IFCT116 Gestión de la seguridad informática en la empresa

Sku: PC969

Horas: 60

Formato: HTML

OBJETIVOS

Gestionar la seguridad informática en la empresa, adquiriendo los conocimientos necesarios para poder establecer protocolos adecuados de seguridad sobre los equipos informáticos de la empresa y redes empresariales.

CONTENIDOS

Unidad 1.-Fundamentos y elementos de la seguridad informática

Para comenzar

- En esta lección introductoria descubrirás el propósito, el contexto y los principales términos que rigen la gestión de la seguridad informática en la empresa. Conocerás los pilares básicos de la disciplina, por qué es más relevante que nunca y cómo afecta a todos los sectores y personas de la organización. Te ayudaremos a identificar algunos conceptos clave que desarrollarás en profundidad a lo largo de la unidad.
- Navega por este módulo para preparar el terreno antes de adentrarte en los contenidos principales, ejercicios y casos prácticos.

Definición y alcance de la seguridad informática

- En esta lección descubrirás qué es la seguridad informática, cómo se ha desarrollado históricamente y cuál es su alcance en la empresa actual. Profundizarás en los conceptos de información segura, los atributos principales (confidencialidad, integridad y disponibilidad) y las dimensiones de personas, procesos, tecnología y entorno físico.
- Explorarás los marcos más relevantes (ISO/IEC 27001, NIST, CIS), los principios rectores modernos como Zero Trust, las responsabilidades de los diferentes roles y los indicadores clave que permiten medir el éxito. La lección combina explicaciones teóricas, infografías interactivas, ejemplos prácticos y preguntas para consolidar tus conocimientos.

Activos, amenazas y vulnerabilidades

- Esta lección profundiza en el triángulo fundamental de la gestión de la seguridad informática: activos, amenazas y vulnerabilidades. Aprenderás a identificar y clasificar activos críticos, analizar el panorama actual de amenazas —incluyendo actores internos y externos, tendencias como ransomware y deepfakes— y a detectar y gestionar vulnerabilidades usando marcos actuales como ISO 27005 y MAGERIT. El objetivo es que consolides una comprensión integral y aplicada del ciclo de riesgo, lista para ser llevada a tu organización.
- Incluye casos prácticos, indicadores clave, ejercicios de reforzamiento y recursos visuales interactivos para que domines la base sobre la que se apoya cualquier programa de ciberseguridad moderno.

La triada confidencialidad, integridad y disponibilidad

- En esta lección profundizaremos en la tríada fundamental de la seguridad informática: confidencialidad, integridad y disponibilidad (CIA). Analizaremos en detalle cada uno de estos pilares, sus controles asociados, amenazas actuales, tendencias emergentes y su equilibrio dinámico en los sistemas de información. Se utilizarán ejemplos reales, marcos de referencia como ISO/IEC 27001 y NIST CSF 2.0, y se revisarán indicadores clave para medir la eficacia de los controles. Además, pondrás en práctica lo aprendido con ejercicios, actividades y casos de estudio.

Evaluación y análisis de riesgos

- En esta lección realizarás un recorrido práctico y en profundidad sobre la evaluación y análisis de riesgos en la seguridad informática. Abordarás conceptos clave como activo, amenaza, vulnerabilidad, impacto, probabilidad y riesgo, e interiorizarás los marcos y metodologías más importantes del sector (ISO 27005, FAIR, MAGERIT, OCTAVE Allegro e ISO 31000). Aprenderás a convertir los datos técnicos en lenguaje de negocio, a construir mapas de calor y cuadros de mando, y a comunicar recomendaciones alineadas con los objetivos estratégicos de la organización. Incluye casos reales y ejercicios de análisis para preparar la gestión integral del riesgo.

Controles y medidas básicas de protección

- En esta lección se abordan los controles esenciales de seguridad que forman la primera línea defensiva de cualquier organización. Descubrirás por qué la higiene digital es clave para reducir la probabilidad y el impacto de incidentes, explorando medidas prácticas de inventario, endurecimiento, controles de acceso, parches, monitoreo, copias de respaldo y cultura organizacional.
- Analizaremos marcos y guías reconocidos (CIS Controls, ISO 27001, NIST CSF 2.0), ejemplos reales de brechas, errores frecuentes y cómo evitarlos, acompañados de ejercicios interactivos y preguntas de refuerzo para ayudarte a consolidar conceptos y preparar tu aplicación en entornos profesionales.

