Diploma en Ciberseguridad

A. Antecedentes Generales

Descripción

El desarrollo y amplia utilización de las Tecnologías de la Información y la Comunicación (TIC) han brindado beneficios a la sociedad en muchos aspectos que apuntan a la calidad de vida, pero igualmente trae consigo grandes retos asociados al uso apropiado que se debe dar a tales desarrollos tecnológicos, evitando que sean utilizados para cometer delitos, maltrato, violación de privacidad, amenazas a la tranquilidad, entre otros y con ellos ser utilizadas como herramientas sofisticadas para cometer actos inapropiados.

Es una tarea fundamental en este momento comenzar desde las universidades, organizaciones, empresas y sociedad a generar los planes y políticas que ayuden a que se pueda minimizar la vulnerabilidad a la cual se está expuesto ante posibles ciberataques.

El Diploma en Ciberseguridad, que ofrece la Universidad Técnica Federico Santa María (UTFSM) a través de su Departamento de Informática, es un programa de continuidad de estudios para profesionales, enfocado en brindar conocimientos sobre ciberseguridad, sus fundamentos, aspectos organizacionales y técnicos, herramientas y aplicaciones, habilitando a los participantes para la identificación de riesgos y vulnerabilidades asociados a sistemas de información. Adicionalmente, podrá determinar los requerimientos organizacionales asociados a la gestión y la implementación de soluciones de ciberseguridad.

Objetivo del Programa

Formar profesionales en el campo de las Tecnologías de Información y Comunicaciones (TIC) asociados al área de ciberseguridad, capacitándolos específicamente para:

- Comprender globalmente el área de la Ciberseguridad, considerando los aspectos legales, los riesgos existentes en el ciberespacio, desarrollando capacidades de análisis, evaluación y defensa en seguridad de la información.
- Analizar riesgos y vulnerabilidad asociados a organizaciones y personas para el desarrollo de políticas de ciberseguridad.
- Conocer y comprender las soluciones técnicas y herramientas tecnológicas para la implementación de las políticas de ciberseguridad.
- Estudiar casos reales del área de ciberseguridad.

Audiencia

Podrán postular al programa profesional de cualquier área con conocimientos en Tecnologías de Información y Comunicaciones (TIC), que buscan formarse, adquiriendo conocimientos sobre la ciberseguridad, sus aspectos legales, organizacionales, técnicas, herramientas y aplicaciones incluyendo gerentes o directivos de empresas, organismos públicos o privados que deseen adquirir conocimientos para integrar soluciones de ciberseguridad en sus entornos profesionales.

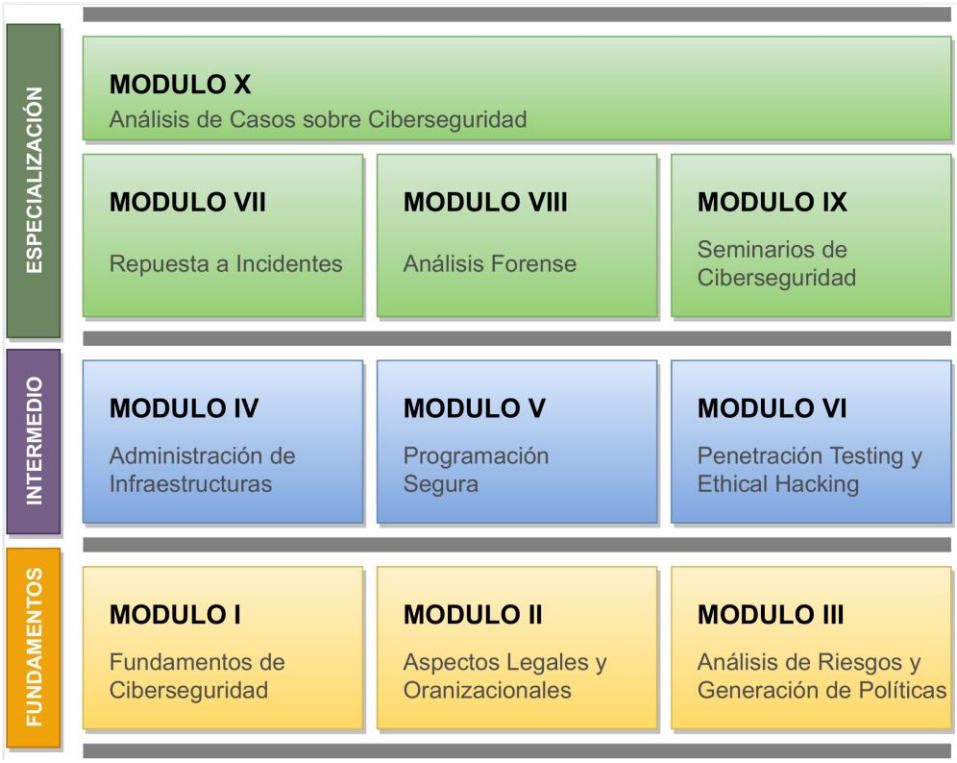
Modalidad de Clases

Las clases se impartirán de la siguiente forma:

