



Expertos en educación online

¿Por qué estudiar en IACC?

- Líderes en Educación 100% Online.
- Consejeros para guiar al alumno.
- Admisión todos los meses.
- Compatibiliza estudio, trabajo y familia.
- Profesores vinculados al mundo laboral.

Diplomado en Ciberseguridad



Nombre: Diplomado en Ciberseguridad.

Duración: 130 horas cronológicas.

Modalidad de Estudio: 100% online.

DIRIGIDO A:

Técnicos o profesionales con experiencia intermedia en programación e infraestructura con necesidades de especializarse en temas de seguridad informática.

DESCRIPCIÓN:

Esta acción formativa se enmarca en la cuarta revolución industrial, ya que ofrece una mirada sistemática al fenómeno de la Ciberseguridad, que se orienta a abordar los conocimientos y herramientas necesarios para identificar, reconocer amenazas informáticas y resguardar la seguridad informática de manera física y lógica, evitando la pérdida de información, garantizando así la continuidad de las tareas que ejecutan los usuarios de la red. El propósito fundamental de esta formación se centra en desarrollar dentro de los estudiantes los conocimientos y habilidades para identificar las principales amenazas a los sistemas informáticos, de forma tal que se reconozcan desde los componentes teóricos hasta las herramientas y procesos de configuración, implementación y administración de los protocolos, normas y políticas de seguridad que garanticen la integridad de la información.

Es importante resaltar que las temáticas abordadas resultan fundamentales a la hora de diseñar, administrar y analizar amenazas informáticas para el resguardo de la información, competencias que debe tener en la actualidad cualquier profesional del área de la computación y la informática.

Esta acción formativa considera un carácter teórico – analítico, para lo cual se abordarán conceptos asociados a la Ciberseguridad, evolución, modelos de seguridad basados en OSI, así como también la legislación

nacional e internacional que regula los delitos informáticos. De igual forma contempla la perspectiva analítica, a través de estudios de caso que permitan al estudiante plantear soluciones integrales en materia de Ciberseguridad.

REQUISITOS (ADMINISTRATIVOS Y/O ACADÉMICOS):

- Licencia de Enseñanza Media
- Copia de cédula de identidad
- Experiencia relacionada con análisis de datos.

OBJETIVO GENERAL:

Comprender las características de la Ciberseguridad y de la ciberdefensa, en función de sus aspectos técnicos, legales y procedimentales, utilizando para ello casos prácticos y análisis teóricos.

METODOLOGÍA:

Modalidad online, a través de metodologías activas centradas en la producción de los participantes, que impliquen la aplicación de contenidos en la especialidad.

Las evaluaciones sumativas de los módulos que componen el diplomado, equivalen a un 60% de su totalidad.

La entrega de la evaluación final es de carácter obligatorio y corresponde a un 30% de la nota final

REQUISITOS DE CERTIFICACIÓN:

Para obtener la certificación, el participante deberá obtener una nota igual o superior a 4,0, con un nivel de exigencia del 60%. Además, es requisito obligatorio la entrega de la evaluación final.

*Contenido de la malla sujeto a modificaciones.

INSTITUCIÓN AUTÓNOMA RECONOCIDA POR EL MINEDUC

Diplomado en Ciberseguridad



2 AÑOS
INSTITUCIÓN ACREDITADA
■ GESTIÓN INSTITUCIONAL
■ DOCENCIA DE PREGRADO
Octubre 2019 - Octubre 2021

Nombre: Diplomado en Ciberseguridad.

Duración: 130 horas cronológicas.

Modalidad de Estudio: 100% online.

CONTENIDOS DEL DIPLOMADO:

El diplomado se organiza en un sistema modular que contempla lecciones semanales, siendo estos:

MÓDULO I: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA.

Objetivo del módulo: Identificar la historia y los conceptos básicos de seguridad informática.

MÓDULO II: SEGURIDAD FÍSICA Y LÓGICA.

Objetivo del módulo: Identificar la seguridad física y lógica de Hardware y Software.

MÓDULO III: SEGURIDAD EN LA RED.

Objetivo del módulo: Reconocer el modelo de seguridad, elementos de seguridad de una red y herramientas defensivas.

MÓDULO IV: SEGURIDAD EN SISTEMAS OPERATIVOS, APLICACIONES WEB Y BASES DE DATOS.

Objetivo del módulo: Analizar la seguridad de sistemas operativos, de aplicaciones web y de bases de datos.

MODULO V: ETHICAL HACKING I.

Objetivo del módulo: Reconocer el Ethical Hacking y sus pasos.

MODULO VI: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo del módulo: Diferenciar los objetivos de la gestión de la seguridad en organizaciones, clasificación y diseño de controles.

MODULO VII: ETHICAL HACKING II.

Objetivo del módulo: Identificar el footprinting activo, la enumeración, técnicas de Hacking y criptografía.

MODULO VIII: AUDITORÍA.

Objetivo del módulo: Emplear evaluaciones para labores de operación, de mantenimiento y soporte en auditorías.

MODULO IX: ETHICAL HACKING III.

Objetivo del módulo: Caracterizar la vigilancia en móviles, evasión de controles y explotación de vulnerabilidades web.

MODULO X: AUDITANDO UN EQUIPO – CASO PRÁCTICO.

Objetivo del módulo: Emplear herramientas de auditoría, utilizando conceptos relacionados.

MODULO XI: ETHICAL HACKING IV.

Objetivo del módulo: Comparar diferentes tipos de ataque, junto a sus técnicas.

MODULO XII: ASPECTOS LEGALES DE LA SEGURIDAD DE LA INFORMACIÓN.

Objetivo del módulo: Caracterizar los aspectos legales de la seguridad de la información.

MÓDULO XIII: ANÁLISIS DE CIBERSEGURIDAD DE UNA EMPRESA Y SU PRESENCIA EN LA WEB.

Objetivo del módulo: Emplear los conceptos de Ciberseguridad para análisis de caso dado.

*Contenido de la malla sujeto a modificaciones.

INSTITUCIÓN AUTÓNOMA RECONOCIDA POR EL MINEDUC