancos, cajas de ahorros, cooperativas de crédito, establecimientos financieros de crédito y sociedades de garantía recíproca, todo ello observamos como está establecido por una norma con rango de ley de aplicación a todas las Administraciones Públicas y dicho requisito debe ser comprobado en todos los casos de recepción de avales.

Por tanto, con independencia de que requiera autorización por parte del Banco de España o del ministro de Asuntos Económicos y Transformación Digital (Economía y Competitividad), se entiende que su inscripción en el Registro Especial de Establecimientos Financieros de Crédito es obligatoria.

Respectos a los usos del aval en términos generales estas garantías se establecen en las Entidades Locales el marco de:

a) El Derecho Urbanístico.
b) La contratación pública.

c) La aplicación de los tributos, fundamentalmente en los aplazamientos y fraccionamientos, así como en materia de revisión de actos.
d) En aplicación de la Ley 38/2003, de 17 de noviembre, General de Subvenciones

Quizás la más conocida sea la garantía en forma de aval referida en el artículo 108 de la Ley 9/ 2017, de contratos del Sector público.

Por todo ello en este artículo vamos a circunscribirnos al aval como modalidad principal de garantía, además de su peculiaridad electrónica.

En el Estado su normativa básica es el RD 937/2020 de 27 de octubre (Reglamento Caja General de Depósitos).
El órgano que gestiona y custodia el aval constituido a disposición de la Administración es el Tesorero Público, a través del Servicio Electrónico de la Caja General de Depósitos, denominado SECAD. El Tesoro tiene establecido un sistema por el cual las garantías mediante aval o seguro de caución solo se pueden presentar de manera telemática a través de esta plataforma.

3. Requisitos del aval electrónico.

El aval debe incluir la cláusula de pagadero al primer requerimiento, este "**primer requerimiento** "otorga al beneficiario una mayor seguridad en el cumplimiento de la obligación garantizada, pues obliga al avalista al pago de la deuda de forma incondicional, autónoma, inmediata e irrevocable, porque ya comentábamos que el aval: es un contrato de naturaleza "accesoria" del contrato principal, que se realiza en función de otro contrato, del que trae causa.
En particular conviene detenerse en el análisis de la figura del **aval a primer requerimiento**, y como la jurisprudencia del Tribunal Supremo se ha encargado de perfilar su naturaleza jurídica.
Consiste en un pacto o acuerdo por el que la entidad **garante**, garantiza el cumplimiento de una obligación del **deudor** frente a un **acreedor** que, de pasar a ser beneficiario del aval, podrá exigir el pago por la falta de cumplimiento de la obligación garantizada.
Otro requisitito esencial es la renuncia expresa al beneficio de división y excusión.
Por lo general el fiador, avalista, o garante, no puede ser compelido a pagar al acreedor sin hacerse antes la excusión de todos los bienes del deudor (ex art. 1830 CC), lo que se denomina **beneficio de excusión**, salvo que medie renuncia expresa o se haya obligado solidariamente con el deudor (art.1.831 CC). El beneficio de excusión consiste en el derecho del fiador a permanecer liberado de la obligación de pago mientras el deudor tenga bienes suficientes para cubrir el importe de la deuda.
Y dice el artículo 1.837 que "siendo varios los fiadores de un mismo deudor y por una misma deuda, la obligación de responder se divide entre todos…".; lo que se denomina también como **beneficio de división**, que cesará por los mismos casos y las mismas causas que el de excusión contra el deudor principal.

Con la renuncia expresa al beneficio de excusión y división el fiador pierde los beneficios que le son inherentes como tal fiador,

Y nada podrá ser reclamado al fiador, sin antes haberse reclamado al deudor principal: beneficio de orden, salvo renuncia expresa o que la fianza lo sea de forma **solidaria**, que no es otra cosa sino una fianza sin que existan beneficios de ningún tipo, pues se podrá demandar a deudor y fiador a la vez, lo que potencia las acciones del beneficiario contra el garante.

El resumen: el aval debe ser solidario respecto al obligado principal, con renuncia expresa a los beneficios de excusión y división, y pagadero a primer requerimiento de la Caja.

El aval será de duración indefinida, permaneciendo vigente hasta que la autoridad a cuya disposición se constituya resuelva expresamente declarar la extinción de la obligación garantizada y ordenar la cancelación del aval.

4.Reglamento Caja General de Depósitos y aval electrónico.

El jueves 26 de noviembre de 2020 en el número 310 el BOE se publicó el Real Decreto 937/2020, de 27 de octubre, por el que se aprueba el Reglamento de la Caja General de Depósitos, que entró en vigor el día 2 de enero de 2021. Por todo ello entendemos que esta normativa de la Caja General de Depósitos es supletoria par las Haciendas Locales, y por tanto debemos asimilar la caja Local con la Caja Estatal.

Servirá por tanto para que, en materia de depósitos, y en los aspectos concernientes a las modalidades, los requisitos y la gestión de las garantías de que se constituyan ante la Entidad Local, sirva como marco de referencia. De la misma forma puede orientar la elaboración de bases de ejecución, pliegos y reglamentos en esta materia.

Hay que tener en cuenta, a este respecto, lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que impone la obligación de adaptar los procedimientos de las administraciones públicas a las nuevas previsiones en materia de implantación de medios electrónicos. Así, en su artículo 14 prevé la obligación por parte de las personas jurídicas de relacionarse a través de medios electrónicos con las Administraciones Públicas, permitiendo a las personas físicas elegir en todo momento si se comunican con ellas a través de medios electrónicos, salvo que estén obligadas a ello.

Las actuaciones ante la Caja que deban realizarse por medios electrónicos se tramitarán necesariamente a través de los canales de acceso, sistemas y aplicaciones que se establezcan a estos efectos por la Secretaría General del Tesoro y Financiación Internacional. Estaremos pendientes por tanto a dicha regulación, muy importante para adaptar la gestión de garantías a Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En este sentido **el artículo 6 del Reglamento de la Caja General de Depósitos** (Real Decreto 937/2020, de 27 de octubre) referente a las actuaciones ante la caja, diferencia dicha realidad, expresando que:

1. Las actuaciones ante la Caja de los sujetos a que se refiere el artículo 14.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se realizarán a través de medios electrónicos.

2. Las personas físicas podrán realizar sus actuaciones ante la Caja de manera presencial o a través de medios electrónicos.

3. Los órganos, organismos y entidades que integran el sector público deberán realizar todas sus actuaciones ante la Caja por medios electrónicos.

4. Las actuaciones ante la Caja que deban realizarse por medios electrónicos se tramitarán necesariamente a través de los canales de acceso, sistemas y aplicaciones que se establezcan a estos efectos por la Secretaría General del Tesoro y Financiación Internacional.

El **artículo 10 del Reglamento de la Caja**, expresa que:

"***1. Las garantías y depósitos se presentarán en formato electrónico, sin perjuicio de aquellas personas que puedan presentar garantías o depósitos en formato papel de acuerdo con lo previsto en el artículo 6***.

2. *Los interesados presentarán los documentos ante la Caja de acuerdo con los modelos previstos mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital cuando lo presenten en formato papel. En caso contrario, la presentación se realizará de acuerdo con los formatos previstos en los canales de acceso, sistemas y aplicaciones electrónicos que se hayan estab*lecido al efecto en la sede electrónica correspondiente".

En definitiva, la gestión de estos avales se realizará por medios electrónicos en la mayoría de los casos dado que las Entidades Financieras emiten el formato electrónico con carácter general, y sin perjuicio que alguna Entidad financiera o persona física pueda presentar el aval en formato físico.

5**. Formato del aval electrónico.**

El aval electrónico también se le denomina aval digital, y por tanto se emite y gestiona a través de medios electrónicos, sin necesidad de documentación física. Al ser medio electrónico y estar en poder del avalado puede establecer dudas la custodia, ejecución y cancelación de dicho aval.

Este aval electrónico tiene muchas ventajas, y una principal es que agiliza la gestión y permite un tratamiento informatizado de la información, disminuye el riego de suplantación o fraude y resuelve el problema de la perdidas documentales, máxime cuando en todo momento se puede acudir de forma acreditada a la Entidad Financiera para la información del aval, facilitando la gestión y el seguimiento de las garantías tanto para el avalado como para el beneficiario.

Además, el aval electrónico tiene la misma validez legal que un aval tradicional en papel, se emite a través de plataformas digitales seguras, utilizando firmas electrónicas y certificados digitales, y la información del aval se almacena de forma digital, lo que permite un acceso rápido y sencillo, con mayor seguridad y control de la información.

En resumen, el aval electrónico es una alternativa moderna y eficiente al aval tradicional en papel, que ofrece numerosas ventajas tanto para empresas como para particulares.

Existen diversos formatos de aval electrónico, cada uno con sus propias características y usos específicos. Los principales formatos son:

1. **XML (Extensible Markup Language**).

a) Este formato permite un tratamiento automatizado de los datos del aval, lo que facilita su gestión y procesamiento.

b) Es especialmente útil en entornos donde se maneja un gran volumen de avales, como en la contratación pública.

c) Permite que los datos del aval sean leídos e interpretados por diferentes sistemas informáticos de manera estandarizada.

Los formatos XML permiten un tratamiento automatizado de los datos, de ahí que sea utilizado por el Tesoro Público y grandes Corporaciones. Con escasa implementación aún en el ámbito local.

2. **PDF (Portable Document Format) con firma electrónica.**

a) Este formato conserva la apariencia y el diseño del aval tradicional en papel, pero se emite y firma digitalmente.

b) Es ampliamente utilizado por su compatibilidad con diferentes dispositivos y sistemas operativos.

c) La firma electrónica garantiza la autenticidad e integridad del documento.

3. Formatos propios de plataformas digitales.

a) Algunas entidades financieras y plataformas especializadas ofrecen sus propios formatos de aval electrónico, que suelen estar integrados con sus sistemas de gestión.

b) Estos formatos pueden ofrecer funcionalidades adicionales, como el seguimiento en tiempo real del estado del aval o la notificación automática de eventos relevantes.

4. **Formatos para la Caja General de depósitos.**

La caja general de depósitos usa formatos que permiten la creación de garantías que se depositan en sus oficinas.

Es importante tener en cuenta que la validez legal de un aval electrónico depende de que cumpla con los requisitos establecidos por la normativa vigente, como la utilización de firmas electrónicas cualificadas y certificados digitales reconocidos.

6.Procedimiento de gestión.

Se debe establecer un procedimiento electrónico en materia de garantías en forma de aval o mediante seguro de caución, teniendo en cuenta las posibles fases que puedan originarse en su desarrollo, que bien podríamos, esquematizar de la siguiente forma:

1. Acreditación de poderes
2. Bastanteo
3. Acto de constitución.
4. Custodia
4. Solicitud de devolución / cancelación
5. Ejecución.

En este esquema por acotar el artículo, no se analizará el procedimiento de ejecución que suele ser de fácil implementación, y por ello solo analizaremos en sentido amplio para el aval electrónico la: constitución, custodia y procedimiento de devolución

Es necesario normalizar jurídica y electrónicamente dicho procedimiento, mediante el acto de aprobación del correspondiente reglamento regulador del servicio (que bien podría serlo, regulando en su integridad el servicio de la tesorería municipal, dentro del cual se regularía el régimen de garantías, o concretando el procedimiento especial y regulando lo que podríamos denominar como caja municipal de depósitos),o en su defecto regular en Bases de Ejecución del Presupuesto o modelos predeterminados en bases y pliegos el procedimiento de gestión, sin perjuicio de los procedimientos que se refieran a los actos de gestión (tributarios, contratos, …) El contemplar este procedimiento en la Sede Electrónica es esencial.

Sea de una u otra forma, el procedimiento electrónico se realizará en sede electrónica municipal o provincial, y posibilitará su acceso a las personas físicas y jurídicas, con el carácter obligatorio para ambas, y ello sobre la base de, sentada la obligatoriedad para las jurídicas (art. 14.2 ley 39/2015) establecer también su exigencia para las físicas, de conformidad con lo dispuesto en el apartado 3 del referido artículo, que dice:

3. "*Reglamentariamente, las Administraciones podrán establecer la obligación de relacionarse con ellas a través de medios electrónicos para determinados procedimientos y para ciertos colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación*

profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

En la práctica casi la totalidad de las actuaciones electrónicas se realizan a través de sede electrónica y puede también constituir estas un aval físico, por ello debe ser, aunque excepcional contemplar en el modelo la gestión de estos, tanto la constitución como custodia del aval físico.

El procedimiento electrónico considera los roles de cada uno de los intervinientes en esa relación "triangular" en que se articula la institución de la fianza o garantía: garante, garantista y garantizado, o avalista y avalado en su traslación a la figura del aval.

Y es el garante, que necesariamente y sólo para los avales, deberá ser una entidad financiera: "*los bancos, cajas de ahorros, cooperativas de crédito, establecimientos financieros de crédito y sociedades de garantía recíproca autorizados para operar en España,* expresa en su literalidad el art.108 LCSP, quien deberá acreditar su representación, con poder bastante, que deberá ser bastanteado, por la administración ante quien se va a depositar, en nuestro caso por el órgano correspondiente dentro de la estructura local: asesoría jurídica, secretaría general, o aquel otro creado "ex proceso" para tal fin con las correspondientes autorizaciones. También se puede excepcionar un limite de importe para la necesidad del bastanteo, aunque siempre se verificaran las firmas.

Dicha representación que podrá ser anexada, con copia de las escrituras de apoderamiento o aportando los datos necesarios para la consulta de los poderes notariales, adjuntando el código seguro de verificación (CSV) para su consulta en la plataforma de intermediación, surtirá efectos una vez realizado el protocolo de verificación y / o bastanteo, pasando a incluir dichos datos en un registro de apoderamientos local para actos de esta naturaleza, dependiente de la tesorería.

Y este registro de apoderamientos de la tesorería, aunque nuevo, no escapa de su llevanza y regulación normativa en épocas anteriores, si bien no para el caso que nos ocupa.

