UNIVERSIDAD BERNARDO O'HIGGINS®

ES MOMENTO DE
AVANZAR

DIPLOMADO

Ciberseguridad y Ciberdefensa

ÁREA DE SEGURIDAD

5 AÑOS
Comisión Nacional de Acreditación CNA-Chile
UNIVERSIDAD ACREDITADA
MEDIANTE ACUERDO DEL CONSEJO NACIONAL DE EDUCACIÓN
NIVEL AVANZADO
- *GESTIÓN INSTITUCIONAL*
- *DOCENCIA DE PREGRADO*
- *VINCULACIÓN CON EL MEDIO*

HASTA 9 DE NOVIEMBRE DE 2027

Diplomado en Ciberseguridad y Ciberdefensa

El Diplomado en Ciberseguridad y Ciberdefensa de la Universidad Bernardo O'Higgins (UBO) está diseñado para profesionales que buscan especialización avanzada en seguridad digital. El programa aborda aspectos técnicos, jurídicos y estratégicos, aplicables al contexto latinoamericano y alineados con estándares internacionales como ISO 27001, NIST, CIS, OWASP y DevSecOps.

La relevancia de este programa radica principalmente en la necesidad de que los profesionales de diversas áreas cuenten con una base sólida en la cultura digital, cumplimiento normativo y el resguardo de los activos digitales de sus organizaciones. De esta manera, estarán en condiciones de contribuir a la protección de la infraestructura tecnológica, la gestión segura de los datos y la salvaguarda de la privacidad, mediante la implementación de políticas organizacionales y en la concientización digital.

Asimismo, el diplomado busca fomentar la resiliencia organizacional y personal frente al creciente número de amenazas digitales, promoviendo un enfoque preventivo y estratégico que responda a las exigencias actuales del entorno digital y al marco normativo vigente y emergente en Chile y en el mundo.

Objetivo General

Formar profesionales capaces de comprender, aplicar y promover los principios, marcos normativos, prácticas y estrategias vinculadas a la ciberseguridad y la ciberdefensa, con un enfoque en la Responsabilidad Social que permita responder a los desafíos digitales actuales en el ámbito organizacional, personal y regional, particularmente en el contexto de América Latina.

Objetivos Específicos

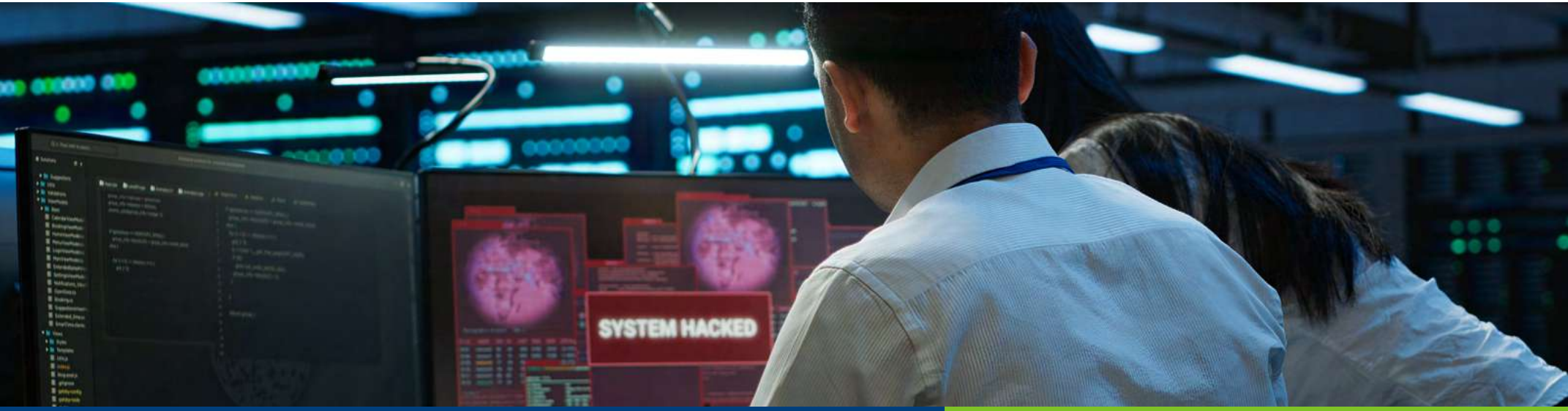
Desarrollar competencias conceptuales y analíticas que permitan comprender los principios básicos de la tecnología de la información, aplicando la triada CIA (confidencialidad, integridad y disponibilidad) y los fundamentos de ciberdefensa e inteligencia, para reconocer el impacto del mundo digital en los entornos organizacionales y personales, con especial atención a los desafíos emergentes en América Latina.

