DIPLOMATURA EN

CIBERSEGURIDAD

BLUE TEAM



INSTITUTO
LEONARDO DA VINCI

100% ONLINE

CLASES EN VIVO

DURACIÓN: 6 MESES

Defensa activa y respuesta ante incidentes.

Fundamentación

Seguridad defensiva, monitoreo y respuesta ante amenazas informáticas.

¿POR QUÉ ESTA FORMACIÓN?

Una propuesta para desarrollar capacidades de defensa activa de una organización, con herramientas de mercado y metodologías de respuesta ante incidentes. Integra infraestructura segura, monitoreo, análisis de amenazas y práctica forense.

AL FINALIZAR, VAS A PODER:

- Implementar arquitecturas de red seguras.
- Comprender y operar el ecosistema moderno de EDR y XDR.
- Desenvolverte en un centro de operaciones de seguridad (SOC).
- Ejecutar análisis forense y respuesta ante incidentes.

Salida Laboral

Analista de Seguridad SOC nivel 1
Monitorización y detección de amenazas en tiempo real.

Operador de Respuesta a Incidentes
Primeras medidas de mitigación ante un ataque informático activo.

Analista de Ciberseguridad
Monitoreo de alertas, gestión básica de vulnerabilidades y soporte en infraestructura de seguridad.

Ámbitos de trabajo: empresas privadas, organismos públicos y ejercicio independiente; banca, salud, energía, tecnología, retail, consultoras de ciberseguridad y startups.

CERTIFICACIÓN

Avales y certificaciones

Certificación final: Diplomatura en Ciberseguridad Blue Team.

CERTIFICACIÓN NACIONAL

Cámara Argentina de Formación Profesional y Capacitación Laboral.
Resolución N° 2517/17.
Certificación arancelada.

CERTIFICACIÓN INTERNACIONAL

OIEP - Organización Internacional para la Educación Permanente.
Resolución IP3 N° 427 C/22.
Certificación arancelada.

AVAL Y CERTIFICACIÓN AAPGRA

Asociación Argentina de Peritos Grafólogos y Ciencias Forenses.
Resolución N° 252/C25.
Certificación arancelada.

Código QR para verificar la autenticidad de la certificación y el cumplimiento de los requerimientos académicos.

PLAN DE ESTUDIO

Contenido

Módulo 1 de 3: Nivelación y contexto.

La industria informática y el mercado laboral

El ecosistema IT y sus roles. Dónde encaja la ciberseguridad. Salidas laborales reales en Argentina y el mundo. Certificaciones valoradas por el mercado.

Redes desde cero para defensores

Modelo OSI simplificado. TCP/IP, DNS, HTTP/S. Puertos clave: 80, 443, 22, 445, 3389. Por qué cada protocolo importa en seguridad defensiva.

Introducción a la ciberseguridad y sus roles

Red Team vs Blue Team vs Purple Team. Kill Chain de Lockheed Martin. Ciclo de vida de un ataque. El SOC como primera línea. Introducción al framework NIST CSF.

MITRE ATT&CK y Kill Chain

Estructura de MITRE ATT&CK: tácticas, técnicas, sub-técnicas. Kill Chain vs ATT&CK. Cómo leer una técnica (T-codes). Mapeo de incidentes reales.

Threat Intelligence y análisis de brechas

IOCs vs IOAs. Fuentes de inteligencia pública: VirusTotal, AlienVault OTX, AbuseIPDB. Cómo leer un Threat Report. Ciclo de inteligencia de amenazas.

Normativa: ISO 27001, NIST CSF y RGPD

ISO 27001: controles y certificación. Funciones de NIST CSF. RGPD: aplicación extraterritorial, obligaciones, notificación de brechas en 72 hs, sanciones. Impacto en el trabajo del Blue Team

Organización y operación del SOC

Niveles L1/L2/L3 y sus responsabilidades. Flujo de una alerta: detección → triage → escalado → cierre. Herramientas típicas: SIEM, SOAR, ticketing. Día a día de un analista.

