CERTIFICADO PROFESIONAL

GIUSEPPE ACADEMY · FORMACIÓN EN IA

Ciberseguridad Empresarial y Hacking Ético

Identificar, explotar de forma controlada y remediar: defender lo que la empresa no puede perder.

- 4 cursos · 16 módulos
- NIST CSF 2.0 y ISO 27001
- Pentesting aplicado
- Redes seguras y criptografía
- SIEM / SOAR y respuesta
- Enfoque práctico

01 El programa

CONTEXTO

Faltan profesionales para defender lo digital

La creciente digitalización de los procesos organizacionales y el aumento exponencial de los ciberataques generaron una demanda crítica de profesionales capaces de proteger activos digitales. Existe una brecha de talento global de más de cuatro millones de profesionales, y Latinoamérica es una de las regiones más vulnerables. Este programa surge para cubrir esa brecha, donde las empresas requieren no solo conocimientos teóricos, sino habilidades prácticas para mitigar riesgos reales.

El campo laboral es amplio: abarca desde consultoras de seguridad y departamentos de IT del sector financiero hasta la administración pública. La formación responde a la necesidad de fortalecer capacidades operativas y estratégicas, alineándose con marcos internacionales como NIST e ISO 27001.

El enfoque es eminentemente práctico: el egresado no solo identifica riesgos y vulnerabilidades, sino que ejecuta ataques controlados para validar la postura de seguridad y lidera equipos de respuesta ante incidentes.

> *Proteger la integridad, la disponibilidad y la confidencialidad de la información en entornos corporativos.*

02 Objetivos

OBJETIVO GENERAL

META PRINCIPAL

Capacitar en la identificación, explotación controlada y remediación de vulnerabilidades, integrando la gestión de riesgos y la respuesta ante incidentes para proteger la integridad, disponibilidad y confidencialidad de la información en entornos corporativos.

OBJETIVOS ESPECÍFICOS

01 Gestionar el riesgo digital y la protección de datos bajo marcos internacionales como NIST CSF 2.0 e ISO 27001.

02 Planificar y ejecutar pentesting utilizando herramientas como Nmap, Metasploit y Burp Suite para presentar hallazgos a management.

03 Implementar mecanismos criptográficos y protocolos de seguridad para proteger la transmisión de datos en redes.

04 Aplicar técnicas de hacking ético y protocolos de respuesta ante incidentes para neutralizar amenazas activas.

03 Competencias

COMPETENCIAS GENÉRICAS

Habilidades transversales

Pensamiento crítico y resolución de problemas

Formular hipótesis ante un incidente, contrastar evidencia y decidir acciones de mitigación.

Comunicación efectiva

Documentar hallazgos técnicos en informes ejecutivos de riesgo para la toma de decisiones.

Ética y responsabilidad profesional

Actuar bajo lineamientos legales y de confidencialidad en el manejo de vulnerabilidades.

COMPETENCIAS ESPECÍFICAS

Lo que sabrás hacer

Gestión de riesgos

Operar un SGSI alineando controles a estándares internacionales como ISO 27001 y NIST CSF 2.0.

Pentesting

Ejecutar análisis de vulnerabilidades y explotar fallos de seguridad de forma ética y reproducible.

Criptografía y redes

Manejar algoritmos criptográficos y configurar firewalls para el blindaje de infraestructuras de red.

Respuesta a incidentes

Operar herramientas SIEM/SOAR y aplicar playbooks para contener amenazas activas.

04 Perfil del egresado

PERFIL DEL EGRESADO

Preparado para proteger y responder

El certificado habilita a desempeñarse en roles técnicos y de gestión dentro del área de seguridad de la información.

Pentester Jr · Auditor de Seguridad · Investigador · Consultor IT · Sysadmin · Ingeniero de Redes · Analista SOC · Arquitecto de Seguridad · Auditor Lead · IT Manager

QUÉ SABRÁ

Fundamentos de hacking ético, vectores de ataque moderna, criptografía aplicada y marcos de gobierno (GRC).

QUÉ SABRÁ HACER

Realizar escaneos de vulnerabilidades, ejecutar exploits controlados, configurar perímetros seguros y liderar la respuesta técnica ante una brecha de seguridad.

DIRIGIDO A

Perfiles técnicos que quieren especializarse

Pensado para quienes se interesan tanto por la seguridad ofensiva como por la defensiva y buscan sumar habilidades prácticas para mitigar riesgos reales en entornos corporativos.

- Profesionales IT
- Analistas junior
- Administradores de sistemas
- Emprendedores tecnológicos
- Perfiles técnicos

05 Plan de estudio

CURSO 01

Riesgo Digital y Protección del Negocio

Gobierno, continuidad y cumplimiento

M1 · Aplicar frameworks (NIST, ISO 27001)

U1 · SGSI e ISO 27001:2022
Estructura de la norma · Roles y alcances · Ciclo PDCA · Evidencias auditables

U2 · NIST CSF 2.0
Funciones Identify y Protect · Detect, Respond y Recover · Gobernanza y riesgos · Métricas operativas

M2 · Riesgos, continuidad y terceros

U1 · Continuidad del negocio y DRP
Análisis de impacto (BIA) · Métricas RTO/RPO · Estrategias de recuperación · Pruebas de continuidad

U2 · Gestión de terceros y legal
Riesgo en la cadena de suministro · Ley 25.326 de Protección de Datos · Cláusulas contractuales y confidencialidad · Ética profesional

