UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA
Departamento de Informática

DIPLOMA EN CIBERSEGURIDAD

I. Descripción

Los desarrollos 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.

II. 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.
- Conocer y comprender las soluciones técnicas y herramientas tecnológicas para respuestas a incidentes y su análisis forense.
- Estudiar casos reales del área de ciberseguridad.

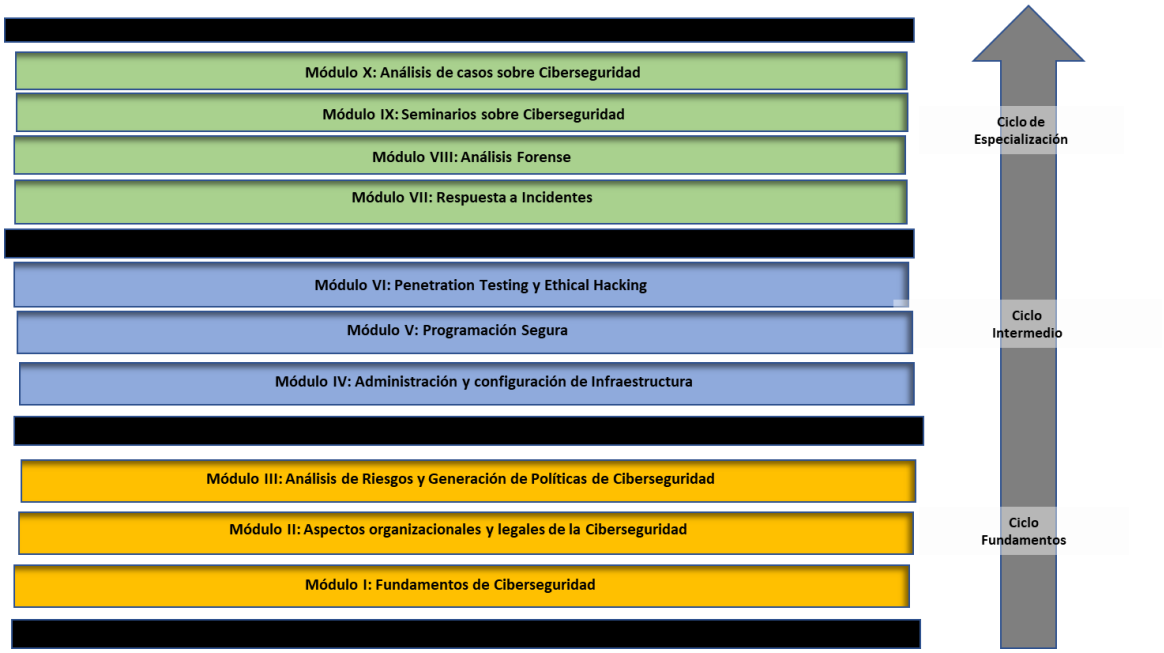
III. Dirigido a

Podrán postular al programa profesionales 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.

IV. 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).



1. Ciclo de Fundamentos

I. Fundamentos de Ciberseguridad (12 horas)

- **a. Criptografía**
  - i. Introducción a la criptografía
  - ii. Algoritmos de cifrado Simétricos
  - iii. Algoritmos de cifrado Asimétricos
  - iv. Firmas digitales
  - v. Certificados X509 (Web)
  - vi. Funciones de Hash (MD5, SHA*…)
  - vii. PKI
  - viii. Distribución de claves
    1. Diffie Hellman, etc.
- **b. Tokenization**
  - i. Definición y objetivos
  - ii. Aplicaciones
- **c. Gestión de los recursos humanos y comportamientos**
  - i. Gestión de contraseñas y credenciales
  - ii. Buenas prácticas de manejo de la información

II. Aspectos organizacionales y legales de la Ciberseguridad (12 horas)

- **a. Normas ISO-27xxx**
- **b. Framework NIST**
- **c. Organización en la empresa**
  - SOC
  - SIEM
- **d. Aspectos legales**

III. Análisis de Riesgos y Generación de Políticas de Ciberseguridad (12 horas)

- **a. Ingeniería Social**
  - i. Introducción y objetivos
  - ii. Técnicas y herramientas para recolectar informaciones de tipo OSINT (Open Source INTelligence) usando Internet:
    1. Redes sociales, páginas web, informes disponibles, emails, etc
    2. Softwares tipo Maltego, KALI Linux, y otros
  - iii. Análisis de datos OSINT y producción de grafos de relaciones.

