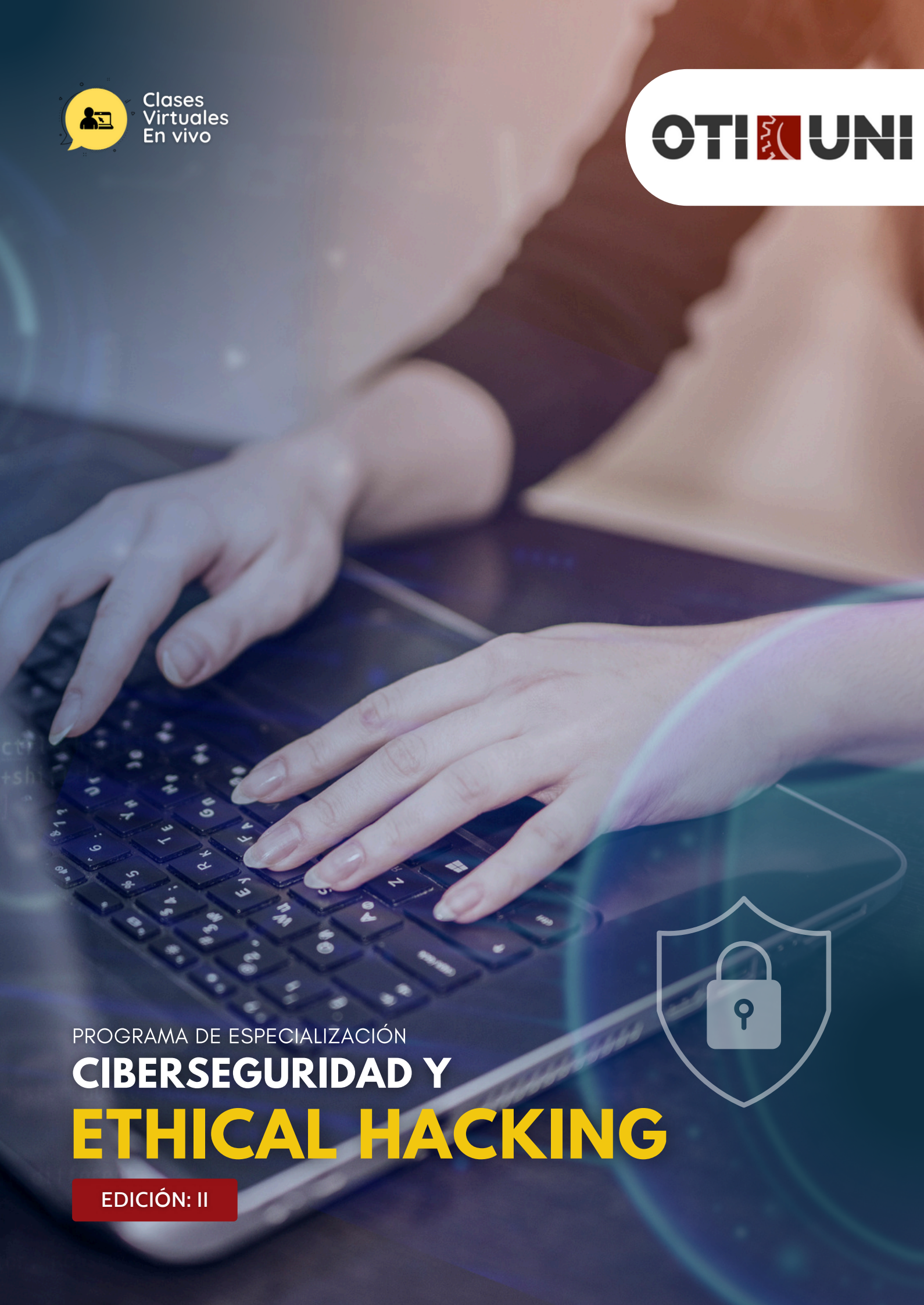
Clases
Virtuales
En vivo

OTI UNI



PROGRAMA DE ESPECIALIZACIÓN

CIBERSEGURIDAD Y ETHICAL HACKING

EDICIÓN: II

DESCRIPCIÓN

Este programa de especialización está diseñado para brindarte las herramientas, técnicas y conocimientos necesarios para proteger infraestructuras críticas, identificar vulnerabilidades, y responder ante incidentes de manera profesional. A lo largo del programa, aprenderás a implementar estándares internacionales, realizar auditorías de seguridad, y ejecutar pruebas de penetración en redes, aplicaciones web, móviles y entornos corporativos como Active Directory.