PLAN DE ESTUDIO

Contenido

Módulo 2 de 3: Defensa de infraestructura.

Detección de amenazas con Sysmon

IDs de evento clave: 1 (proceso), 3 (red), 11 (archivo), 13 (registro). Configuración básica. Detección de PsExec y técnicas de movimiento lateral. Integración con SIEM.

Firewalls e IDS/IPS

Tipos de firewall: stateful, NGFW. IDS vs IPS: modo pasivo vs inline. Reglas de Snort: sintaxis básica y ejemplos reales. Dónde encajan en el flujo del SOC.

Gestión de vulnerabilidades

CVE y CVSS scoring. Ciclo de vida de una vulnerabilidad. Priorización de findings. Lectura e interpretación de reportes de escaneo. Cómo comunicar un hallazgo.

OWASP Top 10 desde el lado del defensor

Las 10 vulnerabilidades web más comunes (OWASP 2021). Para cada una: qué es el ataque y qué hace el Blue Team para detectarlo y prevenirlo. SQLi, XSS, Broken Auth, SSRF.

EPP EDR XDR con Sophos Intercept X

Evolución de la protección de endpoints. Detección por firmas vs comportamiento. Cómo funciona Sophos Intercept X. Demo en vivo: árbol de procesos, alertas y respuesta desde Sophos Central.

SIEM: arquitectura y centralización de logs

Qué es un SIEM y para qué sirve. Arquitectura: agentes, colectores, motor de correlación. Wazuh como SIEM open source. Tipos de logs que ingesta. Navegación del dashboard.

PLAN DE ESTUDIO

Contenido

Módulo 3 de 3: Monitoreo, IR y forense.

Hardening de sistemas Windows y Linux

Principio de mínimo privilegio. GPOs básicas, servicios a deshabilitar, gestión de cuentas, actualizaciones. CIS Benchmarks como referencia. Checklist de hardening.

Threat Hunting básico

Ciclo de Threat Hunting: hipótesis → búsqueda → análisis → conclusión. Diferencia entre detección reactiva y proactiva. Fuentes de datos para la caza. Casos de uso reales.

Incident Response — NIST 800-61

Fases NIST 800-61: preparación, detección y análisis, contención, erradicación, recuperación, lecciones aprendidas. Roles en cada fase. Tiempos promedio de detección en la industria.

Playbooks y simulación de incidente

Anatomía de un playbook: trigger, pasos, decisiones, escalado. Diferencia entre playbook y runbook. Ejercicio de simulación en vivo: phishing → acceso inicial → exfiltración.

Forense en memoria con Volatility

Qué contiene la memoria RAM. Comandos clave de Volatility: pslist, pstree, netscan, malfind. Cómo leer e interpretar el output. Identificación de artefactos maliciosos en memoria.

Integrador Blue Team — caso completo

Simulación end-to-end: detección → análisis → contención → forense → reporte

Docente

Experiencia en ciberseguridad, consultoría y capacitación tecnológica.



JORGE MIRO

Técnico en ciberseguridad.
Consultor de ciberseguridad.

EMPRENDIMIENTO

Co-fundador de
Netsentry Security.

FORMACIÓN Y EXPERIENCIA DESTACADAS

- Data Analytics (alianza BetaHub - Mercado Libre).
- Capacitador del programa Redes y Conectividad del Gobierno de la provincia del Chaco.
- Sophos Certified Engineer/Architect (MSP Partner Program).
- Miembro activo de la Asociación Internacional de Ciberseguridad.

INFORMACIÓN DE CURSADO

PREPARATE PARA DEFENDER SISTEMAS Y RESPONDER A INCIDENTES

MODALIDAD

100% online

DURACIÓN

6 meses

CURSADO

Clases semanales en vivo por Google Meet

RECURSOS DE APRENDIZAJE

Campus virtual y grupos de apoyo

Monitoreo, defensa y análisis de incidentes.

Diplomatura en Ciberseguridad

Blue Team