1. Generación de metadatos e inferencias a partir de los datos OSINT.
2. Grafos de relaciones (Maltego, ...)

iv. Planificación de ataques

b. Políticas de seguridad

i. Usuarios y Comportamientos de riesgo
ii. Identificación de riesgos y vulnerabilidades

2. Ciclo Intermedio

I. Administración y configuración de Infraestructura (12 horas)

a. Seguridad de los Sistemas Operativos

i. Instalación y configuración segura de sistemas operativos
ii. Sistemas de archivos seguros
iii. Instalación de herramientas de seguridad
iv. Antivirus, Anti-Malware, etc…

b. Seguridad de los Equipos de Redes

i. Instalación y configuración de Firewalls
ii. IDS (Intrusion Detection Systems)
iii. IPS (Intrusion Prevention Systems)
iv. Monitoreo

II. Programación Segura (12 horas)

a. Programación Segura

i. Introducción
ii. Errores de programación en C/C++, Java, etc…
iii. Reglas de buenas prácticas en programación
iv. Herramientas de verificación de código

b. Desarrollo de Aplicaciones Web Seguras

i. HTTPS
ii. Verificación y validación de argumentos (Inyecciones SQL, Buffer Overflow, ...)
iii. WordPress, etc…

III. Penetration Testing y Ethical Hacking (12 horas)

a. Penetration Testing

i. Introducción al Ethical Hacking y Penetration Testing

ii. Vulnerabilidades y fallas
    1. Buffer overflow, injección SQL, Password Cracking, etc…
iii. Herramientas de Penetration Testing
    1. Scanners, Enumeración, Footprint, Sniffing, …
    2. Análisis de resultados
    3. Adecuación de políticas de seguridad
iv. Ataques de redes Wifi
    1. WEP, WPA, WPA2, WPS
v. DOS, DDOS, …
vi. Evasión de IDS, Firewall & Honey Pots

3. Ciclo de especialización

I. Respuesta a Incidentes (12 horas)

a. Procedimientos post-ataque

i. Detección
ii. Recolección de evidencias
iii. Analisis del ataque
iv. Reacción

b. Procedimientos en caso de ataques

II. Análisis Forense (12 horas)

a. Recolección de evidencias

i. Análisis del tráfico de red
ii. Análisis de datos (logs, etc…)
iii. Análisis de sistema de archivos (discos)
iv. Análisis de memoria (RAM)

b. Ingeniería inversa

i. Extracción de información (archivos ELF, etc…)
ii. Disassembling & Decompiling
iii. Tracing & Debugging
iv. Unpacking

III. Seminarios sobre Ciberseguridad (12 horas)

a. Seminario sobre experiencias reales de Ciberseguridad

IV. Análisis de casos sobre Ciberseguridad (12 horas)

a. **Análisis con los participantes del Diploma sobre casos propios que ameriten el uso de la ciberseguridad**

V. Metodología

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.

VI. Organización

Dirección Académica del Programa

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

Dirección Ejecutiva del Programa

- Dr. Francklin Rivas (firivas@inf.utfsm.cl)

Relatores asociados al programa

- Xavier Bonnaire (DI-UTFSM)
- Horst Von Brand (DI-UTFSM)
- Erika Rosas (DI-UTFSM)
- Javier Cañas (DI-UTFSM)
- Miguel Varas (DI-UTFSM)
- Yonathan Dossow (DI-UTFSM)
- Gabriel Torres (UTFSM)
- Hugo Miranda (PDI)
- Renzo Benni (PDI)
- Claudio Delgado (Agile Ing.)
- Jorge Olivares (Business Continuity)
- Pablo Itaim (Jefe Ciberoperaciones Armada)
- Miguel Díaz (Sonda)
- Gabriel Bergel (Eleven Path)
- Nicolás Contador (Duoc, Inacap)
- Andrés Pumarino (Legal Trust)

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

VII. Información general

Horario: viernes 15:30-21:30 horas; sábado 08:30-14:30 horas.

Lugar: Campus Casa Central Valparaíso, Universidad Técnica Federico Santa María. Avenida España 1680, Valparaíso.

Inicio: abril 2020
Término: julio 2020

Costo del programa
Derecho a reserva: 2 UF
Valor Diploma: 100 UF (98 UF considerando la reserva)

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.

VIII. Contacto y consultas

Ivonne Barra
Departamento de Informática
Universidad Técnica Federico Santa María
Fono: 2232028200
Email: sec-postitulos@inf.utfsm.cl

Carolina Leal
Departamento de Informática
Universidad Técnica Federico Santa María
Fono: 322654424
Email: vinculacion@inf.utfsm.cl