Ejercicio práctico de libre expresión escrita

- Esta lección te desafía a aplicar los conocimientos adquiridos sobre fundamentos y elementos clave de la seguridad informática en situaciones reales o hipotéticas. A través de ejercicios de expresión escrita, pondrás a prueba tu capacidad para analizar riesgos, argumentar soluciones y comunicar tus conclusiones de manera clara y profesional. Es la oportunidad perfecta para conectar teoría y práctica, y demostrar cómo la creatividad y el pensamiento crítico impulsan la ciberseguridad en las organizaciones.
- Al desarrollar estos ejercicios, fortalecerás tanto tu razonamiento técnico como tu capacidad de explicar conceptos complejos a públicos diversos, una habilidad esencial para el éxito en el sector.

Role playing y estado de avance

- En esta lección de repaso consolidarás los conocimientos fundamentales sobre seguridad informática adquiridos en la unidad. Comenzarás revisando conceptos clave mediante tarjetas didácticas interactivas, y luego participarás en una simulación de rol práctico para aplicar tu aprendizaje al contexto real de una empresa y mejorar tu capacidad de comunicar riesgos y soluciones.
- La combinación de actividades está diseñada para que refuerces tu memoria, integres las ideas principales y practiques las habilidades de comunicación clave para profesionales de la ciberseguridad.

Evaluación de la unidad

- Comprueba tus conocimientos sobre los fundamentos y elementos de la seguridad informática a través de un cuestionario de opción múltiple. Responde cuestiones clave acerca de la tríada C-I-A, activos, amenazas y vulnerabilidades, gestión del riesgo, controles esenciales, y mejores prácticas. Este test consolida los aprendizajes necesarios para avanzar con seguridad a las siguientes unidades del curso.

Unidad 2.-Políticas y auditoría de seguridad

Para comenzar

- En esta lección introductoria descubrirás la importancia de las políticas y auditorías en la seguridad informática empresarial. Conocerás los conceptos clave que estructuran el gobierno y control de la seguridad, las motivaciones regulatorias y los beneficios que aporta la gestión activa de políticas y auditorías. Al finalizar, estarás preparado para afrontar los temas que se abordarán en profundidad en el resto de la unidad.

Marco normativo: ISO 27001 y legislación

- En esta lección descubrirás el corazón normativo y legal de la gestión de la seguridad informática: la familia de normas ISO 27000, con especial énfasis en ISO/IEC 27001:2022, y las principales leyes y marcos regulatorios que impactan a las empresas en Europa y Latinoamérica, como RGPD, NIS2, DORA, PCIDSS y otros. Aprenderás cómo estos marcos se integran, qué requisitos legales son obligatorios y cómo construir una hoja de ruta práctica para que tu organización demuestre cumplimiento

ante clientes, autoridades y aseguradoras.
- Conocerás los atributos clave de ISO 27001:2022, los pasos para la certificación, el papel de la gestión de riesgos y el valor estratégico de enlazar controles técnicos con requisitos legales. Además, te guiaremos a través de casos reales, buenas prácticas, retos emergentes y herramientas para navegar el laberinto regulatorio y convertir la conformidad en una ventaja competitiva.

Componentes de una política de seguridad

- En esta lección profundizaremos en los elementos que dan forma a una política de seguridad de la información efectiva. Analizaremos los quince componentes fundamentales que debe incluir este documento clave, su propósito, buenas prácticas de redacción inclusiva, ejemplos concretos y reglas para asegurar que la política sea clara, medible y auditable. También exploraremos el proceso de desarrollo paso a paso, herramientas útiles, fragmentos comentados, métricas KPIs/KRIs y errores frecuentes a evitar. Al finalizar, estarás preparado para diseñar, redactar y evaluar políticas alineadas con los estándares ISO 27001, PCIDSS, NIS2 y RGPD.

Desarrollo y documentación de políticas

- En esta lección aprenderás en profundidad cómo desarrollar, documentar y mantener políticas de seguridad de la información alineadas con las mejores prácticas internacionales y los requisitos regulatorios actuales.
- Exploraremos el ciclo de vida de una política, desde la planificación inicial y la recopilación de requisitos, hasta la redacción, revisión, aprobación ejecutiva, divulgación, medición y auditoría continua. Se detalla cómo emplear herramientas y metodologías modernas, como "policy-as-code", control de versiones y plataformas GRC, para automatizar evidencias y facilitar el cumplimiento. También se incluyen casos prácticos, ejemplos tangibles, KPI/KRI accionables y tendencias emergentes, para que puedas liderar un proyecto de políticas robusto, auditable y eficaz en tu organización.