- Cada módulo es de 12 horas en total (sin incluir las evaluaciones),
- Un módulo se divide en 6 horas de cápsulas de video y 6 horas de clases por Zoom.
- Las clases por Zoom serán los viernes 18:00 - 21:00, y los sábados 10:00 - 13:00.
- Los videos estarán disponibles en el sistema de enseñanza online en la semana antes por Zoom.
- Las clases por Zoom tienen como objetivo:
    - Profundizar la materia vista en los videos.
    - Ver casos prácticos.
    - Resolver las dudas y responder a las preguntas de los alumnos.
- Se usará la plataforma de enseñanza online Moodle (iCampus) para poner a disposición los videos de cursos, las diapositivas y otros documentos relacionados a cada módulo.
- Se usará la plataforma Moodle para las evaluaciones de cada módulo.

B. Plan de Estudios

El Diploma posee diez módulos de 12 horas cada uno con Tres ciclos (Fundamentos, Intermedio y Especialización), con un total de 120 horas de duración.



El ciclo de Fundamentos tendrá una duración de 36 horas y está compuesto por los tres primeros módulos: Fundamentos de Ciberseguridad, Aspectos organizacionales y legales de la Ciberseguridad y Análisis de Riesgos y Generación de Políticas de Ciberseguridad. El Ciclo Intermedio será de 36 horas y está compuesto por los tres módulos siguientes: Administración y configuración de Infraestructura, Programación Segura y Penetration Testing y Ethical Hacking. Por último, el Ciclo de Especialización durará 48 horas y considera los cuatro módulos restantes: Respuesta a Incidentes, Análisis Forense, Seminarios sobre Ciberseguridad y Análisis de casos sobre Ciberseguridad.

Ciclo I - Fundamentos de Ciberseguridad - 36 Horas

Módulo I : Fundamentos de Ciberseguridad

El objetivo de este módulo es presentar los fundamentos de la ciberseguridad en una empresa, una organización o institución, y con respecto a las personas. Incluye los siguientes temas:

- Definición de la ciberseguridad y del ciberespacio.
- La ciberseguridad en el ámbito de una empresa u organización.

- Gestión de recursos humanos y de los comportamientos.
- Bases de seguridad de datos
    - Nociones básicas de criptografía aplicada
    - Algoritmos de cifrado simétricos y asimétricos
    - Funciones de Hash seguras
    - Distribución de claves

Módulo II : Aspectos Legales y Organizaciones de la Ciberseguridad

Entregar una visión panorámica de la importancia de las nuevas tecnologías de la información y familiarizarlos con los temas jurídicos más recurrentes en las plataformas electrónicas:

- Uso de las tecnologías en el trabajo
- Delitos informáticos
- Protección de datos, contratos y propiedad intelectual

Todo ello bajo una visión general y acotada. Además, de un breve análisis de las principales modificaciones legales introducidas en los últimos años y que se encuentran vigente, así como una presentación los diversos proyectos de ley que se encuentran en estudio.

Módulo III : Análisis de Riesgos y Generación de Políticas de Ciberseguridad

Este módulo presenta los aspectos de análisis de riesgos y generación de políticas de ciberseguridad en función de estos riesgos.
El análisis de riesgo es uno de los procesos más importantes en el ámbito de la Ciberseguridad (incluso en la vida) y es fundamental entenderlo para poder **hacer una adecuada gestión del riesgo tecnológico**, pero también para entender bien cómo **enfrentar las nuevas amenazas** cibernéticas. Este proceso es cada vez más reconocido dentro de la industria, existen muchas metodologías, ISO (ISO 27005) y cada vez se exige en más procesos de certificaciones internacionales, como el caso de PCI DSS que lo incluye como exigencia en el proceso de Ethical Hacking.
Muy alineados con el Análisis de Riesgos, están “Las políticas de seguridad” que son la base a la hora de implementar un gobierno de Ciberseguridad, ya que nos permiten definir una postura respecto a la seguridad, serán nuestra línea base de seguridad, también son necesarias para delimitar las acciones “aceptables” que no pondrán en riesgo nuestra línea base.

Ciclo II - Intermedio- 36 horas

Módulo IV : Administración y configuración de Infraestructura

Este módulo presenta la administración segura de los dispositivos y sistemas que conforman el ciberespacio y las redes computacionales de una empresa. Se hará uso de ejemplos prácticos en sistemas operativos basados en Linux.

