Diplomatura en Seguridad de la Información

Temario

- El rol y perfil del CISO: se profundiza en la función del máximo nivel de responsabilidad en seguridad de la información, así como también los conocimientos necesarios para aspirar al rol.

- Plan estratégico de seguridad: se plantea en profundidad el plan rector de seguridad de la información como línea de trabajo a seguir y como ordenador del resto de actividades del área.

- Frameworks, regulaciones y estándares: se presenta una serie de regulaciones, estándares, leyes y documentos formales que requieran cumplimiento, a fin de familiarizarse con los diferentes requisitos.

- Metodología de gestión de activos: se plantea la gestión de activos en base a los principales estándares de mejores prácticas estándar pilar para la gestión de la seguridad.

- Metodología de gestión de riesgos: se profundiza en la gestión de riesgos de ciberseguridad en función de diferentes estándares metodológicos existentes.

- Seguridad Física: se presentan las cuestiones a resolver desde el punto de vista físico de la ciberseguridad, con foco en el datacenter, pero extensivo a otros entornos, y considerando una planificación general.

- Gestión de accesos e identidades: se presentan las tecnologías y desafíos principales relacionados con la gestión de accesos e identidades en entornos corporativos y grandes estructuras.

- Diseño de redes seguras: se plantean los elementos, dispositivos y servicios con los que se cuenta a la hora de diseñar un ecosistema de red seguro.

- Tecnologías en la nube: se presentan las cuestiones de seguridad presentas en las tecnologías y soluciones basadas en la nube como respuesta a las necesidades de la industria.

- Operaciones de seguridad y gestión de incidentes: se plantea el funcionamiento integral de un centro de operaciones de seguridad, incluyendo la respuesta a incidentes desde un enfoque completo, orientado a procesos, y en entornos complejos.

- Continuidad de negocios: se plantea la resiliencia en tecnología como respuesta a las problemáticas de la continuidad de negocios, y se profundiza en los planes específicos para abordarla.

- Cibercrimen avanzado e investigaciones: se presentan las cuestiones relacionadas con la investigación de casos, informática forense, y temas legales a considerar.

- Procesos de auditoria: se presentan los procesos de auditoría como base para la operación de las organizaciones en entornos regulados o estandarizados.

- Inteligencia en ciberseguridad: se plantea el desarrollo de conocimientos corporativos en materia de ciber inteligencia e inteligencia de amenazas, orientadas a la protección proactiva de las organizaciones.

- DevSecOps: se plantean las formas modernas de producir software y de operar en entornos dinámicos de constante cambio y actualización.

- Criptografía Aplicada: se presentan los desafíos de la criptografía aplicada para su uso en organizaciones, en formas de protocolos y estándares.

- Evaluaciones de seguridad ofensiva: se plantea el proceso completo de un trabajo profesional de seguridad ofensiva, detallando la metodología estándar de hacking ético y las consideraciones necesarias a lo largo de la ejecución.

- Temas avanzados: se plantea una serie de tópicos más avanzados, tanto de seguridad ofensiva como defensiva, entre los cuales se encuentran ingeniería reversa, pentesting en dispositivos móviles, hardware hacking, tecnologías SOAR, ciberdefensa activa, cyber deception, caza de amenazas y purple teaming.

Cronograma de clases

Clase 1
Gestión de la seguridad de la información

- Introducción a la gestión de la seguridad
- Perfil y funciones del CISO
- Gobernanza de la seguridad
- Roles profesionales en seguridad
- El mercado de la ciberseguridad
- Certificaciones profesionales

Clase 2
Frameworks y estándares

- Estandarización y trabajo bajo norma
- ISO 27.000
- PCI-DSS
- NIST CSF

Clase 3
Organización de la seguridad

- Políticas de seguridad de la información
- Roles y responsabilidades
- Separación de funciones
- Responsabilidades de gestión
- Contacto con autoridades
- Contacto con grupos de interés
- Inteligencia de ciber amenazas
- Seguridad en la gestión de proyectos

Clase 4
Gestión de activos de información

- Ciclo de vida de la información
- Inventario de activos de información
- Uso aceptable de recursos y activos
- Devolución de activos
- Clasificación de la información
- Etiquetado de la información
- Transferencia de información
- Períodos de retención
- NIST 800-53 y ISO 55.000

Clase 5
Gestión de riesgos de seguridad

- Procesos de negocios
- Triple línea de defensa
- Riesgo inherente y residual
- Perfil de riesgos, apetito y tolerancia
- Eventos y modelado de amenazas
- Escenarios y registro de riesgos
- Metodologías de gestión de riesgos
- Evaluación de riesgos
- Análisis de impacto en el negocio
- Tratamiento de riesgos
- Indicadores de riesgo
- Diseño, implementación y efectividad de controles
- Gestión de excepciones y riesgos emergentes
- Monitoreo y reporte de riesgos

Clase 6
Gestión de identidades y accesos

- Principios y conceptos
- Protocolos y tecnologías
- Integración de la identidad como servicio

- Servicios de identidad de terceros
- Ciclo de vida del aprovisionamiento
- Control de acceso
- Gestión de identidades
- Información de autenticación
- Derechos de acceso

Seguridad con terceras partes

- Relaciones con proveedores
- Acuerdos con proveedores
- Seguridad en la cadena de suministro
- Supervisión y gestión del cambio en proveedores
- Seguridad para servicios en la nube

Clase 7
Gestión de incidentes de seguridad

- Responsabilidades de gestión de incidentes
- Evaluación y decisión sobre eventos
- Respuesta a incidentes de seguridad
- Aprendizaje de los incidentes
- Recolección de evidencias
- Seguridad durante disrupciones
- Continuidad de negocios y resiliencia
- NIST SP800-34 e ISO/IEC 27031
- Forense Informático y ISO 27.037
- CSIRT

