ANNEX D. Continguts mínims de l'Acció Formativa en Ciberseguretat: Formació o Mòdul d'Administració, Configuració i Protecció de sistemes IT (tecnologies de la informació i comunicacions) i/o sistemes OT (sistemes operacionals)

1. Introducció a la seguretat tecnològica

- Principis bàsics de ciberseguretat aplicats a entorns IT i OT.
- La seguretat com a part inherent de les tasques tècniques.
- Breu referència al Esquema Nacional de Seguretat (ENS): àmbit, objectiu i mesures rellevants.
  Referència ENS: M.1, M.2, M.3.

2. Instal·lació física segura d'equips

- Bones pràctiques de muntatge i protecció física.
- Control d'accessos físics i mesures de prevenció de manipulació.
  Referència ENS: M.7, M.12.

3. Configuració i bastionat segur

- Configuració segura d'equips IT i OT.
- Eliminació de superfícies d'atac (ports, serveis).
- Bastionat de sistemes operatius i dispositius de xarxa.
- Gestió segura de firmware i versions.
  Referència ENS: M.6, M.10, M.11.

4. Gestió d'identitats, usuaris i accessos

- Principi de mínim privilegi i segregació de funcions.
- Gestió de comptes privilegiades, temporals i de servei.
- Registre, control i traçabilitat d'operacions.
  Referència ENS: M.4, M.5, M.15.

5. Inventari d’actius i control de canvis

- Inventari de maquinari, programari, versions i configuracions.
- Procediments de control de canvis: validació, documentació i supervisió. **Referència ENS:** M.6, M.10, M.11.

6. Posada en marxa segura de sistemes i components

- Validació de configuracions prèvies a la producció.
- Revisió de credencials predeterminades.
- Segmentació de xarxa (VLAN, ACL, zones OT). **Referència ENS:** M.6, M.12.

7. Operació i manteniment amb criteris de seguretat

- Ús segur de dispositius mòbils i eines de manteniment.
- Bones pràctiques en entorns operatius i industrials.
- Actualitzacions i gestió de vulnerabilitats. **Referència ENS:** M.11, M.13.

8. Monitorització, detecció i registre

- Registre d’operacions i canvis.
- Identificació de comportaments anòmals en IT/OT.
- Coordinació amb equips de ciberseguretat (SOC/CSIRT). **Referència ENS:** M.15, M.17.

9. Resposta davant incidents

- Accions bàsiques en cas d’incident o anomalia.
- Contenció segura i procediments d’escalat.
- Comunicació i traçabilitat dels incidents. **Referència ENS:** M.17, M.18.

10. Ús segur de la Intel·ligència Artificial (IA) en entorns tècnics

La formació haurà d'incloure continguts específics sobre l'ús responsable i segur d'eines basades en IA, en particular:

10.1. Bones pràctiques d'ús responsable de IA generativa

- Riscos de filtració d'informació sensible.
- Limitacions i validació de resultats generats per IA (scripts, configuracions, diagnosi).
- Prohibició d'incorporar dades operatives, credencials o configuracions crítiques en serveis públics no controlats.

10.2. IA en operacions IT i OT

- Riscos de dependència i automatització insegura.
- Anàlisi de riscos en l'ús d'IA per diagnòstic o revisió de configuracions.
- Casos típics d'errors provocats per IA en entorns industrials.

10.3. Normes d'ús corporatiu

- Polítiques internes i entorns autoritzats d'IA.
- Consideracions de privacitat, seguretat i confidencialitat.

10.4. Relació amb les mesures del ENS

- Mesures aplicables a l'ús de IA:
    - Protecció de dades i informació (M.8, M.9).
    - Control d'accessos i identitats (M.4, M.5).
    - Seguretat en la configuració i programari (M.6, M.10).
    - Gestió de vulnerabilitats i incidents (M.11, M.17).
    - Registre i monitorització d'ús (M.15).

11. Casos pràctics i exercicis

- Situacions reals d'instal·lació, configuració, bastionat i ús d'IA.
- Anàlisi de configuracions insegures.
- Exercicis de relació entre tasques tècniques i mesures ENS.

Yolanda Roldán Millán

Tècnica Assessoria Jurídica Laboral TMB