PÚBLICO OBJETIVO

- Profesionales de TI que buscan especializarse en ciberseguridad.
- Aspirantes a roles como analistas de seguridad, auditores de seguridad o pentesters.
- Responsables de proteger infraestructuras críticas y responder a incidentes.
- Estudiantes que desean fortalecer su perfil con conocimientos prácticos en estándares internacionales y herramientas de vanguardia.

¿QUÉ APRENDERÁS EN ESTE PROGRAMA?

- Implementar sistemas de gestión de seguridad de la información basados en estándares internacionales.
- Identificar y mitigar vulnerabilidades en redes, aplicaciones y sistemas.
- Responder de manera profesional ante incidentes de seguridad.
- Realizar pruebas de penetración avanzadas en aplicaciones web, móviles y entornos corporativos.
- Generar informes técnicos y ejecutivos que comuniquen hallazgos y recomendaciones de seguridad.

REQUISITOS ACADÉMICOS

- Conocimiento básico de Linux
- Equipo Windows/Linux/Mac (AMD) con mínimo 16GB de RAM

CERTIFICACIÓN

1. Certificado Digital

Al haber aprobado el programa con un **promedio ponderado mayor ó igual a 14**, se le otorga al participante un Certificado de aprobación a nombre de la Universidad Nacional de Ingeniería.

2. Constancia de Asistencia

Al participante que no cumpla con los requisitos de certificación, se le otorgará una Constancia de Asistencia del Curso, **para lo cual el alumno deberá contar con una asistencia a clase mínima del 80%**. En el caso de no cumplir con dicho requerimiento no se emitirá dicha Constancia.

EVALUACIÓN

La nota del programa se obtendrá de la siguiente manera:

El programa está estructurado de la siguiente manera: cada módulo incluirá un proyecto cuyo resultado será evaluado con una nota. El promedio final se calculará sumando las notas de los cinco módulos (N1 + N2 + N3 + N4 + N5) y dividiendo el total entre 5.

La asistencia del curso se obtendrá de la siguiente manera:

La asistencia a cada sesión se apertura automáticamente **en la plataforma CTIC VIRTUAL durante el horario de la clase.**

PLAN DE ESTUDIOS

MÓDULO 1 - SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE INCIDENTES

ENFOQUE: ISO 31000:2018, ISO/IEC 27001:2022, ISO/IEC 27005:2022, ISO/IEC 27035-1:2023, NIST CYBERSECURITY FRAMEWORK, CCSK

TEMA	NOMBRE DEL TEMA	DESCRIPCIÓN
1	▪ Contexto General e ISO/IEC 27001:2022	▪ Conceptos básicos de seguridad de la información y ciberseguridad. ▪ Estándares internacionales más importantes ▪ ISO / IEC 27001:2022 ▪ Contexto de la Organización ▪ Liderazgo, Planificación, Apoyo, Operación.
2	▪ ISO/IEC 27001:2022 y sus controles	▪ ISO/IEC 27001:2022 ▪ Operación, Evaluación de Desempeño, Auditoría Interna, Mejora ▪ Anexo A Controles de Seguridad de la Información ISO/IEC 27001:2022 ▪ Controles Organizacionales, Personas, Físicos, Tecnológicos.
3	▪ Marco de Trabajo NIST e Implementación	▪ NIST (National Institute Of Standards and Tecnology). ▪ Componentes del marco. ▪ Referencias informativas, Niveles, Perfiles ▪ Identificación del perfil actual en ciberseguridad (AS IS). ▪ Identificación del perfil deseado en ciberseguridad (TO BE). ▪ Entendimiento de la organización y alcance. ▪ Definición del modelo de madurez a utilizar. ▪ Elaboración del Programa de Ciberseguridad
4	▪ Gestión de Riesgos de Ciberseguridad	▪ Estándares de Gestión de Riesgos. ▪ Conceptos de riesgos (amenaza, vulnerabilidad, probabilidad, impacto, riesgo). ▪ Análisis para identificar riesgos de seguridad de la información y ciberseguridad. ▪ Ataques de red

TEMA	NOMBRE DEL TEMA	DESCRIPCIÓN
5	▪ Seguridad en la nube	▪ Estándares internacionales. ▪ Conceptos y arquitecturas de la computación en la nube. ▪ Gobierno y estrategias de la nube. ▪ Riesgo, auditoría y cumplimiento. ▪ Tecnologías y estrategias relacionadas.
TOTAL DE HORAS		18