Promover la formación ética y legal en el ámbito de la ciberseguridad, y lograr la construcción de una cultura de responsabilidad en ciberseguridad, con la finalidad que los estudiantes comprendan y apliquen los marcos normativos nacionales e internacionales, considerando las brechas regulatorias de América Latina, para resguardar de manera efectiva la protección de la información digital mediante su integridad, confidencialidad y disponibilidad.

Adquirir y desarrollar habilidades técnicas y prácticas para la detección de amenazas cibernéticas, a través del conocimiento de métodos y tácticas de ataque de ciberdelincuentes identificando los principales riesgos que afectan a organizaciones, gobiernos y ciudadanos, favoreciendo la implementación de buenas prácticas de seguridad de la información.

Fomentar competencias en la gestión de riesgos y protección de datos personales y organizacionales, mediante la aplicación de planes de continuidad operacional y protocolos de respuesta ante incidentes, considerando las vulnerabilidades estructurales de la región.

Adquirir habilidades y destrezas en seguridad en redes, infraestructura y sistemas operativos, a través de pruebas de penetración bajo principios de hacking ético, utilizando herramientas OSINT y análisis forense digital en dispositivos y redes que permitan garantizar la continuidad y resiliencia de la información en el entorno organizacional.



Desarrollo de la Actividad

136 horas cronológicas, en modalidad E-Learning (sincrónico), los módulos se desarrollan en Plataforma E-Learning de la universidad de manera profesional y acorde a la normativa vigente.

Módulo 1	Módulo 2	Módulo 3	Módulo 4
Panorama Estratégico de la Ciberseguridad y Ciberdefensa en América Latina	Gobernanza, Riesgos y Cumplimiento Normativo (GRC)	Criptografía, Certificación Digital y Blockchain	Seguridad en Redes, Infraestructura y Sistemas Operativos
Módulo 5	**Módulo 6**	**Módulo 7**	**Módulo 8**
Gestión y Respuesta ante Incidentes de Seguridad	Hacking Ético y Pruebas de Penetración	Análisis Forense y Ciberinvestigacion Legal	Taller Final Integrador: Simulación de Incidente Crítico

UNIVERSIDAD BERNARDO O'HIGGINS

ES MOMENTO DE AVANZAR

Requisitos de Admisión

Estar en posesión de un grado académico, título profesional, título técnico como: Profesionales de TI, derecho, defensa, gestión pública y privada, interesados en fortalecer sus competencias en seguridad digital, ciberdefensa y protección de datos.

Documentación Requerida

Certificado de Grado Académico, Título Profesional o Título Técnico (original o fotocopia legalizada ante notario).

Todo documento proveniente del extranjero deberá venir apostillado desde el país de origen y, posteriormente, acogerse al trámite de reconocimiento de estudios del Ministerio de Educación.

Cédula de identidad o pasaporte (en caso de extranjeros/as).

Metodología de Estudio

Clases teóricas E-Learning (Sincrónico)

Discusión de textos científicos

Estudios de casos

Foro en el Aula Virtual

Requisitos de Aprobación

Para aprobar el diplomado, el alumno debe cumplir con lo siguiente:

- Aprobar con promedio mínimo 4.0
- Asistencia mínima: 75% por unidad.
- Entrega oportuna de productos e instancias de evaluación.

UNIVERSIDAD BERNARDO O'HIGGINS

ES MOMENTO DE AVANZAR

CONTENIDO

Módulo 1

Panorama Estratégico de la Ciberseguridad y Ciberdefensa en América Latina

- Conocer las amenazas digitales y los riesgos asociados a la seguridad en la tecnología moderna.
- Comprender el rol de la ciberdefensa en el ámbito público y privado.
- Evaluar políticas públicas y estrategias nacionales de ciberseguridad.
- Características del Ciberespacio y el impacto en ámbito profesional y personal.
- Principios de Confidencialidad, Integridad y Disponibilidad (tríada CIA).
- Conceptos básicos de ciberdefensa y ciberinteligencia, aplicado en el contexto profesional y personal.

Aprendizaje Esperado

- El estudiante comprenderá el contexto regional de amenazas digitales y será capaz de analizar políticas públicas y estrategias de ciberseguridad desde una perspectiva estratégica y ética.

