

ANNEX A. Continguts mínims de l'Acció Formativa en Ciberseguretat: Mòdul bàsic de Ciberseguretat

1. Introducció a la ciberseguretat en el Sector Públic

- Situació actual de la ciberseguretat a nivell nacional.
- Per què els serveis públics i operadors de mobilitat són un objectiu.
- Impacte d'una ciberincidència en els serveis essencials.
- L'ENS com a mecanisme de protecció del Sector Públic explicat de manera simplificada.

2. Amenaces en el ciberespai

- Suplantació d'identitat (phishing, smishing, vishing).
- Enganys i estafes digitals dirigides a personal de serveis públics.
- Malware i ransomware.
- Enganys digitals avançats basats en IA (deepfakes de veu, missatges generats per IA).

3. Vectors d'infecció

- Fitxers adjunts maliciosos.
- Enllaços fraudulents.
- Aplicacions no oficials.
- QR fraudulents i enganyosos.
- Ús indegut de dispositius externs.

4. Ús segur del correu electrònic

- Identificació de correus sospitosos.
- Bones pràctiques en la gestió de missatges.
- Característiques dels correus generats per IA fraudulenta.

5. Ús segur de la navegació web

- Identificació de portals fraudulents.
- Precaucions bàsiques en navegació i descàrrega d'arxius.
- Exemples de webs generades amb IA per enganyar usuaris.

6. Ús segur dels dispositius mòbils

- Configuració segura del dispositiu.
- Control de permisos d'aplicacions.
- Riscos en connexions Wi-Fi públiques o desconegudes.

7. Deep Web i Dark Web

- Explicació bàsica i diferenciació conceptual.
- Com afecta la Dark Web als serveis públics (credencials robades, dades personals).

8. Seguretat en xarxes sense fil

- Riscos de punts d'accés falsos.
- Bones pràctiques en connexions en espais públics i zones operatives.

9. Internet of Things (IoT)

- Explicació senzilla del concepte.
- Riscos associats a dispositius connectats.
- Bones pràctiques en l'ús personal i laboral.

10. Missatgeria instantània i xarxes socials

- Estafes i enganys freqüents per WhatsApp, Telegram i xarxes.
- Falsos comunicats o ordres generats per IA.
- Bones pràctiques de privacitat i verificació de la informació.

11. Ús segur de la Intel·ligència Artificial (IA)

- Què és la IA i com es fa servir en enganys digitals.
- Riscos per al personal base:
 - Deepfakes (veu i vídeo)
 - Missatges i comunicats falsos molt convincents
 - Pages web fraudulent generades per IA
- Normes d'ús segur:
 - No introduir informació laboral o personal sensible en IA pública.
 - Com verificar informació i contingut creat artificialment.
- Bones pràctiques en l'ús de IA per a tasques quotidianes (consulta, aprenentatge, resums).

12. Bones pràctiques generals de ciberseguretat

- Com actuar davant un dubte o sospita.
- Com comunicar incidents de manera immediata.

13. L'ENS com a marc de seguretat del Sector Públic

- Què és l'ENS i per què és rellevant.
- Principals mesures aplicades a l'àmbit de l'usuari final.
- Com contribueix cada persona a la seguretat global de TMB.

Yolanda Roldán Millán

Tècnica Assessoria Jurídica Laboral TMB