Comisión Nacional de Acreditación CNA-Chile

3 AÑOS ACREDITADO
GESTIÓN INSTITUCIONAL
DOCENCIA DE PREGRADO
DESDE MARZO 2022 HASTA MARZO 2025

Academia Digital

Del Instituto Profesional CIISA

DIPLOMADO:

CIBERSEGURIDAD

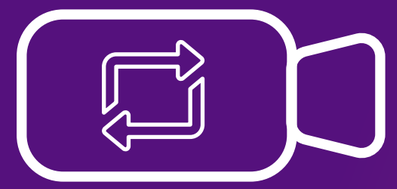
EL DIPLOMADO

DESCRIPCIÓN Y CONTENIDOS DEL PROGRAMA

El Diplomado de Ciberseguridad está orientado a especialistas o administradores del área TI, que buscan adquirir los conceptos teóricos y prácticos de la seguridad de la información para resguardar los datos e información. Además, de administrar sistemas de bases de datos, Internet, protección de la seguridad y redes en empresas públicas y privadas.

MODALIDAD 100% ONLINE

ACTIVIDADES ASINCRÓNICAS



CLASES SINCRÓNICAS

MÓDULOS

M-1 Fundamento de la Ciberseguridad

18 HORAS *DOCENTE: DANIEL ASTUDILLO*

Objetivo General:

Conocer los fundamentos principales de la Ciberseguridad para lograr la aplicación de mejores prácticas globales, a través del análisis de un entorno TI, implementando herramientas y criterios de evaluación en el marco de seguridad de la información, según el contexto organizacional.

Fundamentación Técnica:

En este módulo los estudiantes conocerán los fundamentos claves sobre seguridad de la información y ciberseguridad. Hoy en día, mantener la seguridad informática juega un rol esencial en las organizaciones debido al aumento de amenazas y vulnerabilidades cibernéticas. Es importante que se reconozca el entorno TI y cómo gestionar la ciberseguridad a nivel organizacional, mediante el seguimiento y una mejora continua.
Cabe mencionar que toda esta información crea la base del conocimiento para que, en los módulos siguientes, los estudiantes sean capaces de desenvolverse de manera óptima en todas las áreas relacionadas.

M-2 Marco Normativo

18 HORAS *DOCENTE: JOSÉ MIGUEL VARGAS*

Objetivo General:

Entender las distintas normas, regulaciones, sanciones y buenas prácticas que contempla el Marco Normativo Chileno, identificando las falencias propias de algunas Leyes que se encuentran desactualizadas y en trámite legislativo para su mejora y adecuación con los convenios internacionales que ha suscrito nuestro país.

Fundamentación Técnica:

Este módulo surge como una respuesta a las necesidades de las organizaciones frente a un aumento de la Ciberdelincuencia y riesgos emergentes del ciberespacio, para lo cual se requiere una compresión amplia de la aplicación de las leyes y normativas vigentes que regulan el comportamiento de las personas naturales y jurídicas. Asimismo, se busca potenciar a los participantes del Diplomado, en conocimientos transversales e integrales de la normativa vigente, a fin de mejorar y fortalecer la gestión de los riesgos relacionados con delitos tipificados por la legislación chilena.

M-3 Seguridad Perimetral

18 HORAS *DOCENTE: ROBERT ARIAS*

Objetivo General:

Distinguir los diferentes tipos de vulnerabilidad y los protocolos adecuados para la mitigación, de acuerdo a la gestión idónea y eficaz de la seguridad de red de una organización, utilizando herramientas existentes en la industria.

Fundamentación Técnica:

En este módulo los estudiantes analizarán la importancia del reforzamiento de la seguridad de redes de datos, donde se abordará cómo protegerlas y prevenir amenazas, velando siempre por la continuidad operativa del negocio y los estándares adecuados.

M-4 Criptografía

18 HORAS *DOCENTE: JAIME GÓMEZ*

Objetivo General:

Reconocer las principales funciones criptográficas, tales como: Cifrado, HASH, firma digital y su aplicación en la Ciberseguridad para la protección de la seguridad de la información. Además, de realizar aplicaciones prácticas con las diferentes funciones criptográficas aplicadas a casos de uso cotidiano.