MÓDULO 2 - HACKING ÉTICO

ENFOQUE: CEH, ECPPT, CPTS

TEMA	NOMBRE DEL TEMA	DESCRIPCIÓN
1	▪ Fundamentos de Ethical Hacking	▪ Introducción a las amenazas y vulnerabilidades comunes. ▪ Fundamentos de la protección contra ataques. ▪ Fases de Ethical Hacking.
2	▪ Recopilación de información y enumeración	▪ Introducción a la recopilación de información. ▪ Concepto y objetivos de la enumeración. ▪ Recopilación pasiva: técnicas y herramientas (WHOIS, Shodan,Google Dorking) ▪ Recopilación activa: técnicas y herramientas (Nmap, Recon-ng).
3	▪ Análisis de Vulnerabilidades y Escaneo	▪ Herramientas para redes y sistemas. ▪ Uso de Nessus, OpenVAS y Nikto. ▪ Referencias informativas, Niveles, Perfiles ▪ Identificación y clasificación de vulnerabilidades. ▪ Priorización y reporte inicial de hallazgos.
4	▪ Explotación y Post-Explotación	▪ Tipos de exploits: locales, remotos, servicios. ▪ Uso de Metasploit Framework. ▪ Técnicas de post-explotación (Dumping de contraseñas y enumeración del sistema.) • Ejecución de comandos y movimiento lateral
5	▪ Escalamiento de Privilegios en Sistemas Linux	▪ Técnicas comunes de elevación de privilegios en Linux. ▪ Kernel Exploits, Service Exploits, Weak File Permissions, SUID/SGID Executables, Cron Jobs. ▪ Herramientas útiles (LinPEAS, Linux Exploit Suggester, GTFOBins).

TEMA	NOMBRE DEL TEMA	DESCRIPCIÓN
6	▪ Escalamiento de Privilegios en Sistemas Windows	▪ Técnicas comunes de elevación de privilegios en Windows. ▪ Kernel Exploits, Service Exploits, Weak File Permissions, Scheduled Tasks, Password Hunting,Token Impersonation. ▪ Herramientas útiles (WinPEAS, PowerUp, Mimikatz, Metasploit).
7	▪ Generación de Informes y Buenas Prácticas	▪ Importancia de la documentación y reporte. ▪ Resumen ejecutivo. ▪ Hallazgos detallados con pruebas. ▪ Recomendaciones y remediación. ▪ Cómo comunicar resultados a clientes y equipos técnicos.
TOTAL DE HORAS		18

MÓDULO 3 - PENTESTING EN APLICACIONES WEB

ENFOQUE: BSCP, EWPTX, OSWE

TEMA	NOMBRE DEL TEMA	DESCRIPCIÓN
1	▪ Fundamentos de Tecnologías Web y Redes	▪ Arquitectura de aplicaciones web. ▪ Protocolo HTTP/HTTPS. ▪ Cookies, sesiones y autenticación. ▪ Introducción a redes y DNS. ▪ Prácticas básicas
2	▪ Metodologías y Planeación de Pentesting Web	▪ Introducción a las metodologías de pentesting. ▪ Definición del Scope (alcance). ▪ Tipos de pruebas de penetración. ▪ Introducción a estándares de seguridad.
3	▪ Reconocimiento, Enumeración y OSINT	▪ Introducción a la fase de reconocimiento y enumeración. ▪ Enumeración de dominios y subdominios. ▪ Recolección de información de servidores web. ▪ Identificación de archivos y directorios ocultos ▪ Recolección de información mediante OSINT
4	▪ Vulnerabilidades Server-Side	▪ Pruebas de autenticación y control de acceso (Server-Side). ▪ Inyección SQL (SQLi). ▪ Deserialización insegura. ▪ Remote Code Execution (RCE). ▪ Server-Side Request Forgery (SSRF). ▪ Server-Side Template Injection (SSTI).
5	▪ Vulnerabilidades Client-Side	▪ Cross-Site Scripting (XSS). ▪ Cross-Site Request Forgery (CSRF). ▪ Manejo de cookies y seguridad en el cliente. ▪ WebSockets ▪ DOM-based vulnerabilities
TOTAL DE HORAS		18