Así, la Regla 40 de la Instrucción de contabilidad de las corporaciones locales, anexa al Reglamento de Haciendas Locales de 1.952, establecía que:

"*los proveedores no podrán percibir cantidad por medio de otras personas sin presentar copia del poder o autorización, bastanteados por el secretario o funcionarios letrados de la corporación.*

La depositaría llevará un libro registro de poderes y autorizaciones y conservará copias simples cotejadas con los originales"

EL R.D 128/2018, 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional en aplicación del apartado segundo del art 5.1 atribuye a la tesorería la ***"organización de la custodia de fondos, valores y efectos, de conformidad con las directrices señaladas por la Presidencia".***

Acreditado en dicho registro, en los sucesivos trámites de presentación de garantías por la entidad financiera, ya no será preciso acreditar nuevamente la vigencia de los poderes junto con el documento de constitución del aval.

El acto de constitución debe realizarse en sede electrónica normalmente facilitando un modelo autorrellenable, donde se adjunte el aval debidamente firmado por los apoderados de la entidad, lógicamente mediante firma electrónica.

El aval expedido en formato electrónica genera alguna incertidumbre al estar en poder del tercero, pero la misma virtualidad y valor tiene el documento en papel como el electrónico, siempre que uno u otro reúnan todos los requisitos.

El mismo planteamiento tiene el resto de los documentos electrónicos que las Tesorerías puedan recibir. Lo importante es definir el repositorio donde se archivan y donde se alojarán para su custodia, teniendo en cuenta que es necesario el documento de cancelación para su baja ante la Entidad Financiera.

Acreditados el complimiento de los requisitos necesarios y verificada la validez del documento aval, el titular de la tesorería expedirá y firmará documento electrónico que acredite la constitución del aval o seguro de caución, con traslado automático al libro/ registro electrónico de avales/ seguros de caución en el que se "depositará" para su constancia, registro y control de garantías otorgadas en forma de aval.

"Depositado, archivado, y registrado en dicho sistema, de forma automática cabría la posibilidad de generar los correspondientes justificantes para su traslado por los canales internos de comunicación al área correspondiente, contratación u otros, y al garante y garantizado, avalista o avalado, que ya lo sería por sede electrónica.

En esta relación triangular a la que hacíamos referencia, la figura del avalado, garantizado, escapa a cualquier tipo de actuación ante la administración, dejando que dicha relación se sustente sólo entre el avalista y la administración, ostentando el garantizado una posición pasiva que sólo le llevaría a recibir el resguardo acreditativo del depósito del aval.

En los supuestos de devolución del aval, por el cumplimiento del plazo de garantía, se iniciaría un trámite electrónico de devolución por la tesorería, o caja municipal de depósitos, sobre la base

de un acto administrativo del órgano competente, que ordene su devolución al garante y garantizado, lo que llevaría aparejado la expedición y firma por el tesorero de un documento de cancelación/devolución, que se trasladarían por sede electrónica a la entidad financiera avalista y avalado, para su constancia documental.

En parecidos términos cabría operar en los supuestos de incautación de la garantía, de ejecución del documento de garantía: aval o seguro de caución.

Notificada la resolución o el acto por el que se acuerda la incautación, por la tesorería se expedirá orden de ejecución del aval o de cumplimiento de la función aseguradora para el caso del seguro de caución, quien lo notificará por medios electrónicos a la entidad financiera con todos aquellos pronunciamientos que se consideren oportunos: plazo y el canal y medio de ingreso de la cantidad adeudada.

De llegarse a ejecutar e ingresar, por la tesorería se procederá a expedir documento electrónico de cancelación/devolución del documento electrónico aval, dándose de baja del libro registro de avales al que hemos hecho referencia.

Aunque no hay un modelo fijo y predeterminado, cada administración podrá diseñar el que considere más acorde a su estructura interna, todo se fundamenta en la voluntad/ necesidad de crear un procedimiento más rápido, ágil y seguro que el actual, de relación electrónica y / o digital en general, y sobre todo con la administración.

Un esquema- modelo de procedimiento digital de garantía digital partiría de las siguientes premisas.

1. Existe una fase previa a la constitución digital una vez presentado el aval en Sede Electrónica mediante sistemas de acceso digital:

    a) Se comprueba el Bastanteo (poder de los firmantes para realizar estas operaciones) en el Registro de Bastanteos efectuado en nuestro caso por la Asesoría Jurídica. En cuanto a la verificación o bastanteo de los firmantes para ver si tienen poder bastante para obligar a la entidad a la que representan (normalmente como avalista), requieren que los poderes para la constitución o depósitos sean bastanteados **con carácter previo** y por una sola vez.

    Las Entidades Locales no suelen disponer de una base de datos previa de poderes, por ello la necesidad de crearla, hasta que se implemente el registro de apoderamiento), y con cada constitución de garantía se suele requerir la acreditación de los poderes, al no dar por válidos, por no poder comprobar, los

bastanteos efectuados por la Caja General de depósitos del Tesoro Público, porque Cantidades pequeñas se podrían admitir con el bastanteo de la Caja General de Depósitos del Tesoro Público

b) Comprobar según plantilla de aval si reúne los requisitos mínimos exigible y se atiene al modelo especificado.

c) Verificar CSV. El Código Seguro de Verificación es un término informático que designa al código único que identifica a un documento electrónico

Si el resultado de este ITER es negativo por cualquier causa, se realiza una comunicación (NOTIFICA) o mail en su caso indicando la necesidad de rectificación.

Si persiste la problemática se comunicará su inadmisión. El órgano de contratación o de aplicación de los tributos resolverá la exclusión del procedimiento de licitación o no concesión de fraccionamiento o admisión para la suspensión del procedimiento de apremio en su caso, de forma motivada y dando pie de recurso al tercero.

d) Si es positivo, hemos optado por incorporarlo al módulo de terceros de SICAL (Sistema de Información Contable de la Administración Local) responsabilidad del Tesorería en cuanto a su mantenimiento, que posibilitaría una información más amplia y detallada del tercero.

Antes de subir el fichero digital al módulo SICAL de terceros, se verifican las firmas de forma automática. El sistema lo somete de forma automática y online a una nueva validación a través de la plataforma VALIDe .

e) Una vez subido el fichero (normalmente PDF con firma digital, aunque se debe habilitar opciones de XLM u otras) y seleccionado la tipología de garantía, se genera una carta de pago o talón de cargo firmado con Sello electrónico de la Tesorería.

Esta constitución y custodia del aval tiene un valor añadido frente al sistema tradicional del aval físico:

a) Se puede consultar este aval a Entidad Financiera garante de forma telemática.

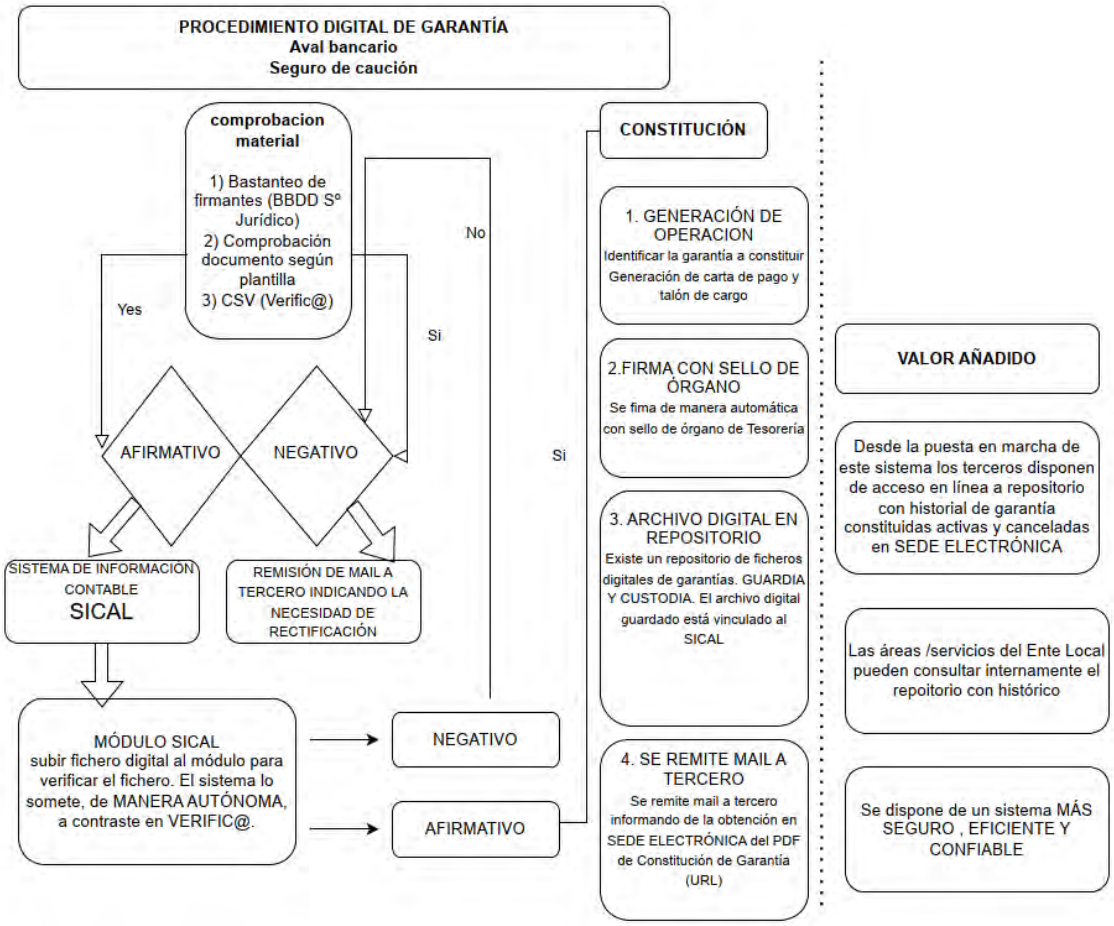
b) Existe un repositorio de guarda y custodia, donde el archivo digital está vinculado a SICAL. Con un histórico por terceros que disponen en línea de las garantías constituidas y canceladas.

c) Se remite mail o comunicación (NOTIFICA) al tercero informado de la constitución y descarga del justificante o carta de pago por medios electrónico.

d) Las áreas/servicios gestores pueden consultar internamente el repositorio con datos históricos.

f) El procedimiento de cancelación para la Tesorería se inicia con la Resolución de cancelación de la garantía, se notifica al tercero (la fecha de apertura de la notificación electrónica la consideramos como fecha de cancelación) indicando que pueden acceder al documento de cancelación (firmado por sello de órgano tesorería) y al aval (aunque este lo disponía previamente), así como a la Resolución de cancelación en su caso,a través de la sede electrónica, y esto permitirá al tercero remitir a la Entidad Financiera garante la documentación, cancelar el aval y dar de baja del registro especial de avales de cada entidad.

Diagrama procedimental: un modelo de gestión.



GESTION DE PAGOS EN LA ADMINISTRACIÓN LOCAL: CIBERSEGURIDAD Y VALIDACION DE CUENTAS

José Manuel Farfán Pérez
Tesorero General
Diputación de Sevilla y OPAEF

1. Introducción.

2. Ejecución de pagos.

3. Suplantación de identidad. Medidas de prevención.

4. Efectos jurídicos de la suplantación de identidad.

5. Herramientas para validación de cuentas.

6. Nuevo Reglamento de Pagos.

1. Introducción.

En las dos últimas décadas la Gestión de Tesorería ha sufrido una fuerte evolución. El desarrollo de la banca digital se ha convertido en una herramienta esencial para todas las personas y empresas que quieren mejorar su vida cotidiana con tecnología aplicada a las finanzas.
En lo referente a la gestión de pagos, esta debe circunscribirse a un esquema de objetivos de: eficiencia y seguridad.
a) Eficiencia: alude a los costes de emisión de pagos y sus formas de realización. En un esquema de automatización de operaciones.
b) Seguridad: estableciendo un conjunto de requisitos mínimos de seguridad en la lucha contra el fraude (protocolo de buenas prácticas). Dado que la suplantación de identidad y los fraudes en los procesos de pagos es moneda común de estos tiempos.
El análisis de la eficiencia en la gestión de los procesos de pagos de obligaciones con un esquema propio de seguridad de las transacciones es el objeto de reflexión de este artículo
Para delimitar el artículo y dado que existen muchas tipologías, instrumentos o medios de pago, nos circunscribiremos al ámbito de las transferencias realizadas a través de los proveedores de servicios de pago (PSP), en terminología de PSD2 (nueva directiva de pagos, Directiva (EU) 2015/2366), ya que es el medio de pago más frecuente utilizado por las Administraciones Locales.

2. Ejecución de pagos.

En relación con el pago material, se autoriza con firma de apoderados, y el procedimiento supone enviar la relación de pagos, donde se debe subir el fichero (CSB 34) a la plataforma de la Entidad y ejecutar esos pagos con los protocolos de la “PSD2”.
El pago mediante transferencia bancaria en los 34 países de la zona europea se normalizo gracias a la identificación de las cuentas con IBAN (International Bank Account Number; 20 números + cuatro caracteres que identifican el país y el número de control del IBAN), fuera de la UE se utiliza el BIC (Business Identifier Code) o SWIFT.

Como actos preparatorios, el tesorero elabora la fase P (ordenación de pagos) y la orden de transferencia firmada (electrónicamente por los tres claveros (autorizados) para pagos, y:
1. Sube el fichero CSB 34 por terminal banco.
2. Utiliza la doble autenticación, para la ejecución del pago.

Gracias a la **PSD2** se introducen controles de seguridad que evitan fraudes online como la suplantación de identidad en el momento del pago. De esta forma, es impracticable que un posible infractor pueda realizar operaciones en nuestro nombre y acceder a los productos y servicios contratados.

El refuerzo de la seguridad introducido por la **directiva PSD2** evita los pagos online no autorizados y evita que se pueda hacer incluso uso de una tarjeta de crédito robada gracias a los procedimientos **PSD2 de SCA de doble factor de autenticación**.

SCA son las siglas de la expresión anglosajona "Strong Customer Authentication", que se refiriere directamente como autenticación reforzada.

