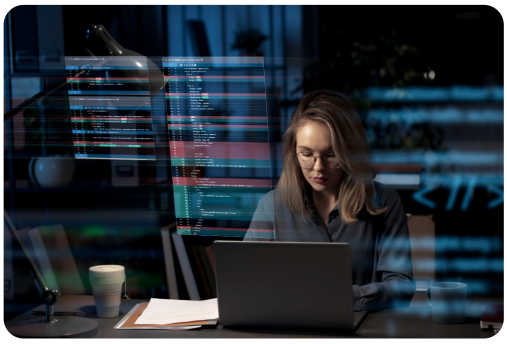

IFCT121. Ciberseguridad. Riesgos y amenazas en la red

Sku: PC820

Horas: 10

Formato: HTML

OBJETIVOS

Concienciar a los usuarios de los posibles riesgos que pueden afectarle a nivel individual y de empresa, así como facilitarles una serie de “buenas prácticas” que puedan aplicar no sólo en su espacio de trabajo sino ta vida personal.

CONTENIDOS

Unidad 1: Identidad digital y navegación segura

1.2 Para comenzar

- Bienvenido a la unidad Identidad digital y navegación segura. Aquí vas a entender, sin tecnicismos, qué es tu identidad digital (lo que declaras, lo que se observa y lo que se infiere de ti), cómo se forma tu huella (activa y pasiva) y por qué la privacidad significa tener control sobre tus datos.
- También aprenderás señales prácticas para navegar con seguridad más allá del icono del candado, y te llevarás cinco acciones rápidas que puedes aplicar hoy mismo: actualizar, activar MFA o passkeys, usar un gestor de contraseñas, entrar desde marcadores y activar DNS seguro/GPC. Esta es una introducción breve para arrancar con buen pie antes de profundizar en las lecciones de contenido.

1.3 Identidad digital: elementos, huella y derechos

- Tu identidad digital es el retrato de quién eres en línea: lo que declaras sobre ti, lo que los servicios observan y lo que infieren de tus hábitos. En esta lección desgranamos sus piezas (identificadores, atributos y credenciales), diferenciamos la huella activa de la pasiva, trabajamos la reputación online y revisamos los derechos que te protegen (UE y otros marcos). Además, aprenderás a usar identidad federada con criterio (OpenID Connect y SAML) y a aplicar un mini plan de control con acciones inmediatas.
- El objetivo es práctico: que puedas decidir qué compartes, con quién y para qué, protegerte de riesgos como la suplantación o el doxxing, y saber ejercer tus derechos

(acceso, rectificación, supresión, oposición, portabilidad, decisiones automatizadas, y el llamado «derecho al olvido» en buscadores). Terminaremos con un plan accionable y desmontando mitos frecuentes.

1.4 Protección de identidad y privacidad: medidas y herramientas prácticas

- En esta lección transformarás conceptos en hábitos. Construirás un sistema de seguridad personal por capas: contraseñas únicas con gestor, autenticación multifactor y passkeys, navegador y móvil configurados para la privacidad, dispositivos cifrados, copias de seguridad que resisten el peor día, y una rutina clara ante phishing, Wi-Fi pública y brechas de datos.
- El objetivo es que termines con un plan práctico y realista que puedas aplicar hoy mismo, y con el criterio necesario para adaptarlo a tu realidad: trabajo, estudios, ocio o gestión de una pequeña web o tienda en línea. No hace falta ser técnica o técnico: hace falta método, calma y decisiones informadas.

1.4 Navegación segura: prácticas y uso de protocolos (HTTPS, TLS, DNSSEC)

- En esta lección abrimos la “caja negra” de una visita web y la convertimos en decisiones prácticas. Verás, paso a paso, qué ocurre cuando escribes una URL: cómo DNS traduce el nombre, cómo TLS protege la conexión y cómo HTTP transporta el contenido. Aprenderás a leer las señales del navegador sin caer en falsas confianzas, a comprender el papel de los certificados y su cadena de confianza, y a usar políticas como HSTS para evitar atajos inseguros.
- Además, clarificaremos cómo se complementan DNSSEC (autenticidad e integridad) con DoH/DoT (privacidad del transporte de consultas), y te presentaremos ECH, una mejora de privacidad en TLS en despliegue progresivo. Cerrarás con una rutina de navegación segura, mini-prácticas guiadas, un memorama de conceptos y un cuestionario final. Todo con un enfoque aplicado para que navegues con criterio, en casa o en una Wi-Fi pública.