MÓDULO 4 - PENTESTING EN ACTIVE DIRECTORY

TEMA	NOMBRE DEL TEMA	DESCRIPCIÓN
1	▪ Active Directory Introducción	▪ Introducción a Componentes Lógicos. ▪ Introducción a Componentes Físicos. ▪ Introducción a Objetos del Active Directory.
2	▪ Creación de nuestro Laboratorio	▪ Levantamiento de Máquina Virtual. ▪ Configuración de Active Directory.
3	▪ Enumeración del Active Directory	▪ Enumeración de Políticas e información del Forest. ▪ Enumeración de OUs y GPOs. ▪ Enumeración de Objetos. ▪ Enumeración de ACLs. ▪ Enumeración de Relaciones de Confianza.
4	▪ Explotación de Protocolos que Interactúan en una red con AD	▪ Protocolos de Autenticación. ▪ Protocolos de Comunicación. ▪ Protocolos de Resolución.
5	▪ LSA Internals y Movimiento Lateral	▪ Autenticación de Windows. ▪ Manipulación de Tokens. ▪ Manipulación de Credenciales. ▪ Inyección de Credenciales.
6	▪ Escalación de Privilegios en Active Directory	▪ Escalación por Grupos. ▪ Security Descriptors y ACL Attacks. ▪ Ataques de Forzado de Autenticación. ▪ Across Forest (Saltar entre Dominios y Forest)..
TOTAL DE HORAS		18

MÓDULO 5 - PENTESTING EN APLICACIONES MÓVILES (ENFOQUE ANDROID)

ENFOQUE: EMAPT

TEMA	NOMBRE DEL TEMA	DESCRIPCIÓN
1	▪ Creación del laboratorio	▪ Configuración de entornos virtuales para Android (Android Studio y Emuladores Genymotion, Nox, etc). ▪ Uso de dispositivos físicos: preparación y conexión mediante ADB. ▪ Instalación de herramientas esenciales: MobSF, Apktool, Dex2Jar, JD-GUI, Jadx. ▪ Configuración de entornos de análisis dinámico con emuladores y dispositivos rooteados.
2	▪ Configuración de Burp Suite y módulos	▪ Configuración de Burp Suite para interceptar tráfico de aplicaciones Android. ▪ Instalación y configuración de certificados en dispositivos/emuladores Android. ▪ Captura y análisis de tráfico HTTP y HTTPS. ▪ Extensiones de Burp Suite para Android.
3	▪ Análisis estático (Android)	▪ Descompilación de APKs con herramientas como Apktool y JADX-GUI. ▪ Identificación de endpoints sensibles y secretos (API Keys, tokens, etc.) ▪ Análisis de permisos declarados en el archivo AndroidManifest.xml. ▪ Identificación de malas prácticas en el código fuente.
4	▪ Objection y Frida (Android)	▪ Introducción a Objection para auditorías sin root ▪ Hooking dinámico en Android con Frida. ▪ Uso de Objection para tareas comunes: bypass de detección de root, SSL Pinning y extracción de datos sensibles.

TEMA	NOMBRE DEL TEMA	DESCRIPCIÓN
5	▪ Frida Scripts (Omisión de controles) - Práctico	▪ Desarrollo de scripts personalizados con Frida. Ejemplos prácticos: ▪ Bypass de validación SSL Pinning. ▪ Omisión de detección de root. ▪ Manipulación de funciones críticas en tiempo de ejecución.
6	▪ Magisk y módulos	▪ Introducción a Magisk como herramienta para ocultar el acceso root en Android. ▪ Instalación y configuración de Magisk en dispositivos físicos. ▪ Uso de módulos de Magisk para evadir medidas de seguridad (Detección de root). ▪ Ejercicios prácticos en aplicaciones Android con medidas de seguridad avanzadas.
7	▪ Pentesting para aplicaciones en Flutter (Android)	▪ Introducción a Flutter y su impacto en pruebas de seguridad. ▪ Análisis de APKs de Flutter. ▪ Técnicas para identificar lógica de negocio en Flutter ▪ Pruebas prácticas en aplicaciones Flutter específicas para Android
TOTAL DE HORAS		18

DOCENTE

MANUEL FLORES FARFAN

Especialista en Ciberseguridad con amplia experiencia en proyectos de seguridad ofensiva, enfocado en pentesting contra infraestructuras críticas, aplicaciones web y móviles. Posee conocimientos sólidos en Red Team, seguridad aplicativa y ciberinteligencia, combinando estrategias de seguridad ofensiva y defensiva. Ha trabajado en empresas líderes de los sectores de banca y telecomunicaciones en el país. Cuenta con certificaciones reconocidas a nivel internacional, como eCPPT, CRTP, eMAPT, eWPTX y CEH Master. Además, ha sido expositor en destacados eventos de seguridad, como Ekoparty (Argentina), BSIDES, entre otros.

