UNIVERSIDAD BERNARDO O'HIGGINS®

Dirección de Educación Continua y Capacitación

Vicerrectoría de Vinculación con el Medio e Investigación

Diplomado en Ciberseguridad Defensiva

Dirección de Educación Continua y Capacitación

Fundamentación

Actualmente la necesidad de profesionales de Seguridad de la Información y Ciberseguridad se ha incrementado con fuerza. El costo de los ciberataques en el mundo durante el 2019 ocasionó pérdidas por la acción de cibercriminales de alrededor de USD $2,2 billones a nivel global y durante el 2020 se estima que fue de USD $6 billones.

Chile no es la excepción y últimamente se han materializado ataques cuantiosos a infraestructura crítica y financiera, siendo hoy la cantidad de profesionales insuficiente para la demanda que existe en el mercado. Por ello los profesionales de Ciberseguridad Defensiva Técnica juegan un rol clave en la Seguridad Digital del país.

Considerando lo anterior, una propuesta orientada a la formación de profesionales especialistas en Ciberseguridad Defensiva es imperativa.

Objetivo General

Profundizar y actualizar el dominio de competencias de especialidad y desarrollar nuevos conocimientos y competencias en el participante que lo habiliten para integrarse a equipos de proyecto de alto desempeño en contextos de Seguridad de la Información y Ciberseguridad relacionados al desarrollo de la Industria 4.0.

Diplomado Ciberseguridad Defensiva

Objetivos Específicos

1. Formar especialistas con conocimientos avanzados en el ámbito de la Ciberseguridad que puedan ser parte fundamental en el asesoramiento al desarrollo de proyectos informáticos y en la gestión de la Ciberseguridad de las organizaciones.

2. Formar especialistas capaces de comprender y aplicar procesos de Ciberseguridad que aseguren la disponibilidad, confidencialidad e integridad de la información corporativa de las empresas.

3. Formar especialistas en gestión de la Seguridad de la Información utilizando metodologías y estándares de uso frecuente actualmente en la industria.

Dirigido a

Profesionales y técnicos con responsabilidades y desempeño en funciones relacionadas con la ciberseguridad.

Duración

6 meses.

Metodología

La metodología de enseñanza-aprendizaje para este diplomado ha sido diseñado con orientación hacia el aprendizaje, en modalidad no presencial (e-learning asincrónico). Se utilizarán técnicas metodológicas activas donde el participante será el centro del proceso de enseñanza aprendizaje y el profesor-tutor un facilitador. El participante podrá interactuar con sus pares y con el profesor-tutor a través de los recursos tecnológicos que provee la plataforma educativa.

La plataforma provee de un ambiente de aprendizaje con recursos, actividades y apoyo tutorial, en particular a través de zoom, foros, chat en línea y presentaciones con voz, los que permiten la reflexión y aplicación de los contenidos según los objetivos y competencias establecidas.

Requisitos de Postulación

- Licenciatura, título técnico o profesional en carreras de ingeniería y afines.
- Currículum vitae.
- Copia de cédula de identidad (ambos lados).

Requisitos de Aprobación

Los postulantes deben cumplir con los siguientes requisitos:

- Los alumnos aprobarán el diplomado con nota mínima 4.0 en escala de 1 a 7.
- Asistencia de un 75% como mínimo.

Para ello cada módulo debe ser aprobado con la nota mínima, donde se realizarán controles en línea sobre los contenidos de las lecturas y las clases audio-grabadas, tareas de aplicación de los contenidos de las lecturas y prueba final en línea sobre los contenidos de las lecturas y las clases audio-grabadas.

Desarrollo del Diplomado

Este diplomado se ha desarrollado bajo 5 módulos que componen el diplomado con un total de 125 horas cronológicas, de acuerdo con el siguiente detalle:

Plan de Estudio		Modalidad	Duración
I	Seguridad de Control de Acceso e Identidad	E-Learning	25 horas
II	Seguridad en Redes VPN y Wireless	E-Learning	25 horas
III	Seguridad en End Point y Dispositivos Móviles	E-Learning	25 horas
IV	Seguridad en Servidores y Cloud	E-Learning	25 horas
V	Arquitectura Defensiva	E-Learning	25 horas

Contenido

Módulo 01: Seguridad de Control de Acceso e Identidad

Conocer los fundamentos, modelos e identificación de vectores de ataque en materias de autenticación y administración de roles para diferentes tipos de sistemas.

