ANNEX B. Continguts mínims de l'Acció Formativa en Ciberseguretat: Mòdul bàsic de Ciberseguretat (formació online)

1. Introducció a la ciberseguretat en el Sector Públic

- Riscos i amenaces actuals que afecten operadors públics i de mobilitat.
- Casos reals d'incidents en administracions i transport.
- Impacte operatiu, reputacional i en el servei a la ciutadania.
- L'ENS: què és, per què és obligatori i com protegeix TMB i el personal.
- Principals mesures ENS que afecten directament a l'usuari final.

2. Amenaces digitals modernes

- Suplantació d'identitat: phishing, spear-phishing, smishing, vishing.
- Enganys avançats generats per IA (correus perfectes, missatges creïbles, deepfakes).
- Atacs dirigits a usuaris d'oficina:
    - Factures falses
    - Peticions de proveïdors
    - Documents maliciosos
- Ransomware i bloqueig de documents corporatius.
- Estafes via WhatsApp/Teams/Telegram.
- Atacs basats en QR i portals falsos.
- Deep web i dark web: què són i com afecten
    - Explicació bàsica i diferenciació conceptual.
    - Relació amb la ciberseguretat del Sector Públic:
        - Venda de credencials robades.
        - Filtracions d'informació de serveis públics.
        - Anuncis de vulnerabilitats o atacs.
    - Com un error comú (clicar un enllaç, compartir dades, contrasenya feble) pot acabar amb informació de TMB publicada a la Dark Web.

3. Vectors d'infecció i riscos habituals

- Fitxers adjunts perillosos (Word, Excel, PDF, ZIP).
- Macros i continguts actius.
- Navegació a webs fraudulentes o generades per IA.
- Instal·lació no autoritzada d'aplicacions.
- Dispositius externs (USB, discs portàtils, etc.).
- Exemples reals adaptats a TMB.

4. Ús segur del correu electrònic

- Identificació de correus sospitosos.
- Spoofing de companys, caps o proveïdors.
- Indicadors clau d'engany (també quan l'atac ve generat per IA).
- Bones pràctiques en fitxers adjunts, avisos i redireccions.

5. Ús segur de la navegació web

- Validació d'enllaços i portals.
- Webs corporatives falses o modificades.
- Descàrregues segures i programari autoritzat.
- Com evitar infeccions a través de navegació.

6. Ús segur del PC i eines ofimàtiques

- Riscos en programari ofimàtic: macros, OLE, edicions compartides.
- Gestió segura de documents corporatius (SharePoint, OneDrive, xarxes internes).
- Permisos d'accés, versions i historial.
- Bones pràctiques de col·laboració digital.
- Protecció contra modificació fraudulenta de documents.

7. Gestió de contrasenyes, identitats i accessos

- Multifactor (MFA): com funciona i quan s'utilitza.
- Gestió segura d'identitat corporativa (SSO, Azure AD).
- Com evitar robatori de credencials.
- Com reconèixer intents de keylogging o captures fraudulentes.

8. Ús segur dels dispositius mòbils corporatius

- Configuració mínima segura.
- Aplicacions: oficials, autoritzades i prohibides.
- Configuració de permisos d'app.
- Riscos d'SSID i Wi-Fi públiques.
- Coordinació entre PC i mòbil (Teams, correu, gestors).
- Seguretat en xarxes sense fil (Wi-fi)
    - Riscos de punts d'accés falsos.
    - Com poden robar credencials o interceptar trànsit a través de Wi-Fi no fiable.
    - Bones pràctiques en connexions en espais públics i zones operatives.
    - Rellevància per a personal que combina PC + mòbil corporatiu, especialment despatxos mòbils, reunions externes i zones operatives

9. Internet of Things (IoT)

- Conceptes bàsics.
- IoT en entorns de TMB i en entorns personals.
- Riscos típics: privadesa, intercepció, control remot.
- Bones pràctiques per minimitzar l'exposició.

10. Missatgeria instantània i xarxes socials

- Riscos de desinformació interna
- 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)

13.1. Riscos principals

- Contingut fals creat per IA (correus, instruccions, ordres de feina).
- Falsificació de veus, vídeos i documents.
- Webs perfectament imitades.
- IA utilitzada per enganyar administratius i gestors.

13.2. Bones pràctiques d'ús

- No introduir dades internes, confidencials o personals en IA pública.
- Verificar sempre informació generada per IA.
- Detecció bàsica de contingut fals.
- Ús recomanat d'IA corporativa (si n'hi ha).

13.3. Casos d'ús segurs i útils

- Redacció assistida.
- Resums.
- Explicació de conceptes.
- Reforç d'idiomes i comunicació

14. Bones pràctiques generals de Ciberseguretat

- Organització segura de documents.
- Compartició interna i externa.
- Prevenció de pèrdues d'informació.
- Detecció de comportaments anòmals en el PC

15. Com actuar davant d’un incident digital

- Passes immediates segons el tipus d’incident.
- Què fer si s'ha clicat en un enllaç maliciós.
- Com informar l’equip de suport.
- Com reduir el risc en cas d’error

16. L’ENS com a marc de seguretat del Sector Públic

- Principis ENS aplicats a la feina d’oficina.
- Polítiques corporatives que deriven de l’ENS.
- Rol de l’usuari en la seguretat i en la resiliència global.

Yolanda Roldán Millán

Tècnica Assessoria Jurídica Laboral TMB