Metodología y fases de una auditoría

- En esta lección aprenderás cómo se planifica, ejecuta y aprovecha al máximo una auditoría de seguridad informática, con una metodología profesional alineada con marcos como ISO 19011, ISO/IEC 27007 y NIST SP 800-115. Describirás en profundidad cada una de las cinco fases de la auditoría, sus técnicas, herramientas modernas, ejemplos prácticos, y cómo traducir hallazgos técnicos en decisiones de negocio sólidas. Así, conocerás los métodos que convierten la auditoría en motor de madurez y confianza para la organización, y podrás cimentar procesos de auditoría continua mucho más allá del cumplimiento básico.

Herramientas y reporting de auditoría

- En esta lección descubrirás cómo transformar los fundamentos y la metodología de auditoría de seguridad en un proceso automatizado y realmente útil para la toma de decisiones. Aprenderás a seleccionar y combinar plataformas GRC, herramientas de

cumplimiento continuo, tecnología de auditoría asistida por ordenador (CAAT), gestión de postura de seguridad en la nube (CSPM/ASM), y motores policy-as-code para convertir los hallazgos técnicos en planes de acción y reportes ejecutivos claros, comparables y sólidos frente a auditorías externas.
- Profundizarás en ejemplos reales, mejores prácticas, métricas clave y tendencias innovadoras, con un enfoque eminentemente práctico orientado a integrar la auditoría de seguridad en la cultura corporativa y los procesos de negocio.

Ejercicio práctico de libre expresión escrita

- En esta lección tendrás la oportunidad de poner en práctica tus conocimientos sobre políticas y auditoría de seguridad de la información en el contexto empresarial. A través de actividades de expresión escrita, demostrarás tu capacidad para analizar, sintetizar y comunicar conceptos clave, así como aplicar marcos normativos y herramientas reales. Este tipo de ejercicio fomenta la creatividad, la originalidad y la reflexión crítica sobre los retos y mejores prácticas en la gestión de la seguridad informática.
- Cada actividad está diseñada para que explores situaciones reales, respondas a problemáticas actuales y utilices ejemplos basados en lo aprendido a lo largo de la unidad. Prepárate para mostrar tu comprensión, argumentación y capacidad de proponer soluciones o estrategias efectivas en el ámbito de la seguridad de la información.

Role playing y estado de avance

- Refuerza los conceptos clave y pon a prueba tus competencias en políticas y auditoría de seguridad informática. Repasa mediante flashcards todos los hitos de la unidad y simula una reunión realista entre el equipo de ciberseguridad y un/a auditor/a digital externo/a. Este repaso práctico te ayudará a medir tu progreso e identificar las áreas a fortalecer.

Evaluación de la unidad

- Evalúa los conocimientos adquiridos sobre políticas y auditoría de seguridad informática en la empresa. Responde a las preguntas basadas en los contenidos de la unidad para identificar tus avances y áreas de oportunidad en la gestión efectiva y cumplimiento de la seguridad de la información. Este test abarca conceptos normativos, componentes clave, metodología y herramientas del sector.

Unidad 3.-Estrategias de protección y defensa en profundidad

Para comenzar

- En esta lección introductoria descubrirás por qué en la actualidad una única barrera de seguridad resulta insuficiente para proteger a las empresas frente a las amenazas informáticas. Aprenderás los conceptos básicos de la defensa en profundidad, sus capas esenciales y cómo cada una contribuye a proteger la información en las organizaciones modernas. Además, conocerás qué tendencias y riesgos impulsan el cambio en las estrategias de ciberseguridad y te prepararás para explorar, en

profundidad, cada uno de los componentes a lo largo de la unidad.

Concepto de defensa en profundidad

- En esta lección exploraremos a fondo el concepto de defensa en profundidad (Defence-in-Depth, DiD), base de la seguridad informática moderna. Analizaremos por qué una sola barrera ya no basta, cómo funciona la estrategia multicapa y de superposición de controles, y cuáles son sus fundamentos teóricos y prácticos. Aprenderás a identificar y diseñar capas (identidad, red, endpoint, datos, visibilidad y resiliencia), así como a aplicar principios rectores, mapear su alineación con estándares internacionales y visualizar amenazas actuales. La lección incluye ejemplos, ejercicios interactivos y actividades de refuerzo para consolidar el aprendizaje y prepararte para diseñar arquitecturas seguras, eficientes y auditables, en línea con marcos como ISO 27001, NIST CSF, y NIS2.