Para autorizar pagos online se requerirá el uso combinado de dos o más elementos de autenticación (SCA o autenticación fuerte de usuario):

- Algo que el cliente conoce: por ejemplo, una contraseña,
- Algo que el cliente tiene: por ejemplo, un token, un certificado digital, un teléfono, y
- Algo que el cliente es: por ejemplo, un rasgo biométrico como la huella digital o el iris

Este concepto hace referencia a todo un conjunto de herramientas que pretenden proteger los servicios de pago online de peligros como fraude, robo de credenciales o transferencias de fondos ilegales.

En definitiva, para ejecutar cualquier pago se necesitan dos factores: autenticación y transmisión por canal seguro y además hay que generar un código único asociado al importe y beneficiario. Esto hace que p.ej. una orden por e-mail no cumpla PSD2. No podemos enviar una orden de cargo o transferencia al banco por mail o fax ya que no cumple los requisitos de la PSD2.

Como resumen para firmar operaciones, además de transmitir por canal seguro del PSP, se requiere firmar por la app de firma (que pide PIN, huella, etc) o bien con un token, no sería valido usar tarjetas de coordenadas al no cumplir PSD2, y los SMS tampoco porque tienen vulnerabilidades (Scam, Phishing…)

Dicha Directiva ha aumentado la seguridad en las transacciones, pero a la vez se está produciendo un fenómeno de incremento de la ciberdelincuencia en la fase previa al pago material, a través de la suplantación de identidad en la acreditación de las cuentas de terceros.
Las malas prácticas, y no tener un sistema normalizado de pagos, han posibilitado una creciente proliferación de fraudes de suplantación de identidad: pago a un tercero no acreedor por conducta maliciosa de un ciberdelincuente.
En resumen: en la gestión de pagos se debe elaborar un documento normativo interno ("compliance"), que sea un código de conducta que evita las malas prácticas y minimice los

riesgos de las transacciones, por ejemplo: prohibiciones de correos electrónicos, SMS o el teléfono para acreditarse los terceros.

Además, en toda organización es importante implementar los protocolos de seguridad en las transacciones: DKIM Y DMARC, que nos pueden ayudar a **evitar que se manden correos suplantando nuestra identidad**, una actividad conocida como *phishing*. También sirven para dar más seguridad a los servidores de destino de nuestros correos y así evitar, dentro de lo posible, que sean marcados como SPAM.

Uso de cortafuegos, filtrado de aplicaciones, categorización URLs, apertura selectiva tráfico SSL, son algunas de las medidas necesarias en un esquema de seguridad en las transacciones.,

Insistimos que Todas las operaciones se realizarán por canal seguro de transmisión e implementaríamos un modelo de ciberseguridad (seguridad informática) como un principio de actuación y no solo como un medio a aplicar, con la adecuación al ENS (Esquema Nacional de Seguridad).

En resumen, la gestión de pagos debe mantener siempre el equilibrio entre la mayor tecnificación (eficiencia) con un esquema previo de seguridad adecuado

3**. Suplantación de identidad. Medidas de prevención.**

Los ciberdelincuentes utilizan una variedad de **técnicas de "malware** "para llevar a cabo sus actividades maliciosas. **Una de las más comunes es el "phishing"**. Los delincuentes envían **correos electrónicos fraudulentos** para suplantar la cuenta de terceros. Otro ejemplo es **el "ransomware"**, un tipo de malware que cifra los archivos de la víctima y exige un rescate para restaurar el acceso a los mismos.

Existen varios mecanismos que pueden ayudar a detener la acción de los ciberdelincuentes y proteger la **seguridad cibernética**. Estos incluyen el **uso de software antivirus y firewalls** para detectar y bloquear malware, la implementación de **políticas de seguridad sólidas** para **proteger la información confidencial** y la **capacitación de las personas usuarias** para reconocer y responder adecuadamente a las **amenazas cibernéticas.**

Este tipo de fraudes de suplantación de identidad de terceros acreedores legítimos es más común en el sector empresarial, dado que la Administración utiliza preponderantemente las sedes electrónicas, evitando otros medios como sería correos electrónicos o teléfonos.

Es necesario disponer de sede electrónica y a través de certificado digital poder acreditarse a ante la Tesorería Local. En el modelo de ficha de terceros es conveniente indicar: "el Abajo firmante se responsabiliza de los datos detallados anteriormente, tanto generales como bancarios, que identifican la cuenta y la entidad financiera a través de la cual se desean recibir los pagos que puedan corresponder, quedando el Ayuntamiento XXXXX exonerado de cualquier responsabilidad

derivada de errores u omisiones en los mismos". También se recomienda limitar el número de cuentas acreditadas por terceros en Bases de ejecución.

La sede electrónica obligatoria es un medio de acreditación segura (normalmente a través de certificado digital), y la firma electrónica en esa sede permite acreditar la autenticidad de la expresión de voluntad consentimiento del acreedor, así como la integridad e inalterabilidad del documento.

En el supuesto de que no se disponga de sede electrónica en las Entidades Locales, se establecería como objetivo preferente implementarla, y en todo caso se deberán solicitar documentos originales que permitan una identificación del tercero.

Con el objeto de evitar que la obligación formal y material de pago sea correcta y no haya error en el pago el tercero se tiene que justificar la titularidad de cuenta corriente (acreditación del tercero) , y se deberá presentar certificado bancario en la ficha de tercero firmada por este mediante certificado digital y la entidad bancaria acreditará a su vez que ese número de cuenta es del titular. Algunos certificados vienen con CSV (código seguro de verificación), en el resto se coteja la firma de este.

La declaración jurada de titularidad de cuenta corriente no se debe permitir por los posibles efectos de falsedad documental.

El detalle de las fichas de terceros y su tramitación debe ser reflejadas en las Bases de ejecución del presupuesto. Es relevante: la exoneración de cualquier responsabilidad derivada de errores u omisiones, la solicitud de la facultad para para solicitar confirmación de la cuenta, y la declaración del tercero sobre la veracidad de los datos suministrados.

Es necesario, antes de integrar las cuentas bancarias en el módulo de terceros, cotejar los certificados de titularidad de cuentas que deben venir sellados digitalmente o con CSV (conjunto de dígitos que identifica de forma única los documentos electrónicos emitidos por cualquier), y poder utilizar por ejemplo **VALIDe** (servicio on-line ofrecido por el Ministerio de Política Territorial y Función Pública para la validación de Firmas y Certificados electrónicos), que validaría la firma del documento y quedaría cotejado.

Además, en forma de resumen, se deberían tomar las siguientes medidas en el proceso de acreditación de cuentas:

1. Evitar las malas prácticas, con la prohibición de correos electrónicos, teléfonos, etc… como forma de comunicación con los terceros. Uso exclusivo de la Sede Electrónica.

2. Sede Electrónica para acreditación de los terceros accediendo a través de los canales previstos (fundamentalmente con certificado digital) y utilización de **VALIDe** (validez de las firmas) para el cotejo de certificados bancarios**.**

3. El IBAN cotejado se refleja de forma automática en el modulo de tercerso de SICAL, y los permisos para gestionar el módulo de datos bancarios de terceros deben ser muy restrictivos, y solamente asignados al personal de tesorería. De la misma forma que se prohibiría la introducción de un IBAN de un tercero de forma manual.

4. En la ordenación del pago un mecanismo de control esencial es: que en supuesto que la cuenta estipulada y designada por el acreedor en FACE (factura electrónica) no coincida con las que consten como acreditada en la Tesorería, se deberá requerir al acreedor para su nueva acreditación, siendo este un mecanismo de control esencial para evitar la suplantación de identidad.

Una observación en esta materia, el control de fondos públicos le corresponde tanto al Tesorero, tal como establece la Cámara de cuentas de Andalucía como el Tribunal de Cuentas, como al Interventor en base al artículo 32,1c del RD424/2017 de 28 de abril, si hubiera observado área de riesgo, si bien la responsabilidad directa de la acreditación de terceros recae en la Tesorería

En la responsabilidad contable de la función de Tesorería es necesario tener en cuenta los postulados de la Sentencia del Tribunal de Cuentas número 5/2000 de Procedimiento de reintegro por alcance, que determina nítidamente el control material y los supuestos de responsabilidad contable, tanto de la Intervención como de la Tesorería en los pagos a realizar

4. **Efectos jurídicos de la suplantación de identidad.**

La Autoridad Bancaria Europea no solo define como fraudulentas las transacciones de pago no autorizadas, también aquellas en las que se manipuló al pagador para admitir una orden de pago, y, también, el propio Código Civil, en su artículo 1.265 y siguientes considera que el consentimiento será nulo si se presta por error, pero aun siendo fraudulenta y grave, el deudor debe actuar de forma responsable siendo determinante el IBAN suministrado en la Orden de Pago. El artículo 1164 del Código Civil establece que “el pago hecho de buena fe al que estuviese en posesión del crédito liberará al deudor”. La jurisprudencia ha determinado que este precepto protege la confianza en la apariencia jurídica, pero requiere que el acreedor actúe de manera adecuada, razonable y objetivamente verosímil. Además, se destaca que el deudor debe actuar con diligencia debida para asegurarse de que el acreedor aparente sea el legítimo.

En el caso analizado por ejemplo por la Sentencia de la Audiencia Provincial de Granada, sección 4 de 7/11/2022, el correo recibido por la demandada presentaba una apariencia de veracidad y legitimidad, lo que la llevó a realizar el pago de buena fe según las indicaciones de este. Se argumenta que la demandada no puede ser reprochada por no comunicar el pago por otro medio, ya que la relación entre las partes siempre se realizó a través de correos electrónicos.

Si tenemos una suplantación de identidad por estas malas prácticas comentadas o la falta de seguridad de los canales de gestión de cuentas acreditadas, ese pago no ha tenido efectos liberatorios de la cantidad satisfecha porque no se ha producido un ingreso real en el patrimonio del titular de esta, exigiéndose la identidad e integridad de la prestación convenida, en opinión de la Jurisprudencia del Tribunal Supremo (STS 521/2001, de 25 de mayo).

En una transferencia es muy importante introducir correctamente el número de cuenta (en la zona SEPA, el IBAN) del beneficiario pues la entidad del ordenante ejecutará la operación basándose en éste de forma automática, sin más comprobación, ni del ordenante, ni del beneficiario.

La normativa de servicios de pago tampoco establece el deber de las entidades de comprobar que el nombre del beneficiario se corresponde con el del titular del número de cuenta de destino de la transferencia ni otros datos adicionales, más allá de la coincidencia del IBAN beneficiario con el indicado en la orden de pago.

En este contexto, en el asunto C-245/18, el TJUE analizó una cuestión prejudicial planteada por un tribunal italiano, referente a la interpretación de los artículos 741 y 75 de la citada Directiva 2007/64/CE (actualmente derogada por la Directiva 2015/2366), con respecto al abono de una transferencia por parte del proveedor de servicios de pago del beneficiario, pues resultaba en ese caso que la operación se había cursado indicando el ordenante un IBAN o identificador único erróneo y el banco de destino, proveedor de servicios de pago del beneficiario, no había comprobado que el IBAN no se correspondía con el nombre de la persona designada como beneficiaria en la propia operación.

Pues bien, en el referido asunto, el TJUE ha declarado que el artículo 74, apartado 2, de la directiva debe interpretarse en el sentido de que, cuando una orden de pago se ejecute de acuerdo con el identificador único facilitado por el usuario de servicios de pago y tal identificador no corresponda al nombre del beneficiario indicado por ese mismo usuario, la limitación de la responsabilidad del proveedor de servicios de pago establecida en esa disposición se aplicará tanto al proveedor de servicios de pago del ordenante como al del beneficiario.

En consecuencia, cuando una transferencia se ejecuta conforme al identificador único (IBAN), se considera correctamente ejecutada en relación con el beneficiario indicado, no siendo responsable

la entidad de la ejecución defectuosa cuando el identificador único facilitado por el usuario fuera incorrecto, según el artículo 59 Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera). Eso es aprovechado por la ciberdelincuencia para intentar modificar las cuentas bancarias antes del pago, que no corresponderán con el acreedor legitimo

La transferencia se dirige a un IBAN de forma automática, sin comprobación por la entidad del ordenante ni del beneficiario. Igualmente, los demás datos consignados en la orden (entre ellos, el concepto) son mensajes destinados al beneficiario, no a la entidad.

En virtud de la irrevocabilidad de las transferencias, las cantidades abonadas en cuenta al beneficiario solo podrán ser retrotraídas si mediara el consentimiento de éste o la preceptiva orden o mandato legal o judicial, no estando facultadas las entidades para retroceder la transferencia sin consentimiento del beneficiario, o sin la concurrencia de errores demostrables, siempre que se acredite que el error en el que se pudo incurrir no era imputable al ordenante.

En este mismo sentido se pronuncia el Banco de España ante consultas formuladas y en sus memorias de reclamaciones en distintos años.

Es relevante la Sentencia del Juzgado de Primera Instancia Nº 19 de Sevilla, del recurso presentado por el Ayuntamiento de Sevilla, ante el Banco de Santander, en materia de responsabilidad por suplantación de identidad en pagos. En este sentido se detallan los fundamentos jurídicos más esenciales:

a) “En el presente procedimiento se ejercita por la actora, la acción de responsabilidad civil extracontractual o aquiliana que se contempla en el art. 1902 y concordantes del Código Civil contra el Banco Santander, los daños y perjuicios sufridos, esto es, por el importe de las cantidades incorrectamente transferidas, un total de 962.797 euros, por dicha entidad bancaria a una cuenta corriente que no es la del beneficiario de las tres transferencias ordenadas por la demandante, es decir, a Iluminaciones XXX.

b) A dicha pretensión se opone el demandado citado, aduciendo tanto excepciones como motivos de oposición de fondo, que habrá en su caso de ser objeto de esta resolución.