1.5 Ejercicio práctico de libre expresión escrita

- En esta lección vas a escribir tres piezas breves para aterrizar lo aprendido sobre identidad digital, privacidad y navegación segura. No se trata de memorizar siglas, sino de pensar con criterio, contarlo con tu propio estilo y convertir los conceptos en decisiones cotidianas.
- Se valorarán claridad y precisión, la aplicación de hábitos de seguridad (MFA, passkeys, marcadores, DNS seguro, GPC, copias de seguridad) y la capacidad de trasladar estas ideas a tu día a día con argumentos y ejemplos concretos.

1.6 Role playing y estado de avance

- Refuerza lo aprendido sobre identidad digital, privacidad y navegación segura con una sesión de tarjetas de repaso y un role play guiado. Volverás a los conceptos esenciales (MFA, passkeys, HTTPS/TLS, DNSSEC, DoH/DoT, HSTS, cookies seguras, GPC, copias 3-2-1, etc.) y los pondrás en práctica en un escenario realista de intento de phishing.

- El objetivo es consolidar hábitos: verificar dominios y rutas seguras, usar autenticación robusta, reducir rastreo, configurar DNS seguro y saber cómo reportar incidentes. Al final, tendrás un mini-plan de mejoras inmediatas.

1.7 Evaluación de la unidad

- Pon a prueba lo aprendido sobre identidad digital, privacidad y navegación segura. Responderás a una serie de preguntas de opción múltiple que abarcan conceptos clave como huella digital, control de datos, HTTPS/TLS, DNSSEC, DoH/DoT, autenticación (MFA y passkeys), buenas prácticas en Wi-Fi pública y copias de seguridad.
- Lee con calma cada enunciado y elige la opción que mejor refleje las prácticas y definiciones vistas en la unidad. Puedes avanzar y retroceder entre pantallas y debes responder todas las preguntas antes de finalizar.

Unidad 2: Ciberamenazas y buenas prácticas de defensa

2.1 Para comenzar

- Bienvenida a la unidad «Ciberamenazas y buenas prácticas de defensa». En pocos minutos te orientarás en el mapa básico: qué es una ciberamenaza, por qué importa la confidencialidad, integridad y disponibilidad de la información, y cómo pequeños hábitos reducen grandes riesgos.
- Verás un resumen de amenazas frecuentes (malware, ransomware, ingeniería social), la idea de «defensa por capas» (contraseñas únicas, MFA/passkeys, copias 3-2-1, segmentación) y un checklist de primeros pasos. El objetivo: empezar con claridad y motivación para profundizar en las siguientes lecciones.

2.2 Ciberamenazas e incidentes: tipología, características y ciclo de vida

- En esta lección recorrerás el mapa actual de ciberamenazas, desde malware y ransomware hasta ingeniería social, explotación de vulnerabilidades, DDoS, cadena de suministro, nube mal configurada y riesgos en móviles/IoT/OT. Te mostraremos cómo “huelen” los ataques en la práctica (patrones típicos y señales en registros/EDR/SIEM), cómo se encadenan en el tiempo (Kill Chain y MITRE ATT&CK) y cómo interrumpirlos a tiempo con defensas por capas.
- También aprenderás el ciclo de gestión de incidentes (preparación, detección y análisis, contención, erradicación, recuperación y lecciones aprendidas), la diferencia entre IOC y TTP y cómo priorizar vulnerabilidades con CVE, CVSS v4.0, KEV y EPSS. Todo con ejemplos, mini-tablas prácticas, casos de estudio y actividades para consolidar el aprendizaje.

