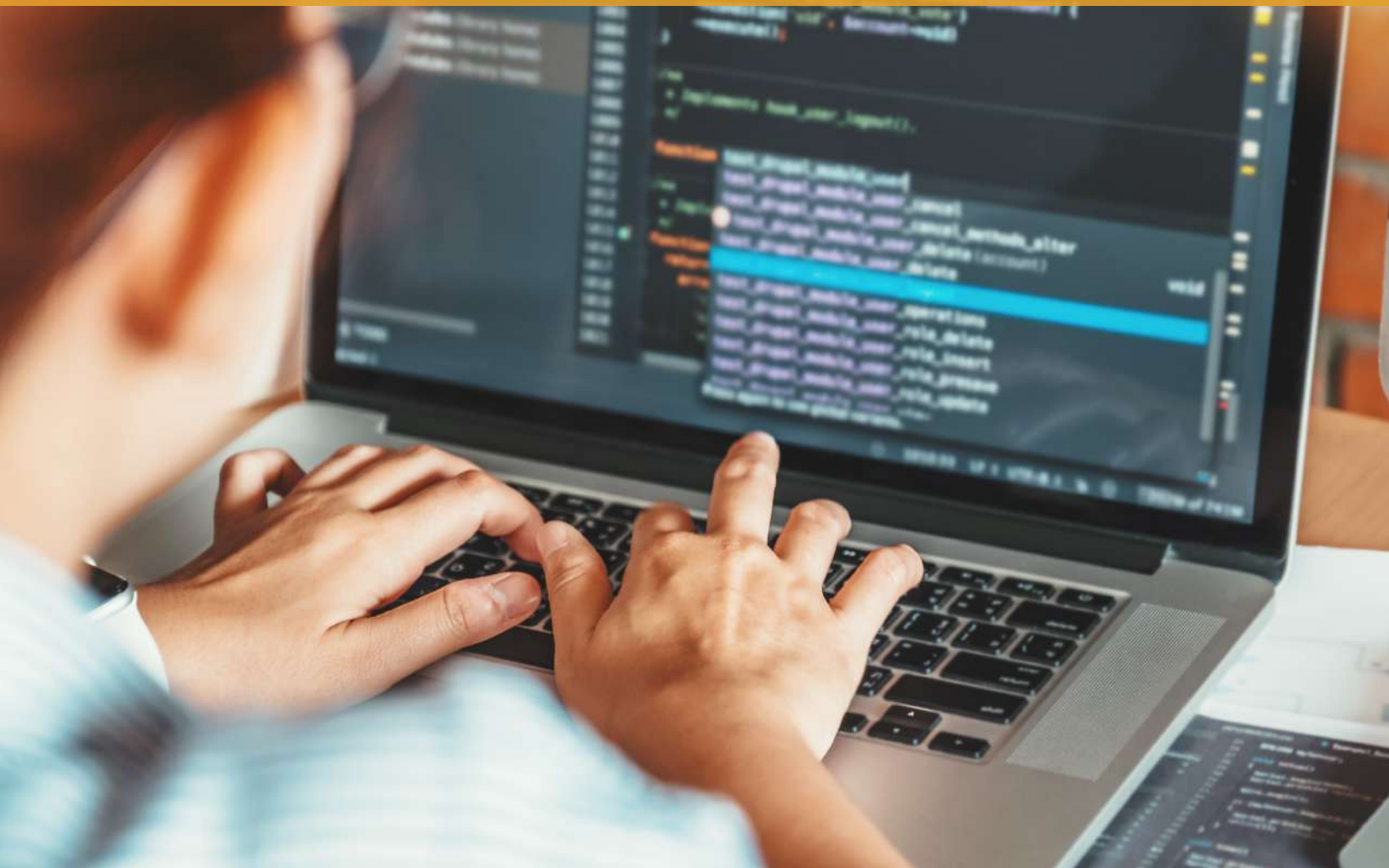
UDLA
UNIVERSIDAD DE LAS AMÉRICAS

Facultad de
Ingeniería y Negocios

DIPLOMADO EN CIBERSEGURIDAD Y GESTIÓN



DESCRIPCIÓN DEL DIPLOMADO

El diplomado en Ciberseguridad y Gestión tiene como propósito formativo que los participantes desarrollen conocimientos, técnicas, herramientas y habilidades para liderar y gestionar proyectos de ciberseguridad, aplicar metodologías, técnicas y herramientas para evaluar riesgos y ejecutar planes que garanticen la seguridad en la organización. Para esto, aprenderán a establecer un gobierno efectivo de la información y la tecnología de las organizaciones, facilitando una adecuada implementación, a la vez, cumpliendo un rol de impulsor de la innovación y la transformación del negocio. Este programa entrega las bases de la evaluación de riesgo y la ciberseguridad como pilar fundamental para garantizar la continuidad del negocio.

RESULTADOS DE APRENDIZAJE

- Aplicar conocimientos, metodologías y herramientas para diseñar, establecer y evaluar políticas de ciberseguridad.
- Implementar y gestionar planes, procedimientos y sistemas de ciberseguridad.