Contenido

- Fundamentos de seguridad y control de acceso.
- Las 5 A's del IAM.
- Proceso de gobierno de la gestión de Identidad empresarial.
- Estándares y Cumplimiento Regulatorio para el control de acceso y gestión de Identidad.
- Riesgos y vectores de ataque en control de acceso.
- Controles de seguridad en control de acceso y gestión de identidad.
- Planificación de un programa de gestión de identidad.

Módulo 02: Seguridad en Redes, VPN y Wireless

El mundo de la seguridad en redes permite proteger tanto los mecanismos como el hardware/software que sirven para la transmisión de información entre dos puntos de comunicación, ya sea de manera analógica o digital. Este módulo busca ampliar los conocimientos en seguridad de las comunicaciones, debido a que es una de las áreas en constante crecimiento y rápida evolución. Por tal razón se requiere de profesionales que se adapten a estos cambios y tengan las competencias para utilizar tanto diferentes herramientas como técnicas para una adecuada protección.

Contenido

- **Redes:**
  Introducción a la Seguridad de Redes, VPN y Wireless, Estándares, Arquitectura de protocolos, Comunicaciones de datos y redes, Transmisión de datos, Medios de transmisión, Técnicas para la codificación de señales, Técnicas de comunicación de datos digitales, Protocolos de control del enlace de datos, Seguridad en redes, Aplicaciones Distribuidas.
- **VPN:**
  Introducción a la Seguridad de Redes, VPN y Wireless, Estándares, Arquitectura de protocolos, Comunicaciones de datos y redes, Transmisión de datos, Medios de transmisión, Técnicas para la codificación de señales, Técnicas de comunicación de datos digitales, Protocolos de control del enlace de datos, Seguridad en redes, Aplicaciones Distribuidas.

Contenido

Wireless:
Introducción de las tecnologías Wireless, Introducción a la Seguridad Wireless, Amenazas Wireless, Tecnologías Wireless y aplicaciones, Estrategias de implementaciones Wireless, Protocolos de seguridad inalámbrica y criptografía, Consideraciones de seguridad para dispositivos inalámbricos, Estándares y tecnologías inalámbricas, Acceso inalámbrico seguro a datos, Evaluación de redes de área local inalámbricas.

Módulo 03: Seguridad en End Point y Dispositivos Móviles

Un EndPoint es un dispositivo informático remoto que se comunica con una red a la que está conectado. Dentro de la familia de los endpoint se tienen: computadores de escritorio, servidores, entre otros. Cabe considerar que dentro de esta familia existe un subconjunto, los cuales son los dispositivos móviles, tales como tablets, smartphones y notebooks.

Contenido

- ¿Qué es un endpoint?.
- Seguridad en Sistemas Operativos de endpoint.
- Seguridad en Aplicaciones de endpoint.
- ¿Qué es un dispositivo móvil?.
- Seguridad en Sistemas Operativos de dispositivos móviles.
- Seguridad en Aplicaciones de dispositivos móviles.

Módulo 04: Seguridad en Servidores y Cloud

Este módulo tiene por objetivo presentar los conceptos asociados a la protección de servidores en función de la infraestructura donde han sido definidos, esto es, On Premise o en la Nube. El propósito es identificar los posibles controles de seguridad de acuerdo al tipo de infraestructura y así gestionar los riesgos asociados a ésta.

Contenido

1. Servidores y/o Infraestructuras de Servidores.
   - Definiciones de servidores en relación a la infraestructura y cómo están definidos.
   - Diferencias entre una infraestructura física y un modelo de servicio en la Nube.
   - Ventajas y riesgos en cada tipo de infraestructura.

Contenido

2. Modelos para gestionar la seguridad.
   - Evolución y los diferentes modelos para gestionar la seguridad en infraestructura.
   - Definición de conceptos: Hardening, gestión de vulnerabilidades en servidores, Red Team, Blue Team, White Team, seguridad por diseño y el modelo Zero Trust.

3. Gestión de la Seguridad bajo el modelo Zero Trust.
   - Desarrollo de la aplicación del modelo Zero Trust en la gestión de la seguridad de los servidores.
   - Diferencias de la infraestructura donde los servidores están definidos.

4. Seguridad en la Nube.
   - Conceptos asociados a los modelos de servicios en la Nube.
   - Elementos asociados a la definición de servidores en los distintos modelos.
   - Diferencias respecto a los servidores físicos.
   - Cómo se gestiona la seguridad de los servidores en el contexto de Zero Trust.
   - Cómo gestionar los incidentes.