Clase 8
Cumplimiento y leyes

- Requisitos legales, regulatorios y contractuales
- Derechos de propiedad intelectual
- Protección de datos
- Privacidad y protección de la PII
- Revisión independiente de seguridad
- Cumplimiento de políticas y estándares
- Procedimientos operativos documentados
- GDPR

Clase 9
Controles de personas

- Preselección
- Términos y condiciones de empleo
- Concientización, educación y formación
- Proceso disciplinario
- Terminación y cambio

- Acuerdos de confidencialidad y no divulgación
- Trabajo remoto
- Informes de eventos de seguridad

Clase 10
Controles físicos

- Perímetro físico
- Controles físicos de entrada
- Protección de oficinas, salas e instalaciones
- Supervisión de seguridad física
- Amenazas físicas y ambientales
- Trabajo en zonas seguras
- Escritorios y pantallas
- Ubicación y protección de equipos
- Activos fuera del establecimiento
- Medios de almacenamiento
- Utilidades de apoyo
- Seguridad del cableado
- Mantenimiento de equipos
- Eliminación o reutilización de equipos
- CPTED
- Plan de seguridad física

Clase 11
Controles tecnológicos

- Dispositivos de punto final de usuario
- Derechos de acceso privilegiados
- Restricción del acceso a la información
- Acceso al código fuente
- Autenticación segura
- Gestión de la capacidad
- Protección contra malware
- Gestión de vulnerabilidades técnicas

Clase 12
Controles tecnológicos (II)

- Gestión de la configuración
- Eliminación de información
- Enmascaramiento de datos
- Prevención de fuga de datos
- Copias de seguridad
- Redundancia de procesamiento
- Logs y registros
- Actividades de monitoreo
- Sincronización de relojes

Clase 13
Controles tecnológicos (II)

- Uso de programas privilegiados
- Instalación de software
- Controles de red
- Seguridad de servicios de red
- Filtrado web
- Segregación en redes
- Uso de la criptografía
- Ciclo de vida de desarrollo seguro
- Requisitos de seguridad de las aplicaciones
- Arquitectura de seguridad e ingeniería

Clase 14
Seguridad en el desarrollo de software

- Programación segura
- Pruebas de seguridad en desarrollo
- Desarrollo externalizado
- Separación de los entornos
- Gestión del cambio
- Información de prueba
- Protección durante auditorías y pruebas

Clase 15
Planificación estratégica de la seguridad

- Planeamiento a distintos plazos
- Ejecución de los planes
- Gestión de proyectos de seguridad

Clase 16
Procesos de auditoría

- Auditorías internas y externas
- Preparación de controles
- Proceso de auditoría
- Resultados y planes de acción

Clase 17
Arquitectura de seguridad en redes

- Dispositivos de seguridad
- Sistemas SIEM
- Protocolos de seguridad
- Zero Trust
- Análisis de tráfico
- EPP, EDR y XDR
- Tecnologías inalámbricas

Clase 18
Seguridad en entornos de nube

- Tecnologías subyacentes
- Contenedores y orquestadores
- Gestión de identidades y accesos
- Gestión de Configuraciones
- Protección de datos y automatización
- Redes en la nube
- Cumplimiento en entornos de nube
- Respuesta a incidentes
- Pruebas de penetración
- Buenas prácticas de seguridad
- Controles y guías

Clase 19
DevSecOps

- Principios de agilidad
- CI/CD
- Entrega y Despliegue
- Diseño de Pipeline
- Herramientas asociadas
- Arquitecturas y APIs
- Seguridad en la nube
- Representaciones de código
- Proveedores de nube
- Servicios de nube
- Entornos multi-nube

Clase 20
Redacción de informes técnicos

- Características de la escritura técnica
- Formatos estándar y citado
- Uso de imágenes, gráficos y tablas
- Informes de seguridad ofensiva
- Reportes e informes modelo

Clase 21
Evaluaciones de seguridad

- La mentalidad hacker
- Investigación de vulnerabilidades
- Vulnerability Assessment
- Penetration Testing
- Red Team Testing
- Prueba de seguridad física

Clase 22
Metodología de ataque

- Cybersecurity killchain
- ATT&CK Framework
- Malware y botnets
- Ransomware y cibercrimen

Clase 23
Recopilación de información

- Escaneo y enumeración
- Escaneo de vulnerabilidades
- Explotación y post-explotación

Clase 24
Criptografía

- Conceptos y elementos
- Usos de la criptografía
- Tipos de algoritmos
- Protocolos criptográficos
- Estándares de cifrado
- Protección de datos locales y en tránsito
- Esteganografía y esteganálisis
- Desafíos de la criptografía moderna
- Criptografía liviana

Clase 25
Técnicas de ataque

- Técnicas generales
- Password Cracking
- Anonimidad y privacidad
- Ingeniería Social y OSINT
- Sistemas de inteligencia y amenazas
- Deep Web y Dark Web
- Vulnerabilidades web y OWASP Top 10

Clase 26
Seguridad física ofensiva

- Tipos de amenazas
- Componentes de seguridad física
- Sistemas de suministro
- Perímetro e interiores
- Controles de acceso físico
- Protecciones en datacenters
- Detección y supresión de incendios

Clase 27
Temas avanzados de seguridad ofensiva

- Ingeniería reversa
- Pentesting en dispositivos móviles
- Hardware hacking

Clase 28
Temas avanzados de seguridad defensiva

- Tecnologías SOAR
- Ciberdefensa activa
- Cyber Deception
- Caza de amenazas
- Purple Teaming

Clase 29
Presentación de trabajos finales

Clase 30
Presentación de trabajos finales

Clase 31
Examen final teórico

Clase 32
Recuperatorios