UNIVERSIDAD BERNARDO O'HIGGINS

Dirección de Educación Continua y Capacitación

Vicerrectoría de Vinculación con el Medio e Investigación

Diplomado Seguridad Digital

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 a esta compleja realidad, y en nuestro país se han materializado ataques cuantiosos a la infraestructura crítica y financiera, siendo hoy la cantidad de profesionales insuficiente para la demanda que existe en el mercado. Por ello los profesionales de Seguridad Digital constituyen un rol clave en el desarrollo de la Seguridad Digital nacional.

Considerando lo anterior, la formación de profesionales con una actualización profesional en Seguridad Digital con foco en los procesos y las personas desde punto vista táctico y estratégico es imperativo.

Objetivo General

El objetivo general del programa de Diplomado en Seguridad Digital es 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 de la Ciberseguridad relacionados al desarrollo de la Industria 4.0 en diversos sectores productivos de Chile y Latinoamérica.

Diplomado Seguridad Digital

Objetivos Específicos

1. Formar especialistas con conocimientos avanzados en el ámbito de la Ciberseguridad que puedan ser parte fundamental de los comités de Seguridad de la Información y de Gerencias relacionadas a la Seguridad Digital.

2. Formar especialistas capaces de comprender y aplicar procesos de Ciberseguridad que aseguren la disponibilidad, confidencialidad e integridad de la información corporativa de las organizaciones, tanto en el nivel táctico, cómo estratégico.

3. Formar especialistas en gestión de la Seguridad de la Información utilizando metodologías y estándares basados en procesos y personas.

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	Gestión de Activos y Gestión de Riesgos	E-Learning	25 horas
II	Gestión de Incidentes	E-Learning	25 horas
III	Desarrollo Seguro de Software	E-Learning	25 horas
IV	Seguridad en las Ciberoperaciones	E-Learning	25 horas
V	Seguridad Física para Infraestructura Crítica	E-Learning	25 horas

Contenido

Módulo 01: Gestión de Activos y Gestión de Riesgos

La gestión de riesgos de seguridad de la información se basa en una de las etapas de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) a través de las normas ISO de la familia 27000, dentro de las cuales se encuentra la norma ISO 27001, donde una de sus tareas es la realización del inventarios de activos de información. Es por este motivo que se hace indispensable el conocimiento de la gestión de activos, debido a que esto deriva en una gestión de riesgos, de la cual se nutre la seguridad de la información.

Contenido

- ¿Qué son los activos de información en Seguridad de la Información?
- ¿Cómo hacer una matriz de riesgos?
- ¿Cómo gestionar el riesgo?
- Controles para mitigar el riesgo.

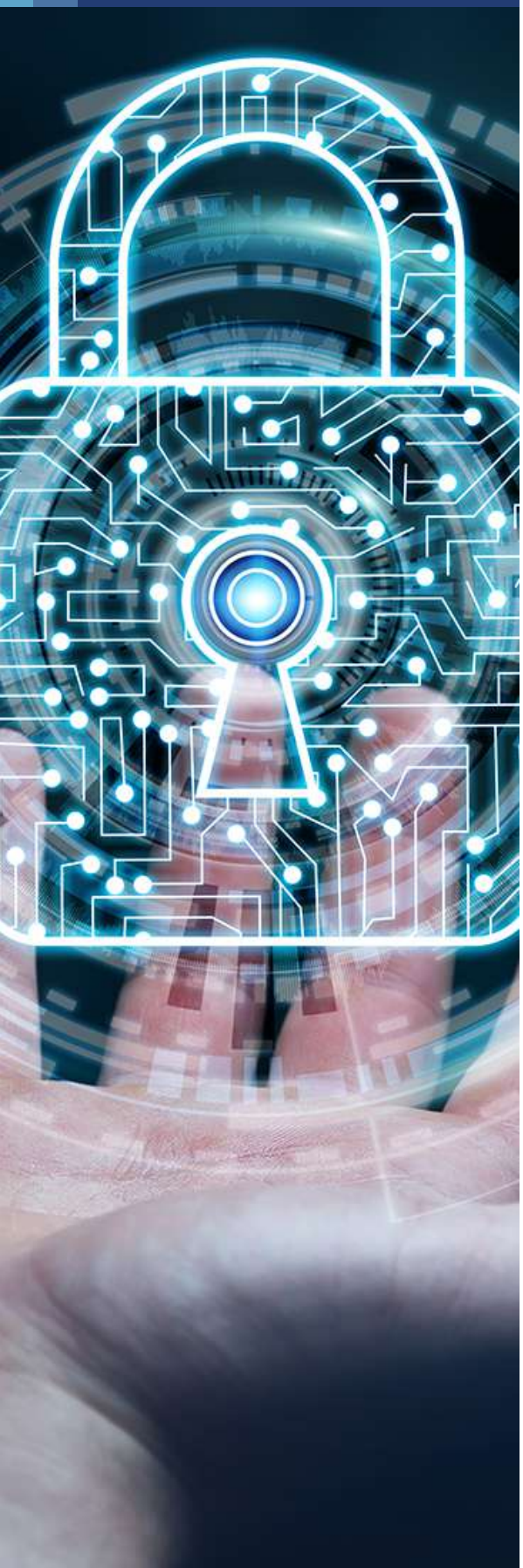
Módulo 02: Gestión de Incidentes

Hoy en la actualidad las organizaciones requieren poder hacer frente a ciber incidentes de una manera profesional, ordenada y procedimental, puesto que en un momento de Incidentes no se pueden cometer errores o improvisar. Este Módulo permite enfrentar el desafío de cómo hacer sostenible este tipo de metodologías a escala organizacional.