5. Seguridad en servidores y gestión de riesgos.
   - Gestión de riesgos con foco en los servidores.
   - Modelos de Gestión de la seguridad y gestión de riesgos.
   - Propuesta de un modelo de indicadores de gestión de riesgo para servidores.

Módulo 05: Arquitectura Defensiva

En la actualidad tener una red conectado a Internet es algo riesgoso. El Internet, ahora se ha convertido en un medio hostil e inseguro, con la aparición de nuevos malwares y diversos tipos de ataques en la red. Por lo que, se ha vuelto importante proteger las organizaciones de manera práctica de los ciberdelincuentes ante ataques.

Contenido

1. Firewall con Linux.
   - Que es un firewall, Tipos de firewall, Ventajas de un firewall, Implementación de firewall, Bloqueo de puertos, bloqueo de servicios.
2. Sistema de Prevención de Intrusos.
   - Que es un Sistema de Prevención de Intrusos, Clasificación de los IPS, Funcionamiento del IPS, Implementación de IPS con Snort.
3. SIEM.
   - Que es un SIEM: Importancia de contar con un SIEM, Como funciona la tecnología SIEM, Beneficios de los sistemas SIEM, Implementación de Alient Vault OSSIM.

Contenido

4. Monitoreo de Evento de Red.
   - Porque monitorear, Ventajas del monitoreo, Tipos de monitoreo, implementación de Zabbix.
5. Control de Acceso a la Red.
   - Que es NAC, Importancia de contar con un NAC, Capacidades de la una solución NAC, Implementación de NAC con PacketFence.

Equipo Docente

Ing. Rodrigo Pérez

Ingeniero en Ciberseguridad CIISA, Ingeniería de Ejecución en Informática mención Desarrollo de Sistemas (AIEP), Diplomado de Seguridad de la Información (Duoc UC), Certificado en Gobierno y Gestión de Ciberseguridad usando COBIT (USACH), Scrum Foundation Professional Certificate (SFPC-Certiprof), Lead Cybersecurity Professional Certificate (LCSPC-Certiprof), Certificación Auditor Líder ISO 27.001, Certificación Fundamentos ITIL v201.

Se ha desempeñado en cargos de Oficial de Seguridad de la Información y Asesor de Seguridad de la Información y Ciberseguridad como implementado Sistemas de Gestión de Seguridad de la Información, coordinando equipos de tecnologías de la información, desarrollo, recursos humanos, capacitación, comunicaciones y equipos directivos , además ha realizado análisis de riesgos en concordancia con normativas nacionales e internacionales, con los lineamientos estratégicos de la organización, proponiendo políticas y procedimientos al Comité de Seguridad de la Información. Actualmente se desempeña como colaborador del Jefe de Estado en el diseño, formulación e implementación de políticas, planes y programas que contribuyan al desarrollo cultural y patrimonial de manera armónica y equitativa en todo el territorio nacional, en el El Servicio Nacional del Patrimonio Cultural.

Ing. Ricardo Urbina

Ingeniero en Informática y Gestión, Universidad Diego Portales, certificado en GSPT Scada Penetration Tester, Cybertrust Academy. Más de veinte y cinco años de experiencia en servicios de Tecnologías de la Información y Comunicaciones (TIC), siendo en los últimos 16 años Oficial de Seguridad de la Información (OSI), gestionando los distintos temas asociados a la Seguridad de la Información tanto dentro de las Organizaciones como para clientes de éstas. Actualmente se desempeña como OSI en el Grupo Elecmetal, correspondiendo a un Grupo de Empresas Productivas donde debe interactuar transversalmente en todas ellas, apoyando la Gestión de la Seguridad de la Información con foco en Redes Productivas y SAP. De manera paralela, se desempeña como Presidente del Capítulo Chileno del Cloud Security Alliance, organización sin fines de lucro cuyo objetivo es difundir las mejores prácticas de Seguridad de la Información para ambientes tecnológicos en la Nube.