- Establecer un Gobierno TI corporativo, que promueva la protección de los activos de información, facilitando la implementación de planes, procedimientos y sistemas de ciberseguridad, cumpliendo a la vez un rol impulsor de la innovación y la transformación digital bajo marcos de referencia de la industria.
- Liderar, evaluar y gestionar los riesgos de ciberseguridad en la organización, garantizando la continuidad del negocio, bajo los principales marcos de referencias de la industria, ISO 22301, ISO20000, ISO27000 y COBIT 2019.

A QUIÉN SE DIRIGE

- Profesionales del área de administración de empresas e industrias, tecnologías, auditores, contralores, abogados, administradores públicos, junto con ingenieros de todas las especialidades.
- Profesionales egresados de UDLA o de otras instituciones de educación superior, docentes que deseen perfeccionar sus conocimientos y trabajadores que, en su ejercicio, deseen perfeccionarse en ciberseguridad.

METODOLOGÍA

Este programa se extiende por un semestre, abordando los principales tópicos de la industria de ciberseguridad, a través de tres ejes temáticos:

- Ciberseguridad.
- Gestión.
- Negocio.

Proporcionando a los estudiantes metodologías, técnicas y buenas prácticas para la implementación de políticas de ciberseguridad en sus empresas, basadas en una Gestión de Riesgos práctica, cumpliendo las normas y estándares, necesarios para una eficiente Gestión de Ciberseguridad.