Diseño de arquitecturas multicapa

- En esta lección aprenderás cómo diseñar arquitecturas multicapa de defensa en profundidad, un enfoque estratégico para gestionar riesgos y maximizar la resiliencia de los sistemas de información modernos. Analizaremos ocho principios rectores, la integración de las seis capas esenciales, el mapeo contra normas internacionales, metodologías de implementación y validación (incluyendo chaos engineering y auditoría automatizada), así como errores frecuentes, tendencias 2025-2030 y recomendaciones prácticas para cumplir con los estándares más exigentes (ISO 27001, NIS2, DORA, PCIDSS 4.0, IEC 62443).
- Pondremos especial énfasis en la automatización, la medición mediante indicadores (KPI/KRI) y la gestión de evidencias. Al terminar, dispondrás de herramientas y argumentos para exponer prototipos de arquitecturas multicapa ante la dirección o el Comité de Riesgos.

Seguridad perimetral: firewalls y UTM

- En esta lección exploraremos el papel actual de la seguridad perimetral en la protección de infraestructuras empresariales. Analizaremos la evolución de los firewalls, el valor añadido de las plataformas Unified Threat Management (UTM), la arquitectura en capas para defender la red, así como las mejores prácticas y errores frecuentes. Incluiremos ejemplos reales, métricas clave, tendencias tecnológicas y su integración en esquemas modernos como SASE y Zero Trust. Al finalizar, dominarás cómo diseñar, implementar y optimizar soluciones perimetrales alineadas con los requisitos de normativas internacionales (ISO 27001, NIS2, IEC 62443) y el enfoque de defensa en profundidad.

Seguridad interna: segmentación y hardening

- En esta lección explorarás a fondo las estrategias para blindar el "corazón" de la red empresarial. Analizaremos cómo la segmentación —desde VLAN hasta microsegmentación y nano-segmentación— limita la propagación de ataques dentro de la organización. Además, aprenderás a aplicar técnicas modernas de hardening para

reducir vulnerabilidades desde la BIOS hasta las aplicaciones y la nube, basándose en estándares como CIS, IEC 62443 y Zero Trust. Incluiremos ejemplos prácticos, metodologías de automatización y métricas clave para medir la eficacia de estas estrategias. Al terminar, estarás capacitado para diseñar y justificar una arquitectura segmentada y endurecida, preparada para auditorías rigurosas y amenazas avanzadas.

Gestión y respuesta a incidentes

- En esta lección aprenderás en detalle cómo preparar, gestionar y responder de manera profesional y eficaz a los incidentes de seguridad informática en la empresa moderna. Analizarás la convergencia de marcos normativos actuales (NIST 800-61, ISO/IEC 27035, NIS2, DORA), las fases clave del ciclo de incidentes (de la preparación al aprendizaje), el uso de tecnologías avanzadas (SOAR, XDR, backups inmutables), las cadenas de decisión y notificación, las métricas y KPIs relevantes y ejemplos prácticos.
- El objetivo es que seas capaz de diseñar y auditar un programa IR (Incident Response) moderno, automatizado y orientado al aprendizaje, que minimice la probabilidad e impacto de los ciberincidentes, cumpla requisitos regulatorios y convierta la resiliencia en ventaja competitiva.

Ejercicio práctico de libre expresión escrita

- En esta lección pondrás en práctica tu comprensión de las estrategias de protección y defensa en profundidad mediante ejercicios de redacción libre. Tendrás la oportunidad de profundizar en escenarios reales y analizar dilemas de seguridad donde podrás aportar creatividad, ejemplos propios y soluciones originales. Los temas de los ejercicios giran en torno a la aplicación de arquitecturas multicapa, respuesta ante incidentes críticos y la relación entre inspección TLS y privacidad, todo ello vinculado a normativas como ISO 27001, NIS2 y RGPD.
- Aborda cada ejercicio reflexionando no solo sobre los conceptos técnicos, sino también sobre cómo estos influyen en la gestión, cumplimiento y cultura de seguridad de una organización.

Role playing y estado de avance

- En esta lección de repaso te prepararás para consolidar todo lo aprendido sobre estrategias de protección y defensa en profundidad. A través de tarjetas didácticas, reforzarás los conceptos clave, buenas prácticas, métricas y errores comunes de la unidad. Posteriormente, participarás en un ejercicio interactivo de role-playing, poniéndote en el lugar de un analista que debe diseñar, justificar y adaptar una arquitectura de defensa en profundidad ante retos reales, con la guía de un tutor IA que simula a un directivo o consultor experimentado del sector.
- Recuerda aprovechar ambas actividades para identificar cualquier duda y repasar las áreas que más lo requieran.

Evaluación de la unidad

- En esta evaluación podrás poner a prueba tu comprensión sobre las estrategias de protección y defensa en profundidad, desde los conceptos básicos hasta controles técnicos como NGFW, MFA FIDO2, microsegmentación y respuestas ante incidentes. Lee cada pregunta con atención y selecciona la respuesta más adecuada según lo aprendido en la unidad.
- No olvides repasar conceptos clave como capas de defensa, gobernanza cuantitativa, automatización de evidencias y la aplicación de métricas (KPI/KRI).

