Plan de Estudios

Diploma de Especialización en Seguridad Informática

Antecedentes y Fundamentación

El surgimiento de la sociedad de la información, y con ello el incremento en el uso de las Tecnologías de la Información y las Comunicaciones (TIC), hace que la información y los recursos informáticos que la gestionan tengan un rol principal en las actividades económicas, sociales y culturales. Asociado a este crecimiento es también cada vez mayor la cantidad de amenazas y ataques que se producen a las aplicaciones y recursos informáticos. Es en este contexto que la información se convierte en un recurso crítico al que hay que proteger. La seguridad informática se vuelve imprescindible como forma de garantizar la integridad, disponibilidad y confidencialidad de la información.

Las organizaciones deben estar preparadas para proteger sus activos de información. Esto implica conocer y aplicar de forma adecuada los conceptos, metodologías, herramientas, normativas y estándares existentes en esta materia, para lograr el objetivo de seguridad. Para ello se requiere de recursos humanos profesionales debidamente capacitados y actualizados, que puedan aplicar de forma exitosa las metodologías y adaptarse rápidamente a los cambios tecnológicos y las exigencias de un área que esta en constante evolución y cambio.
Un profesional especializado en seguridad informática, debe ser capaz de aplicar las metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas, como ser criptografía, modelos formales, análisis forense, etc. , así como en las áreas en las que la seguridad informática tiene su aplicación: redes, sistemas operativos, aplicaciones. Deben también ser capaces de gestionar la seguridad de la información, aplicando las normativas y estándares existentes, gestionando los incidentes, los riesgos y garantizar la continuidad del negocio, protegiendo los activos críticos.

En la actualidad, e impulsada por el surgimiento de estándares, leyes y normativas, la seguridad se convierte en un requisito fundamental para cualquier tipo de organización. No sólo es un requerimiento de los bancos u organizaciones financieras, sino que se extiende a todo tipo y tamaño de organización. Los riesgos de ataques informáticos alcanzan a todas las organizaciones por igual, impactando directamente en su negocio. Los profesionales informáticos deben estar preparados para poder gestionar, enfrentar y mitigar estos riesgos.

Este escenario lleva a la necesidad de ofrecer formación académica, de forma de preparar recursos humanos de alto nivel para enfrentar los nuevos retos asociados a la Seguridad Informática. Brindar una especialización en el área que permita a los profesionales incorporar un sólido marco teórico y a través del uso de laboratorios y trabajos prácticos, adquirir la práctica necesaria para enfrentar los nuevos retos que presentan las vulnerabilidades y amenazas.

1. Objetivos

El objetivo de este plan de estudios es la formación de Especialistas en Seguridad Informática capacitándolos en las temáticas relacionadas en esta área. Este Diploma de Especialización se dirige a profesionales en informática, que deseen especializarse en el área Seguridad Informática y apunta a formar profesionales éticos capaces de implementar las mejores prácticas y tendencias, conocer y cumplir las normativas y regulaciones nacionales e internacionales, generar y transmitir conocimiento en el área de forma de alcanzar mayores y mejores niveles de seguridad de la información.

2. Perfil del egresado

El egresado adquirirá la capacidad de aplicar con profundidad y solvencia en su actividad profesional los temas incluidos en el Diploma; asimismo, adquirirá los elementos metodológicos que junto con la capacidad de abordar bibliografía especializada le permitan comprender y emplear las nuevas tecnologías para la resolución de problemas relativos a la Seguridad Informática en su actividad profesional.
Se espera que el egresado de este diploma tenga la capacidad para:

- Dominar las áreas fundamentales de la Seguridad Informática
- Ser capaz de tomar decisiones éticas y practicar un comportamiento ético profesional
- Implementar un plan estratégico para gestionar la seguridad de la información en cualquier organización
- Gestionar los riesgos y el impacto que los mismos puedan tener en el negocio de la organización
- Conocer y aplicar las mejores prácticas, tendencias y herramientas para mitigar los riesgos asociados a las diferentes tecnologías de la información
- Implementar metodologías adecuadas para garantizar la continuidad del negocio de la organización
- Aprender nuevos modelos, técnicas y tecnologías cuando estas emergen, y apreciar la necesidad de ese desarrollo profesional continuo.
- Diagnosticar la situación de una organización y brindar asesoramiento en materia de seguridad informática
- Gestionar los incidentes de forma efectiva y profesional

3. Ordenamiento

La Sub Comisión Académica de Posgrado de Informática (SCAPA-Informática) supervisará las actividades ligadas al desarrollo del Diploma de Especialización en Seguridad Informática; sin perjuicio de las competencias que correspondan a la Comisión Académica de Posgrado (CAP) y al Consejo de la Facultad de Ingeniería.
La SCAPA-Informática nombrará para cada estudiante un Director de Estudios, responsable de la organización de las actividades y de la orientación del mismo.

Los aspectos reglamentarios no mencionados explícitamente se ajustan a lo establecido por los documentos: Ordenanza de las Carreras de Posgrado de la Universidad de la República, aprobado en fecha 25/09/01 por el Consejo Directivo Central y el Reglamento General de las Actividades de Posgrado y Educación Permanente de la Facultad de Ingeniería (RGP-FING), 2003.

