2026

TECH_
SENATI
Escuela de Postgrado Tecnológico

DIPLOMADO TECNOLÓGICO_

GESTIÓN DE LA CIBERSEGURIDAD

INICIO_
18 de Junio

MODALIDAD_
Online

EL **DIPLOMADO TECNOLÓGICO EN GESTIÓN DE LA CIBERSEGURIDAD** ESTÁ DISEÑADO PARA FORMAR PROFESIONALES CAPACES DE PROTEGER Y DEFENDER ACTIVOS CRÍTICOS EN ENTORNOS DIGITALES, INTEGRANDO GOBIERNO, RIESGO Y CUMPLIMIENTO, ARQUITECTURA DE SEGURIDAD, CIBERDEFENSA Y ETHICAL HACKING, CON UN ENFOQUE PRÁCTICO Y ACTUALIZADO QUE INCORPORA INTELIGENCIA ARTIFICIAL PARA ANTICIPAR AMENAZAS Y OPTIMIZAR LA TOMA DE DECISIONES EN ORGANIZACIONES MODERNAS.

DIRIGIDO A_

Profesionales técnicos, ingenieros y egresados de carreras afines a tecnologías de la información, ingeniería, telecomunicaciones, electrónica, sistemas, informática y disciplinas relacionadas, que buscan desarrollar o fortalecer competencias en la gestión integral de la ciberseguridad, tanto a nivel operativo, táctico y estratégico, incorporando enfoques modernos de gobierno, riesgo y cumplimiento (GRC), arquitectura de seguridad, ciberdefensa, aseguramiento de sistemas, seguridad ofensiva e inteligencia artificial aplicada, para desempeñarse en organizaciones públicas y privadas en entornos locales, híbridos y en la nube.

OBJETIVO_

- Formar profesionales capaces de diseñar, implementar, gestionar y evaluar integralmente la ciberseguridad organizacional, alineando el gobierno, la gestión de riesgos y el cumplimiento normativo con arquitecturas modernas de seguridad, ciberdefensa, aseguramiento de sistemas y operaciones ofensivas controladas, incorporando inteligencia artificial para la detección de amenazas, automatización de decisiones y fortalecimiento continuo de la postura de ciberseguridad en entornos locales, híbridos y en la nube.

BENEFICIOS_

- **Diseñar e implementar estrategias integrales de ciberseguridad,** alineadas a los objetivos del negocio, aplicando marcos internacionales de gobierno, riesgo y cumplimiento (GRC).
- **Desarrollar arquitecturas modernas de seguridad para entornos locales, híbridos y en la nube,** incorporando enfoques como Zero Trust, defensa en profundidad y protección de datos.
- **Fortalecer la capacidad de prevenir, detectar y responder a ciberamenazas, mediante el uso de ciberdefensa,** SOC (Security Operations Center), SIEM/XDR (Security Information and Event Management / Extended Detection and Response) y análisis de incidentes de seguridad.
- **Aplicar técnicas de aseguramiento de sistemas, redes y aplicaciones,** reduciendo vulnerabilidades y mejorando la continuidad operativa de los servicios tecnológicos.
- **Comprender y ejecutar pruebas de seguridad ofensiva (Ethical Hacking)** para identificar debilidades reales y proponer controles efectivos desde una perspectiva profesional y ética.
- **Integrar inteligencia artificial en la gestión de la ciberseguridad,** automatizando análisis, optimizando la toma de decisiones y anticipando amenazas en entornos corporativos.

¿POR QUÉ ESTUDIAR EN TECH SENATI?_

Diploma a nombre de la **Escuela de Postgrado Tecnológico TECH SENATI.**

Calidad de enseñanza respaldada por SENATI con más de 60 años en el mercado educativo ofreciendo programas de formación y capacitación.

Las **sesiones online en directo** tendrán lugar los días señalados según el horario establecido.

Las sesiones serán impartidas por docentes expertos en la industria que atenderán todas las consultas de los participantes conforme se vayan planteando.

