ANEXO A. Contenidos mínimos de la acción formativa en ciberseguridad: Módulo básico de ciberseguridad

1. **Introducción a la ciberseguridad en el sector público**

    - Situación actual de la ciberseguridad a nivel nacional.
    - Por qué los servicios públicos y los operadores de movilidad son un objetivo.
    - Impacto de una ciberincidencia en los servicios esenciales.
    - El ENS como mecanismo de protección del sector público, explicado de forma simplificada.

2. **Amenazas en el ciberespacio**
    - Suplantación de identidad (phishing, smishing, vishing).
    - Engaños y estafas digitales dirigidos al personal de los servicios públicos.
    - Malware y ransomware.
    - Engaños digitales avanzados basados en IA, como deepfakes de voz y mensajes generados mediante IA.

3. **Vectores de infección**

    - Archivos adjuntos maliciosos.
    - Enlaces fraudulentos.
    - Aplicaciones no oficiales.
    - Códigos QR fraudulentos y engañosos.
    - Uso indebido de dispositivos externos.

4. **Uso seguro del correo electrónico**

    - Identificación de correos sospechosos.
    - Buenas prácticas en la gestión de mensajes.
    - Características de los correos fraudulentos generados mediante IA.

5. **Uso seguro de la navegación web**

    - Identificación de portales fraudulentos.
    - Precauciones básicas en la navegación y descarga de archivos.
    - Ejemplos de sitios web generados mediante IA para engañar a las personas usuarias.

6. **Uso seguro de los dispositivos móviles**

    - Configuración segura del dispositivo.
    - Control de permisos de aplicaciones.
    - Riesgos en conexiones Wi-Fi públicas o desconocidas.

7. **Deep Web y Dark Web**

    - Explicación básica y diferenciación conceptual.
    - Cómo afecta la Dark Web a los servicios públicos: credenciales robadas y datos personales expuestos.

8. ## Seguridad en redes inalámbricas

- Riesgos de puntos de acceso falsos.
- Buenas prácticas en conexiones en espacios públicos y zonas operativas.

9. ## Internet de las cosas (IoT)

- Explicación sencilla del concepto.
- Riesgos asociados a dispositivos conectados.
- Buenas prácticas en el uso personal y laboral.

10. ## Mensajería instantánea y redes sociales

- 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)

- Qué es la IA y cómo se utiliza en engaños digitales.
- Riesgos para el personal usuario:
    - Deepfakes (voz y vídeo)
    - Mensajes y comunicados falsos altamente convincentes.
    - Páginas web fraudulentas generadas mediante IA.
- Normas de uso seguro:
    - No introducir información laboral o personal sensible en IA pública.
    - Cómo verificar información y contenido creado artificialmente.
- Buenas prácticas en el uso de IA para tareas cotidianas, como consultas, aprendizaje y elaboración de resúmenes.

12. ## Buenas prácticas generales de ciberseguridad

- Cómo actuar ante una duda o sospecha.
- Cómo comunicar incidentes de manera inmediata.

13. ## El ENS como marco de seguridad del sector público

- Qué es el ENS y por qué es relevante.
- Principales medidas aplicadas al ámbito del usuario final.
- Cómo contribuye cada persona a la seguridad global de TMB.