Unidad 4.-Exploración y monitorización de redes

Para comenzar

- Comienza el módulo "Exploración y monitorización de redes" entendiendo por qué las redes forman el sistema nervioso de la empresa moderna y cómo la visibilidad es la base de la ciberdefensa. En este módulo, descubrirás conceptos esenciales como la exploración de red, el escaneo de puertos, la monitorización de tráfico y la cuantificación de riesgos. Esta introducción te guiará por los principios clave que dominarás y te permitirá identificar los retos que abordarás en las próximas lecciones.
- Te invitamos a explorar cómo se descubren los activos, por qué es importante analizar el tráfico y cómo convertir los datos de la red en decisiones proactivas para la seguridad de tu organización.

Introducción a la exploración de redes

- En esta lección descubrirás los fundamentos y la importancia de la exploración de redes en ciberseguridad. Aprenderás por qué es esencial tener visibilidad sobre los dispositivos, servicios y riesgos dentro de una red moderna, y cómo las técnicas de descubrimiento y mapeo sirven como punto de partida de cualquier programa de defensa. Además, conocerás ejemplos reales, conceptos como el fingerprinting y las diferentes capas de observación, junto con herramientas y buenas prácticas para llevar a cabo un inventario fiable. Al finalizar la lección, sabrás cómo empezar a cartografiar una infraestructura híbrida, qué información es fundamental recolectar y cómo estos datos te ayudarán a proteger tu organización frente a amenazas cada vez más avanzadas.

Métodos y técnicas de escaneo de puertos

- En esta lección descubrirás los fundamentos, métodos y técnicas modernas de escaneo de puertos, una de las disciplinas más longevas y relevantes en ciberseguridad defensiva y ofensiva. Aprenderás qué es exactamente un puerto y cómo interpretan los sistemas operativos sus estados; explorarás desde el clásico SYN scan hasta variantes avanzadas (XMAS, NULL, Idle), técnicas de alto rendimiento con Masscan y ZMap, métodos para priorizar la superficie de ataque, detección de servicios y versiones (incluyendo fingerprinting TLS JA3/JA4), tácticas de evasión y consideraciones específicas para entornos industriales, nube y despliegues multinube.
- Consolidarás los conceptos prácticos mediante ejercicios, actividades y preguntas que pondrán a prueba tu comprensión sobre el impacto real del escaneo en la gestión de riesgos y cumplimiento normativo.

Detección de servicios y sistemas operativos

- En esta lección aprenderás cómo identificar con precisión los servicios que exponen los equipos de una red, así como los sistemas operativos que utilizan. Profundizaremos en técnicas activas y pasivas de fingerprinting, el uso de banners, scripts NSE, flujos DevSecOps, y las métricas que permiten convertir una exploración técnica en inteligencia accionable. También abordarás el uso de técnicas como JA3/JA4 para analizar tráfico cifrado, integración en entornos cloud e industriales, y métodos de priorización de riesgos usando EPSS y FAIR. Al finalizar, tendrás las competencias necesarias para transformar simple información de puertos y servicios en un mapa completo de exposición y riesgo empresarial.

Análisis de tráfico con capturadores de paquetes

- En esta lección aprenderás cómo la captura y el análisis de paquetes (PCAP) se ha convertido en una herramienta fundamental tanto para la respuesta a incidentes como para la monitorización y auditorías de seguridad. Abordaremos desde los conceptos y técnicas principales de packet capture, pasando por arquitecturas y herramientas para escenarios de diferente escala, hasta el análisis práctico de las capturas y su integración con plataformas de detección, visualización y automatización.
- También aprenderás a seleccionar y configurar herramientas como tcpdump, Wireshark, Zeek y Suricata, aplicar filtros BPF avanzados, y emplear estrategias efectivas para distintas necesidades técnicas, normativas y de privacidad. Verás un laboratorio realista paso a paso, cómo interpretar y proteger las evidencias, buenas prácticas y errores a evitar.

Monitorización proactiva y alertas

- En esta lección, descubrirás cómo las organizaciones modernas utilizan la monitorización continua, el análisis de datos y la automatización para detectar amenazas, prevenir incidentes y responder rápidamente antes de que los riesgos se materialicen en ciberseguridad. Aprenderás el papel de los datos de red, plataformas, aplicaciones y usuarios en el monitoreo proactivo, así como el diseño de flujos de trabajo efectivos, sistemas de alertas inteligentes y la integración con soluciones SIEM y SOAR. Además, entenderás cómo se cuantifica el riesgo, se reducen falsos positivos y se optimiza el retorno de inversión de una arquitectura de monitorización. Ejemplos reales, infografías, ejercicios y preguntas te guiarán para aplicar estos conceptos en entornos complejos, físicos, industriales y en la nube.