Equipo Docente

Ing. Diego Muñoz

Master en Seguridad Ofensiva ©, Universidad Católica de Murcia-España, Magíster de Ingeniería en Seguridad de la Información©, Universidad Mayor-Chile, Ingeniero en Informática mención Ciberseguridad, IPP. Especialista en Inteligencia Militar mención Contrainteligencia – Escuela de Inteligencia Naval, Armada de Chile. Posee una investigación en: Methodology for malware scripting analysis in controlled environments based on Open Source tools (2019), Communications Computer and Information Science, México. Actualmente se desempeña como Investigador y Jefe Sección Capacitaciones en Ciberseguridad Online del Centro de investigación en Ciberseguridad, Universidad Mayor y Director Ejecutivo de Sombrero Blanco Ciberseguridad. Desarrolla cátedras en la Universidad Mayor, Universidad Diego Portales, CO-CHAIR of track information security en International Congress of Telematics & Computing, México, entre otras. Ha gestionado y participado en seminarios 2020: II Conferencia de Ciberseguridad "Cibercrisis" de Sombreros Blancos, I Criptofestival, CONVID 2020, Derecho y Tecnologías de Información SEGDATA y Ciberseguridad Blue & Red de Sombreros Blancos.

Ing. Eder Patricio Moran

Ingeniería en Tecnologías de la Información y Comunicaciones, Universidad San Sebastián, Ingeniería de Sistemas e informática, Universidad Privada Telesup, Perú. Diplomado en Gobernanza, Gestión y Auditoría a la Ciberseguridad (USACH) Lead Cybersecurity Professional Certificate LCSPC° (Certiprof). Certificaciones en Gobierno y gestión de la ciberseguridad usando NIST (USACH) Cyber Security Foundation (CSFPC) – Certiprof, Gobierno y Gestión de TI usando COBIT (USACH), Auditor LIDER ISO 27001 (USACH), Seguridad en la nube (USACH) CCNA Instructor Cyber Ops (Cisco, ICND1 CISCO CCNA Routing And Switching (Cisco) ICND2 CISCO CCNA Routing And Switching (Cisco) NSE1 Fortinet. Facilitador de aprendizajes, investigador, orientador y con vocación de servicio, registrado en SENCE, experiencia en la dirección académica y administrativa de la educación superior. Docente virtual con manejo de herramientas como; blackboard, canvas y Moodle. Docente presencial de cursos relacionados a: Ciberseguridad, Administración de Servidores Linux, Redes informáticas y tecnologías de la información. Docente instructor de Cisco CCNA Instructor Cyber Ops.

Equipo Docente

Ing. Cristián Vargas

Ingeniero de Ejecución en Informática - Duoc-UC, Postgrado en Gerencia de Seguridad de la Información - UAI, Diplomado Gobernanza, Gestión y Auditoría a la Ciberseguridad – USACH. Certificado en ITIL.f v3 / director SOCHISI. Actualmente se desempeña como Ingeniero senior de Seguridad de la Información y Ciberseguridad, Gestión de Vulnerabilidades y levantamiento de Proceso de Tecnologías de la Información en Institución de Gobierno de Chile SERNAGEOMIN

Desde el año 2017 a la fecha, trabaja en colaboración directa en comunidades digitales abiertas, como Fundación Whilolab compartiendo conocimiento y aportando medidas de seguridad digital en la sociedad, además de la participación en la directiva de la Sociedad Chilena de Seguridad de la Información Sochisi, fomentando la transferencia de conocimiento de Seguridad y ciberseguridad en Sector Público, gestión de riesgo y adherencia hacia estándares de Seguridad de la Información Nch-ISO 27001/27001/31000, labores de gestión de charlas comunicacionales de Concientización en Ciberseguridad y elaboración de material de difusión de seguridad.

Ficha Técnica

Matrícula	Valor Arancel	Duración
$100.000	$1.200.000	125 horas

Consulte por modalidades de pago.

Todos los programas están sujetos, en cuanto a su apertura y fecha de inicio, al logro de la matrícula mínima requerida.

La Universidad Bernardo O´Higgins se reserva el derecho de hacer modificaciones en cuanto cuerpo docente y calendarización de los programas. Los cursos y diplomados no generan grado académico.

UNIVERSIDAD BERNARDO O'HIGGINS®

Dirección de Educación Continua y Capacitación

Vicerrectoría de Vinculación con el Medio e Investigación

camila.cisternas@ubo.cl / +56 **9 9103 3610**

General Gana 1702, Edificio Rondizzoni I, Santiago

/uboeducacioncontinuaycapacitacion

/uboeducacion

/company/ubo-educación-continua-y-capacitación

Comisión Nacional de Acreditación CNA-Chile

INSTITUCIÓN ACREDITADA 4 AÑOS

- *GESTIÓN INSTITUCIONAL*
- *DOCENCIA DE PREGRADO*
- *VINCULACIÓN CON EL MEDIO*

HASTA JULIO DE 2022