2.3 Estrategias de protección: contraseñas robustas, MFA, antivirus y gestión de accesos

- En esta lección vas a construir una defensa por capas que funciona en el mundo real: contraseñas largas y únicas con gestor, autenticación multifactor (MFA) y passkeys

resistentes al phishing, protección del dispositivo con antivirus/EPP + EDR y lista de aplicaciones permitidas (allowlisting), y una gestión de accesos basada en mínimo privilegio, SSO y buenas prácticas para identidades privilegiadas y cuentas de servicio.
- El objetivo no es memorizar siglas, sino tomar decisiones concretas: qué activar hoy, cómo configurarlo sin fricción y cómo medir que de verdad reduce riesgo. Trabajaremos con ejemplos, mini-casos y checklists accionables, y remataremos con una autoevaluación para afianzar lo aprendido.

2.4 Vulnerabilidades y conductas de riesgo: detección temprana y guías de CCN-CERT/INCIBE

- En esta lección aprenderás a reconocer vulnerabilidades y conductas de riesgo que se convierten en incidentes, a detectar señales tempranas en correo, accesos, equipos, red y nube, y a priorizar parches con criterio usando CVSS v4.0, KEV y EPSS. También conocerás recursos prácticos de CCN-CERT e INCIBE —incluida la línea 017— y pondrás a prueba pequeños laboratorios guiados (como canary tokens) que mejoran la detección sin ruido.
- El enfoque es pragmático: menos jerga, más decisiones acertadas. Saldrás con listas claras de señales, primeras acciones, un mapa de priorización de vulnerabilidades y una mini-guía de recursos oficiales para pedir ayuda y actuar con método.

2.5 Ejercicio práctico de libre expresión escrita

- En esta lección vas a transformar lo aprendido sobre ciberamenazas y buenas prácticas de defensa en propuestas propias, claras y accionables. La actividad te invita a usar creatividad y criterio para adaptar los conceptos a tu realidad o a un caso ficticio verosímil.
- Redactarás un plan de protección por capas, diseñarás pequeñas automatizaciones defensivas y definirás un esquema simple de clasificación y manejo de la información. El objetivo es justificar decisiones con sentido práctico y medir su efectividad.

2.6 Role playing y estado de avance

- Refuerza lo aprendido con dos actividades: primero, un repaso intensivo de conceptos clave mediante fichas (flashcards). Después, un role play guiado en el que liderarás el triage y la contención de un incidente con varios hilos (BEC, ransomware y exposición en la nube), tomando decisiones prácticas y justificadas.
- El objetivo es llegar al test con ideas frescas y accionables: identificar señales tempranas, priorizar defensa por capas (MFA/passkeys, EDR y copias 3-2-1) y ordenar la gestión de vulnerabilidades con CVSS v4.0 + KEV + EPSS.

2.7 Evaluación de la unidad

- Comprueba lo aprendido en la unidad «Ciberamenazas y buenas prácticas de defensa». Encontrarás preguntas sobre amenazas habituales (ransomware, phishing/BEC), señales tempranas, Kill Chain y MITRE ATT&CK, contraseñas y MFA/passkeys, EDR y allowlisting, gestión de vulnerabilidades (CVSS v4.0 + KEV + EPSS), nube y clasificación de la información.

- Lee cada enunciado con calma y elige la opción más adecuada según los conceptos y buenas prácticas vistas. Puedes avanzar y retroceder entre pantallas antes de finalizar.

Unidad 3: Evaluación final

3.1 Evaluación final

- Esta evaluación final pone a prueba los conocimientos esenciales del curso "CIBERSEGURIDAD. RIESGOS Y AMENAZAS EN LA RED". Encontrarás preguntas de opción múltiple sobre identidad digital, privacidad y navegación segura (HTTPS/TLS, DNSSEC, DoH/DoT, HSTS, cookies seguras), así como sobre ciberamenazas y defensa por capas (ransomware, phishing/BEC, EDR, allowlisting, MFA/passkeys, gestión de vulnerabilidades con CVSS v4.0, KEV y EPSS).
- Al finalizar el bloque de preguntas también realizarás un ejercicio escrito (se te mostrará uno de tres posibles) para aplicar lo aprendido en un escenario práctico. Mantén la calma, lee con atención y toma decisiones basadas en las buenas prácticas vistas.