Ejercicio práctico de libre expresión escrita

- En esta lección podrás aplicar los conocimientos clave de exploración y monitorización de redes en ejercicios abiertos que requieren análisis, creatividad y argumentación. Te enfrentarás a situaciones reales y análisis técnico, donde deberás proponer respuestas y planes personalizados siguiendo buenas prácticas y criterios normativos del sector.
- Es tu oportunidad para demostrar tus competencias integrando aspectos técnicos, éticos y de gestión del riesgo, valorando la importancia de la visibilidad en la seguridad informática y la toma de decisiones informada.

Role playing y estado de avance

- En esta lección de repaso consolidarás todo lo aprendido sobre exploración y monitorización de redes. Reforzarás conceptos clave mediante tarjetas didácticas y practicarás la resolución de incidentes reales a través de una dinámica de role play asistido por IA. Este espacio te prepara para afrontar la evaluación de la unidad, detectando posibles vacíos y afianzando tus habilidades prácticas.

Evaluación de la unidad

- Pon a prueba tus conocimientos sobre exploración y monitorización de redes en la empresa. Responde correctamente a las preguntas de opción múltiple para comprobar que dominas los conceptos, técnicas y buenas prácticas vistos en el módulo.

Unidad 5.-Ataques y seguridad en redes inalámbricas

Para comenzar

- En esta lección introductoria conocerás la importancia de la seguridad en redes inalámbricas empresariales, los riesgos principales que enfrentan las organizaciones y los conceptos básicos que dominarás en la unidad. También podrás poner a prueba tus conocimientos previos con preguntas sencillas. Prepárate para descubrir cómo el "aire" se ha convertido en un nuevo frente de defensa esencial para la continuidad del negocio.

Clasificación de ataques remotos

- En esta lección aprenderás a identificar y clasificar los principales ataques remotos sobre redes Wi-Fi corporativas. Profundizaremos en las seis familias de ataques más relevantes —desde la intercepción de tráfico y los famosos "Evil Twin", hasta ataques sofisticados como KRACK y Dragonblood, pasando por denial-of-service y manipulación espectral (ej. GPS spoofing sobre AFC). Analizaremos la metodología, impacto, ejemplos reales y principales medidas de defensa para cada familia, con el objetivo de darte un marco sólido para diseñar controles efectivos, evaluar riesgos y justificar inversiones en seguridad.
- Al finalizar serás capaz de reconocer los diferentes vectores de ataque, su potencial de impacto, y sabrás conectar cada amenaza remota con métricas de riesgo, controles de contención y requisitos regulatorios, ayudando a tu organización a reducir la superficie de exposición inalámbrica.

Ataques locales y escalada de privilegios

- En esta lección exploraremos el panorama de los ataques locales a redes Wi-Fi corporativas, un ámbito donde el adversario ya ha superado la "barrera del aire" y dispone de acceso físico parcial, control sobre una VLAN interna o capacidad para interactuar directamente con dispositivos o configuraciones. Analizaremos tácticas como el abuso de WPS, explotación de puertos UART/JTAG, vulnerabilidades de firmware y drivers, técnicas para escalar privilegios, y métodos de persistencia pos-

explotación, siempre relacionando impacto técnico y riesgo económico real.
- Aprenderás, además, cómo priorizar controles defensivos, desarrollar un programa de "hardening" Wi-Fi y medir el éxito mediante KPIs y buenas prácticas, ayudando a blindar la organización frente a amenazas avanzadas más allá del perímetro inalámbrico.

Fundamentos de Wi-Fi y estándares 802.11

- Esta lección ofrece una visión completa de los fundamentos técnicos y de seguridad del Wi-Fi en el entorno empresarial moderno. Recorrerás la evolución de los estándares IEEE 802.11, desde sus orígenes hasta Wi-Fi 7, y entenderás cómo la Wi-Fi ha transformado la capa física y lógica de la empresa: desde la modulación de la señal y la anatomía de una trama, hasta tecnologías como OFDMA, MU-MIMO y la Multi-Link Operation. Profundizarás en los mecanismos de seguridad, desde WEP hasta WPA3 y el uso de Protected Management Frames (PMF), así como aspectos regulatorios críticos como DFS y AFC. El objetivo es que obtengas un marco integral para comprender, diseñar y defender redes inalámbricas de alto rendimiento y riesgo controlado. Terminarás la lección con actividades prácticas, preguntas y reflexiones críticas para aplicar los conceptos adquiridos.