Por el demandado Banco Santander, se aduce la prescripción de la acción ejercitada conforme al art. 1968.2 del Código Civil, conforme al cual: “Prescriben por el transcurso de un año: la acción para exigir la responsabilidad civil por injuria o calumnia y por las obligaciones derivadas de la culpa o negligencia de que se trata en el artículo 1.902, desde que lo supo el agraviado.”

c) Sin embargo, incluso en el hipotético caso de que la acción no estuviera prescrita, también existen motivos de fondo para desestimar esta pretensión ejercitada por la demandante. Es en esta situación, tras verificarse que dicho correo electrónico no fue enviado por xxxx y que habían sido fruto de una posible estafa, donde la Gerencia reclama al Banco Santander (entidad a través de la cual se realizan las transferencias) una mayor diligencia y control para haber evitado el fraude, debiéndose haber cerciorado que el IBAN indicado no correspondía al verdadero beneficiario.

d) Santander Digital Services (empresa perteneciente al grupo Santander), en el departamento de tecnología, banca electrónica y ciberfraude nos explica en el acto de la vista de manera clara y comprensible, que el banco no puede realizar bloqueos de transferencias por el motivo alegado por la Gerencia, es decir, que el IBAN no coincide con la razón social del destinatario. Y ello lo explica con datos que clarifican a este juzgador: en el caso que nos ocupa se trata de transferencias SEPA. Las transferencias SEPA son aquellas en las que el único dato validable es el IBAN, es decir, tras la comprobación por parte del banco que este dato está correctamente indicado, la transferencia se realiza con normalidad.

A las alegaciones realizadas sobre este punto por parte de la Gerencia del Ayuntamiento, de que el que NIF y la razón social o beneficiario son campos obligatorios para poder realizar dichas transferencias y que el banco debería haberlos comprobado, el Sr. AAA de Santander nos explica que son campos que deben aparecer rellenos formalmente, pero que en ningún caso son validables.

En conclusión, si el IBAN es válido y existente, la transferencia se realiza a la cuenta correspondiente a dicho IBAN, independientemente de lo que se haya indicado, materialmente, en los otros campos.

Estas manifestaciones, además, se ven apoyadas en las instrucciones del Cuaderno 34 de la Asociación Española de Banca, que especifica que las transferencias no podrán realizarse si no constan los datos que aparecen como obligatorios, reafirmando que se trata de unos datos que deben estar cumplimentados formalmente, en ningún caso a su validación.

d) Además de una prueba pericial en el mismo sentido; Todo ello nos lleva a la conclusión de que la Gerencia actuó sin la debida diligencia, no se preocupó ni siquiera en comprobar y verificar que el IBAN del correo electrónico que recibió coincidía con el de las facturas por las que se transfirieron sendas cantidades de dinero.

e) En conclusión, este juzgador da credibilidad al informe y ratificación del perito por su claridad, sus conclusiones y su análisis basado en diferentes elementos.

Y tras una valoración conjunta de la prueba podemos afirmar que la entidad bancaria Santander actuó como debió hacerlo, verificando y validando el único dato necesario (el IBAN) para realizar la transferencia. Sin embargo, la Gerencia actuó sin la diligencia debida, no pudiendo pechar terceros con las consecuencias derivadas de esta actuación negligente.

No se le puede exigir responsabilidad al banco una vez validado el IBAN, aunque el nombre que aparezca en el campo "beneficiario" fuese distinto al que aparece como tal según dicho IBAN".

En este sentido debemos analizar la STS 507/2025, 27 de Marzo de 2025. RESPONSABILIDAD DEL PROVEEDOR SERVICIOS DE PAGO. TRANSFERENCIA ELECTRÓNICA ERRÓNEA.

"Ni el proveedor de servicios de pago del ordenante ni el del beneficiario están obligados a verificar si el identificador único (IBAN) proporcionado por el usuario corresponde efectivamente a la persona designada como beneficiaria. No existe disposición normativa que imponga a los proveedores de servicios de pago un deber adicional de diligencia en función de circunstancias específicas, como la identidad del beneficiario, el concepto o el importe de la transferencia. La responsabilidad del proveedor se limita a ejecutar correctamente la orden de pago de acuerdo con el identificador único facilitado por el ordenante".

En resumen: el Tesorero como gestor de pagos deberá tener en cuenta las siguientes actuaciones.
1. Protocolo de actuación de la Organización (Entidad Local) y de la propia Tesorería.
a) En la Tesorería: las medidas generales pasan por la utilización de forma casi excluyente de la Sede Electrónica y la acreditación de los terceros (acreedores) ante esta. En caso contrario incurriríamos en un riesgo importante de fraude con las consecuencias económicas que ello conlleva.
Este cumplimiento normativo interno ("compliance") es un código de conducta que evita las malas prácticas y minimiza los riesgos de las transacciones, por ejemplo: prohibiciones de correos electrónicos, SMS o el teléfono para acreditarse los terceros.
2. La Tesorería debe tener su propia plataforma con autonomía para gestionar pagos con criterios de seguridad.
Todas las operaciones se realizarán por canal seguro de transmisión.
En definitiva, implementar un modelo de ciberseguridad (seguridad informática) como un principio de actuación y no solo como un medio a aplicar, con la adecuación al ENS (Esquema Nacional de Seguridad).
3. Diseño de las actuaciones en los procesos de firma de las órdenes de pago de los distintos apoderados. Normalmente Interventor, Alcalde-presidente, y Tesorero.

a) Utilización de la firma electrónica
b) Portafirmas propio de la Entidad Local.
c) Secuencias y control de firmas.

Todo ello bajo un esquema de digitalización que permita el máximo grado de automatización de los procesos de pagos, que evitara malas prácticas que pueden devenir en un supuesto de suplantación de identidad.
Siendo el responsable del manejo de fondos públicos, por motivos de seguridad y eficiencia, las claves bancarias solo deben estar en poder del Tesorero.

Como conclusión diremos que la gestión de pagos debe mantener siempre el equilibrio entre la mayor tecnificación (eficiencia) con un esquema previo de seguridad adecuado.

5. **Herramientas para validación de cuentas.**

Una vez realizado el procedimiento de incorporación de datos de cuentas del tercero en el módulo SICAL, y teniendo en cuenta que se cotejará la cuenta designada en FACE por el Tercero y la acreditación del tercero en la Tesorería Local, debemos implementar un control más: el sistema de validación de cuentas.

Afortunadamente a través de IBERPAY, que es la empresa privada que gestiona el **Sistema Nacional de Compensación Electrónica** (SNCE) del sistema español de pagos al por menor, y sus accionistas son las entidades participantes en el SNCE (Sistema Nacional de Compensación Electrónica), existe un proyecto (ya muchas empresas y Administraciones están ejecutando) para que podamos validar las cuentas de nuestros acreedores de forma fidedigna. Este servicio será online 24x7, con respuesta en tiempo real y con alcance de +75M cuentas (99% cuentas españolas), trata de ayudar a la prevención del fraude (Validación de titularidad inmediata), en un sistema con integración en la web o en sistemas de gestión del cliente (participante indirecto). Tendrá un bajo coste, pero tiene un coste interbancario. La Infraestructura será de IBERPAY.

En la actualidad ya se estaba implementado ese sistema de verificación de cuentas de terceros para operaciones entre entidades y clientes de esa entidad. Ahora se está implementando para el resto de Las Entidades Financieras.

Dado que IBERPAY sólo presta servicio a las Entidades Financieras, este servicio de validación de cuentas se debe realizar a través de las que presten el servicio de pagos a la Entidad Local.
La Entidad local comunica con la Entidad financiera y esta a su vez con IBERPAY. Existiendo unos flujos equivalentes en vía de regreso. El usuario realiza la solicitud para ello suministra: IBAN de la cuenta; nombre del titular y tipo de identificación (NIF, CIF,NIE). La Entidad financiera verifica el formato y genera una solicitud, creando un código univoco. El usuario en cuestión de segundos consulta el resultado de la verificación, que como respuesta recibirá uno de los siguientes valores: OK, en caso de correspondencia y cuenta activa o, KO, en caso de no correspondencia o cuenta inactiva.

La Verificación de titularidad de cuenta tiene dos funcionalidades:

a) Solicitud de verificación de titularidad.

b) Consulta el estado de la verificación de titularidad.

El proceso de verificación actuará de forma automática y además se habilitará desde el mantenimiento de datos bancarios de terceros la activación manual (de una cuenta en estado pendiente de verificar o verificada con resultado incorrecto (por cualquier motivo).

6. **Nuevo Reglamento de Pagos.**

El Reglamento (UE) número 260/2012 estableció requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros. Las transferencias inmediatas en euros constituyen una categoría relativamente nueva de transferencias en euros que surgió en el mercado solo después de la adopción de dicho Reglamento. Por consiguiente, es necesario establecer requisitos específicos aplicables a las transferencias inmediatas en euros, además de los requisitos generales aplicables a todas las transferencias, para asegurar el funcionamiento y la integración adecuados del mercado interior. Pero estas transferencias inmediatas (abono al acreedor el mismo día que se ejecutan por parte del ordenante), que entraron en vigor en 2018 sólo para la zona SEPA, tienen unas limitaciones:

1ª. Coste para el ordenante.

2ª Limitación de 15.000 euros.

3ª PSP receptor debe estar acogido a este sistema de pagos inmediatos. En la actualidad, al menos un tercio de los proveedores de servicios de pago de la Unión no ofrecen el servicio de pago consistente en enviar y recibir transferencias inmediatas en euros.

Estas limitaciones hacen que las Transferencias inmediatas (mismo CSB 34, pero con una modificación en un campo especifico: INSTANT) sea usada esencialmente para pagos de nóminas, permitiendo a todo el personal de la organización cobrar el mismo día.

Recientemente se ha aprobado en la Unión Europea, el 13 de marzo: **Reglamento (UE) 2024/886 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, por el que se modifican los Reglamentos (UE) Nº 260/2012 y (UE) 2021/1230 y las Directivas 98/26/CE y (UE) 2015/2366 en lo que respecta a las transferencias inmediatas en euros**.

En ella se regula la inmediatez de las transferencias que deberá garantizarse con independencia del día o la hora; el dinero deberá llegar a la cuenta del destinatario en un plazo de 10 segundos. El ordenante también debe ser informado en un plazo de diez segundos de si los fondos transferidos se han puesto a disposición del receptor. **Sin cargos extra para el cliente: l**os

cargos aplicados por las transferencias inmediatas en euros no podrán ser superiores a los aplicados a las operaciones convencionales de transferencia «no instantánea» en euros.

Define una transferencia inmediata como: aquella que se ejecuta inmediatamente las veinticuatro horas del día y cualquier día natural. Establece además que: los proveedores de servicios de pago que ofrezcan a sus usuarios de servicios de pago un servicio de pago para el envío y recepción de transferencias deberán ofrecer a todos sus usuarios de servicios de pago un servicio de pago para el envío y la recepción de transferencias inmediatas.

Los proveedores de servicios de pago a que se refiere el párrafo primero velarán por que todas las cuentas de pago que sean accesibles para transferencias sean también accesibles para las transferencias inmediatas las veinticuatro horas del día y cualquier día natural.
Los proveedores de servicios de pago (PSP) que estén localizados en un Estado miembro y cuya moneda sea el euro deberán ofrecer: el servicio de recepción de transferencias inmediatas a partir del 9-1-2025 y. el servicio de envío de transferencias inmediatas a partir del 9-10-2025.

Características esenciales del nuevo Reglamento:
1ª El servicio de garantía de la verificación debe prestarse, en la medida de lo posible, de conformidad con un conjunto de reglas y normas a escala de la Unión, a fin de fomentar una aplicación sin trabas e interoperable. Este conjunto de reglas y normas podría ser elaborado por organizaciones compuestas por proveedores de servicios de pago o que los representen.
2. Autorizar una transferencia en la que no se haya verificado el beneficiario puede dar lugar a la transferencia de fondos a un beneficiario no intencionado. Los proveedores de servicios de pago no deben ser considerados responsables de la ejecución de una operación enviada a un beneficiario no intencionado por causa de un identificador único incorrecto, tal como se establece en el artículo 88 de la Directiva (UE) 2015/2366, en la medida en que los proveedores de servicios de pago hayan prestado correctamente el servicio que garantice la verificación. No obstante, cuando los proveedores de servicios de pago, incluidos los proveedores de servicios de iniciación de pagos no presten correctamente dicho servicio y esto dé lugar a una operación de pago ejecutada de manera defectuosa, dichos proveedores de servicios de pago deberán reembolsar sin demora el importe transferido al ordenante y, cuando proceda, restablecer el saldo de la cuenta de pago en la cual se haya efectuado el adeudo a la situación en la que habría estado si no hubiera tenido lugar la operación de pago. Los proveedores de servicios de pago deben informar a los usuarios de servicios de pago de las consecuencias que la decisión de estos últimos de desatender una notificación facilitada con arreglo al presente Reglamento modificativo tenga con respecto a la responsabilidad y los derechos al reembolso de los usuarios de los servicios de pago.
3. Los proveedores de servicios de pago necesitan tiempo suficiente para cumplir las obligaciones establecidas en el presente Reglamento modificativo. Procede, por tanto, introducir gradualmente

esas obligaciones, permitiendo a los proveedores de servicios de pago un uso más eficiente de sus recursos. Por lo tanto, la obligación de ofrecer el servicio de pago para el envío de transferencias inmediatas debe aplicarse posteriormente, precedida por la obligación de ofrecer el servicio de pago para la recepción de transferencias inmediatas, ya que el envío de transferencias inmediatas tiende a ser el servicio más costoso y complejo de los dos que deben ejecutarse y, por lo tanto, su ejecución requiere más tiempo. El servicio de garantía de la verificación es pertinente para los proveedores de servicios de pago en el caso del envío de transferencias.
Los proveedores de servicios de pago deben tener implantadas medidas sólidas y actualizadas de detección y prevención del fraude, diseñadas para evitar que se envíe una transferencia a un beneficiario no deseado como consecuencia de un fraude o error, dado que el ordenante podría no poder recuperar los fondos antes de que se abonen en la cuenta del beneficiario.

4. Por lo tanto, ningún tipo de comisión cobrada a ordenantes y beneficiarios por la ejecución de transferencias inmediatas en euros, incluidas las comisiones por operación o las comisiones a tanto alzado, debe ser superior a la comisión aplicada al mismo usuario de servicios de pago para los tipos equivalentes de otras transferencias en euros.

