ESCUELA DE INGENIERÍA
FACULTAD DE INGENIERÍA

(ISC)²

Diplomado en

Gestión Técnica de la Ciberseguridad

Gestiona la ciberseguridad desde una perspectiva técnica para proteger a la organización de las amenazas de hoy.
El diplomado conduce opcionalmente a la certificación Certified Information Security Systems Professional (CISSP), otorgado por la International Information System Security Certification Consortium (ISC)².

(ISC)² TRAINING OFFICIAL PROVIDER

"La particularidad de este programa es que fue diseñado en conjunto con (ISC)² para dar la posibilidad a los participantes de acceder opcionalmente a la certificación CISSP. Además, incluye una suscripción al Estudio Nacional de Ciberseguridad que realiza el Centro de Estudios de Tecnologías de la Información de la Pontificia Universidad Católica de Chile (CETIUC), todo lo cual permitirá entregar aún más valor para una adecuada gestión técnica de la ciberseguridad."

Francisco Valenzuela
Jefe del Diplomado en Gestión Técnica de la Ciberseguridad
Profesor Adjunto de la Escuela de Ingeniería y Director Ejecutivo de CETIUC.

DIRIGIDO A

» Profesionales que se desempeñan o desean hacerlo en áreas de: seguridad, centros de operaciones de ciberseguridad, ingeniería y análisis de ciberseguridad, administración de infraestructura tecnológica, operación de redes, servicios de tecnologías de información, y otros similares que sean responsables de la planificación, gestión de recursos, organización y administración de la operación de la ciberseguridad, monitoreo permanente y desarrollo de capacidades para responder frente a incidentes de ciberseguridad.

EL EGRESADO PODRÁ SER RESPONSABLE DE

» La planificación, gestión de recursos, organización y administración de la operación de la ciberseguridad.

» El monitoreo permanente y el desarrollo de capacidades para responder frente a incidentes de ciberseguridad.

OBJETIVOS DE APRENDIZAJE

» Reconocer las particularidades de las organizaciones, entornos y su impacto en las distintas arquitecturas de ciberseguridad.

» Comprender los distintos enfoques y frameworks asociados a la operación de un CSIRT e identificar las necesidades y estructura de un equipo de monitoreo y respuesta a incidentes, según las necesidades de la empresa.

» Aplicar las distintas fases del manejo de incidentes de ciberseguridad, un modelo de gestión de crisis y su integración con los otros procesos.

» Aprender las distintas técnicas, herramientas, distinguir las fuentes de información colaborativa para una operación activa de ciberseguridad.

» Comprender cómo proteger los activos de la organización a través de todo su ciclo de vida. Evaluar modelos de control de acceso para cumplir con los requisitos de seguridad empresarial.

ESTRUCTURA Y CONTENIDOS DEL PROGRAMA

Curso:
PLANIFICACIÓN DE LA CIBERSEGURIDAD Y GESTIÓN DE RECURSOS

- **PLANIFICACIÓN DE LA CIBERSEGURIDAD.**
  - La ciberseguridad en el contexto de hoy.
  - Arquitectura de seguridad.
  - Marcos de referencia para la seguridad en entornos industriales.
  - Seguridad en entornos tradicionales.
  - Seguridad en entornos cloud.
  - Situational awareness.
  - Tecnología y servicios de tecnologías de información (TI):
    - » Operación TI.
    - » Operación centro de operación de redes.
    - » Operación centro de operaciones de seguridad.
  - Modelo de seguridad detallado.

- **GESTIÓN DE RECURSOS Y CAPACIDADES DE CIBERSEGURIDAD.**
  - La realidad en Chile de la gestión de presupuesto, capital humano y la evaluación de los proveedores de ciberseguridad.
  - Mejores prácticas para la gestión de servicios de ciberseguridad.
  - Talleres para el desarrollo de habilidades blandas (liderazgo, engagement, dirección, gestión del cambio).
  - Gestión de proyectos de ciberseguridad.
    - » Gestión de proyectos tradicionales.
    - » Gestión de proyectos ágiles.
    - » Necesidades ciber de la organización (anticipación, detección y recuperación) y los proyectos que las implementan.
    - » Ejercicio aplicado de gestión de proyectos ciber (taller grupal).