Amenazas y vulnerabilidades inalámbricas

- En esta lección estudiarás la amplia gama de amenazas y vulnerabilidades a las que están expuestas las redes Wi-Fi en 2025. Comprenderás por qué el "aire" se ha convertido en un vector esencial de riesgo, conocerás las principales familias de ataque (intercepción, Evil Twin, manipulación de tramas, DoS, fallas zero-click y manipulación espectral), y analizarás ejemplos reales, métricas de riesgo (EPSS, FAIR), controles de defensa y prácticas recomendadas. Al finalizar, podrás identificar, cuantificar y priorizar los peligros para diseñar estrategias de protección basadas en el valor de negocio y el costo del ataque.

Configuración segura de redes inalámbricas

- En esta lección aprenderás cómo diseñar y mantener redes Wi-Fi robustas frente a los riesgos actuales, abordando desde el cifrado y la autenticación avanzada hasta la segmentación lógica, la gestión de firmware, y la monitorización continua. Explorarás las mejores prácticas, herramientas y procedimientos para proteger la infraestructura inalámbrica corporativa, reducir la exposición a amenazas y justificar inversiones en seguridad. Cada capítulo integra ejemplos reales, estudios de caso y actividades interactivas para interiorizar los conceptos clave de seguridad inalámbrica en la empresa moderna.

Ejercicio práctico de libre expresión escrita

- En esta lección tendrás la oportunidad de aplicar y conectar los conceptos aprendidos sobre ataques y defensa en redes inalámbricas corporativas a través de ejercicios de redacción abierta. Este tipo de actividad te permite explorar escenarios reales o imaginarios, analizar riesgos, diseñar respuestas y justificar medidas de seguridad

usando tu propio criterio y creatividad. Aprovecha para demostrar tu capacidad de análisis técnico, argumentación y comunicación eficaz.
- Los ejercicios te pedirán que analices situaciones de riesgo en redes Wi-Fi, plantees estrategias de respuesta frente a incidentes recientes, y comuniques propuestas a audiencias no técnicas. Avanza por cada sección a tu ritmo y profundiza siempre que puedas aportar ejemplos o reflexiones propias.

Role playing y estado de avance

- En esta lección de repaso consolidarás los conocimientos clave sobre ataques y defensa en redes inalámbricas en entornos corporativos. Usarás tarjetas educativas para reforzar conceptos críticos y, después, participarás en un role play con un experto IA para practicar la respuesta ante incidentes y la comunicación de riesgos. Al concluir, estarás listo para afrontar la evaluación con confianza y visión práctica.

Evaluación de la unidad

- Pon a prueba tus conocimientos sobre ataques y seguridad en redes inalámbricas. La siguiente evaluación cubre los temas clave de la unidad: amenazas y vulnerabilidades, ataques remotos y locales, controles y buenas prácticas, y el impacto de la gestión de riesgos en Wi-Fi corporativo.
- Lee atentamente cada pregunta y selecciona la opción correcta en base a lo aprendido. La evaluación te ayudará a consolidar conceptos y prepararte para los desafíos reales en la gestión de la seguridad inalámbrica empresarial.

Unidad 6.-Criptografía y autenticación

Para comenzar

- Descubre por qué la criptografía y la autenticación son la base invisible de la seguridad digital en la empresa moderna. En esta introducción exploraremos los conceptos clave que harán posible proteger datos, identidades y procesos en un entorno controlado por normativas, ataques avanzados y tecnologías en constante evolución. Prepárate para aprender cómo estos pilares impactan en tu día a día, desde el email más rutinario hasta las transacciones críticas de tu organización.

Criptografía simétrica y asimétrica

- En esta lección, explorarás a fondo los fundamentos y aplicaciones prácticas de la criptografía simétrica y asimétrica en el mundo empresarial actual. Aprenderás cómo estos algoritmos forman la base de la seguridad digital, cómo se combinan en protocolos híbridos como TLS y SSH, y cuáles son las diferencias clave en su funcionamiento, fortalezas y riesgos. Además, conocerás ejemplos reales, tendencias poscuánticas y técnicas modernas de implementación y ataque, con especial atención a la gestión operativa y escenarios críticos en la industria, la banca, la nube y el IoT.