Todas las clases serán grabadas y podrás verlas las veces que deseen.

INFORMACIÓN_

INICIO_
Jueves 18 de junio 2026

HORARIOS_
- **Martes y Jueves**
  De 7:30 p.m. a 10:30 p.m.

DURACIÓN_
144 horas

INVERSIÓN_
S/ 5,160

MODALIDAD_
Online

REQUISITOS ACADÉMICOS_
- Profesionales técnicos, egresados universitarios, de las carreras de ingeniería de sistemas, tecnologías de la información, Informática, Telecomunicaciones, Electrónica y/o a fines.
- Contar con conocimientos de computación, redes y sistemas operativos.
- Experiencia 1 año mínimo en el puesto de trabajo relacionado al área del diplomado.

MALLA CURRICULAR_

MÓDULO 01

GOBIERNO, RIESGO Y CUMPLIMIENTO DE LA CIBERSEGURIDAD

- Desarrollar la capacidad de alinear la ciberseguridad con los objetivos del negocio, gestionando riesgos y asegurando el cumplimiento de marcos y normativas internacionales.

MÓDULO 02

ARQUITECTURA DE CIBERSEGURIDAD

- Diseñar arquitecturas de seguridad modernas y resilientes que protejan datos, sistemas y redes en entornos locales, híbridos y en la nube.

MÓDULO 03

SEGURIDAD DE REDES Y CIBERDEFENSA

- Implementar controles y estrategias de ciberdefensa para prevenir, detectar y responder a amenazas en infraestructuras de red corporativas.

MÓDULO 04

ASEGURAMIENTO DE LOS SISTEMAS

- Aplicar configuraciones seguras y estándares internacionales para reducir vulnerabilidades y garantizar la continuidad operativa de los sistemas.

MÓDULO 05

ETHICAL HACKING Y SEGURIDAD OFENSIVA

- Identificar y explotar vulnerabilidades mediante pruebas controladas, fortaleciendo la seguridad desde una perspectiva ofensiva profesional.

MÓDULO 06

GESTIÓN DE LA CIBERSEGURIDAD APLICANDO INTELIGENCIA ARTIFICIAL

- Integrar inteligencia artificial en la detección de amenazas, automatización de procesos y toma de decisiones estratégicas en ciberseguridad.

PLANA DOCENTE_

MARCO PALOMINO

Gerente de Seguridad de la Información - GlobalSec Perú

Cuenta con más de 20 años de experiencia en gestión de la seguridad de la información, gestión de riesgos y TI, continuidad del negocio, así como en la implementación y cumplimiento de estándares de seguridad en empresas de los sectores de telecomunicaciones, financieros, tecnología, consultoría, petrolero, retail y gobierno. Ha ocupado cargos como Gerente de Riesgos, Operaciones y Seguridad de la Información, Oficial de Seguridad de la Información, Coordinador de Seguridad Informática y Consultor de Seguridad de la Información. Es Ingeniero de Sistemas y cuenta con certificaciones internacionales como Chief Information Security Officer (CISO), ISO/IEC 27001 Lead Implementer, Payment Card Industry Professional (PCIP), Project Management Professional (PMP), Certified Information Security Manager (CISM), Scrum Master Certified, Control Objectives for Information and Related Technology (COBIT), Information Technology Infrastructure Library (ITIL) e Information Security Foundation based on ISO/IEC 27002.

DARÍO CÓNDOR

Responsable de Ciberseguridad – Telefónica

Cuenta con más de 20 años de experiencia en planificación, ciberseguridad, gobernanza y gestión de riesgos en TI. Ha ocupado cargos como Oficial de Seguridad de Información, Consultor de Seguridad de Información, Jefe de Sistemas. Es Ingeniero de Sistemas y computación, cuenta con una Maestría en Telecomunicaciones, un MBA, un Máster Internacional en Liderazgo por EADA Business School, un doctorando en Ingeniería de Sistemas; certificaciones internacionales como Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Lead Auditor ISO/IEC 27001, Certified ISO 31000 Risk Manager e ITIL Certificate Foundation «Certificate in IT Service Management».