Fundamentación Técnica:

En este módulo los estudiantes aprenderán sobre la Criptografía, una de las ramas de la Ciberseguridad que mayor aplicación tiene en la actualidad, dado que nos permite resolver las principales problemáticas de Seguridad de la Información, tales como: Confidencialidad, autenticación de usuarios e integridad de los datos. Adicionalmente, se han generado nuevas tecnologías basadas en Criptografía, con un sinnúmero de nuevas aplicaciones como es el caso de BlockChain. Por otro lado, existen una serie de protocolos de comunicación que utilizan la criptografía como base de seguridad, entre las cuales utilizamos diariamente como: SSL/TLS, SSH, PGP, entre otros.

M-5 Seguridad Ofensiva I

18 HORAS *DOCENTE: JAIME GÓMEZ*

Objetivo General:

Aplicar un análisis de seguridad en los activos de información de una organización, identificando las vulnerabilidades de más alto riesgo a través de la explotación.

Fundamentación Técnica:

En este módulo los estudiantes aprenderán las principales técnicas de Seguridad Ofensiva, con el propósito de realizar un análisis de seguridad de los activos de Información de una organización, identificando las vulnerabilidades de los sistemas, aplicaciones y la obtención de evidencia a través de la explotación.

M-6 Seguridad Ofensiva II

18 HORAS *DOCENTE: JAIME GÓMEZ*

Objetivo General:

Reconocer las principales técnicas de explotación de vulnerabilidades en aplicaciones web, además de la realización de scripts para la generación de sus propias herramientas de hacking.

Fundamentación Técnica:

En este módulo los estudiantes aprenderán las habilidades de Pentesting avanzado, a través de técnicas de Scripting para crear sus propias herramientas y técnicas de Ingeniería Social, con el objetivo de evaluar las capacidades de los usuarios y detectar ataques cibernéticos. Además, de conocer técnicas avanzadas de explotación de vulnerabilidades en aplicaciones web.

¿ QUÉ PODRÁS HACER AL TERMINAR EL DIPLOMADO ?

- Diseñar soluciones y auditorías de ciberseguridad para proteger los activos e intangibles, relacionados a la información, considerando las normativas legales vigentes del país en diferentes contextos de sector privado y público.

- Podrá desempeñarse en organizaciones públicas y/o privadas que manejen plataformas informáticas y demanden la evaluación e implementación de sistemas de seguridad.

- Trabajar integradamente en equipos multidisciplinarios para contribuir en proyectos, procesos de riesgos y diseño de soluciones de seguridad informática, considerando las normas legales vigentes del país, estándares y requerimientos de seguridad en diferentes contextos de su ejercicio profesional.

¿POR QUÉ ESTUDIAR EN CIISA ?

Capacitarse es el medio para expandir tus conocimientos y habilidades en el ámbito que tú quieras especializarte, para ser parte del cambio digital.

Experiencia exitosa en educación Online desde el 2017

+

45 Años de trayectoria en educación tecnológica

+

Entorno Virtual de Aprendizaje, plataforma interactiva con acceso 24/7

+

Docentes que trabajan en el sector tecnológico

+

INFORMACIÓN GENERAL

DURACIÓN

108 horas totales

REQUISITOS

Requisitos académicos:

- Manejo en el uso del computador
- Dominio en MS Office (Word, PowerPoint)

Requisitos Técnicos Básicos:

- Notebook o PC, con al menos Pentium Core 5, 8 GB RAM y 500 GB HD.
- Conexión a Internet.

*Los requisitos son de exclusiva responsabilidad del participante. La Academia Digital CIISA se excluye del pago de estos servicios.

REQUISITOS DE APROBACIÓN

- Tener al menos un 70% de asistencia en clases sincrónicas por cada unidad.
- La calificación mínima por unidad es Nota 4.0.
- Se entregará un “Certificado de Aprobación” al término de cada Módulo y otro por el diplomado terminado, si se cumplen los requisitos nombrados.

ATENCIÓN ONLINE:

Correo: contacto@ciisa.cl
Horario: Lunes a Viernes de 10.00 a 18.30 horas