



# DIPLOMADO EN SEGURIDAD INFORMÁTICA

[www.dsinf.cl](http://www.dsinf.cl)

Ábrase al mundo de la Capacitación, una  
oportunidad para seguir creciendo...



## DIPLOMADO EN SEGURIDAD INFORMÁTICA

El Diplomado en Seguridad Informática es una alternativa que permitirá a los asistentes conjugar no sólo la **técnica informática** sino que identificar el bien jurídico protegido que se pretende cautelar frente a conductas que las lesionan.

Proporcionará además **herramientas tecnológicas** de uso público para ser utilizadas como sistemas de inteligencia informática de mitigación de ataques.

El diplomado será dictado bajo la modalidad **Blended Learning**, esto es una proporción será **presencial y sincrónica** y la otra **asincrónica** a través de una plataforma digital de aprendizaje con cursos en línea.

### DIRIGIDO A

El diplomado está dirigido a técnicos, licenciados o profesionales relacionados con el ámbito de la seguridad informática, profesionales chilenos y extranjeros que podrán asistir a las clases presenciales dictadas por los profesores en la propia Universidad Bernardo O'Higgins o acceder a las mismas clases en tiempo real a través del sistema de Webcasting en [www.dsinf.cl](http://www.dsinf.cl) <sup>(1)</sup>.

El avance asincrónico será a través de una plataforma de e-learning habilitada para tales efectos.

(1) Partner Tecnológico → [www.mundovisión.cl](http://www.mundovisión.cl)

### OBJETIVO

Al término del Diplomado, el alumno será capaz de reconocer, buscar e implementar diversos sistemas de protección de ataques informáticos a través de modelos y proyectos preventivos y reparativos basados en las ciencias y tecnologías de la información.

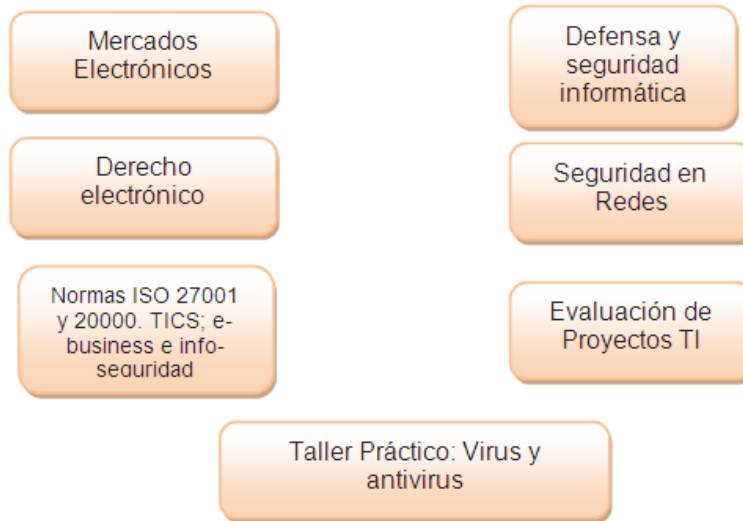
### REQUISITOS DE LOS PARTICIPANTES

Pueden acceder al Diplomado todas aquellas personas que cumplan con uno de los siguientes requisitos: Poseer Título Técnico de nivel superior o Título Profesional ad-hoc.



## PROGRAMA

Nuestra propuesta académica está compuesta por siete cursos más un taller práctico, los que se detallan a continuación:



### **MÓDULO 1: Mercados Electrónicos** (6 horas presenciales; 10 horas e-learning):

Se analizarán los mercados de Hackers y empresas vinculadas con la seguridad y cómo estas impactan a la economía.

El objetivo de este curso es mostrar a los asistentes la dinámica y la cuantía de recursos que transan los mercados de seguridad en el mundo.

Busca analizar los diversos modelos de negocios que se plantean y su evolución hasta nuestros días, mostrando casos prácticos por sector industrial.

Además busca analizar la dinámica microeconómica de estos mercados y como estos afectan a otros como la industria de los seguros.

Se espera analizar el mercado de la defensa informática de software y antivirus además de las formas de ataques informáticos y todas sus manifestaciones.

### **MÓDULO 2: Tópicos Legales sobre Seguridad Informática** (6 horas presenciales; 10 horas e-learning):

Se tratarán temas como: Documento y firma electrónica; contratación electrónica; delitos computacionales e informáticos.

Comprender la significancia jurídica de la sociedad de la información.

Obtener las competencias necesarias para el enfrentamiento de los desafíos que en materia legal presenten los alumnos en el ejercicio de su profesión.

**MÓDULO 3: Normas ISO 27.001 / 20.000** (6 horas presenciales; 10 horas e-learning):

En este módulo se analizan las normas internacionales de aseguramiento de la calidad y específicamente se estudia cómo puede una organización implementar un sistema de gestión de seguridad de la información basado en ISO 27.001. Los participantes conocerán la forma de implementar ISO 27.001 en empresas tecnológicas; Data centers; dedicadas al E-business o al e-government.

**MÓDULO 4: Defensa y Seguridad Informática** (6 horas presenciales; 10 horas e-learning):

Se revisarán aspectos como: Seguridad nacional informática, capacidad de respuesta ante incidentes de seguridad, investigación de incidentes informáticos a objetivos de estado o militares.

El curso está orientado a que los alumnos puedan identificar, analizar y describir los aspectos de riesgo relevantes en un ambiente de información complejo., teniendo en cuenta que la información almacenada trasciende en lo *político, económico, social, y militar*, con énfasis en el último y primer aspecto.

