

DIPLOMADO EJECUTIVO

CIBERSEGURIDAD

Julio a Diciembre de 2019 | Santiago, Chile



Tecnológico
de Monterrey

35

años de experiencia en
actualización ejecutiva a nivel mundial

MÁS DE

300MIL

ejecutivos han asistido
a los programas

LAS TOP

500

empresas se capacitan
con nosotros



Interacción directa con
reconocidos profesores del
TEC de Monterrey.



Comparta experiencias
reales y establezca redes de
contacto de primer nivel.



Cuenta con material
académico en digital y LMS
Canvas.



HOTELES
PLAZA EL BOSQUE

Hotel Plaza El Bosque
Ebro 2828, Las Condes,
Santiago.



*Inspiring Your
Full Potential*

DIPLOMADO EJECUTIVO

CIBERSEGURIDAD

En 2018, Chile debió enfrentar dos ciberataques dejando al descubierto los pocos avances que se han hecho en esta materia. Según Kaspersky América Latina, cada segundo se producen casi nueve ataques de código malicioso en Latinoamérica, superando en 5 veces a regiones como Europa e India.

Este exclusivo diplomado en Ciberseguridad diseñado en conjunto con TEC de Monterrey le permitirá identificar los servicios y mecanismos necesarios para construir un sistema informático operacional seguro y alineado a los objetivos de su organización, con el fin de implementar una estrategia de ciberseguridad exitosa.

Cada módulo tiene una duración de dos días consecutivos, una vez al mes, para un total de 6 meses, incluyendo un módulo desarrollado por un experto local para abordar temáticas de ciberseguridad en Chile.

MALLA CURRICULAR



ANTECEDENTES ACADÉMICOS

- Evaluación online en cada módulo.
- Certificación con insignia digital.
- Duración total: 96 horas.
- Inicio del programa: Julio de 2019
- Término del programa: Diciembre de 2019



BIBLIOTECA CAMPUS
TECNOLÓGICO DE MONTERREY

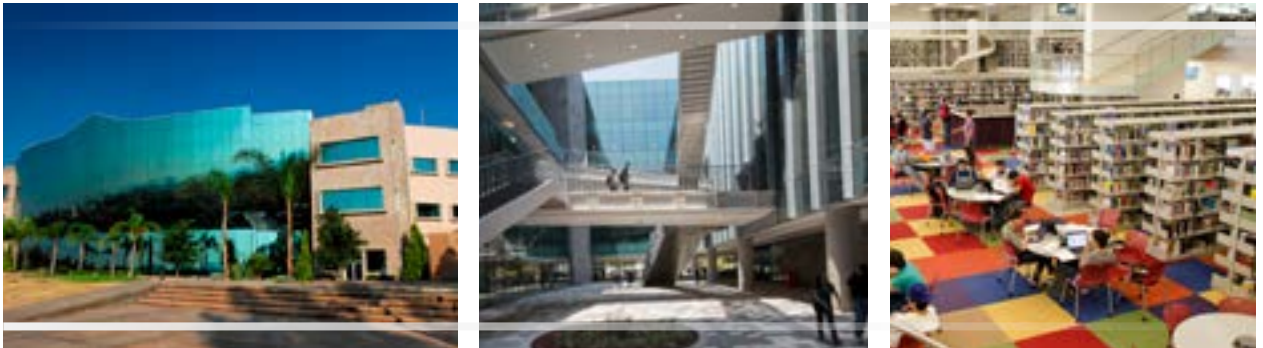
Entre las **universidades privadas**, el **TEC** se coloca en el

TOP **30** MUNDIAL

#1 En **México** se posiciona como la universidad privada **N°1**.

#5 En toda **Latinoamérica** se posiciona como la universidad privada **N°5**.

TEC de Monterrey es el sistema universitario más grande de América Latina. Su visión es formar personas que se conviertan en agentes de cambio que apoyen la transformación de otros a través de un modelo educativo de vanguardia, enfocado en el desarrollo del espíritu emprendedor y la formación con sentido humano.



TEC CYBERSECURITY HUB

El Tecnológico de Monterrey, de la mano de Cisco, Citibanamex, Deloitte, IBM, Thales y la Universidad de Texas, San Antonio (UTSA), presentaron el Tec Cybersecurity Hub, el primer centro de operaciones de ciberseguridad con servicios integrales en México y Latinoamérica, el cual brindará espacios para que startups, investigadores, profesores, alumnos e inversionistas se sumen a la misión de capacitar talento actual y futuro, investigar, sensibilizar y concientizar sobre las amenazas cibernéticas.



METODOLOGÍA:

La estrategia didáctica principal del diplomado es la exposición y análisis de los instructores especialistas en su tema y con experiencia, quienes se apoyarán en reflexiones de la práctica, casos y en ejercicios para consolidar el aprendizaje de cada tema.



MODALIDAD DE ESTUDIO:

6 módulos presenciales, de 2 días cada uno, impartido en Santiago entre Julio y Diciembre.
Duración: 96 horas / 6 meses.



