CURS SEMIPRESENCIAL

Planificació i maduresa dels Serveis de Seguretat Gestionats (SSG) i SOC. Alinear la metodologia del ENS amb els principis de la Directiva NIS2

19, 23, 28 i 30 d'octubre de 2026

Presentació

Les entitats públiques depenen cada vegada més de serveis TIC complexos i interconnectats, que requereixen un nivell elevat de protecció davant amenaces i vulnerabilitats. Els Serveis de Seguretat Gestionats (SSG) permeten externalitzar funcions clau de seguretat, com la gestió d'incidents, el monitoratge d'amenaces, l'anàlisi de vulnerabilitats o la protecció de xarxes i aplicacions, garantint continuïtat i qualitat en la prestació dels serveis digitals. La seva importància és especialment rellevant en àmbits com la protecció de dades personals, la seguretat en el correu electrònic i en la navegació web, la prevenció del frau digital o la vigilància de la reputació institucional.

Aquesta formació capacitarà el personal de l'administració per planificar l'adopció d'SSG de manera estratègica, entendre els diferents models de servei disponibles i coordinar-se amb proveïdors per assegurar que els nivells de maduresa i governança de la seguretat siguin adequats a les necessitats de cada organisme públic.

Objectius

- Comprendre què són els SSG i el seu marc regulador (ENS, NIS2, PCE-SSG).
- Identificar els serveis de prevenció, protecció, detecció, resposta i gestió de la ciberseguretat.
- Avaluar els requisits operatius i tècnics dels proveïdors de SSG.
- Determinar els nivells de maduresa d'un SOC i la seva vinculació amb la RNS (Red Nacional de SOC).
- Capacitar-se per planificar, coordinar i validar la contractació d'SSG dins de l'administració pública.

FMC

programa

1. Marc i definició dels SSG

Concepte i abast segons la Directiva NIS2 i l'ENS.
Requisits de certificació PCE-SSG.
Relació entre proveïdors de SSG i administració pública.

2. Serveis de seguretat gestionats

Prevenció: anàlisi de vulnerabilitats, pentesting, vigilància digital.
Protecció: operació d'EDR, firewall, IPS/IDS, etc.
Detecció: monitorització, threat hunting, intel·ligència d'amenaces.
Resposta: equips IRT i gestió d'incidents.
Gestió: coordinació estratègica, compliment legal i quadres de comandament.

3. Nivells de maduresa dels SOC

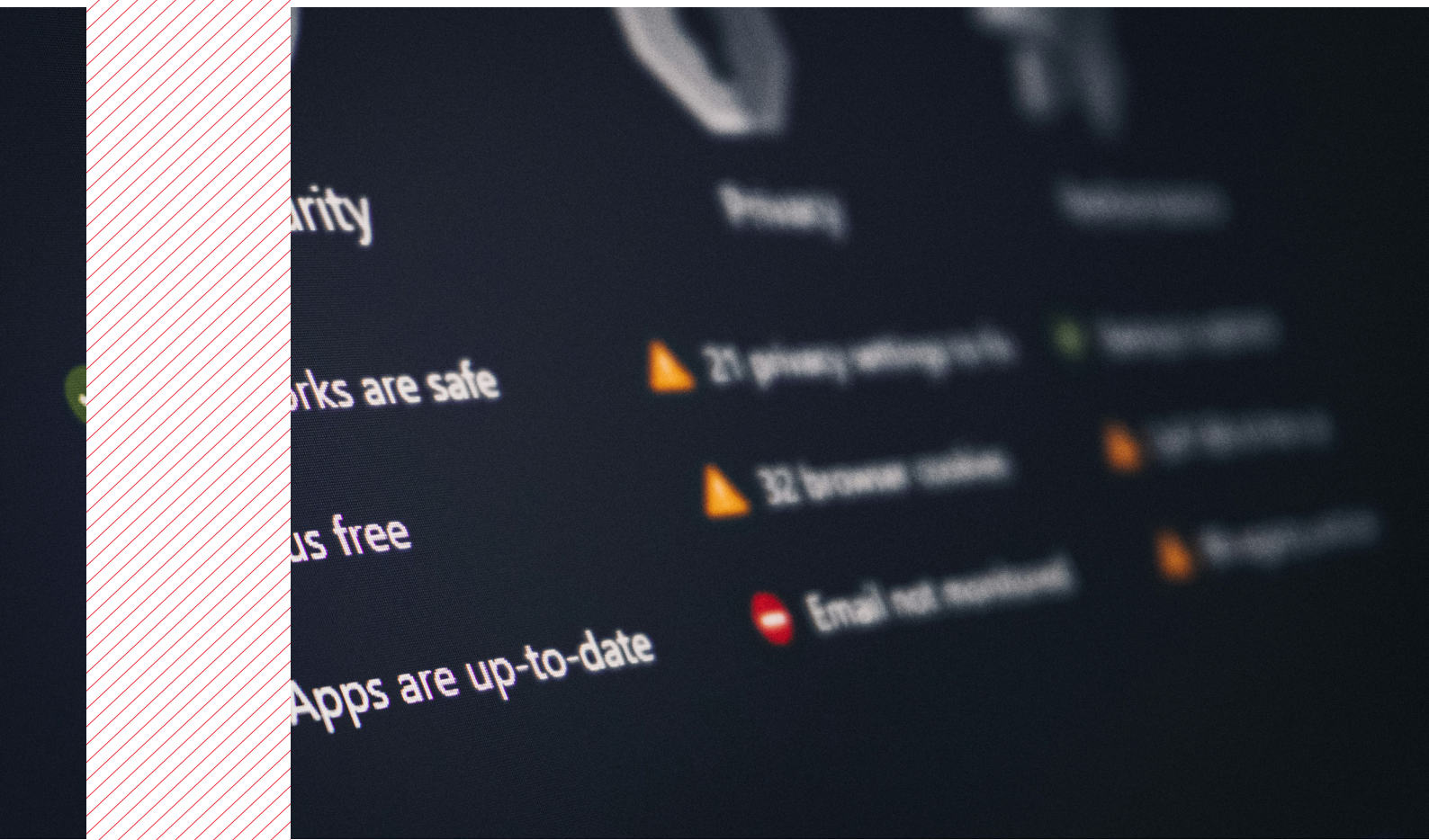
SOC bàsic: serveis mínims requerits.
SOC avançat: ampliació de capacitats.
SOC complet: cobertura integral dels cinc serveis.