5. Las comisiones cobradas por un proveedor de servicios de pago a ordenantes y beneficiarios en relación con el envío y la recepción de transferencias inmediatas no serán superiores a las comisiones cobradas por dicho proveedor de servicios de pago en relación con el envío y la recepción de otras transferencias de tipo equivalente.

Los proveedores de servicios de pago radicados en un Estado miembro cuya moneda sea el euro cumplirán lo dispuesto en el presente artículo a más tardar el 9 de enero de 2025.

6. El *Artículo 5 "quater" desarrolla la :* **Verificación del beneficiario en el caso de las transferencias.** El proveedor de servicios de pago del ordenante le ofrecerá a este un servicio de garantía de la verificación del beneficiario al que el ordenante tenga la intención de enviar una transferencia (servicio de garantía de la verificación). El proveedor de servicios de pago del ordenante prestará el servicio de garantía de verificación inmediatamente después de que el ordenante facilite la información pertinente sobre el beneficiario y antes de que se le ofrezca la posibilidad de autorizar dicha transferencia. El proveedor de servicios de pago del ordenante ofrecerá el servicio de garantía de la verificación con independencia del canal de iniciación del pago utilizado por el ordenante a fin de cursar una orden de pago para la transferencia

La problemática del servicio de validación de cuentas del nuevo Reglamento es que se basa en cruces de IBAN y nombre de beneficiario, y como sabemos algunos atributos del nombre del beneficiario a cuya cuenta el ordenante desea realizar una transferencia, como la presencia de

signos diacríticos o diferentes transliteraciones posibles de nombres en otros alfabetos, diferencias entre los nombres de uso habitual y los nombres indicados en los documentos oficiales, podrían dar lugar a una situación en la que el nombre del beneficiario facilitado por el ordenante y el nombre asociado al identificador de la cuenta de pago que se especifica en el punto 1, letra a), del anexo del Reglamento (UE) n.º 260/2012 (identificador de la cuenta de pago), que fue facilitado por el ordenante, no coinciden de forma exacta, pero sí casi exacta. En tales casos, para evitar una fricción indebida en el tratamiento de las transferencias en euros y facilitar la decisión del ordenante sobre si proceder o no a la operación prevista, el proveedor de servicios de pago debe indicar al ordenante el nombre del beneficiario asociado al identificador de la cuenta de pago facilitado por el ordenante, de modo que quede asegurado el cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

El servicio de garantía de la verificación debe prestarse, en la medida de lo posible, de conformidad con un conjunto de reglas y normas a escala de la Unión, a fin de fomentar una aplicación sin trabas e interoperable. Este conjunto de reglas y normas podría ser elaborado por organizaciones compuestas por proveedores de servicios de pago o que los representen.

Los proveedores de servicios de pago necesitan tiempo suficiente para cumplir las obligaciones establecidas en el presente Reglamento modificativo. Procede, por tanto, introducir gradualmente esas obligaciones, permitiendo a los proveedores de servicios de pago un uso más eficiente de sus recursos. Por lo tanto, la obligación de ofrecer el servicio de pago para el envío de transferencias inmediatas debe aplicarse posteriormente, precedida por la obligación de ofrecer el servicio de pago para la recepción de transferencias inmediatas, ya que el envío de transferencias inmediatas tiende a ser el servicio más costoso y complejo de los dos que deben ejecutarse y, por lo tanto, su ejecución requiere más tiempo. El servicio de garantía de la verificación es pertinente para los proveedores de servicios de pago en el caso del envío de transferencias.

Por todo ello como conclusión general es que sería un cambio importante disponer del servicio de pagos inmediatos, pero para el sistema de verificación del beneficiario al ser en el momento del pago y basado en los caracteres del nombre y apellido (razón social) del perceptor, nos obligaría a establecer un sistema previo de control al acreditar a un tercero, y a la fecha actual el único sistema posible de verificación de cuentas sería el desarrollado por IBERPAY.

Ciberseguretat en les transaccions bancàries i en la gestió d'avals.

José Manuel Farfán Pérez

Interventor- Tesorero de Administración Local. Tesorero de la Diputación de Sevilla y OPAEF. Tesorero Aguas del Huesna.

http://farfantesoreriamunicipal.blogspot.com.es/

https://www.linkedin.com/in/jos%C3%A9-manuel-farf%C3%A1n-p%C3%A9rez-10249a49/

@ jmfarfanperez

https://tienda.wolterskluwer.es/p/la-gestion-de-la-tesoreria-en-las-entidades-locales

CONSECUENCIAS SUPLANTACIÓN IDENTIDAD

José Manuel Farfán Pérez

Interventor- Tesorero de Administración Local. Tesorero de la Diputación de Sevilla y OPAEF. Tesorero Aguas del Huesna.

http://farfantesoreriamunicipal.blogspot.com.es/

https://www.linkedin.com/in/jos%C3%A9-manuel-farf%C3%A1n-p%C3%A9rez-10249a49/

@ jmfarfanperez

https://tienda.wolterskluwer.es/p/la-gestion-de-la-tesoreria-en-las-entidades-locales

Modelo Bases Ejecución.

El pago de las obligaciones exigibles se efectuará por alguno de los medios que a continuación se detallan:

a) **Se realizarán todos los pagos por transferencia bancaria:** previamente, los acreedores deberán haber remitido a la Tesorería Provincial, la ficha de datos bancarios (Modelo Ficha de Terceros), confeccionada a tal efecto. Los nuevos acreedores facilitarán la ficha de terceros habilitada a efecto. Para pagos transfronterizos a acreedores no residentes, se deberán acompañar los Códigos IBAN, el código BIC.

b) **El cheque bancario tendrá carácter excepcional** y su expedición se realizará únicamente cuando lo exija una disposición administrativa o ante la firma en notarias.

c) **Todo acreedor** u obligado tributario que haya constituido una fianza en la Diputación Provincial o sus Organismos Autónomos por cualquier concepto, **podrá retirar su aval bancario o seguro de caución por medio de representantes autorizados**, mediante poder otorgado en forma legal y bastanteado por la Asesoría Jurídica, o por quienes les hayan sido encomendadas estas funciones. La Tesorería que ejecuta la cancelación de fianzas unirá una fotocopia del bastanteo, diligenciado de conformidad con el original, a las órdenes de cancelación de fianzas para antecedentes y archivo, o bien se realizará diligencia en la caja, en las órdenes de pagos, de los bastanteos que obran en poder de la Tesorería Provincial. En caso contrario, se enviará el documento de aval o seguro, a través del Servicio de Correos mediante la modalidad de acuse de recibo, que suponga una notificación fehaciente, quedando constancia de su entrega.

d) Por formalización a otros conceptos del presupuesto o de operaciones de la tesorería, **se formalizará con los ingresos aplicados que procedan, con el distintivo de "en formalización".**

e) **Se realizará el pago telemático**, mediante la obtención del NRC, y el cargo en cuenta, **en las liquidaciones y autoliquidaciones de la AEAT, de la Junta de Andalucía y cualquier otro ingreso de derecho público**.

f) **Las transferencias y los cargos en cuenta deberán ser firmados electrónicamente.**

g) **La orden de cargo en cuenta podrá ser telemática o con conformación en destino.**

DE LA INTERVENCIÓN FORMAL Y MATERIAL DEL PAGO. RESPONSABILIDAD CONTABLE

Intervención formal	Intervención material
Para la ordenación del pago se intervienen los actos por los que se ordenan pagos con cargo a la Tesorería de la Entidad Local. Dicha intervención tendrá por objeto verificar que las órdenes de pago se dictan por órgano competente, se ajustan al acto de reconocimiento de la obligación y se acomodan al plan de disposición de fondos.	Firmará los documentos que autoricen la salida de los fondos y valores. Si no la encuentra conforme en cuanto a la identidad del perceptor o la cuantía del pago formulará reparo motivado y por escrito.
ACTUACIONES	**ACTUACIONES**
a) Comprobar la acomodación de las órdenes de pago al plan de disposición de fondos.	a) Verificación de la competencia del órgano para la realización del pago
b) Comprobar la existencia de retenciones judiciales o de compensaciones de deudas del acreedor.	b) Comprobar la correcta identidad del perceptor y por el importe debidamente reconocido.
Otras actuaciones: 1. Comprobar cesiones de crédito. 2.Comprobar existencia de Diligencias de embargo	**Otras actuaciones:** 1. Verificar ficha de terceros y datos bancarios.

La Sentencia del Tribunal de Cuentas número 5/2000 de Procedimiento de reintegro por alcance, determina nítidamente el control material y los supuestos de responsabilidad contable, tanto de la Intervención como de la Tesorería en los pagos a realizar.

Sentencia del Tribunal de Cuentas número 5/2000

FUNDAMENTOS DE DERECHO.

INTERVENCION

A la vista de la normativa expuesta resulta patente que en el proceso de disposición de fondos públicos al servicio de los fines a los que se han de destinar, corresponde al ordenador del gasto y al ordenador del pago la función directiva y ejecutiva en materia de contracción y reconocimiento de obligaciones, así como de impulso del proceso de satisfacción de las mismas, teniendo el interventor la responsabilidad de controlar que tanto el gasto autorizado como el pago ordenado se ajustan a la legalidad aplicable y a la realidad de la situación presupuestaria del ente público afectado, pudiendo en el ejercicio de sus funciones producir las notas de reparo que en su caso procedieran, tratando de evitar que en el ciclo presupuestario se produzca cualquier clase de infracción normativa.

En particular le corresponde el seguimiento de las órdenes de pago libradas con el carácter a justificar, examinando y censurando los justificantes, así como reclamándolos en su caso a su vencimiento.

Sentencia del Tribunal de Cuentas número 5/2000

Fundamentos de derecho.
TESORERIA

En este esquema la función del depositario o tesorero dentro del ciclo presupuestario se plantea como una tarea meramente material en cuyo desempeño debe comprobar que el mandamiento de pago que se le libra o presenta **ha sido ordenado por el órgano competente y debidamente intervenido por el órgano de control**, **sin que consten reparos o, en su caso, solventando los mismos.** **Deberá comprobar si sobre el destinatario del pago pesan retenciones judiciales o administrativas de la clase que sean, y practicándolas en su caso así como las que legalmente correspondan.** **En definitiva, la orden de pago recibida por el tesorero, siempre que esté debidamente intervenida, es una orden que está obligado a cumplir.**

Artículo 31.- De la Ordenación del Pago.
Bases Diputación de Sevilla

1. La ordenación del pago corresponde al Presidente en las competencias no delegadas por la Resolución nº 2579/15, modificada por Resolución xxxx, de 18 de enero xxxx **.** A tal efecto, y de conformidad con lo previsto en la normativa vigente, se expedirán por la **Tesorería Provincial las órdenes de pago, a tenor de los estados previsionales diarios en fecha valor,** que tienen como objetivo distribuir en el tiempo las disponibilidades dinerarias para la puntual satisfacción de obligaciones, y en todo caso, se deberá recoger la prioridad de la deuda pública, los gastos de personal y de las obligaciones contraídas en ejercicios anteriores, todo ello bajo el principio de unidad de caja de la Tesorería Provincial, y no discriminación de fondos.

2. El Plan de Tesorería recogerá las previsiones de pago anuales, en cumplimiento de la Ley de Estabilidad Presupuestaria y Sostenibilidad Financiera y de la Orden HAP/2082/14 de 7 de noviembre por la que se desarrollan las obligaciones de suministro de información previstas en la Ley Orgánica 2/2012 de 27 de abril.

3. Deberá comprobarse si sobre el destinatario del pago pesan retenciones judiciales o administrativas de la clase que sean y practicarlas

4. Todos los actos de la ordenación de pagos serán intervenidos por la Intervención Provincial.

SUPLANTACION IDENTIDAD. EFECTOS JURIDICOS.

Juzgado de Primera Instancia Nº 19 de Sevilla. N.I.G: 4109142120220046188.
Tipo y número de procedimiento: Procedimiento Ordinario 1588/2022. Negociado: 1A
Materia: Responsabilidad extracontractual (excluido tráfico) .

Demanda de juicio declarativo ordinario frente al demandado (**Banco Santander**) en la que tras alegar los hechos y fundamentos de derecho que tuvo por convenientes, terminaba suplicando que tras los trámites legales, se dictase sentencia por la que se condenase al demandado a abonarle la suma de 962. 797 euros, más intereses legales de dicha suma, y costas.

El testigo D. Ramón Gavilán, empleado de Santander Digital Services (empresa perteneciente al grupo Santander), en el departamento de tecnología, banca electrónica y ciberfraude nos explica en el acto de la vista de manera clara y comprensible, que el banco no puede realizar bloqueos de transferencias por el motivo alegado por la Gerencia, es decir, que el IBAN no coincide con la razón social del destinatario. Y ello lo explica con datos que clarifican a este juzgador: en el caso que nos ocupa se trata de transferencias SEPA. **Las transferencias SEPA son aquellas en las que el único dato validable es el IBAN, es decir, tras la comprobación por parte del banco que este dato está correctamente indicado, la transferencia se realiza con normalidad.**

A las alegaciones realizadas sobre este punto por parte de la Gerencia, de que el que NIF y la razón social o beneficiario son campos obligatorios para poder realizar dichas transferencias y que el banco debería haberlos comprobado, el Sr. Gavilán nos explica que son campos que deben aparecer rellenos formalmente, pero que en ningún caso son validables. En conclusión, si el IBAN es válido y existente, la transferencia se realiza a la cuenta correspondiente a dicho IBAN, independientemente de lo que se haya indicado, materialmente, en los otros campos.

Estas manifestaciones, además, se ven apoyadas en las instrucciones **del Cuaderno 34** de la Asociación Española de Banca, que especifica que las transferencias no podrán realizarse si no constan los datos que aparecen como obligatorios, reafirmando que se trata de unos datos que deben estar cumplimentados formalmente, en ningún caso a su validación.

CONCLUSIONES

En una transferencia es muy importante **introducir correctamente el número de cuenta** (en la zona SEPA, el IBAN) del beneficiario pues la entidad del ordenante ejecutará la operación basándose en éste de forma automática, sin más comprobación, ni del ordenante, ni del beneficiario. La normativa de servicios de pago tampoco establece el deber de las entidades de comprobar que el nombre del beneficiario se corresponde con el del titular del número de cuenta de destino de la transferencia ni otros datos adicionales, más allá de la coincidencia del IBAN beneficiario con el indicado en la orden de pago.