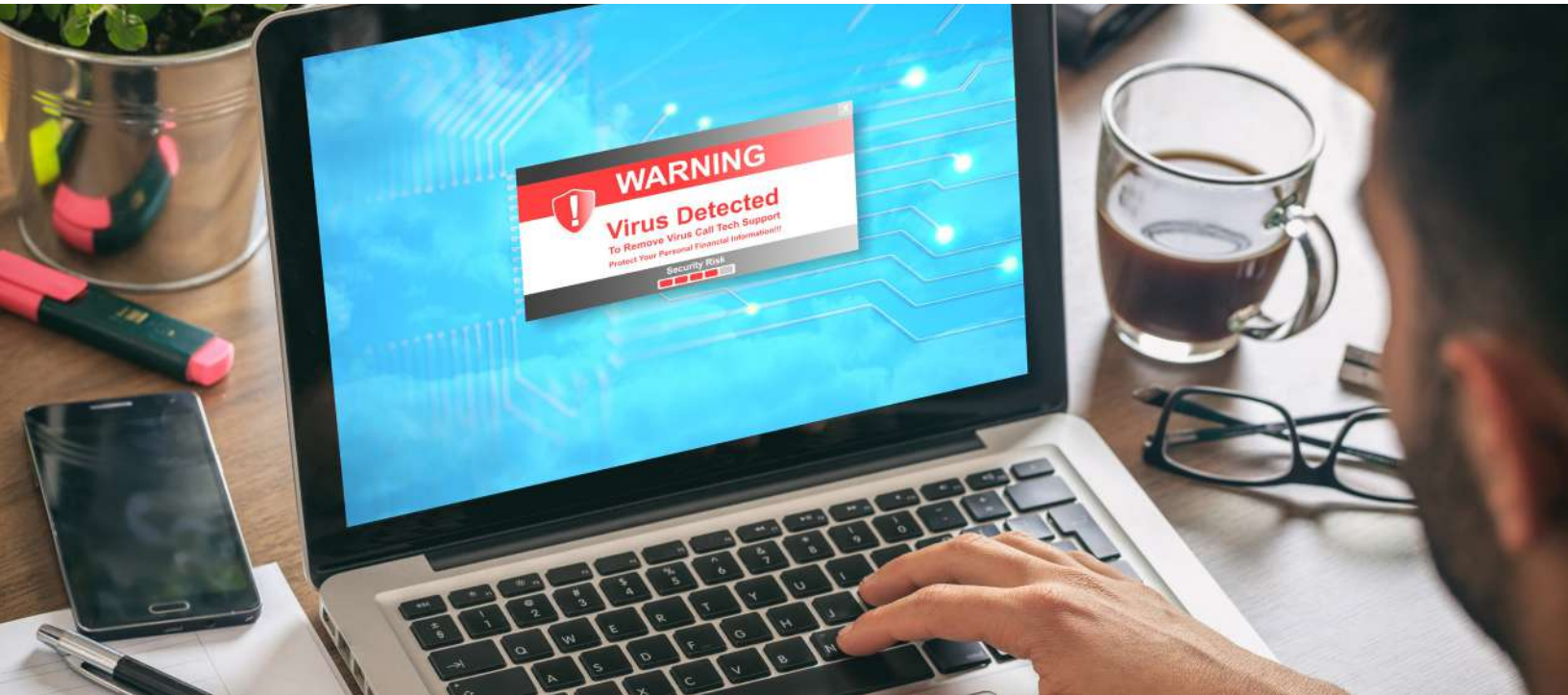
Este programa considera el desarrollo de un proyecto de ciberseguridad aplicado que abarcará todo el Diplomado, y que se enriquecerá con la participación de los estudiantes y un bootcamp (actividad final de cierre del diplomado), que tendrá como relatores a destacados profesionales de la industria, en representación de empresas líderes del mercado de ciberseguridad, junto a otros actores relevantes del medio.

El diplomado se desarrollará en modalidad Online Sincrónico, esto es, mediante el uso de una plataforma donde el material queda disponible semana a semana para cada módulo, así como también, las actividades prácticas y los espacios para desarrollar las actividades evaluativas. En esta plataforma se dispondrá de un espacio de interacción para las clases síncronas, las grabaciones de estas clases, material complementario, actividades, y recursos de aprendizaje. Los contenidos, se distribuirán en seis módulos, cada uno a cargo de un docente especialista en el área. Asimismo, a través de la plataforma, se podrán plantear dudas y consultas por medio de foros.

Cada semana se realizarán sesiones sincrónicas, donde todos los estudiantes podrán interactuar en forma directa con el docente del módulo en una sala virtual, lugar desde donde podrán explicar los contenidos, intercambiar experiencias y desarrollar actividades que propendan al aprendizaje de las temáticas tratadas, garantizando así el logro de los resultados de aprendizaje del programa. Se realizarán foros de discusión, desarrollo de casos, lectura de artículos y documentos, tareas y evaluación formativa.

Complementando lo anterior, cada módulo cerrará con una evaluación que corresponde a la actividad final, donde se realizará un trabajo aplicado. Todas las actividades se realizarán de manera sincrónica mediante una plataforma que permitirá la interacción de todos los participantes.

La evaluación se realizará a través de actividades teórico-prácticas desarrolladas en cada módulo, más un proyecto que se abordará en forma incremental, donde el estudiante desarrollará una propuesta de aplicación profesional de los contenidos del Diplomado, y que concluye en el bootcamp de cierre del programa.



CONTENIDOS

Módulo I
Fundamentos, infraestructura y marco legal para la Ciberseguridad

- Introducción a Infraestructura TI & Sistemas / Operaciones TI.
- Fundamentos de Ciberseguridad.
- Protección de datos personales.

Módulo II
Ciberseguridad y negocios

- Ciberseguridad alineada con el negocio (COBIT 2019).
- Implementación de un Sistema basado en Ciberseguridad.
- Plataformas digitales & Gestión de servicios TI.
- Estrategia de ciberseguridad y plan maestro (Nist Cy)

Módulo III
Gestión de riesgos, análisis, controles y Plan de prueba de sistemas de ciberseguridad

- Gestión de riesgos.
- Análisis de Amenazas & Vulnerabilidades en procesos críticos.
- Definición de Controles & Plan de pruebas de sistemas de ciberseguridad.