4. Planificació i coordinació

Procediments de contractació i SLA.
Relació amb proveïdors externs i validació de serveis.
Gestió de la maduresa i vinculació a la RNS.

5. Capacitats pràctiques

Casos d'ús en administracions locals.
Exercicis de classificació de serveis i SOC.
Elaboració d'un pla de maduresa per a un organisme públic



programa

Metodologia

• Sessions presencials i online amb experts en ciberseguretat i gestió de serveis TIC.

• Presentacions interactives i debats orientats a la realitat de les administracions locals.

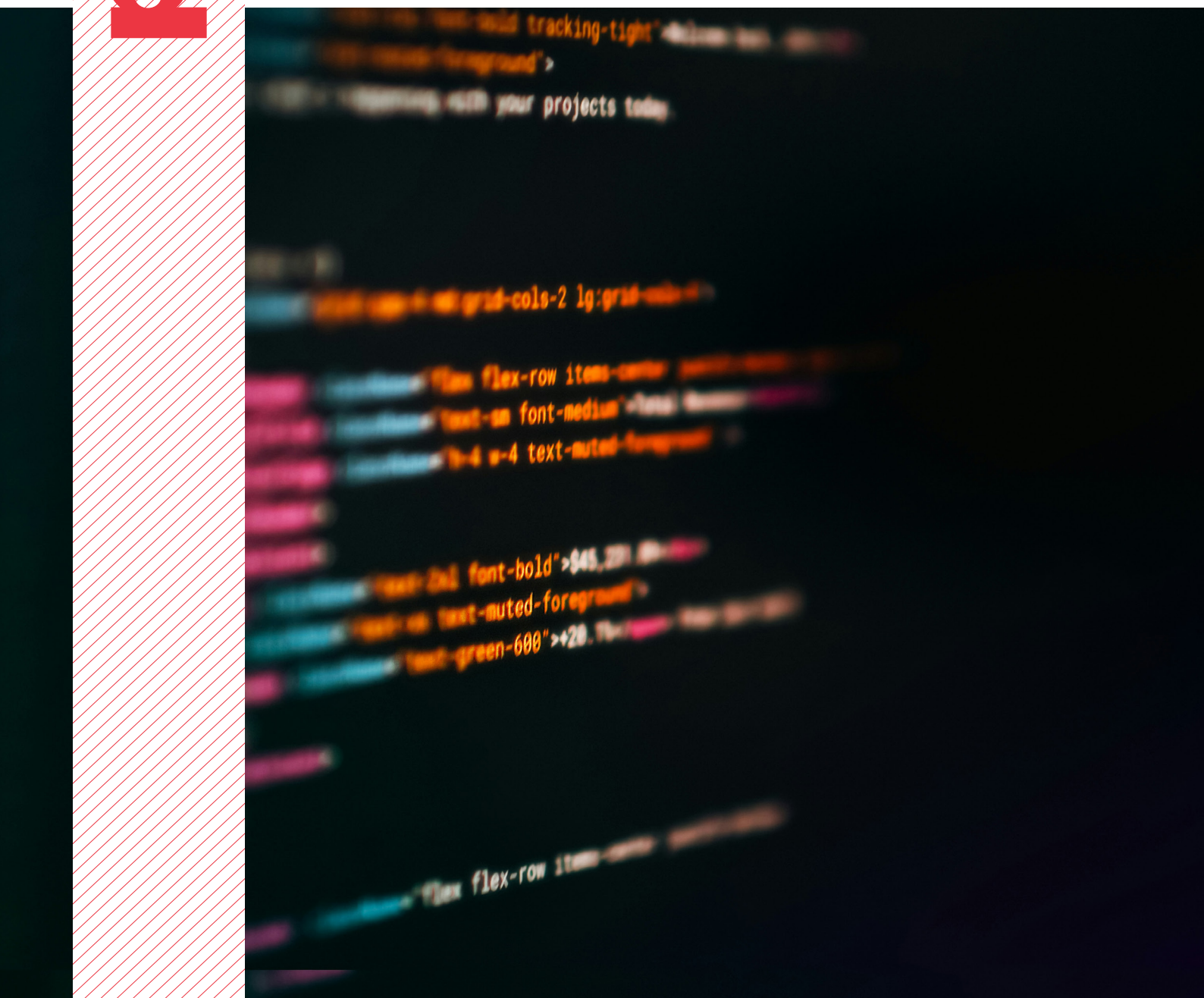
• Treball en grup amb casos pràctics inspirats en experiències reals del sector públic.