Contenido

- Historia de incidentes de Ciberseguridad.
- Clasificación de incidentes – Triage.
- Identificación.
- Detección.
- Protección.
- Recuperación.
- Plan de respuesta a incidentes.
- Playbook de respuesta a incidentes.

Contenido



Módulo 03: Desarrollo Seguro de Software

En la actualidad, no basta con tan solo desarrollar, es necesario proteger dichos desarrollos para minimizar los riesgos en aplicaciones que finalmente sustentan los negocios en diferentes organizaciones, identificando buenas practicas que permitan mejorar el proceso completo de desarrollo y reduciendo el riesgo mediante el apoyo de herramientas, frameworks o estándares para su ejecución.

Contenido

- Introducción al Módulo.
- Seguridad en el Software.
- Características Base de la Seguridad.
- Introducción al Ciclo de Vida del Software (SSDLC).
- Seguridad en el Ciclo de Vida del Software.
- Seguridad en las Tecnologías de Desarrollo.
- DevSecOps.

Módulo 04: Seguridad en las Ciberoperaciones

Las organizaciones en su desarrollo de giros del negocio dependen de una manera critica de las técnicas. Es por ello por lo que, junto con obtener mejoras en procesos, también se presentan riesgos. Estos riesgos se generan por distintos componentes sean humanos, técnicos, tecnológicos y de procesos.
Este módulo permite enfrentar el desafío de cómo hacer sostenible este tipo de metodologías a escala organizacional.

Contenido

- Conceptos y Definiciones Básicos de Ciberseguridad.
- Gestión de Activos (por ejemplo, ciclo de vida de los equipos, licencias de Software).
- Centro de Operaciones de Seguridad.
- Gestión de la Vulnerabilidad.
- Protección de Puntos Finales.
- Gestión de Cambios y Configuración (versionado, líneas de base, etc.).

Contenido

Módulo 05: Seguridad Física para Infraestructura Crítica

El Módulo seguridad física para infraestructura crítica tiene por objetivo general conocer los entornos de seguridad aplicada a data-center y activos industriales que prestan servicios esenciales, lo que habitualmente se conoce como ciberseguridad industrial.

Contenido

- Automatización, Digitalización y Ciberseguridad Industrial.
- Impacto de las Principales APT en Entornos Industriales e Infraestructuras Críticas.
- Gobernanza, Marcos de Gestión del Ciber riesgo.
- Defensa en Profundidad y Estándares Ot.
- Seguridad en Redes Industriales.
- Seguridad en Protocolos Industriales.
  Seguridad en Dispositivos de Control y Sistemas de Gestión en tiempo real. Ataques Específicos y Contramedidas.
  Seguridad en Industrial Internet of Things (IOT).
- Monitorización y Detección Temprana.
- Plan de Respuesta ante Incidentes y Continuidad de
- Negocio en Infraestructuras Críticas.

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. Sebastián Vargas

Magíster en Gestión de Tecnologías de la información – Universidad Tecnológica de Chile Inacap, Ingeniería Civil en informática, Universidad Tecnológica de Chile Inacap, Licenciatura en Ciencias de la Ingeniería, Universidad Tecnológica de Chile Inacap. Ha sido premiado como #3 Influenciador de Ciberseguridad Chile 2020 top #43 Latinoamérica, TOP 10 Influenciador Ciberseguridad. Cuenta con certificaciones en: Certified Ethical Hacking Practical - EC- council, Certified Junior Penetration Testing - Elearn Security, Certificado de Auditor Líder 27001 - Usach Certified ISO 22301 Foundation - Certiprof Certificado de Gestión y Gobierno con Cobit – Usach, Certificado de Fundamentos de gestión con ITILV3 y v4, Cyber Security Foundation - CSFPC -CyBOK Lead Cybersecurity professional Certicate LCSPC, Certified Certified NetworkSecurity Specialist Darktrace Certified x7, Kaspersky Cybersecurity Fundamentals Certification, Kaspersky Lab - Incident Response Level 2 Critical Infrastructure Protection Associate (OCIPA), Certificado Splunk Fundamentals Devops essentials professional (DEPC), Kanban Foundation Certificate - (KIKF™) Certified NSE 1 y 2 en FORTINET. A la fecha se desempeña en Lider Ciberseguridad como coordinador Eléctrico Nacional.

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. Andres Peñailillo

Ingeniero de Ejecución en Informática, Universidad de las Américas, con más de 10 años como encargado de áreas informáticas y 9 años como encargado de seguridad, 16 años de trayectoria gestionando proyectos y realizando análisis de sistemas, Ingeniero de Gestión y Desarrollo. Actualmente se desempeña como Oficial de Seguridad de la Información en la Universidad de Chile. Fue jefe de la unidad de informática del Ministerio de Energía, Ministerio Secretaría General de Gobierno, entre otros. Ha realizado cátedras en el Instituto Profesional de Chile, Duoc UC, Facultad de Derecho, Economía y Negocios de la Universidad de Chile. Cuenta con certificaciones en Certificación como Auditor Líder NCh ISO 27., Universidad de Santiago de Chile, Certificación Ejecutiva en Liderazgo y Estrategia de Ciberseguridad impartido por Florida International University en alianza con la Universidad Técnica Particular de Loja y el programa de ciberseguridad de la Organización de los Estados Americanos OEA, Ecuador, certificación Certified Information Systems Security Professionals (CISSP), Curso Oficial de ISC2 impartido por NeoSecure.

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