Módulo IV
Continuidad del negocio, Plan de recuperación de desastres y Gestión de mejora continua

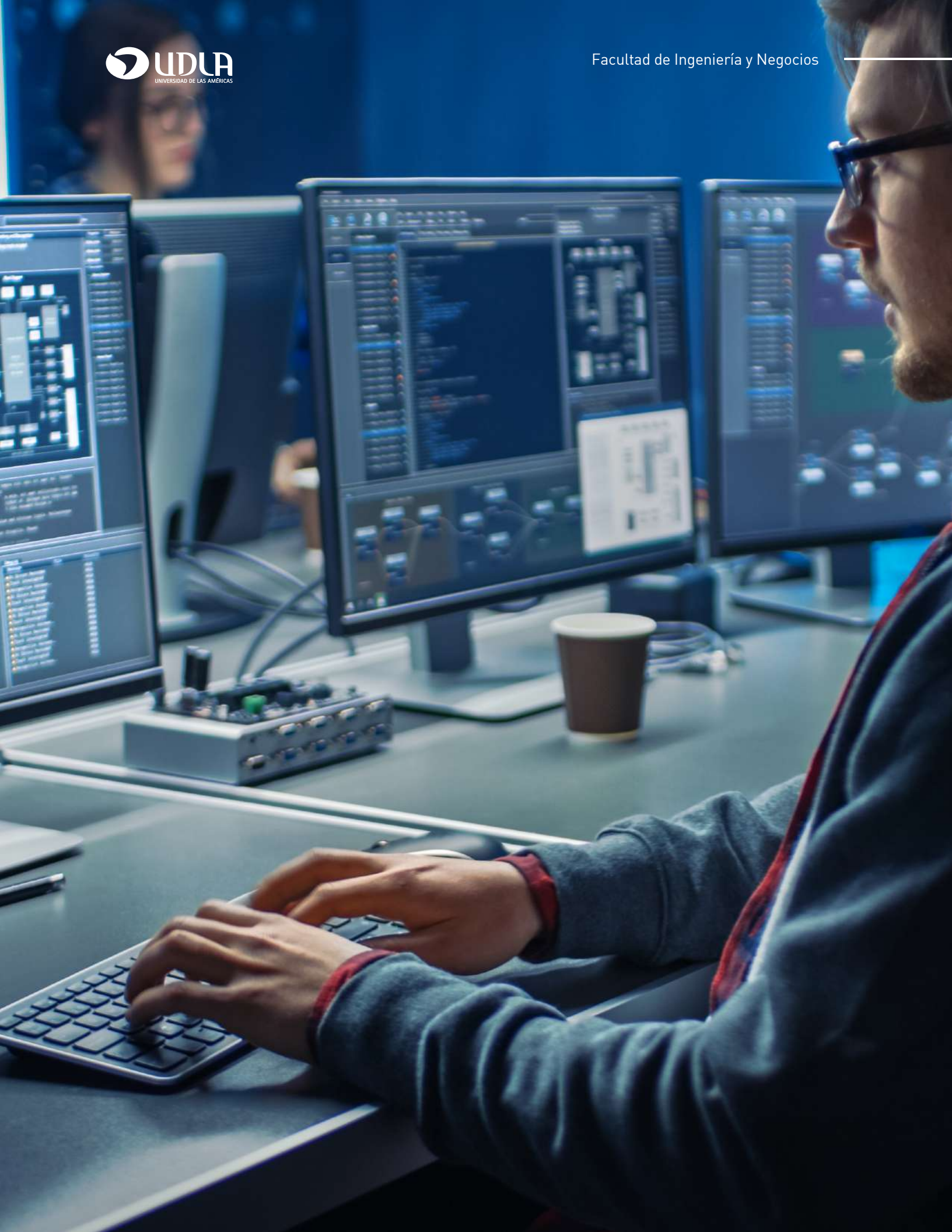
- Continuidad del negocio (BCP).
- Plan de recuperación de desastres (DRP).
- Gestión de mejora continua.