M3 · Protección de datos y clasificación

U1 · Prevención de pérdida de datos (DLP)
Inventario de activos · Clasificación y propietarios · Puntos de fuga · Telemetría de datos

U2 · Resguardo y backup
Estrategia de backup 3-2-1 · Cifrado en reposo · Gestión de llaves · Pruebas de restauración

M4 · Auditoría y mejora continua

U1 · Procesos de auditoría interna
Programa anual · Hallazgos y no conformidades · Acciones correctivas · Reporte ejecutivo

U2 · Métricas y roadmap de seguridad
Definición de KPIs y KRIs · Dashboards de control · Lecciones aprendidas · Plan de mejora trimestral

CURSO 02

Vulnerabilidades y Pentesting Aplicado

Del reconocimiento al informe ejecutivo

M1 · Reconocimiento y enumeración

U1 · OSINT y footprinting
Metodología de reconocimiento · Análisis de dominios · Búsqueda en fuentes públicas · Identificación de superficies de ataque

U2 · Escaneo con Nmap
Tipos de escaneo · Detección de servicios y versiones · Scripts NSE básicos · Evasión de firewalls

M2 · Análisis técnico de vulnerabilidades

U1 · Escaneo automatizado
Configuración de herramientas · Interpretación de resultados · Falsos positivos · Priorización por criticidad

U2 · Análisis manual
Verificación de versiones · Identificación de misconfiguraciones · Análisis de banners · Documentación de vectores

M3 · Pentesting de aplicaciones web

U1 · OWASP Top 10 – Parte A
Broken Access Control · Cryptographic Failures · Insecure Design

U2 · OWASP Top 10 – Parte B
Security Misconfigurations · Vulnerable Components · Identification Failures · Software Integrity Failures

M4 · Seguridad ofensiva (Metasploit y Burp Suite)

U1 · Ejecución de ataques controlados (Metasploit)
Uso de Metasploit · Desarrollo de exploits básicos · Técnicas de post-explotación · Movimientos laterales en la red

U2 · Pentest web (Burp Suite)
Interceptación de tráfico · Repetir y ejecutar pentest · OWASP Top 10 · Presentar hallazgos a management

CURSO 03

Redes Seguras, Accesos y Protección de Datos

Blindar la infraestructura

M1 · Infraestructura de clave pública (PKI)

U1 · Herramientas criptográficas
Uso de OpenSSL · Generación de CSR · Certificados Let's Encrypt · Automatización con ACME

U2 · Seguridad en capa de transporte
Protocolos TLS 1.2/1.3 · Cipher suites · Endurecimiento de servicios · Validación con testssl.sh

M2 · Arquitectura y segmentación segura

U1 · Diseño de red resiliente
Segmentación con VLANs · Listas de control de acceso (ACL) · Principios de Zero Trust · Modelos de confianza

U2 · Microsegmentación
Políticas deny-by-default · Hardening de equipos de red · Visibilidad inter-VLAN · Rollback de cambios

M3 · Perímetro y acceso remoto

U1 · Firewalling avanzado
Reglas de firewall y NAT · Publicación segura de servicios · Integración de IDS/IPS · Exportación de logs

U2 · Tecnologías de VPN
Implementación con WireGuard · Perfiles en OpenVPN · Túneles IPsec (StrongSwan) · Split-tunneling y seguridad

M4 · Identidades y redes inalámbricas

U1 · Federación y SSO
Gestión con Keycloak · Protocolos SAML/OIDC · Autenticación multifactor (MFA) · Mapeo de roles

U2 · Wi-Fi Enterprise
Seguridad WPA3 · Aseguramiento 802.1X · Integración con RADIUS/LDAP · Mitigación de amenazas wireless

CURSO 04

Hacking Ético

Detectar, usar y responder ante amenazas activas

M1 · Detección y prevención (IDS/IPS)

U1 · Reglas y firmas
Reglas de Emerging Threats · Firmas personalizadas · Gestión de falsos positivos · Análisis de performance

U2 · Acciones de contención
Bloqueos selectivos en pfSense · Integración con Security Onion · Playbooks de red · Registro de evidencias

M2 · Análisis de protocolos y caza de amenazas

U1 · Telemetría de red
Uso de Wireshark y Zeek · Análisis de flujos (conn.log) · Scripts de enriquecimiento · Rotación de archivos pcap

U2 · Caza de uso de hosting
Detección de beaconing · DNS respectivamente · HTTP/TLS anómalos · Análisis de conexiones largas

M3 · Operación de SIEM y XDR

U1 · Implementación con Wazuh
Registro de agentes · Normalización de eventos · Dashboards de seguridad · Correlación de alertas

U2 · Orquestación (SOAR)
Gestión de casos en TheHive · Automatización con Shuffle · Integración de inteligencia (Cortex) · Métricas de respuesta

M4 · Gestión de incidentes y post-mortem

U1 · Ciclo de respuesta
Triage y priorización · Protocolos de escalamiento · Documentación del incidente · Línea de tiempo de investigación

U2 · Reportar incidentes a directorio
Redacción ejecutiva · Storytelling de incidentes · Métricas de impacto · Comunicación efectiva

¿Estás listo para dar el primer click?

Empezá a construir tu perfil en ciberseguridad.

¡Contactanos! · Más info

WEB
giuseppeacademy.com.ar

EMAIL
info@giuseppeacademy.com.ar

DIRECCIÓN
Villa del Rosario · Córdoba · Argentina