DIEGO HERRERA

Head of CoE Security – Telefónica

Cuenta con más de 18 años de experiencia en seguridad de la información, estrategias de ciberseguridad, implementación de tecnologías de ciberdefensa, y gestión de proyectos de cumplimiento y certificación de estándares internacionales de seguridad. Ha ocupado cargos como Arquitecto de Seguridad, Especialista en Ciberseguridad, Especialista PCI DSS y Oficial de Seguridad y Cumplimiento. Es Ingeniero Empresarial y de Sistemas, con una especialización en Prevención de Lavado de Activos y Auditoría Forense; y cuenta con certificaciones internacionales como Certified Professional Penetration Tester Extreme (eWPTX), Certified Professional Penetration Tester (eCPPT), Web Penetration Testing (eWPT), Payment Card Industry Professional (PCIP), Cybersecurity Fundamentals Certificate (CSX) e ISO 31000 Risk Manager.

ADEMIR CUADROS

Auditor Interno de TI & Ciberseguridad - Banco de Crédito BCP

Cuenta con más de 15 años de experiencia en seguridad de la información, auditoría de TI, gestión de riesgos, hacking ético y cómputo forense. Ha ocupado cargos como Subgerente de Seguridad de la Información, Auditor Interno de TI y Ciberseguridad, así como Especialista y Consultor en Seguridad de la Información. Es Ingeniero en Seguridad y Auditoría Informática, con una Maestría en Ciberseguridad y Gestión de la Información; y cuenta con certificaciones internacionales como Certified Penetration Testing Engineer, Certified Secure Web Application Engineer, ISO/IEC 27032 Senior Lead Cybersecurity Manager, ISO/IEC 27005 Senior Lead Risk Manager, ISO/IEC 27001 Auditor y AWS Certified Cloud Practitioner.

BRIAN DEXTRE

Especialista en Ciberdefensa – Banco Central de Reserva del Perú BCRP

Cuenta con más de 10 años de experiencia en ciberseguridad, seguridad ofensiva, ethical hacking, aseguramiento de aplicaciones, inteligencia de amenazas, evaluación de riesgos tecnológicos, y gestión de infraestructura de TI. Ha ocupado cargos como Especialista en Ciberseguridad, Infrastructure Security Specialist Senior - Threat Intelligence, Senior Application Analyst, Ingeniero de Servicios Especializados e Infraestructura & Soporte. Es Ingeniero en Seguridad y Auditoría Informática, con una Maestría en Ciberseguridad y Gestión de la Información; y certificaciones internacionales como eLearnSecurity Junior Penetration Tester, eLearnSecurity Web Application Penetration Tester, ELearnSecurity Certified Web Application Penetration Tester eXtreme, ELearnSecurity Certified Professional Penetration Tester, Jr Pentetration Tester (PT1), Offensive Security Wireless Professional (OSWP) y CEH Master.

TAHIRI DIKOVEC

Subgerente de Seguridad Ofensiva – MiBanco

Cuenta con más de 15 años de experiencia en ciberseguridad, pruebas de penetración, red team, ingeniería social y ciberinteligencia. Ha ocupado cargos como Experto en Ciberseguridad, Especialista en Seguridad Tecnológica y Especialista en Seguridad de la Información. Profesional en Seguridad Ofensiva y Ciberseguridad, con especializaciones internacionales en Inteligencia y Contrainteligencia, Operaciones Psicológicas y Psicosociales, Inteligencia Artificial y Marketing Político; así como certificaciones internacionales en Ciberinteligencia Ingeniería Social & OSINT, FIRST Learning Honor Code Certificate of Completion in Mastering CVSS, eLearnSecurity Junior Penetration Tester, API Security Architect, Lead Cybersecurity Professional Certificate y Certified Penetration Testing Engineer.

TECH_
SENATI
Escuela de Postgrado
Tecnológico

techsenati.edu.pe

KATIA MANSILLA
937 049 621
kmansilla@senati.edu.pe