En este contexto, en el asunto C-245/18, **el TJUE** analizó una **cuestión prejudicial** planteada por un tribunal italiano, referente a la interpretación de los artículos 741 y 75 de la citada Directiva 2007/64/CE (actualmente derogada por la Directiva 2015/2366), con respecto al abono de una transferencia por parte del proveedor de servicios de pago del beneficiario, pues resultaba en ese caso que la operación se había cursado indicando el ordenante un IBAN o identificador único erróneo y el banco de destino, proveedor de servicios de pago del beneficiario, no había comprobado que el IBAN no se correspondía con el nombre de la persona designada como beneficiaria en la propia operación. **Pues bien, en el referido asunto, el TJUE ha declarado que el artículo 74, apartado 2, de la directiva debe interpretarse en el sentido de que, cuando una orden de pago se ejecute de acuerdo con el identificador único facilitado por el usuario de servicios de pago y tal identificador no corresponda al nombre del beneficiario indicado por ese mismo usuario, la limitación de la responsabilidad del proveedor de servicios de pago establecida en esa disposición se aplicará tanto al proveedor de servicios de pago del ordenante como al del beneficiario. En consecuencia, cuando una transferencia se ejecuta conforme al identificador único (IBAN), se considera correctamente ejecutada en relación con el beneficiario indicado, no siendo responsable la entidad de la ejecución defectuosa cuando el identificador único facilitado por el usuario fuera incorrecto, según el artículo 59 Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera)**.

La transferencia se dirige a un IBAN de forma automática, sin comprobación por la entidad del ordenante ni del beneficiario. Igualmente, los demás datos consignados en la orden (entre ellos, el concepto) son mensajes destinados al beneficiario, no a la entidad. En virtud de la irrevocabilidad de las transferencias, las cantidades abonadas en cuenta al beneficiario solo podrán ser retrotraídas si mediara el consentimiento de éste o la preceptiva orden o mandato legal o judicial, no estando facultadas las entidades para retroceder la transferencia sin consentimiento del beneficiario, o sin la concurrencia de errores demostrables, siempre que se acredite que el error en el que se pudo incurrir no era imputable al ordenante.

En este mismo sentido se pronuncia el Banco de España ante consultas formuladas y en sus memorias de reclamaciones en distintos años.

RESPONSABILIDAD DEL PROVEEDOR SERVICIOS DE PAGO. TRANSFERENCIA ELECTRÓNICA ERRÓNEA.

Ni el proveedor de servicios de pago del ordenante ni el del beneficiario están obligados a verificar si el identificador único (IBAN) proporcionado por el usuario corresponde efectivamente a la persona designada como beneficiaria. No existe disposición normativa que imponga a los proveedores de servicios de pago un deber adicional de diligencia en función de circunstancias específicas, como la identidad del beneficiario, el concepto o el importe de la transferencia. La responsabilidad del proveedor se limita a ejecutar correctamente la orden de pago de acuerdo con el identificador único facilitado por el ordenante. STS 507/2025, 27 de Marzo de 2025 *(Sentencia Reciente)*

MEDIOS DE PAGO

- **Pago en efectivo/pago en metálico: NO .RECOMENDACIONES OCEX DE SUPRESION.**
- **Cheque: EXCEPCIONAL**
- **Domiciliación bancaria: NO.** *(Informe de la IGAE de 14 de junio de 1996, no los admite ni para ACF)*
- **Cargo en cuenta: EXCEPCIONAL** *.Entidades financieras / AEAT /Tributos .* ***NRC***
- **Tarjeta:** *Utilizable en ACF y PJ con un solo habilitado- pagador. TARJETA MONEDERO*
- **Bizum:** *Equivale a tarjeta. Autorización.* ***ACF***
- **Transferencia bancaria. MEDIO MAS COMUN Y SEGURO**
- **Descuentos en pagos.**
- **Compensación de deudas.**
- **Pago en especie.**

El art. 198.2 del TRLRHL dispone que las Entidades Locales podrán pagar sus obligaciones por cualquiera de los siguientes medios :

"efectivo, transferencias, cheques o cualquier otro medio o documento de pago, sean o no bancarios, que se establezcan"

Con esta expresión **«medios o documento de pago que se establezcan»,** el TRLRHL está remitiendo a la **normativa interna** de cada una de las entidades locales la decisión última sobre cuáles serán los medios de pago que va a utilizar la entidad local en cuestión.

PAGO POR TRANSFERENCIA. TIPOS DE TRANSFERENCIAS

- **TRANSFERENCIA SEPA** (acrónimo de Single-Euro Payment Zone)
- SEPA. zona única de pagos en euros. Compuesta por 36 países, los 27 países miembros de la UE y seis países más (Islandia, Liechtenstein, Mónaco, Noruega, San Marino y Suiza).
- Es necesario conocer el IBAN del beneficiario (identificador único).
- El IBAN (International Bank Account Number) es un código bancario internacional que identifica de forma única cada cuenta bancaria en el espacio SEPA .En España, el IBAN consta de 24 caracteres y sirve para realizar transferencias nacionales e internacionales, facilitando el proceso de pago
- **TRANSFERENCIA INTERNACIONAL**, fuera de la zona SEPA. Es necesario conocer el código SWIFT/BIC del beneficiario (identificador único)
- Coste: según importe enviado, urgencia y comisiones bancarias. Cambio de divisas.
- AGE: Orden PCM/917/2021, de 1 de septiembre, por la que se regula el procedimiento para el pago en el exterior y el pago en divisas de las obligaciones de la Administración General del Estado.
- **Libertad del acreedor en la designación de la cuenta bancaria para recibir el pago, la normativa no establece ninguna limitación**.

PAGOS INDEBIDOS / VERSUS SUPLANTACION

- Definición: El pago indebido es el que se realiza por error material, aritmético o de hecho, en favor de persona en quien no concurra derecho alguno de cobro frente a la Administración con respecto a dicho pago o en cuantía que excede de la consignada en el acto o documento que reconoció el derecho del acreedor.

- Ni el TRLRHL ni el RD encontramos regulación sobre los pagos indebidos. El artículo 77 de la LGP recoge dos posibilidades: pagos indebidos (en sentido estricto) y revisión de los actos de los que se deriven reintegros distintos a los correspondientes a los pagos indebidos. **PROCEDIMENTO DE REINTEGRO DE PAGOS.**

- El perceptor de un pago indebido queda obligado a su restitución.

- Ejemplo: pago sin retención de IRPF

- Regla especial para el caso de errores materiales en el pago de la nómina: el art. 5 del Decreto 680/1974, de 28 de febrero permite su reintegro “deduciéndolas de los siguientes libramientos que se formulen”.

EVOLUCION CIBERSEGURIDAD

1. **Fraude al CEO**. *Hace más de 10 años.*

2. **Originales y certificados**. *No seguridad.* NO SEDE.
   a) Certificados falsos y no CSV
   b) Vigilábamos escaneo y tipo de letras.

FRAUDE: Procesos malas prácticas versus ciberseguridad.

SUPLANTACION IDENTIDAD MEDIDAS INICIALES

1. **Fraudes SMS.**
2. **No correos electrónicos. NO TELEFONO……**

Instrucciones precisas.

SITUACION ACTUAL SEDE ELECTRONICA. *Seguridad.*

1. **VALIDe.**
2. **Firma digital certificados.**
3. **Tesorería gestión fichas terceros y mantenimiento cuentas. Limitaciones.**

La Tesorería debe tener su propia plataforma con autonomía para gestionar pagos con criterios de seguridad.

Todas las operaciones se realizarán por canal seguro de transmisión. **SEDE ELETRONICA Y WEB BANCARIA. CUENTA FACE VERSUS CUENTA ACREDITADA.**

Ejecución de Pagos

PSD2 (nueva directiva de pagos, Directiva (EU) 2015/2366)

LA ORDENACION DEL PAGO.

Posicion de tesoreria. Estados previsionales Pdf y presupuesto de Tesoreria.

Actualmente el desarrollo de la Ley de servicios de pagos (Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago) que incorpora la Directiva 2007/64/CE, PSD2 (nueva directiva de pagos, Directiva (EU) 2015/2366) el desarrollo de la nueva Directiva Europea sobre pagos (conocida por PSD2)

1. Preparación: El tesorero elabora la fase P (ordenación de pagos) y la orden de transferencia firmada electrónicamente por los tres claveros autorizados para pagos.

2. Subida de Fichero: Se sube el fichero CSB 34 por terminal banco. **DIFERENCIA EN CADA ENTIDAD FINANCIERA.**

3. Autentificación: Se utiliza la doble autenticación para la ejecución del pago, cumpliendo con los requisitos de la PSD2. MOVIL….

Deberá comprobarse si sobre el destinatario del pago pesan retenciones judiciales o administrativas de la clase que sean y practicarlas.

REQUISITOS PARA LA ORDENACIÓN DEL PAGO:

Datos fiscales y bancarios suministrados a la Tesorería Provincial, a través de la ficha de terceros en Tesorería (dipusevilla.es) / *Google: "Tesorería Diputación de Sevilla"*

GESTION DE PAGOS: TRANSFERENCIAS INMEDIATAS Y VERIFICACION DE CUENTAS DE TERCEROS

Actualidad

El refuerzo de la seguridad introducido por la directiva PSD2 (Payment Services Directive 2) evita los pagos online no autorizados y evita que se pueda hacer uso de una tarjeta de crédito robada gracias a los procedimientos PSD2 de SCA de doble factor de autenticación.

SCA son las siglas de la expresión anglosajona "Strong Customer Authentication", que se refiriere directamente como **autenticación reforzada**. Este concepto hace referencia a todo un conjunto de herramientas que pretenden proteger los servicios de pago online de peligros como fraude, robo de credenciales o transferencias de fondos ilegales.

En definitiva, para ejecutar cualquier pago se necesitan dos factores: **autenticación y transmisión por canal seguro** y además hay que generar un código único asociado al importe y beneficiario. Esto hace que p.ej. una orden por e-mail no cumpla PSD2. No podemos enviar una orden de cargo o transferencia al banco por mail o fax ya que no cumple los requisitos de la PSD2.**NO CONFIRMACION EN DESTINO**

Como resumen para firmar operaciones (**especialmente pagos**):
1.Se requiere firmar por la app de firma (que pide PIN, huella, etc) o bien con un token. NO DESTION
2.Las tarjetas de coordenadas no cumplen PSD2 y los SMS tienen vulnerabilidades (Scam, Phishing)
3. Payment Services Directive 3 (PSD3)
Extensión de la verificación de IBAN/nombre para pagos instantáneos
Mejora de la Strong Customer Authentication (SCA)

SUPLANTACION IDENTIDAD. EFECTOS JURIDICOS.

VER EN LA MESA REDONDA

Juzgado de Primera Instancia Nº 19 de Sevilla. N.I.G: 4109142120220046188.
Tipo y número de procedimiento: Procedimiento Ordinario 1588/2022. Negociado: 1A
Materia: Responsabilidad extracontractual (excluido tráfico) .

Demanda de juicio declarativo ordinario frente al demandado (**Banco Santander**) en la que tras alegar los hechos y fundamentos de derecho que tuvo por convenientes, terminaba suplicando que tras los trámites legales, se dictase sentencia por la que se condenase al demandado a abonarle la suma de 962. 797 euros, más intereses legales de dicha suma, y costas.

El testigo D. Ramón Gavilán, empleado de Santander Digital Services (empresa perteneciente al grupo Santander), en el departamento de tecnología, banca electrónica y ciberfraude nos explica en el acto de la vista de manera clara y comprensible, que el banco no puede realizar bloqueos de transferencias por el motivo alegado por la Gerencia, es decir, que el IBAN no coincide con la razón social del destinatario. Y ello lo explica con datos que clarifican a este juzgador: en el caso que nos ocupa se trata de transferencias SEPA. **Las transferencias SEPA son aquellas en las que el único dato validable es el IBAN, es decir, tras la comprobación por parte del banco que este dato está correctamente indicado, la transferencia se realiza con normalidad.**

A las alegaciones realizadas sobre este punto por parte de la Gerencia, de que el que NIF y la razón social o beneficiario son campos obligatorios para poder realizar dichas transferencias y que el banco debería haberlos comprobado, el Sr. Gavilán nos explica que son campos que deben aparecer rellenos formalmente, pero que en ningún caso son validables. En conclusión, si el IBAN es válido y existente, la transferencia se realiza a la cuenta correspondiente a dicho IBAN, independientemente de lo que se haya indicado, materialmente, en los otros campos.

Estas manifestaciones, además, se ven apoyadas en las instrucciones del Cuaderno 34 de la Asociación Española de Banca, que especifica que las transferencias no podrán realizarse si no constan los datos que aparecen como obligatorios, reafirmando que se trata de unos datos que deben estar cumplimentados formalmente, en ningún caso a su validación.

CONCLUSIONES

En una transferencia es muy importante introducir correctamente el número de cuenta (en la zona SEPA, el IBAN) del beneficiario pues la entidad del ordenante ejecutará la operación basándose en éste de forma automática, sin más comprobación, ni del ordenante, ni del beneficiario. La normativa de servicios de pago tampoco establece el deber de las entidades de comprobar que el nombre del beneficiario se corresponde con el del titular del número de cuenta de destino de la transferencia ni otros datos adicionales, más allá de la coincidencia del IBAN beneficiario con el indicado en la orden de pago.

