ANEXO D. Contenidos mínimos de la acción formativa en ciberseguridad: Formación o módulo de administración, configuración y protección de sistemas IT (tecnologías de la información y las comunicaciones) y/o sistemas OT (sistemas operacionales)

1. Introducción a la seguridad tecnológica

- Principios básicos de ciberseguridad aplicados a entornos IT y OT.
- La seguridad como parte inherente de las tareas técnicas.
- Breve referencia al Esquema Nacional de Seguridad (ENS): ámbito, objetivo y medidas relevantes.
  Referencia ENS: M.1, M.2, M.3.

2. Instalación física segura de equipos

- Buenas prácticas de montaje y protección física.
- Control de accesos físicos y medidas de prevención de manipulación.
  Referencia ENS: M.7, M.12.

3. Configuración y bastionado seguro

- Configuración segura de equipos IT y OT.
- Reducción de la superficie de ataque (puertos, servicios).
- Bastionado de sistemas operativos y dispositivos de red.
- Gestión segura de firmware y versiones.
  Referencia ENS: M.6, M.10, M.11.

4. Gestión de identidades, usuarios y accesos

- Principio de mínimo privilegio y segregación de funciones.
- Gestión de cuentas privilegiadas, temporales y de servicio.
- Registro, control y trazabilidad de operaciones.
  Referencia ENS: M.4, M.5, M.15.

5. Inventario de activos y control de cambios

- Inventario de hardware, software, versiones y configuraciones.

- Procedimientos de control de cambios: validación, documentación y supervisión.
  Referencia ENS: M.6, M.10, M.11.

6. Puesta en marcha segura de sistemas y componentes

- Validación de las configuraciones antes de su puesta en producción.
- Revisión de las credenciales predeterminadas.
- Segmentación de red (VLAN, ACL, zonas OT).
  Referencia ENS: M.6, M.12.

7. Operación y mantenimiento con criterios de seguridad

- Uso seguro de dispositivos móviles y herramientas de mantenimiento.
- Buenas prácticas en entornos operativos e industriales.
- Actualizaciones y gestión de vulnerabilidades.
  Referencia ENS: M.11, M.13.

8. Monitorización, detección y registro

- Registro de operaciones y cambios.
- Identificación de comportamientos anómalos en IT/OT.
- Coordinación con equipos de ciberseguridad (SOC/CSIRT).
  Referencia ENS: M.15, M.17.

9. Respuesta ante incidentes

- Acciones básicas en caso de incidente o anomalía.
- Contención segura y procedimientos de escalado.
- Comunicación y trazabilidad de los incidentes.
  Referencia ENS: M.17, M.18.

10. Uso seguro de la Inteligencia Artificial (IA) en entornos técnicos

La formación deberá incluir contenidos específicos sobre el uso responsable y seguro de herramientas basadas en IA, en particular los siguientes:

10.1.1. Buenas prácticas de uso responsable de IA generativa

- Riesgos de filtración de información sensible.

- Limitaciones y validación de los resultados generados por IA (scripts, configuraciones y diagnóstico).
- Prohibición de introducir datos operativos, credenciales o configuraciones críticas en servicios públicos no controlados.

10.1.2. IA en operaciones IT y OT

- Riesgos de dependencia y automatización insegura.
- Análisis de riesgos en el uso de IA para el diagnóstico o la revisión de configuraciones.
- Casos típicos de errores generados por IA en entornos industriales.

10.1.3. Normas de uso corporativo

- Políticas internas y entornos autorizados de IA.
- Consideraciones de privacidad, seguridad y confidencialidad.

10.1.4. Relación con las medidas del ENS

- Medidas aplicables al uso de IA:
    - Protección de datos e información (M.8, M.9).
    - Control de accesos e identidades (M.4, M.5).
    - Seguridad en la configuración y el software (M.6, M.10).
    - Gestión de vulnerabilidades e incidentes (M.11, M.17).
    - Registro y monitorización de uso (M.15).

11. Casos prácticos y ejercicios

- Situaciones reales de instalación, configuración, bastionado y uso de IA.
- Análisis de configuraciones inseguras.
- Ejercicios de relación entre tareas técnicas y medidas ENS.