Gestión de claves y PKI

- En esta lección estudiarás el ciclo completo de la gestión de claves criptográficas y la Infraestructura de Clave Pública (PKI): qué es, por qué es esencial para la empresa moderna y todos sus componentes. Aprenderás cómo se generan claves robustas, cómo se distribuyen y almacenan de forma segura, qué riesgos y vulnerabilidades existen en cada fase, y cómo diseñar e implementar una PKI corporativa moderna que cumpla los requisitos de ciberseguridad y normativas actuales (ISO 27001, NIS 2, PCIDSS 4.0). Incluimos buenas prácticas, ejemplos operativos y estudios de caso recientes centrados en la continuidad de negocio, la protección frente a ataques, y la optimización del ciclo de vida de certificados y claves.

Firma digital y certificados

- En esta lección, descubrirás el papel fundamental que desempeñan las firmas digitales y los certificados en la economía digital y la ciberseguridad empresarial. Analizaremos cómo funcionan las firmas digitales, los algoritmos más importantes, la anatomía y ciclo de vida de los certificados X.509, y las mejores prácticas actuales para su gestión, auditoría y aplicación operativa. Aprenderás sobre los retos emergentes, incluyendo la transición hacia algoritmos poscuánticos y la defensa contra amenazas como el robo de claves o certificados engañosos. Esta lección integra aspectos técnicos, regulatorios y prácticos, preparándote para diseñar, auditar y mejorar infraestructuras de confianza en cualquier organización moderna.

Autenticación y autorización: métodos clásicos

- Explora en profundidad los métodos clásicos de autenticación y autorización que siguen sustentando la seguridad de sistemas empresariales en 2025. Desde contraseñas y funciones hash resistentes, hasta protocolos como Kerberos, RADIUS/TACACS+, 802.1X y los modelos históricos de control de acceso, esta lección te dota de un conocimiento técnico-operativo esencial para diagnosticar, fortalecer y evolucionar infraestructuras híbridas.
- Analiza las amenazas más comunes, errores frecuentes y mejores prácticas para integrar estos métodos en una arquitectura moderna de seguridad, minimizando riesgos en entornos donde la coexistencia entre lo heredado y lo nuevo es inevitable.

Multi-factor y gestión de identidades

- En esta lección estudiarás en profundidad la autenticación multifactor (MFA) y la gestión moderna de identidades digitales en entornos empresariales. Analizaremos los distintos factores de autenticación, desde los clásicos como contraseñas y tokens TOTP, hasta métodos resistentes a phishing como FIDO2 y passkeys. Verás los protocolos subyacentes (WebAuthn, CTAP2, OAuth 2.1, SCIM) y su integración con flujos corporativos (Joiner, Mover, Leaver).
- También aprenderás a planificar migraciones desde contraseñas hacia MFA y passwordless, gestionar riesgos emergentes, automatizar el ciclo de vida de identidades y cumplir con las normativas NIS2, PCIDSS y NIST SP800-63B. Todo ello a través de escenarios reales, buenas prácticas, checklist y ejemplos actuales de 2025.

Ejercicio práctico de libre expresión escrita

- En esta lección tendrás la oportunidad de aplicar de forma creativa y analítica los conocimientos adquiridos sobre criptografía y autenticación en la empresa. Resolverás desafíos prácticos inspirados en escenarios reales, poniendo a prueba tu capacidad para analizar riesgos, proponer mejoras y argumentar recomendaciones técnicas sólidas. Estas actividades están diseñadas para fomentar tu pensamiento crítico y tu originalidad, preparándote para los retos actuales y futuros de la seguridad informática corporativa.

Role playing y estado de avance

- En esta lección de repaso podrás afianzar los conocimientos clave de la unidad, poner a prueba tu memoria con tarjetas didácticas, y participar en un roleplay estratégico para practicar la toma de decisiones sobre criptografía y autenticación en escenarios reales de empresa. Revisa conceptos críticos, resolución de problemas y fortalece tus habilidades.

Evaluación de la unidad

- En esta evaluación pondrás a prueba tus conocimientos sobre criptografía y autenticación en entornos empresariales. Responderás preguntas que integran conceptos clave vistos en la unidad: cifrado simétrico y asimétrico, gestión operativa de claves, ciclo de vida de certificados, autenticación multifactor y gobierno de identidades.

Evaluación final del curso

Evaluación final

- Este examen final evalúa tus competencias en gestión de la seguridad informática abarcando conceptos, metodologías, normativas, ciberdefensa, criptografía, autenticación y gestión de incidentes en la empresa moderna. Lee bien cada pregunta antes de responder y avanza cuidadosamente, ya que no podrás regresar a preguntas previas. El examen incluye preguntas de opción múltiple y un ejercicio práctico de redacción sobre escenarios reales para validar tu comprensión y capacidad de aplicar lo aprendido en el curso.
- Recuerda organizar tus ideas, usar términos técnicos cuando corresponda y exponer argumentos sólidos para la respuesta abierta que debes desarrollar.