En este contexto, en el asunto C-245/18, **el TJUE** analizó una **cuestión prejudicial** planteada por un tribunal italiano, referente a la interpretación de los artículos 741 y 75 de la citada Directiva 2007/64/CE (actualmente derogada por la Directiva 2015/2366), con respecto al abono de una transferencia por parte del proveedor de servicios de pago del beneficiario, pues resultaba en ese caso que la operación se había cursado indicando el ordenante un IBAN o identificador único erróneo y el banco de destino, proveedor de servicios de pago del beneficiario, no había comprobado que el IBAN no se correspondía con el nombre de la persona designada como beneficiaria en la propia operación. Pues bien, en el referido asunto, el TJUE ha declarado que el artículo 74, apartado 2, de la directiva debe interpretarse en el sentido de que, cuando una orden de pago se ejecute de acuerdo con el identificador único facilitado por el usuario de servicios de pago y tal identificador no corresponda al nombre del beneficiario indicado por ese mismo usuario, la limitación de la responsabilidad del proveedor de servicios de pago establecida en esa disposición se aplicará tanto al proveedor de servicios de pago del ordenante como al del beneficiario. **En consecuencia, cuando una transferencia se ejecuta conforme al identificador único (IBAN), se considera correctamente ejecutada en relación con el beneficiario indicado, no siendo responsable la entidad de la ejecución defectuosa cuando el identificador único facilitado por el usuario fuera incorrecto, según el artículo 59 Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera)**.

La transferencia se dirige a un IBAN de forma automática, sin comprobación por la entidad del ordenante ni del beneficiario. Igualmente, los demás datos consignados en la orden (entre ellos, el concepto) son mensajes destinados al beneficiario, no a la entidad. En virtud de la irrevocabilidad de las transferencias, las cantidades abonadas en cuenta al beneficiario solo podrán ser retrotraídas si mediara el consentimiento de éste o la preceptiva orden o mandato legal o judicial, no estando facultadas las entidades para retroceder la transferencia sin consentimiento del beneficiario, o sin la concurrencia de errores demostrables, siempre que se acredite que el error en el que se pudo incurrir no era imputable al ordenante.

En este mismo sentido se pronuncia el Banco de España ante consultas formuladas y en sus memorias de reclamaciones en distintos años.

RESPONSABILIDAD DEL PROVEEDOR SERVICIOS DE PAGO. TRANSFERENCIA ELECTRÓNICA ERRÓNEA.

Ni el proveedor de servicios de pago del ordenante ni el del beneficiario están obligados a verificar si el identificador único (IBAN) proporcionado por el usuario corresponde efectivamente a la persona designada como beneficiaria.

No existe disposición normativa que imponga a los proveedores de servicios de pago un deber adicional de diligencia en función de circunstancias específicas, como la identidad del beneficiario, el concepto o el importe de la transferencia.

La responsabilidad del proveedor se limita a ejecutar correctamente la orden de pago de acuerdo con el identificador único facilitado por el ordenante.

STS 507/2025, 27 de Marzo de 2025 (Sentecia Reciente)

GESTION DE PAGOS: TRANSFERENCIAS INMEDIATAS Y VERIFICACION DE CUENTAS DE TERCEROS

Actualidad.
La gestión de pagos se circunscribe a un esquema de objetivos de: eficiencia y seguridad.

a) Eficiencia: alude a los costes de emisión de pagos y sus formas de realización. En un esquema de automatización de operaciones.

b) Seguridad: estableciendo un conjunto de requisitos mínimos de seguridad en la lucha contra el fraude (protocolo de buenas prácticas). Dado que la suplantación de identidad y los fraudes en los procesos de pagos es moneda común de estos tiempos.

Las transferencias realizadas a través de los proveedores de servicios de pago (PSP), en terminología de PSD2 (nueva directiva de pagos, Directiva (EU) 2015/2366), ya que es el medio de pago más frecuente utilizado por las Empresas y Administraciones Públicas.

Gracias a la **PSD2** se introducen controles de seguridad que evitan fraudes online como la suplantación de identidad. De esta forma, **es impracticable que un posible infractor pueda realizar operaciones en nuestro nombre y acceder a los productos y servicios contratados.**

GESTION DE PAGOS: TRANSFERENCIAS INMEDIATAS Y VERIFICACION DE CUENTAS DE TERCEROS

El refuerzo de la seguridad introducido por la **directiva PSD2** evita los pagos online no autorizados y evita que se pueda hacer uso de una tarjeta de crédito robada gracias a los procedimientos **PSD2 de SCA de doble factor de autenticación.**

SCA son las siglas de la expresión anglosajona "Strong Customer Authentication", que se refiriere directamente como autenticación reforzada. Este concepto hace referencia a todo un conjunto de herramientas que pretenden proteger los servicios de pago online de peligros como fraude, robo de credenciales o transferencias de fondos ilegales.

En definitiva, para ejecutar cualquier pago se necesitan dos factores: autenticación y transmisión por canal seguro y además hay que generar un código único asociado al importe y beneficiario. Esto hace que p.ej. una orden por e-mail no cumpla PSD2. No podemos enviar una orden de cargo o transferencia al banco por mail o fax ya que no cumple los requisitos de la PSD2.

Como resumen para firmar operaciones (especialmente pagos):

- Se requiere firmar por la app de firma (que pide PIN, huella, etc) o bien con un token
- Las tarjetas de coordenadas no cumplen PSD2 y los SMS tienen vulnerabilidades (Scam, Phishing)

1. En definitiva, dicha Directiva ha aumentado la seguridad en las transacciones, pero a la vez se está produciendo un fenómeno de incremento de la ciberdelincuencia en dichos procesos, a través de la suplantación de identidad en los procesos de acreditación de terceros.

2. Este tipo de fraudes de suplantación de identidad de terceros acreedores legítimos es más común en el sector empresarial, dado que la Administración utiliza preponderantemente las sedes electrónicas.

La sede electrónica necesita un medio de acreditación seguro (normalmente a través de certificado digital), y la firma electrónica en esa sede permite acreditar la autenticidad de la expresión de voluntad consentimiento del acreedor, así como la integridad e inalterabilidad del documento.

En el supuesto de que no se disponga de sede electrónica en las Empresas, se solicitaran documentos originales. Con el objeto de evitar que la obligación formal y material de pago sea correcta y no hay error en el pago el tercero tiene que justificar la titularidad de cuenta corriente, podrá presentar certificado bancario o ficha de tercero firmada por él y por la entidad bancaria que acredite que ese número de cuenta es del titular. La declaración jurada de titularidad de cuenta corriente no se debe permitir por los posibles efectos de falsedad documental.

Es necesario que los certificados de titularidad de cuentas deban venir sellados digitalmente o con CSV (conjunto de dígitos que identifica de forma única los documentos electrónicos emitidos por cualquier), y poder utilizar por ejemplo **VALIDe** (servicio on-line ofrecido por el Ministerio de Política Territorial y Función Pública para la validación de Firmas y Certificados electrónicos), que validaría la firma del documento y podríamos cotejarlo.

En la gestión de pagos se debe **elaborar un documento normativo interno** (“compliance”), que sea un código de conducta que evita las malas prácticas y minimice los riesgos de las transacciones, por ejemplo: prohibiciones de correos electrónicos, SMS o el teléfono para acreditarse los terceros.

Si tenemos una **suplantación de identidad por estas malas prácticas** comentadas no ha tenido el pago efectos liberatorios de la cantidad satisfecha porque no se ha producido un ingreso real en el patrimonio del titular de la misma, exigiéndose la identidad e integridad de la prestación convenida, en opinión de la Jurisprudencia del Tribunal Supremo (STS 521/2001, de 25 de mayo).

En una transferencia es muy importante **introducir correctamente el número de cuenta** (en la zona SEPA, el IBAN) del beneficiario pues la entidad del ordenante ejecutará la operación basándose en éste de forma automática, sin más comprobación, ni del ordenante, ni del beneficiario.

La normativa de servicios de pago **tampoco establece el deber de las entidades de comprobar que el nombre del beneficiario** se corresponde con el del titular del número de cuenta de destino de la transferencia ni otros datos adicionales, más allá de la coincidencia del IBAN beneficiario con el indicado en la orden de pago.

COBROS Y PAGO DE OBLIGACIONES.
ADMINISTRACIÓN ELECTRÓNICA

Recaudar derechos y pagar obligaciones y cuanto derive de lo anterior es competencia de la Tesorería Local, es una función necesaria y reservada a Funcionarios con Habilitación Nacional, y en este campo si se han producido evoluciones importantes. Las actividades más desarrolladas han sido:

1. **La generalización de los CSB.** Problemática PSD 2 y la confirmacion en destino. Doble autenticacion. Psd2.

2. Factura Electrónica y el Registro Contable. Seguridad transacciones y validacion cuentas. Actual sede electronica.
https://www.dipusevilla.es/la-diputacion/areas/area-de-hacienda/tesoreria/
LIMITAR LA MODIFICCION DE CUANTAS. PERMISO SELECTIVOS.

3. VALIDAR CUENTAS CON IBERPAY.

4. **PAGOS CUENTAS FACE VERSUS ACREDITADA.**

TEXTO QUE FIRMA EL PRESENTADOR

"A partir de la fecha de presentación de esta ficha todos los pagos de la Diputación de Sevilla a nuestro favor deberán realizarse a la cuenta anteriormente señalada, de nuestra titularidad, **responsabilizándome** de la veracidad de los datos señalados."

ESENCIAL PARA PERSONAS FISICAS. PROBLEMAS IBERPAY FUTUROS.

"El solicitante se responsabiliza de los datos detallados anteriormente quedando la Excma. Diputación de Sevilla exonerada de cualquier responsabilidad derivada de errores u omisiones en los mismos. "

"De conformidad con el Reglamento Europeo de Protección de Datos Personales y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de derechos digitales, le informamos que los datos que se recogen en esta solicitud/formulario serán objeto de tratamiento por la Tesorería y/o área/servicio en la actividad de tratamiento de tercero de la cual es responsable la DIPUTACIÓN DE SEVILLA con la finalidad y legitimación de que se detalla en el Registro de Actividades de Tratamiento Puede usted obtener más información sobre Protección de Datos Personales en este enlace a la Política de Privacidad y Protección de Datos de la Diputación de Sevilla. Igualmente puede usted ejercer sus derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, presencialmente, ante el responsable, Diputación de Sevilla, Av Menéndez y Pelayo, 32, C.P: 41071 o bien en el siguiente enlace a su Sede Electrónica"

PARA PODER VALIDAR CUENTAS IBERPAY: **SOLICITAR AUTORIZACION.**

MODELO PAIS VASCO: **Autorizo a la Oficina de Control Económico del Departamento de Economía y Hacienda a verificar los datos arriba indicados.**

AUTORIZACIÓN PARA LA CONSULTA Y VALIDACIÓN DE DATOS.
Diputación de Sevilla.

El solicitante autoriza expresamente a la Excma. Diputación de Sevilla a realizar las gestiones necesarias ante la entidad bancaria proveedora de los datos bancarios facilitados en este documento, con el fin de verificar la exactitud y validez de dichos datos.

Esta autorización incluye la facultad de la Excma. Diputación de Sevilla para solicitar confirmación de la titularidad de la cuenta, así como cualquier otro dato relacionado que sea necesario para la correcta ejecución de los pagos y transacciones previstas.

Asimismo, el solicitante consiente de manera inequívoca que la Excma. Diputación de Sevilla pueda consultar y procesar sus datos personales a través de otras administraciones públicas u organismos gubernamentales, en la medida en que dicha consulta sea necesaria para la verificación de la información suministrada, el cumplimiento de obligaciones legales, la prevención de fraudes o cualquier otro propósito legítimo conforme a la normativa aplicable en materia de protección de datos y administración pública. El solicitante reconoce y acepta que dichas consultas y validaciones son indispensables para la adecuada gestión y tramitación de su solicitud, así como para el mantenimiento de la seguridad, transparencia y eficiencia de los procesos administrativos involucrados.

El solicitante declara ser el titular legítimo de los datos personales y bancarios proporcionados y asume la responsabilidad de informar a la Excma. Diputación de Sevilla sobre cualquier cambio o actualización relevante de los mismos. Esta autorización se otorga sin perjuicio de los derechos que asisten al solicitante en materia de protección de datos, incluyendo, entre otros, el derecho de acceso, rectificación, limitación del tratamiento, supresión, portabilidad de los datos y oposición, los cuales podrán ser ejercidos conforme a la normativa vigente."

SITUACION ACTUAL TRANSACCIONES

1. RDL 19/2018. **Autenticacion reforzada**. Contraseña.movil.token.telefono. Orden movil no cumple PSD2.
    1. Uso combinado de **mas de dos elementos** y canal seguro (web propia)
    2. Problemática de falta de homogeneidad.
2. Tarjetas prepago anonimas. Proliferacion servicios sociales.
3. Mit. Tarjetas autenticacion pedida por entidad local.
4. Firma digital de ficheros.editran y sftp.
5. Avancemos en IBERPAY. Validacion tercero/entidad financiera.

En la actualidad a través de IBERPAY, que es la empresa privada que gestiona el Sistema Nacional de Compensación Electrónica (SNCE) del sistema español de pagos al por menor, y sus accionistas son las entidades participantes en el SNCE (Sistema Nacional de Compensación Electrónica), existe un proyecto para que podamos validar las cuentas de nuestros acreedores de forma fidedigna. Este servicio será online 24x7, con respuesta en tiempo real y con alcance de +75M cuentas (99% cuentas españolas), trata de ayudar a la prevención del fraude (Validación de titularidad inmediata), en un sistema con integración en la web o en sistemas de gestión del cliente (participante indirecto). Tendrá un bajo coste, pero tiene un coste interbancario. La Infraestructura será de IBERPAY

En la actualidad ya está implementado para operaciones entre entidades y clientes de esa entidad.

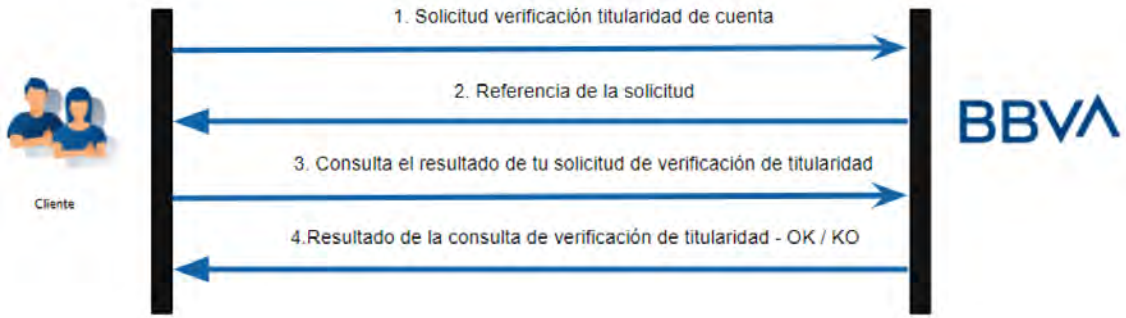
IBERPAY

SITUACION ACTUAL TRANSACCIONES. ESQUEMA IBERPAY

Verificación de titularidad de cuenta tiene 2 funcionalidades:

- Solicitud de verificación de titularidad.
- Consulta el estado de la verificación de titularidad.