Módulo V
Ciberseguridad en plataformas digitales, técnicas de ethical hacking y pentesting, Auditoría de seguridad TI

- Ciberseguridad en plataformas digitales en ambientes On-Premise y Cloud.
- Técnicas de Ethical Hacking / Pentesting.
- Auditoría de Seguridad TI.
- Aplicaciones en negocios digitales.

Módulo VI
Tendencias en la industria y Gestión de proyectos de Ciberseguridad

- Tendencias de la Industria, teletrabajo, Cloud, RPA, IOT, etc.
- Soluciones de Ciberseguridad analítica, IA y automatizadas.
- Gestión de proyectos de Ciberseguridad.
- Bootcamp – Cierre del Programa.



EQUIPO DOCENTE

Rodrigo Vargas
Ingeniero Civil en Computación e Informática, de la Universidad Central. Magíster en Tecnologías de la Información, Universidad Federico Santa María. Máster en Dirección y Organización de Empresas, Universidad de Lleida. Docente, Universidad de Las Américas.

Rodrigo Fernández Vega
Ingeniero en Electrónica con Mención en Computación y Redes por INACAP, actualmente como Gerente de servicios de consultoría en Ciberseguridad. Con 20 años de trayectoria en el liderazgo, diseño, y gestión de proyectos y servicios enfocados al desarrollo de la seguridad de la información y la transformación tecnológica para diversas compañías globales y de Latinoamérica. Cuenta con amplia experiencia en evaluación y lineamiento de prácticas de gobernanza tecnológica y de seguridad de la información basado en estándares y modelos de lideres de la industria, implementación y mantenimiento de tecnologías, educación y entrenamiento a profesionales de la ciberseguridad.

Juan Carlos Saba
Ingeniero Civil en Computación e Informática, de Universidad del Desarrollo. Máster en Ingeniería Industrial, Pontificia Universidad Católica de Chile. Más de 20 años de experiencia en el área TI y en asesorías tecnológicas a empresas. Habilidades de liderazgo, dirección de proyectos, negociación y control de gestión. Actualmente se desempeña como Jefe de División TI en Subsecretaría de Relaciones Económicas Internacionales de Chile.

Jorge Esteban Olivares
Ingeniero Civil en Informática, de la Universidad Federico Santa María. Gerente de Consultoría y Formación en Business Continuity SPA. Consultor Senior en SSI (Soluciones de Seguridad de la Información). Consultor preventa de seguridad CISSP.

Jaime Gómez
Ingeniero Civil Electrónico, de la Universidad Católica de Valparaíso. MBA de la Universidad Adolfo Ibáñez. Más de 20 años de experiencia en Seguridad Informática y Ciberseguridad, dedicado en los últimos años a la evaluación de Seguridad y Pentesting, con certificaciones como CEH, CEHP y CEH Master de Ec-council. Además, es instructor Certificado de Ec-council CEI con más de 15 años de experiencia en la Academia de Seguridad Informática y Ciberseguridad en diferentes Institutos y Universidades, en los cuales ha destacado el amplio contenido práctico de sus cursos.

Francisco Parra
Ingeniero Civil Industrial, de la Universidad de Atacama. Con amplia experiencia en desarrollo e implementación de soluciones de tecnología relacionadas con digitalización, herramientas colaborativas, cloud, IoT, SD-WAN, Networking, Data Center, WiFi y seguridad de redes. Se ha desempeñado en empresas multinacionales como Arquitecto de Sistemas y Gerente de Tecnología e Innovación, liderando el diseño y la implementación de grandes proyectos tanto en el sector privado como público.

REQUISITOS DE ADMISIÓN

- Foto de cédula de identidad por ambos lados.
- Completar Ficha de Inscripción.
- Foto de Título o Certificado de Título.

INFORMACIÓN GENERAL

Fecha de inicio
Mayo 2025

Fecha de término
Agosto 2025

Cantidad de horas
120 horas de instrucción docente

162 horas totales

Modalidad
Online Sincrónico

Días y horarios de clases
Lunes y miércoles de 18:30 a 22:30 horas

CONTÁCTANOS

econtinua.udla.cl

econtinua@udla.cl