

Diplomado

# CIBERSEGURIDAD (GESTIÓN, TÉCNICO Y LEGAL)

---

## OBJETIVO DEL PROGRAMA

Contribuir al desarrollo y mejora de la Ciberseguridad, en aspectos de gestión, de técnicas y de cuestiones legales, en organizaciones públicas y privadas del país, mediante la formación y especialización de las y los profesionales partícipes de los distintos procesos de TICs, permitiendo con ello aportar para tener organizaciones seguras y resilientes frente a riesgos y amenazas de ciberataques internos y externos.

## DESCRIPCIÓN DEL PROGRAMA

El diplomado desarrolla temas que permitan comprender los principales lineamientos en la gestión estratégica para lograr una gestión y gobernanza eficaz en Ciberseguridad. Además, permite diseñar estrategias de ciberseguridad junto con el plan de acción para su implementación. Los alumnos podrán conocer los aspectos legales de la Ciberseguridad a nivel nacional e internacional. Como parte del programa también se dan lineamientos para saber cómo adquirir herramientas para proteger, monitorear, y administrar la infraestructura TI dentro de una organización. Finalmente, el programa proporciona conocimientos para analizar y evaluar los sistemas de Ciberseguridad orientadas a brindar un soporte fundamental a la estrategia del negocio de las organizaciones.

## PÚBLICO OBJETIVO

El programa está dirigido a todos aquellos profesionales vinculados con las Tecnologías de la Información y Comunicación.

## REQUISITOS DE INGRESO

- Título Profesional o Certificado de Egreso (copia original entregada por la institución de educación superior o fotocopia legalizada ante notario).
- Certificado de nacimiento.
- Copia de cédula de identidad (escaneado por ambos lados).
- Currículum Vitae.
- Ficha de inscripción.
- *NOTA: Toda esta documentación debe ser enviada en formato digital por e-mail.*

## REQUISITOS DE APROBACIÓN DEL DIPLOMADO

Los requisitos de aprobación de cada curso corresponden a evaluaciones escritas y trabajos de desarrollo individual y grupal, de acuerdo con lo propuesto por cada profesor. Para aprobar el diplomado completo el alumno deberá:

- Aprobar todos los cursos del diplomado (7 cursos). Tener nota mínima de 4,0 (en escala de 1,0 a 7,0) en cada curso del diplomado.
- Asistencia de un 75% a las horas de clase de cada curso del diplomado.

Al término del programa y habiendo cumplido todos los requisitos de aprobación, el alumno recibirá un certificado de “*Diplomado en Ciberseguridad (Gestión, Técnico y Legal)*” otorgado por la misma Universidad de Santiago de Chile.

## COSTOS DEL PROGRAMA

- El valor total del diplomado asciende a \$3.150.000 (valor año 2022, 1<sup>er</sup> semestre).
- Derecho de inscripción por un valor de \$64.000. (valor referencial año 2021)
- Este diplomado no está adscrito a código SENCE.
- Este diplomado no está adscrito a convenio marco.

## FINANCIAMIENTO

- Financiamiento directo por parte del alumno.
- Para el caso de financiamiento por parte de la empresa o institución interesada, emitir orden de compra a nombre de:
  - SDT USACH Ltda.
  - RUT: 78.172.420-3
  - Dirección: Alameda 1611, Santiago Centro, Santiago, Región Metropolitana.

## FORMAS DE PAGO

- Tarjeta de Crédito, Tarjeta de Débito, Transferencias y Cheques.

## DESCUENTOS

- 25% de descuento para pago al contado en el caso de *financiamiento directo por parte del alumno* (el alumno no viene financiado por una empresa/organización).
- IMPORTANTE:
  - Los descuentos son aplicables solamente para pagos realizados hasta antes del inicio de clases del diplomado.
  - Los descuentos no aplican para los cursos de los diplomados en el caso de que éstos se tomen de manera individual.

## PLAN DE ESTUDIOS

El diplomado tiene una duración de 180 horas cronológicas con 105 horas de docencia directa y está estructurado en 7 módulos. Los módulos y los temas tratados en cada uno de ellos se describen a continuación.

- 1. Fundamentos ciberseguridad y seguridad de la información**
  - Estándares y marcos de trabajo en seguridad de la información
  - Estándares y marcos de trabajo en ciberseguridad
  - Estándares y marcos de trabajo en gestión de riesgos e incidentes
  - Concienciación e Ingeniería Social
- 2. Gestión y operación de la ciberseguridad**
  - Evaluación integral de la seguridad de la información y ciberseguridad
  - Programa gestión y operación de riesgos
  - Programa gestión y operación de incidentes
  - Programa de gestión en ciberseguridad
  - Sistema de gestión de ciberseguridad y controles
- 3. Operación de la ciberseguridad y TI**
  - Gestión de servicios externalizados TI
  - Gestión de disponibilidad de servicios TI
  - Gestión de amenazas y vulnerabilidades
  - Centro de operación de ciberseguridad (CSOC) - (CSIRT)
- 4. Seguridad y protección tecnológica**
  - Criptografía
  - Seguridad en sistemas operativos
  - Seguridad redes
  - Seguridad base de datos
  - Hardening
- 5. Protección aplicativa, hacking ético y forense**
  - Reconocimiento, enumeración y análisis de vulnerabilidades
  - Desarrollo seguro (OWASP, OpenSAMM)
  - Hacking web
  - Wireless, APT y DoS
  - Metodología pentest
  - Forense
  - Peritaje
- 6. Tecnologías relacionadas**
  - Seguridad virtualización
  - Seguridad Cloud
  - Seguridad IoT
  - BlockChain
- 7. Aspectos legales en ciberseguridad**
  - Marco legal, regulatorio y normativa
  - Aspectos legales futuros
  - Legal y hacking ético
  - Legal y forense

## FECHAS Y MODALIDAD DE ESTUDIOS

Fecha de inicio: 11/abril del 2022.

Horario: Lunes y miércoles de 19:00 a 22:00 horas.

Modalidad: El diplomado se dictará en modalidad On-Line.

## INFORMACIONES

Dirección: Departamento de Ingeniería Informática, Universidad de Santiago  
Avenida Ecuador N° 3659, Estación Central

Coordinador: Alcides Quispe, Teléf. 22 71 80 938, [alcides.quispe@usach.cl](mailto:alcides.quispe@usach.cl)

Secretarias: Romina Labrin, Teléf.: 22 71 80 905, [romina.labrin@usach.cl](mailto:romina.labrin@usach.cl)