iacc Expertos en educación online

MALLA CURRICULAR_

Diplomado en Ciberseguridad

Dirigido a:

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

Duración diplomado:
130 horas cronológicas distribuidas en 13 semanas, con una carga de 10 horas por semana.

Modalidad de estudio: 100% online

Comisión Nacional de Acreditación CNA-Chile

INSTITUTO PROFESIONAL
IACC ACREDITADO
- NIVEL AVANZADO
- GESTIÓN INSTITUCIONAL
- DOCENCIA DE PREGRADO

4 Años (junio 2026)

POR QUÉ ELEGIR estudiar en IACC

En IACC contamos con un servicio de acompañamiento único para nuestros estudiantes, compuesto por grandes profesionales que trabajan día a día con el objetivo de lograr una formación excepcional y desarrollar las competencias necesarias para ofrecer profesionales de excelencia en el mundo laboral.

- **Tutores de Inducción:** orientan a los estudiantes en sus inicios.
- **Consejeros Estudiantiles**: los guían durante toda su formación profesional, hasta el término de sus estudios.
- **Docentes:** vinculados al mundo laboral.
- **Unidad Socioafectiva:** un servicio que les brindará ayuda cuando esté en riesgo su avance académico.

Expertos en educación online

MALLA CURRICULAR:

Diplomado en Ciberseguridad

Descripción del diplomado

En la actualidad, la vulneración de la seguridad de la información es un tema recurrente en Internet. Las empresas son víctimas de la materialización de brechas con técnicas tan diversas como la suplantación de identidad, hackeos y adulteraciones de sitios web, secuestro virtual de datos y/o equipos, así como intrusiones con ingeniería social dirigida. Las empresas tienen problemas para conseguir talentos con tan amplias habilidades, debido a la falta de profesionales especialistas en el área de la Ciberseguridad.

De acuerdo con el EY Cybersecurity Summit 2018, se estima un déficit global aproximado de 1,8 millones de profesionales de la seguridad dentro de cinco años. Según la Encuesta de Seguridad de la Información Global de EY 2018-19 (GISS), el 30% de las empresas sufre con la escasez de habilidades mientras un 25% indica tener restricciones presupuestarias. En el rubro financiero, un 31% de las organizaciones advierte que la escasez de habilidades es un obstáculo potencial. Incluso las organizaciones con más recursos tienen problemas para incorporar profesionales con la experiencia que se necesita.

Actualmente, los profesionales de la seguridad de la información están migrando hacia la ciberseguridad, así como otros están en sus primeros acercamientos de la ciberseguridad a su labor diaria, todo esto como consecuencia de la falta de profesionales formados en la materia. Es por este motivo que aquellos que se preparen en este ámbito podrán ser protagonistas en el desarrollo y mejora de la ciberseguridad, aportando a la construcción del futuro de la tecnología.

El Diplomado 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 necesarias 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 este diplomado 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.

El diplomado considera un carácter práctico - teórico y analítico, para lo cual, se abordarán aspectos 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 casos que permitan al estudiante plantear soluciones integrales en materia de ciberseguridad.
Los módulos que contiene este diplomado son:

- Módulo I: Introducción a la ciberseguridad, y su relación con la industria 4.0, las aplicaciones móviles, Big Data y gestión de proyectos.
- Módulo II: Gestión de la ciberseguridad.
- Módulo III: Seguridad en las capas de red y aplicación.
- Módulo IV: Ethical Hacking.
- Evaluación final integradora

Requisitos (Administrativos y/o Académicos)

- Licencia de Enseñanza Media.
- Copia de cédula de identidad.
- Experiencia intermedia en programación e infraestructura.

Resultado de aprendizaje

A modo de resultado de aprendizaje, al término del programa el participante debe realizar una auditoria real o simulada detectando los niveles actuales de seguridad en una organización proponiendo posibilidades de mejoras y gestión de los riesgos detectados, documentando en un informe final ejecutivo y técnico.

Expertos en educación online

MALLA CURRICULAR:

Diplomado en Ciberseguridad

Metodología

Para promover los aprendizajes en el estudiante, se trabaja utilizando estrategias metodológicas y didácticas centradas en la interacción de cada participante con los contenidos dispuestos en la plataforma; con sus compañeros y el docente, quien a su vez cumple un rol motivador y de retroalimentación fundamental para la co-construcción del conocimiento.

En el caso particular de este programa de formación continua la metodología con la cual se abordan los contenidos y actividades es a partir del uso de recursos didácticos tales como (infografías, mapas conceptuales, esquemas comparativos, texto de apoyo, videos, etc.).

Por otra parte, la evaluación es parte del proceso de aprendizaje, por ende, es sistemática y permanente durante el transcurso del programa de formación continua. Las actividades que realizan los participantes son evaluadas de forma modular, siendo de estas una evaluación diagnóstica al inicio del programa, dos evaluaciones formativas por módulo, con el fin de monitorear el estado de avance individual en el proceso educativo; una evaluación sumativa al finalizar cada módulo, y una actividad evaluativa integradora de cierre del programa de formación continua, cuyo fin es articular los aprendizajes adquiridos previamente con fines de producción cognitiva y profesional.