• Exercicis pràctics d'aplicació directa:

Exercici 1 – Mapa de serveis TIC i assignació d'SSG: cada participant elaborarà un inventari simplificat dels serveis TIC de la seva organització (xarxes, correu electrònic, aplicacions de gestió, seu electrònica, etc.) i identificarà quins Serveis de Seguretat Gestionats podrien aplicar-se a cada àmbit (p. ex. monitoratge de correu i firewall, gestió de vulnerabilitats d'aplicacions, serveis de resposta a incidents).

Exercici 2 – Determinació del nivell de maduresa de seguretat: a partir d'un cas d'una administració local fictícia, els participants analitzaran els serveis de seguretat disponibles i determinaran si el nivell de maduresa és bàsic, avançat o complet. S'exploraran quins passos serien realistes per millorar aquest nivell sense requerir grans inversions, prioritzant la gestió eficient i escalable.

• Recursos i materials oficials per aplicar les metodologies de planificació i validació dels serveis de seguretat.



Docent
Genís Margarit i Contel. Enginyer de Telecomunicacions i Enginyeria de Sistemes Electrònics per la Universitat Politècnica de Catalunya - UPC. Auditor de ciberseguretat els darrers 15 anys. Va fundar la seva empresa de consultoria en ciberseguretat fa deu anys. Compagina la seva tasca amb la docència a la Universitat Pompeu Fabra (UPF) i com a instructor d'EC-Council. És membre de l'Associació Professional Espanyola de la Privacitat, fundador del grup de seguretat de Telecos.cat, expert tècnic del European Privacy Seal i Privacy by Design Ambassador.

Durada
16 hores

Horari
De 9.30 a 14.00 hores

Sessions presencials
19 i 30 d'octubre de 2026

Sessions virtuals
23 i 28 d'octubre de 2026

Lloc de realització
UPF-BSM (Barcelona School of Management)
Universitat Pompeu Fabra
Balmes, 134. Barcelona

Llengua d'impartició
Català

Destinataris
El curs està adreçat al personal dels departaments TIC (Tecnologia i Comunicació) de l'administració local catalana.

Certificat
Es lliurarà un certificat d'assistència a les persones que acreditin la participació al 80 per cent de les hores lectives de **tres sessions**, com a mínim, i d'aprofitament sí, a més, realitzen satisfactòriament els exercicis proposats al llarg del curs.

Inscripcions
El termini d'inscripció finalitza el dia **12 d'octubre de 2026**. La inscripció és gratuïta i el nombre de places, limitat. Per a la selecció de les inscripcions es tindrà en compte la cobertura territorial (s'afavorirà la participació del màxim nombre possible d'ajuntaments), l'adequació al perfil del destinatari de l'acció formativa i l'ordre de recepció de les sol·licituds.
La formalització de la inscripció es farà per mitjà del formulari que trobareu al web de la Federació: www.fmc.cat.

Organitza:
Federació de Municipis de Catalunya

Col·labora:
LOCALRET

Federació de Municipis de Catalunya