El alumno conocerá aspectos modernos de guerra de la información y los efectos que podrían producir ataques ciberterroristas a instalaciones de seguridad nacional, entenderá como formar equipos de respuesta y realizar análisis básico de información.

**MÓDULO 5:**

**Seguridad en Redes** (6 horas presenciales; 10 horas e-learning);

Serán tratados, entre otros los siguientes aspectos: Las redes informáticas, seguridad y defensa de ataques de hackers.

Enseñar a los estudiantes a diseñar redes seguras, considerando tanto los riesgos internos en la red como los externos, entre los cuales están las conexiones remotas y vpn. A su vez, entregar las herramientas bases para detectar vulnerabilidades en la red y discutir las estrategias del cómo enfrentar un problema ante una determinada amenaza.

Enseñar y concientizar al estudiante a lo valioso de la información y que ésta permanezca íntegra, confidencial y siempre disponible

**MÓDULO 6: Evaluación de Proyectos de Tecnologías de la Información** (6 horas presenciales; 10 horas e-learning):

Trata temas relacionados con la metodología de formulación y evaluación de proyectos de inversión aplicado al sector de TICS.

Conocer principios de la formulación y evaluación de proyectos, aplicados en mercado intensivo en tecnología, de manera que el alumno pueda utilizar criterios de decisión respecto de la toma de decisiones.

Emplear procedimientos y metodologías de análisis de proyectos, de tal forma que el alumno pueda determinar de forma conveniente y eficiente oportunidades de inversión.

**MÓDULO 7:**

**Taller Práctico: Virus y Antivirus** (6 horas presenciales; 10 horas e-learning)

En este módulo se analizarán la historia de los virus informáticos y la forma en que la industria se ha defendido. Cuáles son las características de los virus más nocivos, que sistemas y archivos destruyen, como mutan y se ramifican en la red.

## **ANTECEDENTES GENERALES**

### **Ficha Técnica**

Código Sence : Consultar  
 Duración : 112 horas cronológicas (42 presenciales, 70 e-learning)  
 Fecha inicio : 15 de Mayo  
 Fecha de término : 07 de Agosto  
 Programación : viernes y sábados (presencial):  
 Presencial 21-22-28-29 Mayo, 4-5-11-12-18-19-25-26 Junio, 2-3  
 E-learning 3 de Junio al 07 de Agosto  
 Horario : Viernes de 19:00 a 22:00 horas, sábado de 09:00 a 13:00 horas

Lugar de realización : Av. Viel 1497, Santiago (metro Rondizonni), instalaciones UBO

Valor participante	VALOR NORMAL	10% ACHS – EX ALUMNO UBO	15% FUERZAS ARMADAS	20% CC LOS ANDES
		\$ 900.000	\$ 810.000	\$ 765.000

La Universidad se reserva el derecho a posponer fecha de inicio o suspender la actividad, si no hay la cantidad de alumnos mínimos.

### **Informaciones**

Dirección de Capacitación  
 Dirección : Av. Viel 1497, Santiago. Metro Rondizonni  
 Teléfonos : 4774155 – 4774187 – 4774188  
 e-mail : [capacitacion@ubo.cl](mailto:capacitacion@ubo.cl) – [lcaticura@ubo.cl](mailto:lcaticura@ubo.cl)  
 Página web : [www.ubocapacitacion.cl](http://www.ubocapacitacion.cl) - [www.ubo.cl](http://www.ubo.cl)

- Todas las actividades de capacitación están reconocidas por SENCE, lo que permite el uso de la franquicia tributaria
- Toda actividad de capacitación deberá inscribirse en SENCE con al menos 24 horas antes de la fecha de inicio del curso.
- Una vez iniciada la actividad de capacitación, no se aceptará la postergación del curso, ni se hará devolución del dinero
- La Dirección de Capacitación de la Universidad Bernardo O'Higgins se reserva el derecho de posponer la fecha de inicio o suspender la actividad, si no hay la cantidad de alumnos mínimos.
- En cada actividad de capacitación, el alumno recibirá un material de apoyo, con los contenidos tratados en clases y con el reglamento interno de las actividades de capacitación.
- Al término de la actividad se entregará un certificado de aprobación a los alumnos que cumplan con una asistencia mínima de un 75% y un promedio de notas igual o superior a 4.0, en escala de 1.0 a 7.0., además se les entregará un Diploma otorgado por la Dirección de Capacitación de la Universidad.
- Si un alumno debidamente inscrito no cumple con estos requisitos, y por consiguiente pierde el derecho a financiamiento de SENCE, no cabrá derecho a devolución de los montos cancelados a la Universidad y el contratante deberá hacerse cargo del pago del 100% del valor del curso para ese alumno si no existe un acuerdo previo. Si un alumno debidamente inscrito en las actividades de capacitación es retirado por el contratante, no cabrá devolución alguna de los montos cancelados por ese alumno.
- Mediante ficha de inscripción interna de la Dirección de Capacitación, orden de compra de la empresa o del Organismo Técnico Intermedio de Capacitación (OTIC) correspondiente, el cliente acepta los términos y condiciones establecidos en este documento.
- Este diplomado será Dictado sólo si cumple el requisito del mínimo de alumnos que se ha fijado en 17 debidamente matriculados antes de la fecha de inicio de clases programada para la versión del diplomado bajo modalidad e-learning asincrónico y 33 bajo modalidad e-learning sincrónico.
- La Dirección de Capacitación de la Universidad Bernardo O'Higgins, realiza cursos cerrados a empresas, de acuerdo a sus necesidades de capacitación.

