PROGRAMA

Nombre del Curso: Ciberseguridad - Marco Legal, Estándares y Respuesta ante Incidentes
Cantidad de Horas Cronológicas: 25 horas en modalidad virtual online
(18 horas docencia directa + 7 aprendizaje autónomo)

Docentes:

Daniel Viveros Sepúlveda

- Ingeniero de Ejecución en Electrónica, Universidad Tecnológica Metropolitana
- Docente de la carrera tecnología en Telecomunicaciones, de la Universidad de Santiago de Chile.
- Coordinador y Relator del Diplomado en Ciberseguridad para Redes de Datos, Facultad Tecnológica, USACH.
- Basta experiencia como ingeniero Senior y Experto en numerosos Proyectos de Ciberseguridad de diferente tipo en Redes de Datos en la Empresa Movistar

Nicolás Montero Torrealba

- Posee dos másteres internacionales en Redes (UPV) y Máster Internacional en Operaciones y Análisis de Amenazas Globales (España, 2021) junto con certificaciones de reconocimiento mundial: CCNP (Enterprise y Service Provider), OSCP y CEH, que avalan su dominio técnico y su capacidad para aplicar estándares de nivel industrial.
- Profesional con más de 20 años de experiencia en redes y ciberseguridad, especializado en diseño, operación y aseguramiento de infraestructuras complejas basadas en tecnologías Cisco, Huawei y protocolos BGP, MPLS y OSPF, entre otros.
- Actualmente se desempeña como CEO de Global Secure Tech Pro, liderando proyectos de pentesting, cumplimiento ISO/IEC 27001 y diseño de arquitecturas seguras, aportando una visión integral entre la ingeniería de redes, la ciberdefensa y la docencia universitaria de excelencia.

Justificación:

El aumento sostenido de ciberataques a nivel nacional e internacional ha evidenciado la necesidad de formar profesionales en telecomunicaciones con competencias sólidas en ciberseguridad. Este curso busca ofrecer una visión integral, abordando los marcos regulatorios vigentes, los estándares técnicos aplicables y las herramientas esenciales para la gestión y respuesta ante incidentes. A través de un enfoque práctico y estratégico, los estudiantes podrán comprender la ciberseguridad como un pilar crítico en el diseño y operación de infraestructuras de red seguras.

Objetivo General:

Desarrollar en los participantes una comprensión integral de la ciberseguridad en el contexto de las telecomunicaciones, abordando su marco legal, los estándares internacionales y la gestión técnica de incidentes, mediante el análisis de casos y ejercicios prácticos orientados a entornos reales.

Requisitos Técnicos:

Conocimientos básicos de redes y protocolos TCP/IP.

Acceso a laptop personal con herramientas open source de análisis instaladas (Wireshark, Nmap, Zeek).

Objetivos Específicos:

- Analizar el marco normativo vigente en ciberseguridad a nivel nacional e internacional, con énfasis en la Ley Marco de Ciberseguridad chilena.
- Comprender y aplicar estándares internacionales como ISO/IEC 27001, NIST CSF y OWASP, en escenarios relacionados con redes y telecomunicaciones.
- Identificar las principales amenazas y vectores de ataque en infraestructuras de red.
- Utilizar herramientas técnicas para la detección, análisis y respuesta ante incidentes cibernéticos.
- Evaluar el rol de la ciber inteligencia y la inteligencia artificial en la prevención y mitigación de amenazas, junto con sus implicancias éticas.

CONTENIDOS

UNIDAD	CONTENIDOS
1	**Panorama Estratégico y Marco Legal** ● Importancia geopolítica de la ciberseguridad ● Ley Marco Chilena, CSIRT, Ciberdefensa ● Normativa internacional: NIST, ISO 27001, GDPR
2	**Gobernanza y Gestión de la Ciberseguridad** ● Rol estratégico en Telecomunicaciones ● Gestión de riesgos (ISO 31000) ● Modelos de madurez y control
3	**Amenazas y Fundamentos Técnicos** ● Principios de seguridad (CIA, criptografía, autenticación) ● Tipología de amenazas: malware, ransomware, phishing, APT ● Seguridad en redes (firewalls, VLAN, IDS/IPS)
4	**Estándares Técnicos y Buenas Prácticas** ● OWASP Top 10, CIS Controls ● Políticas de acceso, MFA, segmentación ● Hardening en dispositivos de red
5	**Respuesta ante Incidentes de Seguridad** ● Ciclo de vida del incidente (NIST IR Lifecycle) ● Herramientas: Wireshark, Zeek, Snort, Nmap ● Simulación: escaneo y análisis de tráfico malicioso
6	**Ciberinteligencia, IA y Desafíos Éticos** ● Introducción al OSINT ● Aplicaciones de IA en ciberseguridad ● Ética y regulación emergente ● Evaluación final: análisis de caso práctico en equipos