CONTENIDO

Módulo 2
Gobernanza, Riesgos y Cumplimiento Normativo (GRC)

- Diseñar políticas de seguridad y privacidad alineadas con la legislación chilena.
- Integrar la ciberseguridad en la estrategia organizacional.
- Normativas y marcos regulatorios en Ciberseguridad en Chile y en Europa.
- Firma digital, herramienta que fortalece la seguridad de la digitalización.
- Estándares y marcos de referencia: ISO 27001, NIST Cybersecurity Framework. Políticas internas de la organización.

Aprendizaje Esperado

- El estudiante aplicará marcos normativos internacionales y diseñará políticas de seguridad alineadas con la legislación chilena, integrando la ciberseguridad en la gobernanza organizacional.

CONTENIDO

Módulo 3

Herramientas y Técnicas de Seguridad: Criptografía, Blockchain, Certificación Digital y OSINT

- Aplicar técnicas de cifrado y firma digital en entornos reales.
- Comprender la infraestructura de clave pública (PKI) y su uso en Chile.
- Explorar el uso de blockchain en seguridad y trazabilidad de la información.
- Métodos y Tácticas de ataque de los ciberdelincuentes.
- Herramientas OSINT, para búsqueda de información mediante fuentes abiertas.

Aprendizaje Esperado

- El estudiante dominará técnicas de cifrado y firma digital, comprenderá el funcionamiento de PKI y explorará el uso de blockchain como herramienta de seguridad y trazabilidad.

CONTENIDO

Módulo 4

Seguridad en Redes, Infraestructura y Sistemas Operativos

- Fundamentos de Arquitectura de Redes, Administración de Sistemas Operativos y Seguridad en Redes.
- Configurar redes seguras y aplicar hardening en dispositivos.
- Detectar vulnerabilidades en sistemas operativos y servicios web.
- Implementar firewalls, IDS/IPS y segmentación de red.

Aprendizaje Esperado

- El estudiante será capaz de configurar redes seguras aplicando hardening en dispositivos y detecta vulnerabilidades en sistemas operativos y servicios web.

CONTENIDO

Módulo 5
Gestión y Respuesta ante Incidentes de Seguridad

- Diseñar planes de respuesta y recuperación ante incidentes.
- Implementar CSIRT y protocolos de actuación.
- Aplicar ITIL, NIST y Security Guidance en la gestión de incidentes.
- Clasificación de eventos e incidentes según impacto y criticidad.

Aprendizaje Esperado

- El estudiante diseñará planes de respuesta ante incidentes, implementará protocolos CSIRT y aplicará frameworks como ITIL y NIST para la gestión de crisis cibernéticas.

CONTENIDO

Módulo 6
Hacking Ético y Pruebas de Penetración

- Realizar auditorías de seguridad y pentesting controlado.
- Utilizar herramientas como OWASP ZAP, Kali Linux y Metasploit.
- Simular ataques para fortalecer la postura defensiva.

Aprendizaje Esperado

- El estudiante ejecutará auditorías de seguridad, utilizará herramientas de pentesting y simulará ataques controlados para evaluar y fortalecer la postura defensiva de sistemas.

CONTENIDO

Módulo 7
Análisis Forense y Ciberinvestigación Legal

- Introducción al Análisis Forense.
- Herramientas de Informática Forense.
- Aplicar técnicas de análisis forense en dispositivos y redes.
- Interpretar evidencia digital bajo la Ley 19.223 y 19.628.
- Elaborar informes periciales para casos de fraude y delitos informáticos.

Aprendizaje Esperado

- El estudiante aplicará técnicas de análisis forense digital, interpretará evidencia bajo el marco legal chileno y elaborará informes periciales para casos de delitos informáticos.

CONTENIDO

Módulo 8

Taller Final Integrador: Simulación de Incidente Crítico

- Participar en un ejercicio de análisis colaborativo que permita identificar los aspectos principales de un ataque cibernético complejo, en un contexto ficticio, con una situación general y particular, y encuadrado en una unidad de estudios y asesoría en el nivel nacional.
- Aplicar conocimientos adquiridos para proponer acciones de respuesta, análisis forense y comunicación estratégica frente a la situación de contexto.

Aprendizaje Esperado

- El estudiante participará en un grupo de estudios y asesoría identificando los aspectos principales de un ataque cibernético proponiendo acciones frente al evento complejo.

