Centro de Entrenamiento Autorizado PLATINO

100% ONLINE

TRAYECTORIA 27 AÑOS 1998 - 2025 CALIDAD COMPROMISO

DIPLOMADO INSTITUTO LINUX

GESTIÓN DE CIBERSEGURIDAD INTELIGENTE

PARA ADMINISTRADORES DE REDES

Certificación UTN-FRD (opcional)

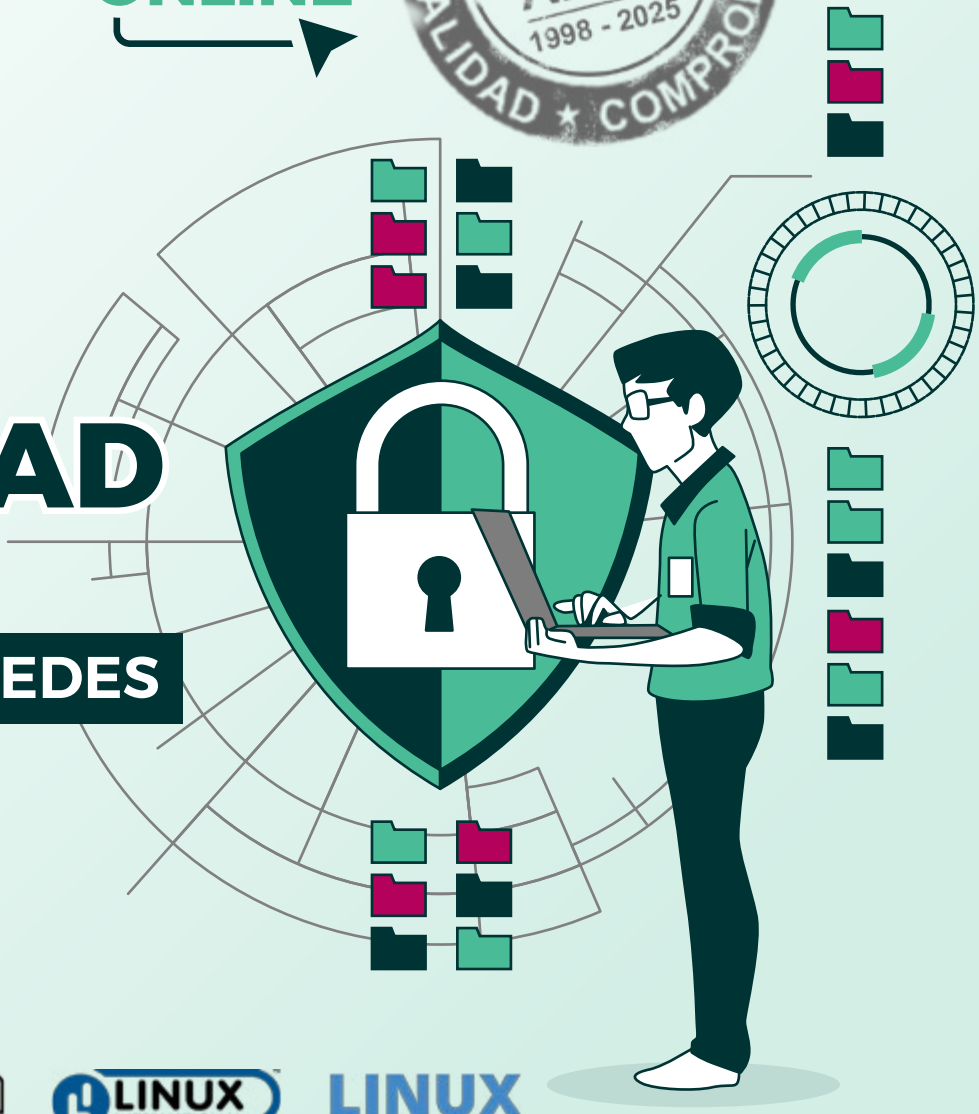

Imagen de storyset en Freepik

TEMARIO POR CLASE

CLASE 1

- Definición de ciberseguridad y su importancia.
- Clasificación y ejemplos de activos.
- Tipos de amenazas cibernéticas comunes.
- Relación entre activos, amenazas y vulnerabilidades.
- Normativas base: ISO/IEC 27001 y OWASP.

CLASE 2

- Características del malware, phishing y ransomware.
- Impacto organizacional de los ataques cibernéticos.
- Estudio de casos reales.
- Tipos de vulnerabilidades (software, hardware, humanas).
- Ataques frecuentes: DoS/DDoS, fuerza bruta, inyección SQL.

CLASE 3

- Principios: confidencialidad, integridad y disponibilidad.
- Criptografía: cifrado simétrico y asimétrico.
- Modelos de amenazas: STRIDE, DREAD, MITRE ATT&CK.
- Análisis de riesgos e impacto.
- Ejemplos prácticos de uso de modelos.

CLASE 4

- Rol del factor humano en la seguridad.
- Errores humanos más comunes en ciberseguridad.
- Tecnologías básicas: firewall, antivirus, IDS/IPS.
- Herramientas SIEM y escáneres de vulnerabilidades.
- Buenas prácticas en protección de datos.

CLASE 5

- Gestión de riesgos: identificación, evaluación, mitigación.
- Evaluación de amenazas y vulnerabilidades.
- Planificación de respuestas a incidentes.
- Tendencias actuales: IA, IoT, ransomware como servicio.
- Normativas recientes en cumplimiento y privacidad.