- **Seguridad de los Sistemas Operativos**
    - Instalación y configuración segura de sistemas operativos
    - Sistemas de archivos seguros

  - Instalación de herramientas de seguridadSeguridad en Máquinas Virtuales y Contenedores
  - Sistemas de Respaldo de datos.
  - Antivirus, Anti-Malware, etc.
- Seguridad de los Equipos de Redes
  - Instalación y configuración de Firewalls
  - IDS (Intrusion Detection System)
  - IPS (Intrusion Prevention System)
  - Cifrado de la red y Monitoreo
- Seguridad Física
  - Control de acceso
  - Control de incendios
  - Respaldo de energía

Módulo V : Programación Segura

Este módulo presenta los riesgos del software inseguro para las organizaciones para las cuales los desarrolladores programan, y las técnicas y herramientas que pueden ser utilizadas con el objetivo de eliminar o mitigar las fallas de seguridad.

- Amenazas actuales al software
  - ¿Quiénes son los atacantes?
  - Vulnerabilidades de software correspondientes a cada etapa del SDLC: Inyecciones, XSS, configuraciones inseguras, autentificación débil, etc.
- Programación segura: Necesaria pero difícil
  - ¿Cuáles son las consecuencias de un ataque exitoso a software?
  - ¿Por qué es difícil programar en forma segura?
- Cómo asegurar software
  - Buenas prácticas de programación segura
  - Herramientas de desarrollo seguro
  - Taller/demostración de programación segura

Módulo VI : Penetration Testing \& Ethical Hacking

Se realizará una breve introducción y descripción de los conceptos clave y fases del Hacking Ético, luego se mostrarán y usarán herramientas abiertas en sistemas operativos Windows y Linux, recomendable para las prácticas Kali Linux en su última versión. El módulo será, principalmente, práctico, usando las herramientas en un entorno controlado, ya sea local y en cloud.

- Introducción: Conceptos básicos del Hacking Ético
- Técnicas y herramientas de reconocimiento
- Uso de herramientas de escaneo y enumeración de servicios
- Análisis de vulnerabilidades
- Explotación de vulnerabilidades

La evaluación será práctica, tipo Capture The Flag (CTF). Donde deberán resolver retos, encontrar y validar las evidencias.

Ciclo III - Especialización - 36 horas

Módulo VII : Respuesta a Incidentes

El módulo de respuestas de incidentes permitirá al alumno **entender, diseñar y discutir** los procesos asociados a la respuesta de un incidente de ciberseguridad en una empresa u organización. Desde la creación del **Playbook de incidentes** hasta los **procesos forenses** asociados a encontrar y erradicar el incidente de seguridad. Adicionalmente, se compartirá con los alumnos experiencias reales durante respuestas de incidentes ocurridas en los últimos años en Chile.

- Explicación y uso de herramientas de respuesta de incidentes
- Procesos de KillChain
- Mitre ATT\&CK
- Procesos NIST (800-86, 800-83, 800-61)

Módulo VIII : Análisis Forense

Este módulo presenta el **análisis forense desde una perspectiva integral**, abordándolo desde una visión global que involucra **aspectos científicos, informáticos, criminalísticos y legales**. Se cubrirán tanto conocimientos teóricos como su aplicación en laboratorios prácticos, donde los alumnos podrán aplicar lo aprendido y comprender cabalmente los conceptos.

- Concepto de Evidencia Digital y aspectos legales relacionados.
- Gestión de Evidencia Digital
- Cadena de Custodia y preservación de evidencia digital
- Etapas de Informática Forense: Identificación, Recopilación, Adquisición, Examen, Análisis y Presentación.
- Laboratorio de Adquisición de Evidencia Digital.
- Laboratorio de Examen y Análisis de Evidencia Digital.

Módulo IX: Seminarios sobre Ciberseguridad

El objetivo de este módulo es presenta casos reales de ciberseguridad, incluyendo ataques exitosos y como enfrentarlos. Se invitarán expertos de varias empresas e instituciones para compartir su experiencia en términos de respuestas a ataques.

- Presentación de casos
- Procedimientos en casos de ataques y respuestas
- Fuentes y origen de los ataques.Trabajo Personal - 12 Horas

Módulo X: Análisis de casos sobre Ciberseguridad

Este módulo corresponde a un trabajo personal de los participantes con el objetivo de analizar el estado de la ciberseguridad en un caso real y proponer los cambios necesarios para mejorar el nivel de ciberseguridad existente.

- Incluye discusiones y trabajo personal de análisis para la producción de un informe final.

C. Organización Académica

El programa combina horas presenciales teóricas y prácticas, realización de trabajos grupales y desarrollo de un proyecto final en el área de ciberseguridad.

