ANEXO B. Contenidos mínimos de la Acción Formativa en Ciberseguridad: Módulo básico de Ciberseguridad (formación online)

1. Introducción a la ciberseguridad en el Sector Público

- Riesgos y amenazas actuales que afectan a operadores públicos y de movilidad.
- Casos reales de incidentes en administraciones y transporte.
- Impacto operativo, reputacional y en el servicio a la ciudadanía.
- El ENS: qué es, por qué es obligatorio y cómo protege a TMB y al personal.
- Principales medidas ENS que afectan directamente al usuario final.

2. Amenazas digitales modernas

- Suplantación de identidad: phishing, spear-phishing, smishing, vishing.
- Engaños avanzados generados por IA (correos perfectos, mensajes creíbles, deepfakes).
- Ataques dirigidos a usuarios de oficina:
    - Facturas falsas
    - Peticiones de proveedores
    - Documentos maliciosos
- Ransomware y bloqueo de documentos corporativos.
- Estafas vía WhatsApp/Teams/Telegram.
- Ataques basados en QR y portales falsos.
- Deep web y dark web: qué son y cómo afectan
    - Explicación básica y diferenciación conceptual.
    - Relación con la ciberseguridad del Sector Público:
        - Venta de credenciales robadas.
        - Filtraciones de información de servicios públicos.
        - Anuncios de vulnerabilidades o ataques.
    - Cómo un error común (hacer clic en un enlace, compartir datos, contraseña débil) puede acabar con información de TMB publicada en la Dark Web.

3. Vectores de infección y riesgos habituales

- Archivos adjuntos peligrosos (Word, Excel, PDF, ZIP).
- Macros y contenidos activos.
- Navegación por webs fraudulentas o generadas por IA.
- Instalación no autorizada de aplicaciones.
- Dispositivos externos (USB, discos portátiles, etc.).
- Ejemplos reales adaptados a TMB.

4. Uso seguro del correo electrónico

- Identificación de correos sospechosos.

- Spoofing de compañeros, jefes o proveedores.
- Indicadores clave de engaño (también cuando el ataque viene generado por IA).
- Buenas prácticas en archivos adjuntos, avisos y redirecciones.

5. Uso seguro de la navegación web

- Validación de enlaces y portales.
- Webs corporativas falsas o modificadas.
- Descargas seguras y software autorizado.
- Cómo evitar infecciones a través de la navegación.

6. Uso seguro del PC y herramientas ofimáticas

- Riesgos en software ofimático: macros, OLE, ediciones compartidas.
- Gestión segura de documentos corporativos (SharePoint, OneDrive, redes internas).
- Permisos de acceso, versiones e historial.
- Buenas prácticas de colaboración digital.
- Protección contra la modificación fraudulenta de documentos.

7. Gestión de contraseñas, identidades y accesos

- Multifactor (MFA): cómo funciona y cuándo se utiliza.
- Gestión segura de identidad corporativa (SSO, Azure AD).
- Cómo evitar el robo de credenciales.
- Cómo reconocer intentos de keylogging o capturas fraudulentas.

8. Uso seguro de los dispositivos móviles corporativos

- Configuración mínima segura.
- Aplicaciones: oficiales, autorizadas y prohibidas.
- Configuración de permisos de app.
- Riesgos de SSID y Wi-Fi públicas.
- Coordinación entre PC y móvil (Teams, correo, gestores).
- Seguridad en redes inalámbricas (Wi-Fi)
    - Riesgos de puntos de acceso falsos.
    - Cómo pueden robar credenciales o interceptar tráfico a través de Wi-Fi no fiable.
    - Buenas prácticas en conexiones en espacios públicos y zonas operativas.

- Relevancia para personal que combina PC + móvil corporativo, especialmente despachos móviles, reuniones externas y zonas operativas

9. Internet of Things (IoT)

- Conceptos básicos.
- IoT en entornos de TMB y en entornos personales.
- Riesgos típicos: privacidad, intercepción, control remoto.
- Buenas prácticas para minimizar la exposición.

10. Mensajería instantánea y redes sociales

- Riesgos de desinformación interna
- Estafas y engaños frecuentes por WhatsApp, Telegram y redes.
- Falsos comunicados u órdenes generados por IA.
- Buenas prácticas de privacidad y verificación de la información.

11. Uso seguro de la Inteligencia Artificial (IA)

13.1. Riesgos principales

- Contenido falso creado por IA (correos, instrucciones, órdenes de trabajo).
- Falsificación de voces, vídeos y documentos.
- Webs perfectamente imitadas.
- IA utilizada para engañar a administrativos y gestores.

13.2. Buenas prácticas de uso

- No introducir datos internos, confidenciales o personales en IA pública.
- Verificar siempre información generada por IA.
- Detección básica de contenido falso.
- Uso recomendado de IA corporativa (si la hay).

13.3. Casos de uso seguros y útiles

- Redacción asistida.
- Resúmenes.
- Explicación de conceptos.
- Refuerzo de idiomas y comunicación

14. Buenas prácticas generales de Ciberseguridad

- Organización segura de documentos.
- Compartición interna y externa.
- Prevención de pérdidas de información.
- Detección de comportamientos anómalos en el PC

15. Cómo actuar ante un incidente digital

- Pasos inmediatos según el tipo de incidente.
- Qué hacer si se ha hecho clic en un enlace malicioso.
- Cómo informar al equipo de soporte.
- Cómo reducir el riesgo en caso de error

16. El ENS como marco de seguridad del Sector Público

- Principios ENS aplicados al trabajo de oficina.
- Políticas corporativas que derivan del ENS.
- Rol del usuario en la seguridad y en la resiliencia global.