Curso:
ADMINISTRACIÓN Y ORGANIZACIÓN DE LA OPERACIÓN DE CIBERSEGURIDAD

- **MONITOREO CONTINUO Y OPERACIÓN DE CIBERSEGURIDAD.**
  - Gobierno y cultura:
    - » Roles y responsabilidades de un CSIRT.
    - » CSIRT framework.
    - » Admninistración de CSIRT.
  - Operación CSOC:
    - » Framework CIS.
    - » Monitoreo de seguridad.
    - » Gestión de eventos e identidades, patch management, etc.
  - Ciberseguridad en la convergencia IT&OT.

- **RESPUESTA A INCIDENTES DE CIBERSEGURIDAD Y RECUPERACIÓN ANTE PÉRDIDA DE CONTINUIDAD DE SERVICIO.**
  - Organización de la capacidad de respuesta.
  - Las fases en el manejo de incidentes.
  - Recuperación de la operación.
  - Enfoques para la recuperación ante pérdida de continuidad de servicio.
  - Comunicación y manejo de crisis.

Curso:

TÉCNICAS Y HERRAMIENTAS DE CIBERSEGURIDAD AVANZADA

- **ANÁLISIS Y EVALUACIÓN DE TÉCNICAS Y HERRAMIENTAS DE CIBERSEGURIDAD.**
  - Threat intelligence.
  - Advanced penetration testing.
  - Threat hunting.
  - ATT&CK framework.
  - OSINT/SOCMINT.
  - Análisis de malware & ingeniería reversa.
  - Detección avanzada y análisis de intrusiones en la red.
  - Herramientas de visibilidad de vulnerabilidades en entornos OT.

- **TALLER DE USO DE HERRAMIENTAS Y TÉCNICAS DE CIBERSEGURIDAD.**
  - Uso de ATT&CK framework.
  - Análisis de malware & ingeniería reversa.
  - Uso y configuración de yara rules.
  - Automatización de fuentes de información.

Curso:

SEMINARIO DE PREPARACIÓN PARA LA CERTIFICACIÓN INTERNACIONAL CISSP

- **SEMINARIO DE PREPARACIÓN PARA LA CERTIFICACIÓN CISSP.**
  - Security and risk management.
  - Asset security.
  - Security architecture and engineering.
  - Communication and network security.
  - Identity and access management.
  - Security assessment and testing.
  - Security operations.
  - Software development.

Nota: *El orden de los cursos dependerá de la programación que realice la Dirección Académica.*

JEFE DE PROGRAMA

FRANCISCO VALENZUELA
Profesor Adjunto de la Escuela de Ingeniería UC. Ingeniero Civil Industrial, Universidad de Santiago de Chile. Diplomado en Gestión de Procesos de Negocios UC. Green Belt Lean Six Sigma, ITIL Expert, Lean IT Foundations. Director Ejecutivo del Centro de Estudios de Tecnologías de Información de la Universidad Católica (CETIUC).

EQUIPO DOCENTE

SOLEDAD BASTÍAS
Magíster e Ingeniero Civil en Informática, Universidad de Santiago de Chile. Posee diversas certificaciones internacionales en ciberseguridad: Certified Information System Auditor (CISA, Isaca), Giac Security Audit Essentials (GSAE, SANS Technology Institute), BS Lead Auditor BS 7799-2 (BSI), Certified Informations System Security Professional (CISSP, (ISC)²). Directora de Ciberseguridad de Codelco.

WILSON ESPAÑA
Ingeniero Ejecución en Computación e Informática, CISSP. Instructor Oficial Certificación CISSP. Miembro del Latin American Advisory Council de (ISC)², miembro del Chapters Advisory Committee de (ISC)², reconocido el año 2018 con el (ISC)² President's Award. Vasta experiencia en Gestión Integral de Riesgo Operacional, Seguridad de la Información y Continuidad de Negocio. Se ha desempeñado en diversos sectores del ámbito financiero, público, educacional y servicios de seguridad. Chief Information Security Officer Corporativo de SONDA S.A.