El equipo de profesores está compuesto por un seleccionado grupo de académicos y profesionales, con sólidos conocimientos y una amplia experiencia en el campo de la ciberseguridad, lo que permitirá brindar a los participantes diferentes visiones y aportes en dicha área.

Dirección Académica del Programa:

Xavier Bonnaire (xavier.bonnaire@inf.utfsm.cl)

- Doctor en Informática, Universidad Pierre et Marie Curie, Paris, Francia
- Habilitado a Dirigir Investigaciones, Universidad Pierre et Marie Curie, Paris, Francia
- Responsable línea de Ciberseguridad del Departamento de Informática

Dirección Ejecutiva del Programa:

Ximena Riff

- Ingeniero Civil Industrial, Universidad Técnica Federico Santa María
- Experta en gestión de proyectos

D. Relatores asociados al Programa:

XAVIER BONNAIRE

- Doctor Hdr. en Informática
- Académico del Departamento de Informática
- Universidad Técnica Federico Santa María
- Responsable de la línea de Ciberseguridad

MARCELO CORTEZ

- Magíster en Control de Gestión, Univ. de Chile
- Chief Information Security Officer
- ZURICH SANTANDER Seguros Generales Chile

ANDRÉS PUMARINO

- Abogado, partner of Legaltrust.cl
- Consulting in Compliance and Information Technology
- Socio Fundador - LegalTrust

FELIPE SÁNCHEZ

- Gerente Técnico - Forensic and Cybercrime Investigation
- Perito Judicial en Ingeniería Informática con mención en Fraudes y Delitos Informáticos - Poder Judicial de Chile
- Perito Informático - Laboratorio de Criminalistica Central - Policia de Investigación de Chile (PDI) (2006 - 2012)

YONATHAN DOSSOW

- Ingeniero Civil en Informática, Universidad Técnica Federico Santa María
- Site Reliability Engineer, Betterfly Chile
- Administration of Databases, e-learning platforms, DNS, Virtualization, email, firewall, web servers, networks, directory servers, authentication services, storages, datacenter (USM 13 años).

CRISTIAN ROJAS

- Magíster en Ciencias (Computer Science), Universidad de Chile
- Profesor de Seguridad de la Información - Universidad Adolfo Ibañez
- Profesor de Seguridad de Software - Universidad de Chile

MIGUEL DÍAZ

- Senior Manager - Cybersecurity Services at CyberTrust SpA
- Certifies Incident Handler - E|CIHv2 (EC-Council)
- Certified Ethical Hacker - C|EHv8 (EC-Council)
- Ingeniero Civil en Informática - Universidad Técnica Federico Santa María
- Magister en Data Science - Universidad Adolfo Ibañez

NICOLÁS CONTADOR

- Jefe de Ciberseguridad, Hunter System Security, Chile
- Director General en OpenHack Chile
- Ingeniero en Sistemas Computacionales - Universidad Técnica Federico Santa María
- Certified CISCO - CCNP, CCS-EAII, CCS-ECore, CCNA
- CCNA-Wireless, CCNA Voip, Técnico de Monterrey

NOTA: La dirección del Programa se reserva el derecho de cambiar algún académico en caso de fuerza mayor.

D. Costo del Programa y Descuentos

Valor total del Diploma: $2.450.000 (70 UF, costo aproximado en pesos)

Existe una política de descuentos acumulativos y que consideran las siguientes alternativas (puede consultar por su situación):

- pago anticipado (en fechas especificadas).
- Alumni (ser exalumno de la Universidad, cualquier título, grado o diploma).
- ser mujer (como una forma de apoyar a disminuir la brecha de genero).
- ser funcionario público, municipal, FFAA, Carabineros o PDI, o bien vivir en zonas extremas o pertenecer a un pueblo originario.
- pertenecer a una misma empresa o institución (que inscribe 3 o más estudiantes de una misma empresa o institución, y con UNA orden de compra).

E. Contacto y consultas:

Email: vinculacion@inf.utfsm.cl
Web: https://www.inf.utfsm.cl/formacion-continua
WhatsApp: +569 44054309
+569 44053325
Personales:

- Ivonne Barra

Fono: 232028200
Departamento de Informática
Campus Vitacura
Universidad Técnica Federico Santa María
Avenida Santa María 6400, oficina B 211
Santiago

- Carolina Leal

Fono: 322654424
Departamento de Informática
Campus Casa Central
Universidad Técnica Federico Santa María
Avenida España 1680, oficina F 118
Valparaíso

F. Fecha de Inicio: 10 de abril de 2023 (fecha termino 26 agosto)

NOTA: El programa se realizará siempre y cuando se complete con el mínimo de participantes. Derecho a reserva sólo se reembolsa en caso de no realizarse el programa.