- **El proceso de validación** se realizará desde el menú de SICAL del MODULO DE TERCEROS-TESORERIA y afectará a las cuentas registradas en esta base de datos y en cualquiera de las entidades restantes (5 entes dependientes mas)
- Para realizar el proceso de verificación se habilitará una nueva opción (mediante un botón) en el mantenimiento de datos bancarios de terceros .
- Este botón se mostrará en rojo cuando haya datos pendientes de validar (Si queréis también se podría avisar enviando un correo electrónico a quien consideréis).
- Desde él se accederá a una consulta donde, por defecto, aparecerán los datos pendientes de verificación para poder realizarla. Aunque se podrán consultar todos los datos validados hasta el momento.
- El proceso de verificación se puede hacer de varias formas:
  a) De todo lo que está pendiente de verificar.
  b) El usuario indica/selecciona los datos a verificar que considere (*creo que es la mejor, sobre todo si hay alguna urgencia y hay mucho datos a verificar*)
- A partir de la implantación, las cuentas bancarias se crearán en un estado "pendiente de verificar" y no serán accesibles para su uso hasta ser verificadas y con resultado correcto. (*De todas formas, creo que se debería añadir alguna activación manual por si no se pudiese llevar a cabo el proceso de verificación porque la api de BBVA no esté disponible, problemas de conexión, etc...*)
- Si la validación de la cuenta devuelve incorrecto (Ko) cual de las siguientes actuaciones os parece bien:
  - Pasa a estado borrada.
  - Pasa a estado borrada y en las observaciones se guarda "cuenta validada con resultado incorrecto".
  - Pasa a estado verificada con resultado KO, un estado nuevo con las mismas características que el estado borrada, es decir, invisible e inaccesible desde la consulta.
  - Pasa a estado verificada con resultado KO, un estado nuevo con características parecidas al de borrada, dato inaccesible pero visible al consultar.
- En el mantenimiento de las cuentas bancarias de tercero, para identificar si la cuenta ha sido verificada y/o se ha registrado después de la versión de verificación o con anterioridad, he pensado añadir a la pantalla los datos de fecha de alta, la cual aparecerá en las altas realizadas a partir de la puesta en producción, para el resto este dato se mostrará como '01/01/1900'. Además, para saber si la cuenta ha sido validada o no, se añadirá otra columna con la fecha de verificación, que se mostrará si se ha verificado correctamente. O, en función de lo que decidáis en el apartado anterior, se mostrará la fecha de verificación y el estado de la misma (correcto o incorrecto).



- El usuario realiza la solicitud de verificación de titular a través del servicio API de BBVA. Informa para ello el IBAN de la cuenta, el nombre del titular, el tipo de identificación y el número de identificación (NIF/CIF/NIE/Pasaporte/...)

- BBVA verifica el formato y genera una referencia de la solicitud. Ésta es un código unívoco de cada petición. Además, completa el resto de datos e inicia la verificación de los datos facilitados

- El usuario consulta el resultado de la solicitud vía API a BBVA, indicando para ello la referencia de la solicitud. Como respuesta, recibirá uno de los siguientes valores:
  - OK, en caso de correspondencia y cuenta activa
  - KO, en caso de no correspondencia o cuenta inactiva

Recientemente se ha aprobado en la Unión Europea, el 13 de marzo: Reglamento (UE) 2024/886 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, por el que se modifican los Reglamentos (UE) Nº 260/2012 y (UE) 2021/1230 y las Directivas 98/26/CE y (UE) 2015/2366 en lo que respecta a las transferencias inmediatas en euros.

Objetivo	Mejorar la seguridad y eficiencia en los pagos de la Administración Local
Alcance	Todas las transacciones financieras realizadas por entidades locales
Medidas Clave	Autenticación reforzada, validación de cuentas, protocolos de ciberseguridad

Nuevo Reglamento de Pagos UE

Transferencias Inmediatas

Se establecen requisitos específicos para transferencias inmediatas en euros.

Plazos de Implementación

Recepción: 9-1-2025. **Envío: 9-10-2025**.

Sin Cargos Extra

Los cargos no serán superiores a los de transferencias convencionales.

Disponibilidad 24/7

Las transferencias inmediatas estarán disponibles las 24 horas, todos los días.

Características del Nuevo Reglamento

Verificación Estandarizada

Se busca un conjunto de reglas y normas a escala de la Unión para la verificación de cuentas.

Responsabilidad del PSP

Los proveedores de servicios de pago serán responsables de la correcta verificación de beneficiarios.

Implementación Gradual

Se introduce gradualmente para permitir a los PSP un uso eficiente de recursos.

Comisiones y Plazos

Concepto	Detalle
Comisiones	No superiores a transferencias convencionales
Plazo de ejecución	10 segundos
Información al ordenante	10 segundos
Implementación en zona euro	9 de enero de 2025

Servicio de Garantía de Verificación

1 **Oferta Obligatoria**

Los PSP deben ofrecer este servicio antes de autorizar una transferencia.

2 **Verificación Inmediata**

Se realiza inmediatamente después de que el ordenante facilita la información del beneficiario.

3 **Independencia del Canal**

Se ofrece sin importar el canal de iniciación del pago utilizado.

Desafíos y Conclusiones

Desafíos de Verificación

Problemas con nombres y transliteraciones pueden complicar la verificación exacta.

Seguridad Mejorada

El nuevo sistema busca prevenir transferencias a beneficiarios no intencionados.

Implementación Gradual

Se introduce por fases para permitir adaptación de los proveedores de servicios.

El servicio de garantía de la verificación debe prestarse, en la medida de lo posible, de conformidad con un conjunto de reglas y normas a escala de la Unión, a fin de fomentar una aplicación sin trabas e interoperable. Este conjunto de reglas y normas podría ser elaborado por organizaciones compuestas por proveedores de servicios de pago o que los representen.

Los proveedores de servicios de pago necesitan tiempo suficiente para cumplir las obligaciones establecidas en el presente Reglamento modificativo. Procede, por tanto, introducir gradualmente esas obligaciones, permitiendo a los proveedores de servicios de pago un uso más eficiente de sus recursos. Por lo tanto, la obligación de ofrecer el servicio de pago para el envío de transferencias inmediatas debe aplicarse posteriormente, precedida por la obligación de ofrecer el servicio de pago para la recepción de transferencias inmediatas, ya que el envío de transferencias inmediatas tiende a ser el servicio más costoso y complejo de los dos que deben ejecutarse y, por lo tanto, su ejecución requiere más tiempo. El servicio de garantía de la verificación es pertinente para los proveedores de servicios de pago en el caso del envío de transferencias.

Por todo ello como conclusión general es que sería un cambio importante disponer del servicio de pagos inmediatos, pero para el sistema de verificación dl beneficiario al ser en el momento del pago y basado en los caracteres del nombre y apellido (razón social) del perceptor, nos obligaría a establecer un sistema previo de control al acreditar a un tercero, y a la fecha actual el único sistema posible de verificación de cuantas sería el desarrollado por IBERPAY.

CONCLUSIONES GENERALES

1. Transferencias inmediatas

2. Doble validación de cuentas.

Gestion de Avales Electrónicos.

NORMATIVA SUPLETORIA AL AMBITO LOCAL

Real Decreto 937/2020, de 27 de octubre, por el que se aprueba el **Reglamento de la Caja General de Depósitos** mediante el cual, se actualizó la forma de organización y funcionamiento de la Caja, **y su aplicación al ámbito local: SUPLETORIA.**

- Dicha norma regula el **funcionamiento de la Caja General de Depósitos** en los aspectos concernientes a las modalidades, los requisitos y la gestión de las garantías y de los depósitos que se constituyan ante la misma.

- De conformidad con lo dispuesto en el artículo 194 del TRLRHL que establece que «la tesorería de las entidades locales se regirá por lo dispuesto en el presente capítulo y, **en cuanto les sean de aplicación, por las normas del capítulo tercero del título cuarto de la Ley 47/2003, de 26 de noviembre, General Presupuestaria»; y, según lo dispuesto en este último, el cual regula lo relativo a la Gestión de la Tesorería del Estado, de ahí su aplicación a la Caja Local.**

Así, y por ser dicha norma de obligación supletoria en el ámbito local, las Entidades Locales deberán adaptar sus regulaciones propias (Bases de Ejecución, Reglamentos, instrucciones internas, pliegos...) a lo dispuesto en la misma.

RD 937 CGD. Disposición final tercera. Aplicación supletoria respecto de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- Las **garantías prestadas** en el ámbito de la **contratación de las administraciones públicas que no hayan sido presentadas ante la Caja se regirán por la Ley 9/2017,** de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, y sus normas de desarrollo, y, de forma supletoria, por el Reglamento de la Caja General de Depósitos que aprueba este real decreto.

- **OJO: FIANZA PROVISIONAL EXPEDIENTE NO METALICO.**

NORMATIVA LOCAL

OTRA NORMATIVA LOCAL APLICABLE.

1.Bases ejecución y Reglamentos. BASES: CONSTITUCION Y CANCELACION . ¿REGLAMENTO?
2.Pliegos Cláusulas Administrativas. IMPORTANTE.
3.Ordenanza General Gestión y Recaudación. REVISION ACTOS Y FRACCIONAMIENTOS.
4.URBANISMO. CONVENIOS.SUBVENCIONES. ACTOS ADMINISTRATIVOS.EJ.LICENCIA.BASES.
5.Otros acuerdos.

CONCLUSIÓN

La Entidad Local, en base a su potestad autoorganizativa, puede aprobar un reglamento local de la caja de depósitos. Ahora bien, en el caso que no lo estime necesario, puede aplicar de forma supletoria el Real Decreto 937/2020, de 27 de octubre, por el que se aprueba el Reglamento de la Caja General de Depósitos.

En términos generales estas garantías se establecen en el marco de:

a) El Derecho Urbanístico.

b) La contratación pública.

c) La aplicación de los tributos, fundamentalmente en los aplazamientos y fraccionamientos, así como en materia de revisión de actos.

d) En aplicación de la Ley 38/2003, de 17 de noviembre, General de Subvenciones.

- Las actuaciones ante la caja, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre, deberán realizarse a través de medios electrónicos. **La utilización de los medios electrónicos tiene una doble dimensión**, pues por un lado implica que **ante la Caja se deberán presentar garantías y depósitos en formato electrónico, y por otro lado conlleva que la forma de relacionarse con la Caja por parte de los ciudadanos, empresas y autoridades, se articulará a través de canales electrónicos, todo ello sin perjuicio de las excepciones previstas con carácter general en la Ley 39/2015, de 1 de octubre**.

NOTA PRACTICA: Las personas jurídicas tendrán obligación de relacionarse a través de medios electrónicos si bien, las personas físicas podrán realizar sus actuaciones de manera presencial o a través de medios electrónicos. ¿INCONGRUENCIA AVAL ELECTRONICO MAYORIA Y ACTUACION PRESENCIAL? PROBLEMATICA NO EXPEDIENTES ELECTRÓNICOS NI ARCHIVOS ELECTRONICOS.

El **artículo 10 del Reglamento de la Caja**, expresa que:

"***1. Las garantías y depósitos se presentarán en formato electrónico, sin perjuicio de aquellas personas que puedan presentar garantías o depósitos en formato papel de acuerdo con lo previsto en el artículo 6***.

INCONVENIENTE. NO VALIDe: " servicio on-line ofrecido por el Ministerio de Política Territorial y Función Pública para la validación de Firmas y Certificados electrónicos".

NO ARCHIVO ELECTRONICO. **CUSTODIA AL MENOS CON MEDIDAS DE SEGURIDAD.**

Artículo 10. Formato de la presentación de documentos.

1. Las garantías y depósitos se **presentarán en formato electrónico**, sin perjuicio de aquellas personas que puedan presentar garantías o depósitos en formato papel de acuerdo con lo previsto en el artículo 6 RCGD.

SOLO PRESENCIAL PERSONAS FISICAS. RESTO INCLUIDO AAPP MEDIOS ELECTRONICOS.

2. Los interesados presentarán los documentos ante la Caja **de acuerdo con los modelos previstos** mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital cuando lo presenten en formato papel. En caso contrario, la presentación se realizará de acuerdo con los formatos previstos en los canales de acceso, sistemas y aplicaciones electrónicos que se hayan establecido al efecto en la sede electrónica correspondiente.

La garantía debe presentarse en la sede electrónica y dicho documento se valida en la plataforma VALIDe del Estado. Ese documento no puede alterarse. PROBLEMAS DE LOS SELLOS DE LAS SEDE.

ACROBAT READER NO ES OFICIAL

ESTABLECER MODELOS EN SEDE ELECTRONICA PARA LAS DISTINTAS GARANTIAS.

OJO ART 26. VALIDAR PODERES. PLATAFORMA VALIDe. PODER PARA OTORGAR Y REQUISITOS NECESARIOS.

Existen diversos formatos de aval electrónico, cada uno con sus propias características y usos específicos. Los principales formatos son:

1. **XML (Extensible Markup Language**). SECAD. ESTADO

2. **PDF (Portable Document Format) con firma electrónica.**

a) Este formato conserva la apariencia y el diseño del aval tradicional en papel, pero se emite y firma digitalmente.

b) Es ampliamente utilizado por su compatibilidad con diferentes dispositivos y sistemas operativos.

c) La firma electrónica garantiza la autenticidad e integridad del documento.

3. **Formatos propios de plataformas digitales**

Diagrama procedimental: un modelo de gestión.