TEMA 1 – INTRODUCCIÓN
En este primer módulo se describen diferentes conceptos de la ciberseguridad: phishing, ransomware,… se hace énfasis en que todos somos objetivos de posibles ataques y en las consecuencias que estos pueden tener, tanto a nivel económico, como reputacional, pérdida de clientes,… por último se ve y se explica qué es la red oscura o dark web, utilizando para ello como ejemplo la red TOR, su uso, ventajas, inconvenientes. Vemos también como se puede localizar la IP geográficamente.
EJERCICIO PRACTICO

TEMA 2 – PHISHING: Reglas de ciberseguridad
En este módulo se explica detalladamente en qué consiste un phishing, los diferentes tipos de phishing que hay, cómo no caer en ellos, qué debemos mirar y qué cosas debemos tener en cuenta, dándole también importancia a nuestra exposición en redes sociales, debemos decidir qué información publicamos y sobre todo cuando; crearemos un phishing sencillo como ejemplo y veremos cómo detectarlo.
EJERCICIO PRACTICO

TEMA 3 – SEGURIDAD EN EL PUESTO DE TRABAJO: Reglas de ciberseguridad
En este módulo vemos la seguridad tanto en nuestro PC, como en nuestro escritorio, cosas que debemos hacer y cosas que no debemos hacer, desde la creación de contraseñas seguras, el uso de gestores de contraseñas, la activación del doble factor de autenticación, gestión de usuarios básica en un equipo, antivirus, verificar si nuestro mail o teléfono ya ha aparecido en alguna brecha de seguridad… y por la parte física cosas o costumbres sanas que debemos adquirir.
EJERCICIO PRACTICO

TEMA 4 – CONCIENCIACIÓN DE USO DE TECNOLOGÍA SMARTPHONE: Reconocimiento local del dispositivo, Reconocimiento de red del dispositivo, APK maliciosas, Ingeniería social -
En el último módulo es similar al anterior, pero orientado al teléfono, cosas que no debemos hacer y herramientas que podemos utilizar para prevenir ataques, desde revisión de permisos, aplicaciones instaladas, sistemas de borrado o acceso remoto…
EJERCICIO PRACTICO