Cuerpo docente

Fernando Santander
Profesor en Historia y Geografía para Enseñanza Media, Licenciado en Educación Universidad Bernardo O'Higgins y Magíster en Sociología, Universidad Alberto Hurtado, Actualmente es candidato a Doctor en Innovación en Ciencias Sociales por la Universidad Pontificia de Salamanca. Se desempeña como Secretario Académico de la Facultad de Ciencias Humanas de la Universidad Bernardo O'Higgins y profesor de la carrera y magister en Educación Diferencial, cuenta con una amplia trayectoria en gestión universitaria, formación inicial docente, docencia de pre y postgrado, e investigación académica. En el ámbito de investigación ha participado activamente en congresos, seminarios, y publicaciones indexadas en educación patrimonial, inclusiva y memoria.

Cinthia Sepúlveda
Oficial Policial de grado de subcomisario de la Policía de Investigaciones de Chile (PDI), de profesión Ingeniera Civil en Computación Informática y además cuenta con un Magíster en Ingeniería en Seguridad de la Información. Con más de 10 años de experiencia en la institución, de los cuales 06 años los ha desarrollado en el área de Ciberseguridad en la PDI, combina su labor policial con la docencia en el plantel educacional de la institución policial. Además participa en proyectos de elaboración de cursos en el ámbito de la educación superior, aportando a la formación de futuros profesionales en el área.

Dr. Gonzalo Díaz de Valdés Olavarrieta
Doctor en Sistemas de Ingeniería Civil por la Universidad Politécnica de Madrid (España) y MBA por Loyola University Maryland (EE.UU.), con más de 25 años de trayectoria en ciberseguridad, gestión de riesgos y transformación digital en el sector financiero y de defensa nacional.
Se desempeñó como Jefe del Departamento de Ciberdefensa y Ciberseguridad del Ministerio de Defensa Nacional y fue Punto Focal de Chile ante el Índice Global de Ciberseguridad de la UIT–ONU. Realizó aportes significativos en la elaboración de la Ley 21.663 de Ciberseguridad, marco regulatorio que hoy rige la seguridad digital en Chile. Es Catedrático del Magíster en Ciberdefensa de la Academia Politécnica Militar y docente en programas de postgrado en diversas universidades del país.

Cuerpo docente

Oscar Bustos
Ingeniero Politécnico Militar con mención en Armamento, Magíster en Docencia de Nivel Superior por la Universidad de los Andes y Diplomado en Planificación Estratégica y Control de Gestión por la Universidad de Chile. Actualmente se desempeña como Jefe de la División de Desarrollo Tecnológico e Industria en la Subsecretaría de Defensa.

Cuenta con una destacada trayectoria en el Ejército y el Ministerio de Defensa Nacional, integrando además los directorios de ASMAR, FAMAE y ENAER, y el Consejo Directivo de la Comisión Chilena de Energía Nuclear (CCHEN). En el ámbito académico, es docente externo en instituciones de formación estratégica y militar, en asignaturas vinculadas a pensamiento crítico e inteligencia artificial.

Antonella Granifo
Abogada con más de 16 años de experiencia en asesoría legal, cumplimiento normativo e integridad empresarial. Inició su trayectoria como Jueza del Tribunal Oral en lo Penal de Arica y actualmente se desempeña como Compliance Officer, Data Protection Officer y Delegada de Ciberseguridad en M. Kaplan y Cía. Ltda.

Cuenta con formación especializada en ciberseguridad, continuidad del negocio e integridad empresarial, combinando experiencia jurídica y visión estratégica en protección de datos, cumplimiento y defensa corporativa. Además, ha sido docente en la Academia Politécnica Militar en asignaturas de Derecho.

Ficha Técnica

Matrícula	Arancel	Duración
-	$1.500.000	136 horas

Consulte por descuentos y 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®

ES MOMENTO DE
AVANZAR

capacitacion@ubo.cl / +562 2988 4850

General Gana 1702, Edificio Rondizzoni I, Santiago

/uboeducacioncontinuaycapacitacion

/uboeducacion

/company/ubo-educación-continua-y-capacitación

5 AÑOS

Comisión Nacional de Acreditación CNA-Chile

UNIVERSIDAD ACREDITADA
MEDIANTE ACUERDO DEL CONSEJO NACIONAL DE EDUCACIÓN
NIVEL AVANZADO
• GESTIÓN INSTITUCIONAL
• DOCENCIA DE PREGRADO
• VINCULACIÓN CON EL MEDIO
HASTA 9 DE NOVIEMBRE DE 2027