Esto, a su vez se nutrirá de la retroalimentación que el docente entrega a cada estudiante, aportando información relevante respecto de los logros obtenidos en función del aprendizaje esperado y los aspectos de mejora.

Para efectos de calificación de los participantes, el programa de formación continua, tiene un total de 100 puntos que corresponden a la nota 7.0. Por cada módulo, el estudiante puede obtener una calificación cuyo puntaje máximo es 6 puntos salvo en la última semana, que corresponde a la evaluación final de la asignatura, que es una instancia integradora y se califica con un total de 28 puntos.

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.

iacc Expertos en educación online

MALLA CURRICULAR:

Diplomado en Ciberseguridad

CONTENIDOS DEL DIPLOMADO

MÓDULO I: INTRODUCCIÓN A LA CIBERSEGURIDAD, Y SU RELACIÓN CON LA INDUSTRIA 4.0, LAS APLICACIONES MÓVILES, BIG DATA Y GESTIÓN DE PROYECTOS.

Aprendizaje esperado del módulo: Distinguir los diferentes hitos y conceptos de la ciberseguridad, y su relación con la revolución industrial 4.0, la seguridad en aplicaciones móviles, Big Data y gestión de proyectos, considerando leyes y normativas asociadas.

Lección 1: Diferenciar hitos y conceptos asociados a la ciberseguridad y su relación con la revolución industrial 4.0, aplicaciones móviles, Big Data y gestión de proyectos.
· Ciberseguridad, industria 4.0, aplicaciones móviles, Big Data y gestión de proyectos.

Lección 2: Distinguir leyes y normativas asociadas a la ciberseguridad.
· Leyes y normativas asociadas a la ciberseguridad.

MÓDULO II: GESTIÓN DE LA CIBERSEGURIDAD.

Aprendizaje esperado del módulo: Utilizar objetivos de la gestión de la ciberseguridad en organizaciones para realizar los procesos de auditoría a servicios TI.

Lección 3: Diferenciar objetivos de la gestión de la seguridad en organizaciones, clasificación y diseño de controles.
· Objetivos de la gestión de la seguridad en organizaciones.

Lección 4: Aplicar herramientas de auditoría utilizando conceptos relacionados.
· Proceso de auditoría a servicios TI.

MÓDULO III: SEGURIDAD EN LAS CAPAS DE RED Y APLICACIÓN.

Aprendizaje esperado del módulo: Emplear herramientas para auditoría de capas de red.

Lección 5: Examinar las capas del modelo TCP/IP identificando debilidades de las capas de enlace de datos, red y transporte.
· Modelos de referencia.

Lección 6: Utilizar los conceptos de seguridad basado en capas de red en el análisis de tráfico.
· Introducción al análisis y protocolos.

Lección 7: Emplear herramientas de auditoría utilizando conceptos relacionados.
· Seguridad de sistemas operativos.

MÓDULO IV: ETHICAL HACKING.

Aprendizaje esperado del módulo: Aplicar técnicas de Ethical Hacking para visualizar los niveles de seguridad dentro de la organización.

Lección 8: Diferenciar las etapas del Ethical Hacking identificando conceptos generales y metodologías.
· Conceptos generales Ethical Hacking.

Lección 9: Aplicar diferentes técnicas y herramientas de reconocimiento y OSINT de la red.
· OSINT.

Lección 10: Utilizar técnicas de escaneo para la identificación de debilidades en dispositivos finales de una red.
· Técnicas de enumeración.

Lección 11: Aplicar técnicas de explotación de debilidades en dispositivos finales de una red.
· Ataques de fuerza bruta.

Expertos en educación online

MALLA CURRICULAR:

Diplomado en Ciberseguridad

CONTENIDOS DEL DIPLOMADO

Lección 12: Utilizar técnicas de evasión y de acceso utilizadas por atacantes para comprometer la organización

· Técnica Esteganografía.

ACTIVIDAD INTEGRADORA: EVALUACIÓN FINAL: ANÁLISIS DE CIBERSEGURIDAD DE UNA EMPRESA Y SU PRESENCIA EN LA WEB.

Aprendizaje esperado del módulo: Realizar una auditoría real o simulada detectando los niveles actuales de seguridad en una organización proponiendo posibilidades de mejoras y gestión de los riesgos detectados, documentando en un informe final ejecutivo y técnico.

Lección 13: Realizar una auditoría real o simulada detectando los niveles actuales de seguridad en una organización proponiendo posibilidades de mejoras y gestión de los riesgos detectados, documentando en un informe final ejecutivo y técnico.

· Evaluación final: Análisis de ciberseguridad de una empresa y su presencia en la web.