UNIVERSIDAD
DE SANTIAGO
DE CHILE

DEPARTAMENTO DE
TECNOLOGÍAS
INDUSTRIALES
UNIVERSIDAD DE SANTIAGO DE CHILE

DIPLOMADO EN

CIBER SEGURIDAD PARA REDES DE DATOS

INTRODUCCIÓN

El vertiginoso avance de las comunicaciones de los últimos 20 años ha sido uno de los pilares fundamentales para el actual desarrollo de nuestra sociedad. De acuerdo a cifras entregadas por el Gobierno de Chile, en su documento Política Nacional de Ciberseguridad (2016), se indica que, los accesos a internet han crecido en un 45,3%, en el último bienio, pasando de 52,2 accesos por cada 100 habitantes a inicios de 2014, a 73,8 accesos por cada 100 habitantes en marzo de 2016. La economía digital nacional, en tanto, creció en torno al 11% en el último bienio, pasando de 34.127 millones de dólares en 2014 a 39.485 millones de dólares en 2015. Este impacto ha generado trasformaciones relevantes también en los usos y miradas de nuestros ciudadanos. Todo este gran avance en las comunicaciones, ha sido fuertemente incorporado al desarrollo tecnológico, económico y financiero del país. Hoy tanto las PYMES como las grandes empresas y corporaciones tienen ligada su consolidación en el mercado a las comunicaciones.

La voz, vídeo y datos que se transmiten entre las empresas, se producen a través de cualquier medio tecnológico, tradicional o moderno. Todos estos avances han generado uno de los más grandes problemas de las empresas y corporaciones, la seguridad de la información que se maneja (pública y privada). En Internet, con todo el volumen de información y el comercio que viaja libremente, se ha transformado en el lugar predilecto para poder tener acceso a ella, la apropiación indebida para su mal uso es algo creciente y aún no bien controlado.

Las legislaciones de los países han debido ser modificadas para poder sancionar este tipo de delitos. La seguridad en Internet ha debido irse incrementando continuamente, siendo uno de los temas de mayor desarrollo últimamente, tanto por aquellos que desean realizar algún tipo de ataque con diversos fines, que van desde detener sus servicios hasta la obtención de alguna información confidencial. Como también por aquellos que deben proteger los servidores y sus servicios de cualquier tipo de ataque.

Bajo este contexto, las necesidades de seguridad son altamente importantes, se debe compatibilizar el complicado equilibrio entre recursos utilizados y la privacidad requerida. También debería ser lo suficientemente flexible para cumplir con los requisitos necesarios para permitir el seguimiento de los culpables a través de distintas jurisdicciones. El área de las auditorias de seguridad, detección de intrusos, Análisis Forense y Ethical Hacking vienen siendo más indispensable cada día.

OBJETIVO GENERAL

- Complementar la formación de los profesionales de área técnica de TIC ***(Tecnologías de la Información y Comunicación)*** con nuevos conocimientos, herramientas y técnicas que le permitan poder identificar, proteger sus sistemas y redes de intrusiones no autorizadas.

OBJETIVOS ESPECÍFICOS

Al término del programa, los participantes serán capaces de:

- Identificar las principales amenazas y vulnerabilidades comunes que se presentan a través de internet.

- Aplicar políticas de ciber seguridad en los distintos estamentos de las empresas, como en las redes de datos bajo su responsabilidad.

- Ofrecer un marco teórico y legal que permita resguardar la operación y daños producidos por un ataque de seguridad cibernético.

PLAN DE ESTUDIO

MÓDULO 1: INTRODUCCIÓN [12 HORAS TEÓRICAS]

1.1 Conceptos Básicos De Seguridad *(3 horas)*
1.2 Acceso y Control Perimetral *(3 horas)*
1.3 Continuidad Operativa *(3 horas)*
1.4 ISO 27000 *(3 horas)*

MÓDULO 2: CONCEPTOS BÁSICOS DE REDES DE DATOS [TOTAL 21 HORAS: 12 TEÓRICAS; 9 LABORATORIO]

2.1 Modelos de Referencia OSI *(3 horas)*
2.2 Stack de Protocolos TCP/IP *(6 horas)*
2.3 Redes de LAN/MAN/WAN *(3 horas)*
2.4 Lab. De Captura y Análisis de Trafico Ethernet *(9 horas)*

MÓDULO 3: CRIPTOGRAFÍA [TOTAL 15 HORAS TEÓRICAS]