CLASE 6

- Definición de hacking ético y pentesting.
- Diferencias entre evaluaciones y pruebas de intrusión.
- Etapas del hacking ético: planificación, escaneo, explotación.
- Equipos red team y blue team.
- Certificaciones reconocidas: CEH, CISSP, CompTIA.

CLASE 7

- Clasificación de amenazas y tipos de ataques.
- Impacto de ataques cibernéticos en la organización.
- Uso del framework MITRE ATT&CK.
- Análisis de casos reales con TTP.
- Estudio de riesgos y consecuencias por tipo de ataque.

CLASE 8

- Herramientas de reconocimiento: Nmap, Wireshark, Maltego.
- Análisis de vulnerabilidades con Nessus y OpenVAS.
- Obtención de información en redes y sistemas.
- Técnicas de ingeniería social.
- Evaluación de vectores de ataque.

CLASE 9

- Defensas de seguridad: prevención, contención, reacción.
- Herramientas: firewall, IDS, IPS, SIEM.
- Casos de estudio y contramedidas.
- Gestión de incidentes y continuidad del negocio.
- Cultura de seguridad organizacional.

CLASE 10

- Planificación de evaluaciones de seguridad.
- Selección de herramientas y metodologías.
- Cronograma y acuerdos de confidencialidad.
- Elaboración de informes técnicos.
- Introducción a tendencias futuras: IA, Cloud, IoT.

CLASE 11

- Análisis de la Ley de Protección de Datos Personales (25326).
- Ley de Delitos Informáticos (26388).
- Ley de Firma Digital (25506).
- Responsabilidades legales del gestor de ciberseguridad.
- Evaluación de marcos legales en sectores críticos.

CLASE 12

- Modelos NIST y COBIT: estructura y objetivos.
- Aplicación práctica en gobernanza de TI.
- Comparación y complementariedad.
- Responsabilidad de la alta dirección.
- Ejemplos de aplicación en empresas reales.

CLASE 13

- Estándares ISO/IEC 27001 y 27002: estructura y controles.
- Gestión del SGSI y mejora continua.
- Implementación de controles: técnicos, físicos, humanos.
- Evaluación de desempeño y métricas.
- Contextualización con normativas locales e internacionales.

CLASE 14

- Buenas prácticas: ITIL, SABSA, OWASP.
- Integración con ISO y NIST.
- Desarrollo de PSI (Política de Seguridad de la Información).
- Evaluación de riesgos y controles apropiados.
- Auditoría y monitoreo continuo.

CLASE 15

- Concepto de continuidad del negocio.
- Normas ISO 22301 y 27031.
- Relación entre continuidad y ciberseguridad.
- Análisis de impacto y planificación estratégica.
- Integración con estándares de gestión de seguridad.

CLASE 16

- Gestión de incidentes en un SOC.
- Ciclo de vida de incidentes: detección, respuesta, recuperación.
- Análisis forense digital: técnicas y preservación de evidencia.
- Comunicación con ERISC y autoridades.
- Evaluación post-incidente y mejora continua.

CLASE 17

- Resiliencia organizacional: definición y principios.
- Diseño de sistemas resilientes: redundancia, disponibilidad.
- Estrategias de recuperación y mitigación.
- Medición de la resiliencia: KPIs y métricas.
- Fomento de una cultura de resiliencia.

CLASE 18

- Concepto y diseño de un SOC.
- Tipos de SOC: interno, gestionado, virtual.
- Componentes clave: personal, procesos, herramientas.
- Uso de SIEM y herramientas de monitoreo.
- Evaluación de la efectividad y mejora continua.

CLASE 19

- Definición y aplicaciones de IA en ciberseguridad.
- Algoritmos de ML y Deep Learning.
- Ventajas y desafíos del uso de IA.
- Aplicaciones reales: análisis de tráfico, predicción de ataques.
- Conceptos clave: NLP, aprendizaje supervisado/no supervisado.

CLASE 20

- Identificación de patrones en datos de seguridad.
- Técnicas de detección de anomalías.
- Análisis de tráfico de red con IA.
- Algoritmos comunes: clustering, correlación, series temporales.
- Casos prácticos con datasets reales (p. ej. CICIDS 2017).

CLASE 21

- Prevención de ataques en tiempo real.
- Sistemas IDS basados en IA.
- Tipos de detección: estadística, ML, heurística.
- Evaluación de efectividad de modelos.
- Técnicas de aislamiento de amenazas en entornos reales.

CLASE 22

- Automatización de análisis y respuesta a incidentes.
- Algoritmos predictivos en ciberseguridad.
- Análisis de logs con herramientas automatizadas.
- Desarrollo de modelos supervisados y no supervisados.
- Uso de transformers y redes neuronales para ciberseguridad.

CLASE 23

- Gobierno de la Seguridad de la Información (GSI).
- Estructura organizacional y normativa (ISO 27014).
- Planificación estratégica de seguridad (PESI).
- Perfil y funciones del CISO.
- Evaluación del contexto y cultura organizacional.

CLASE 24

- Gestión de proyectos de ciberseguridad.
- Fases del proyecto: inicio, ejecución, cierre.
- Análisis de riesgos y cumplimiento normativo.
- Gestión del cambio y concientización.
- Transferencia de conocimiento y mejora continua