JAIR EDSON GARAY ALBURQUEQUE

Profesional titulado en Ingeniería de Sistemas con sólida experiencia en seguridad de la información, ciberseguridad, gestión de riesgos TI y continuidad del negocio. Ha liderado exitosamente proyectos de implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI) en entidades públicas, así como iniciativas de Continuidad Operativa y del Negocio en organizaciones del sector público y privado. En su rol actual como Especialista de Seguridad de la Información, ha desarrollado políticas y procedimientos en ciberseguridad y realizado evaluaciones de riesgos en seguridad de la información y ciberseguridad para proyectos de TI y servicios en la nube.

EDUARDO SARRIA PALACIOS

Actualmente se desempeña como Senior Ethical Hacker en Falabella. En este cargo, lidera las pruebas de vulnerabilidad en microservicios y APIs tanto en entornos de calidad como de producción, utilizando metodologías de Ethical Hacking en modalidades Black Box y Grey Box. Además, elabora informes detallados sobre las vulnerabilidades identificadas y proporciona asesoramiento técnico al equipo de desarrollo para implementar soluciones efectivas. Posee experiencia en el manejo de herramientas como Jira y Confluence.

CRISTHOPER HEREDIA LAPA

Profesional en ciberseguridad con enfoque en pruebas de penetración y análisis de amenazas cibernéticas. Especializado en pentesting de infraestructuras, aplicaciones web y móviles, así como en metodologías de Ethical Hacking (Black Box y Grey Box). Con experiencia en proyectos de seguridad ofensiva para diversos sectores, incluyendo financiero, bancario, industrial, gubernamental, farmacéutico y telecomunicaciones. Apasionado por la investigación y desarrollo en el campo de la ciberseguridad, con habilidades en desarrollo seguro y Active Directory.

(*) La Universidad se reserva el derecho de cambiar algún docente por contingencias inesperadas.

AARON PAUL PALOMINOPICOY

Bachiller en Seguridad y Auditoría Informática con más de 5 años de experiencia en pentesting y ethical hacking, con un enfoque especializado y apasionado en la evaluación y mejora de la seguridad en aplicaciones móviles, consideradas críticas en el ecosistema digital actual. Amplia experiencia en identificar vulnerabilidades y fortalecer aplicaciones móviles frente a amenazas avanzadas, además de asegurar infraestructuras y aplicaciones web mediante metodologías de seguridad reconocidas.

(*) La Universidad se reserva el derecho de cambiar algún docente por contingencias inesperadas.

INFORMACIÓN GENERAL

Horario

Sábados y domingos
de 08:00 a.m a 12:00 p.m.

Modalidad

Virtual
Clases en vivo

Duración

90 horas cronológicas
120 horas pedagógicas
25 sesiones

INVERSIÓN

PRECIO REGULAR	S/2,200

PROCESO DE INSCRIPCIÓN

Los siguientes documentos deberán ser enviado al correo electrónico:
diplomas.oti@uni.edu.pe

1. Completar y firmar la Ficha de Inscripción
2. Completar y firmar el Reglamento y Términos y Condiciones de Cursos/Programas
3. Copia simple del DNI (legible, ambas caras)
4. Voucher de pago

Nota: Una vez enviado los documentos solicitados vía correo electrónico, el participante deberá esperar la confirmación de su matrícula.

MODALIDADES DE PAGO

Banco de Crédito

Aceptamos todas las tarjetas

PASO 1: Solicita a un asesor de ventas de la Unidad de Capacitación activar el ID personal. Indicando los siguientes datos: nombre y apellidos, número de documento de identidad (DNI o pasaporte), correo electrónico, número de celular y monto a pagar.

(*) En el caso de requerir factura, se solicitará los siguientes adicionales: R.U.C, Razón Social, Domicilio Fiscal y correo electrónico donde se enviará dicha factura.

PASO 2: Procede a realizar el pago a través de los siguientes canales de pagos autorizados.

Agente y Ventanilla

Indicar el código 15226 Universidad Nacional de Ingeniería + DNI, Pasaporte o RUC del alumno, Concepto: PAGO DE ESTUDIANTES

Banca móvil - BCP

Selecciona la opción: "PAGAR SERVICIO"
Escribe en el buscador por Empresa o Servicio: "Universidad Nacional de Ingeniería"
Elije la opción de Universidad Nacional de Ingeniería "PAGO ESTUDIANTES"
Coloca tus datos personales: DNI / pasaporte / RUC
y ¡Listo, pago realizado!

Pago en Niubiz

Recibirá automáticamente un correo electrónico con el enlace para realizar el pago en línea.

COMUNÍCATE CON
WhatsApp +51 939 253 667
diplomas.oti@uni.edu.pe
Horario de atención Lun. a Vie. de 09:00 a 17:00hrs.
Oficina de Tecnologías de la Información