3.1 Cifrado Simétrico y Asimétrico *(Total 6 horas teóricas)*
3.2 Estenografía *(3 horas)*
3.3 Firmas Digitales *(3 horas)*
3.4 Hashing *(3 horas)*

MÓDULO 4: SEGURIDAD EN REDES DE DATOS (TOTAL 30 HORAS: 18 TEÓRICAS; 12 LABORATORIO)

4.1 Control de Acceso a Equipamiento de Red *(3 horas)*
4.2 Herramientas de Seguridad (Firewall, IDS/IPS, Proxy) *(6 horas)*
4.3 Aplicaciones *(3 horas)*
4.4 Seguridad en Redes de Acceso *(6 horas)*
4.5 VPN *(3 horas)*
4.6 Laboratorio *(9 horas)*

MÓDULO 5: POLÍTICAS DE SEGURIDAD (TOTAL 12 HORAS: 6 TEÓRICAS; 6 LABORATORIO)

5.1 Definición de Política de Seguridad *(3 horas)*
5.2 Política de Seguridad de Usuarios *(1 hora)*
5.3 Política de Seguridad de Infraestructura *(1 hora)*
5.4 Política de Seguridad de Servidores *(1 hora)*
5.5 Caso Práctico: Aplicación de Política de Seguridad en una Empresa *(6 horas)*

MÓDULO 6: ETHICAL HACKING (TOTAL 24 HORAS: 9 TEÓRICAS; 15 LABORATORIO)

6.1 Conceptos y Definiciones *(3 horas)*
6.2 Análisis de Tráfico y detección de Ataques *(3 horas)*
6.3 Herramientas de PEN Tester *(6 horas)*
6.4 Laboratorios *(12 horas)*

MÓDULO 7: ANÁLISIS FORENSE (TOTAL 21 HORAS: 12 TEÓRICAS; 9 LABORATORIO)

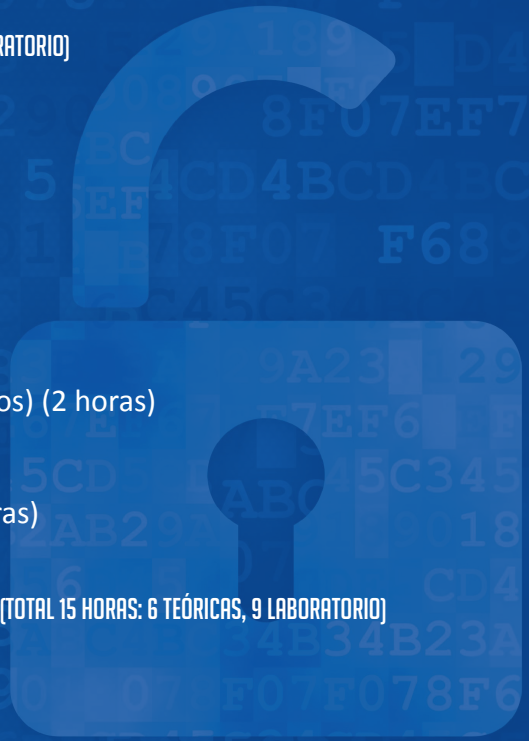
7.1 Conceptos y Definiciones (3 horas)
7.2 Manejo de Respuesta a Incidentes (3 horas)
7.3 Etapas del Análisis Forense (6 horas)
7.4 Laboratorios (9 horas)

MÓDULO 8: ASPECTOS LEGALES (TOTAL 9 HORAS TEÓRICAS)

8.1 Escenario Chileno (Normativa aplicable y seguros) (2 horas)
8.2 Firma y documento electrónico (2 horas)
8.3 Delitos informáticos (3 horas)
8.4 Medios electrónicos en el ámbito laboral (2 horas)

MÓDULO 9: EVALUACIÓN E IMPLEMENTACIÓN DE PROYECTOS (TOTAL 15 HORAS: 6 TEÓRICAS, 9 LABORATORIO)

9.1 Evaluación de Riesgo *(3 horas)*
9.2 Caso de Estudio 1: Costo de Impacto *(3 horas)*
9.3 Caso de Estudio 2: Costos de Implementación *(3 horas)*
9.4 Presentación de Grupo y evaluación *(6 horas)*



TOTAL HORAS TEÓRICAS: 99 HORAS
TOTAL HORAS LABORATORIO: 60 HORAS
TOTAL HORAS DIPLOMADO: 159 HORAS

UNIVERSIDAD
DE SANTIAGO
DE CHILE