REQUISITOS DE APROBACIÓN:

Se realizará una evaluación on line después de cada módulo.
Se debe aprobar con un 75% los módulos.
Requisito de asistencia: 100%



Certificado de aprobación emitido por el Tecnológico de Monterrey

CUERPO ACADÉMICO



ROBERTO GÓMEZ CÁRDENAS

Doctorado en Informática, Universidad de Paris. Ha sido profesor del departamento de TI por 16 años en el Tecnológico de Monterrey, donde se ha destacado por sus publicaciones académicas y premios dados por sus estudiantes como “Profesores que dejan huella”. Es coordinador académico del Diplomado en Seguridad Informática del Tecnológico de Monterrey, el cual lleva 4 generaciones. CISO de Invex, grupo financiero mexicano que genera soluciones para la banca. Además, ha sido consultor de empresas como Bancomer y Santander.



FERNANDO ZEPEDA GONZÁLEZ

Ingeniero en Comunicaciones y Electrónica. Master en Ciencias de la Ingeniería. Ha sido catedrático de diversas universidades entre las que destacan el Instituto Tecnológico y de Estudios Superiores de Monterrey, la universidad Iberoamericana. Ha sido consultor en empresas como BBVA Bancomer, Santander y ALAPSI (Asociación Latinoamericana de Profesionales en Seguridad Informática).



ADRIÁN PALMA CASTILLO

Ingeniero en Ciencias de la Informática. Cuenta con más de 24 años de experiencia como consultor, auditor de seguridad, auditor de sistemas, ventas y normatividad en tecnología de información. Es académico de la Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas (UPIICSA) en temas de auditoría y seguridad informática: es profesor del diplomado de Seguridad en Informática en el Tecnológico de Monterrey. Ha colaborado con Dell, Insys, Integridata.



EDGAR CHILLÓN ESCÁRCEGA

Ingeniero Cibernético y en Sistemas Computacionales. Master en Tecnologías de la Información, Universidad de la Salle. Cuenta con amplia experiencia profesional en el campo de la seguridad informática. Fue Subdirector de Seguridad Informática en la Secretaría de Finanzas del Gobierno de D.F, donde fue encargado de implementar y mejorar la estrategia de Seguridad Informática. ES CEO Fundador de BHacking SA., empresa dedicada a apoyar y especializar en seguridad digital.



ADOLFO GREGO KIBRIT

Ingeniero en Sistemas Computacionales, Master of Science in Computer Science, University of Illinois. Es profesor del Diplomado en Seguridad Informática y profesor de cátedra del departamento de ciencias computacionales donde ha impartido cursos de Redes, Teleproceso y Sistemas Operativo. Es CTO de grupo RF y Director de Tecnología en Mycros Electrónica, empresa especializada en brindar soluciones de ingeniería de seguridad para Instituciones de Seguridad Gubernamentales, contando con más de 30 años de experiencia.



GABRIEL BERGEL

Ing. en Computación e Informática, Doctor en Informática U. de Paris, Máster en Ciberseguridad de IMF Business School y la U. Camilo José Cela. Cuenta con certificaciones, CISSP por (ISC)², Lead Auditor ISO 27001 por BSI, CBCP por DRI, CISM por ISACA y C|CISO por EC-Council. Es CSA de Eleven Paths, miembro del directorio global de (ISC)², co-fundador y organizador de 8.8 Computer Security Conference, chair del Latin American Advisory Council de (ISC)², coordinador del Centro de Ciberseguridad Industrial y director de Políticas Publicas en Whilolab.

PROGRAMA DE ESTUDIOS

Módulo I: Tendencias en Ciberseguridad

11 y 12 de Julio

Objetivo: Obtener los conocimientos necesarios para identificar, evaluar y mitigar los principales riesgos que las redes informáticas actuales presentan a nivel del perímetro de una red corporativa; así como poder seleccionar las contramedidas que pueden implantarse en las redes actuales y las soluciones existentes en el mercado.

- Seguridad informática, seguridad de información y Ciberseguridad.
- Estado actual de la Ciberseguridad.
- Evolución y métricas de la Ciberseguridad.
- Conceptos de la Inteligencia Artificial aplicados a la Ciberseguridad.
- Blockchain y Ciberseguridad.
- Open Source Intelligence (OSINT).
- IOCs, (Indicators Of Compromise), extracción, uso y distribución.
- Deep Web.
- La academia y la ciencia de la Ciberseguridad.
- Técnicas de ataque prevalentes.
- Dispositivos y medidas de seguridad prevalentes.

Módulo II: Ciberseguridad a nivel Software

05 y 06 de Agosto

Objetivo: Conocer los aspectos relacionados con la seguridad en aplicaciones en producción, desarrollo, y las metodologías y herramientas para analizar, diseñar, e implementar controles en el ciclo de vida del desarrollo de aplicaciones. Identificar las características principales del software malicioso, así como las amenazas de este tipo de software. Implementar las contramedidas necesarias para mitigar el riesgo provocado por el software malicioso.