GUILLERMO GARCÍA
Magíster en Gestión de Negocios, Universidad Adolfo Ibáñez. Ingeniero Naval Electrónico, Academia Politécnica Naval. Consultor Senior en Gestión y Seguridad de Tecnologías de Información. Se ha desempeñado en áreas de TIC en destacadas compañías de telecomunicaciones y de servicios financieros como Entel, Banco de Chile, Banco de Chile US, Telefónica Manquehue y Redbanc. Profesor guía en magíster y pregrado (Universidad de los Andes, UC, Universidad Mayor, Universidad Adolfo Ibáñez). Relator de cursos de Ciberseguridad. Certificado CISSP – ITIL v3 Foundations, OSA, PPO y RCV – COBIT 4,1 Foundations – Lean IT Foundations – Scrum Fundamentals.

EQUIPO DOCENTE

CARLOS GAULE
Master en Innovación, Universidad Adolfo Ibáñez. Ingeniero Civil Electrónico, Universidad Técnica Federico Santa María. Más de 15 años de experiencia en el ámbito de la ciberseguridad, como proveedor de servicios gestionados para grandes corporaciones, liderando equipos de trabajo y gestionando las necesidades de las organizaciones. Obtuvo diversas certificaciones de CISO tales como: Network Associate, Firewall Specialist, IPS Specialist, Information Security Specialist y Security Professional. Gerente de Cumplimiento TI de Banco de Chile.

KARINA PÉREZ
Master en Business Administration and Management, Universidad de los Andes. Ingeniera Industrial y Relaciones Laborales, Universidad Católica Andrés Bello. Posee más de 20 años de experiencia en la dirección y gestión de personas, trabajando en empresas como Accenture, Imagibrain. Directora de Robert Half en Chile.

SEBASTIÁN VARGAS
Magíster en Gestión de Tecnologías de la información UOC. Diplomado en Gerencia de Seguridad de la Información, UAI. Ingeniero Civil en Informática. Docente de Posgrado en materias asociadas a Planes de Seguridad, Gestión de Riesgos de Seguridad, Seguridad Física, Linux, Speaker de seminarios y conferencias de Ciberseguridad. Más de 14 años de experiencia profesional en Seguridad de la Información, Tecnologías de la Información, Gestión y Gobierno TI. Posee las certificaciones Certified Ethical Hacking Practical Ec-council - Kaspersky Incidente Response Level 2, eJPT Elearn Security, Auditor Líder 27001, Certified ISO 22301 Foundation, Lead Cybersecurity professional Certificate LCSPC. Actualmente es Líder de Ciberseguridad en Coordinador Eléctrico Nacional.

REQUISITOS

» Los participantes del diplomado deben acreditar estudios o certificaciones en al menos una de las siguientes alternativas:

- Título Profesional Universitario de Ingeniería Civil o de Ejecución en una disciplina afín a la Informática.

- Título Técnico en una disciplina afín a la Informática con experiencia laboral de al menos 2 años en el área o áreas afines.

- El programa se inicia con un quorum mínimo de participantes.
- Las salas son asignadas dentro del Campus de Ejecución, NO NECESARIAMENTE es la misma sala todos los días.
- En caso de fuerza mayor, el programa se reserva el derecho a realizar clases por streaming, modificar fechas, lugar y/o profesores.
- Todas las modalidades del programa (dual, presencial y streaming) tienen el mismo valor. Además, recomendamos preguntar las condiciones de cada una al momento de matricularse.

ESCUELA DE INGENIERÍA
FACULTAD DE INGENIERÍA

DURACIÓN: 148 horas cronológicas

POSTULA EN: programas@ing.puc.cl

Contáctanos para trabajar contigo confeccionando el programa perfecto para tu organización.

+56 9 3353 0870

www.educacionprofesional.ing.uc.cl

Consulta por descuentos, facilidades de pago y convenios con tu banco para pago en cuotas.