- Controles en aplicaciones en producción y en desarrollo.
- CMM.
- Sistemas expertos.
- Redes neurales.
- Control del proyecto y del producto.
- Principios de auditoría.
- Estrategias para el desarrollo de aplicaciones.
- Metodología de seguridad para el desarrollo de aplicaciones.
- Acreditación y Certificación.
- Conversión de las aplicaciones.
- Administración de cambios y configuraciones.
- Acreditación y Certificación.
- Conversión de las aplicaciones.
- Administración de cambios y configuraciones.
- Administración de cambios y configuraciones.
- Mejores prácticas para desarrollo de aplicaciones web
- Criterios de OWASP
- OWASP Top Ten
- Funcionamiento, análisis y contramedidas del software malicioso.

Módulo III: Herramientas de Seguridad

26 y 27 de Septiembre

Objetivo: Conocer el funcionamiento, ventajas y desventajas, de las herramientas más utilizadas en Ciberseguridad.

- Escaneo de puertos TCP/UDP: Nmap.
- Firewalls.
- Detectores de intrusos.
- Sniffers.
- Software para inyección de paquetes.
- Crackeo de contraseñas en línea y fuera de línea.

Módulo IV: Ciberseguridad y su aplicación en Chile

16 y 17 de Octubre

Objetivo: Analizar, a través de los hechos sucedidos en Chile el año 2018, la situación actual del país, los sectores de ataques más populares y cómo se debe enfrentar esta nueva realidad en nuestro país. Identificar las normativas que aplican en Chile y conocer cómo realizar una gestión de riesgos eficiente. .

- ISO / IEC 27001 (Desarrollo de un SGSI).
- ISO / IEC 27032 (Gestión de la Ciberseguridad).
- ISO / IEC 27035 (Gestión de Incidentes de Seguridad de la Información).
- 20 controles Críticos V7 (Center for Internet Security (CIS)).
- Marco de trabajo de la Ciberseguridad del NIST. (National Institute of Standards and Technology).
- PSI-DSS 3.2.1 (Payment Card Industry Data Security Standard).
- Análisis y gestión de riesgos.
- Gestión de incidentes.

Módulo V: Seguridad en Sistemas operativos

18 y 19 de Noviembre

Objetivo: Conocer las ventajas y desventajas desde el punto de vista de seguridad de los sistemas operativos basados en Win32 y Win64 de Microsoft. Definir una lista de mejores prácticas para fortalecer un sistema operativo Unix.

- Seguridad en sistemas operativos Windows
- Orígenes e Historia.
- Básicos Win32 y NT.
- Arquitectura de Seguridad de Windows en todas sus versiones
- Seguridad en sistemas operativos Unix
- Seguridad y Unix.
- Autenticación en Unix.
- Los sistemas de archivos.
- Los archivos de inicialización.
- Monitoreo del sistema.
- Bitácoras en Unix.
- Los servicios de red.

Módulo VI: Seguridad Perimetral

05 y 06 de Diciembre

Objetivo: Conocer el funcionamiento y características de los dispositivos que conforman una red inalámbrica. Definir la arquitectura, y mejores prácticas, de una red inalámbrica que proporcione funcionalidad y seguridad a una organización.

- Antecedentes y conceptos de seguridad informática.
- Mecanismos de autenticación.
- Control de acceso.
- Definición y componentes del perímetro de seguridad.
- Anatomía de ataques a las redes informáticas
- Importancia de la seguridad a nivel red
- Introducción a tecnologías inalámbricas.
- El protocolo IEEE 802.11.
- Antenas.
- WARDriving.
- Wired Equivalent Privacy (WEP)
- Atacando WEP.
- Wifi Protected Access (WPA)
- Atacando WPA
- IEEE 802.11i o WPA2
- WPA3
- Esquemas de defensa para redes inalámbricas.

DIPLOMADO EN
CIBERSEGURIDAD

Julio a Diciembre de 2019 | Santiago, Chile



CUPOS LIMITADOS

**VALOR
INDIVIDUAL**



115 UF

**GRUPO
CORPORATIVO**
3 a 5 Ejecutivos



100 UF

**CONVIERTA SU EQUIPO DE TRABAJO EN UN
HIGH PERFORMANCE TEAM**

Optimice el rendimiento de sus equipos organizacionales incentivando la participación del grupo completo en el programa. Esta dinámica fomenta un mejor trabajo en equipo, potencia los talentos, la motivación y relaciones interpersonales que se traducen en ventajas frente a la competencia.

Incremente el ROI sobre sus iniciativas de actualización y perfeccionamiento ejecutivo.



LMS Canvas
de apoyo al programa.

Entre las **universidades
privadas**, el **TEC** se coloca en el

TOP **30** MUNDIAL

#1 En **México** se posiciona como la universidad
privada **N°1**.

#5 En toda **Latinoamérica** se posiciona como la
universidad privada **N°5**.



www.seminarium.com



[/seminariumchile](https://www.facebook.com/seminariumchile)



[/seminariumchile](https://www.linkedin.com/company/seminariumchile)



[@seminariumchile](https://twitter.com/seminariumchile)