4. Requisitos de ingreso

Podrán ingresar al Diploma de Especialización en Seguridad Informática quienes cumplan con alguna de las siguientes condiciones:

Condición 1: Contar con un título de grado, en informática, otorgado por la Universidad de la República de al menos 360 créditos. Ejemplo: título de Ingeniero en Computación,

Condición 2: Contar con formación equivalente que, a juicio de la Comisión de Postgrado, permita la realización y aprovechamiento del Plan de Estudios del Diploma de Especialización en Seguridad Informática. En este caso, la SCAPA-Informática podrá proponer la realización de cursos de nivelación en caso de ser necesario.

5. Admisión y selección de los candidatos

Las candidaturas deberán ser presentadas a la SCAPA-Informática, quien deberá elevar un informe a la CAP sugiriendo la aprobación o no de la candidatura. La admisión tendrá en cuenta los antecedentes del candidato, pudiéndose realizar una entrevista a los aspirantes para complementar la información presentada. La CAP resolverá la admisión de los candidatos en base a los antecedentes del candidato y al informe de la SCAPA-Informática.

6. Formación

Para cada estudiante, la SCAPA-Informática formulará una propuesta de plan de formación, que será aprobada por la CAP. Los planes de formación se integrarán con actividades programadas (cursos de actualización y/o posgrado, seminarios, etc.), de manera de cumplir un mínimo de 60 créditos (el crédito es la unidad de medida de la carga de trabajo en los planes de estudio de la Facultad de Ingeniería, y un crédito equivale a quince horas de dedicación por parte del estudiante), de los cuales 50 créditos corresponderán a las materias centrales de la especialización. Todas las actividades programadas deberán contar con alguna forma de evaluación de los conocimientos adquiridos.

Este número mínimo de créditos totales y específicos en las materias correspondientes a la especialización, es imprescindible para poder transmitir el conocimiento necesario, tanto en amplitud como en profundidad, de forma de desarrollar las habilidades deseadas en el estudiante.
La duración prevista para la realización de la Especialización en Seguridad Informática es de entre 12 a 18 meses, con una dedicación estimada de entre 15 y 20 horas semanales.

7. Estructura del plan de estudios

El plan de estudios de Especialización en Seguridad Informática está estructurado en Materias. Se requiere un mínimo de 50 créditos en las materias centrales, y un total de 60 créditos para la obtención del Diploma. A continuación se presentan las materias centrales del Diploma:

- **Seguridad de sistemas informáticos y redes**: fundamentos y metodologías para el análisis de amenazas y la selección e implementación de mecanismos de protección asociados a la seguridad informática en los sistemas operativos, redes de datos TCP/IP y aplicaciones.

- **Criptografía aplicada**: conceptos asociados a la criptografía aplicada a la seguridad informática, criptografía de clave publica y privada, primitivas criptográficas, infraestructura de clave pública

- **Gestión de la Seguridad de la Información y Marco Normativo**: conceptos y metodologías asociadas a la gestión de seguridad de la

información, marco normativo internacional y nacional. Metodologías para la implementación de un Sistema de Gestión de Seguridad de la Información y las principales actividades y procesos asociados: gestión de riesgos, gestión de incidentes y gestión de la continuidad del negocio. Marco ético y legal.

- **Ética y conducta profesional:** Esta materia esboza las cuestiones y elementos de una conducta profesional.

La descripción de las Materias arriba descritas se encuentra en el Apéndice A.

8. Título

Cuando el aspirante haya completado los requisitos del programa, la SubComisión Académica de Posgrado de Informática notificará a la CAP, quien propondrá al Consejo de la Facultad el otorgamiento del Título "Especialista en Seguridad Informática". Este diploma será firmado por el Decano de la Facultad de Ingeniería y el Rector de la Universidad de la República.

Apéndice A. Descripción de Materias

SEGURIDAD DE SISTEMAS INFORMÁTICOS Y REDES
Objetivos de la materia: Introducir los conceptos básicos de seguridad informática. Diseñar y/o implantar mecanismos de seguridad, con el objetivo de desarrollar, ampliar o mejorar las plataformas de computación. Adquirir los conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir un sistema informático y establecer los mecanismos de protección adecuados que garanticen la seguridad del mismo. Incluye pero no está limitado a la seguridad informática en los sistemas operativos y redes de datos TCP/IP. Introducir conceptos asociados a la seguridad en el proceso de desarrollo de aplicaciones. Comprender qué hitos tener en cuenta a la hora de construir aplicaciones seguras en el proceso de desarrollo, y entender los errores más comunes que se presentan en la codificación de las aplicaciones.

CRIPTOGRAFÍA APLICADA
Objetivos de la materia: Introducción a los fundamentos principales de criptografía y su aplicación en los mecanismos de protección contra amenazas de seguridad, integrando aspectos teóricos con laboratorios experimentales. Introducción a las infraestructuras de clave pública, su implementación en el Uruguay y su aplicación para el aseguramiento de transacciones electrónicas.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, MARCO NORMATIVO y PRIVACIDAD DE LOS DATOS PERSONALES
Objetivos de la materia: Introducir a los estudiantes en los principales conceptos y metodologías asociadas a la gestión de seguridad de la información, y en el marco normativo internacional y nacional existente. Llevar a la práctica una metodología de rápida aplicación para la implementación de un Sistema de Gestión de Seguridad de la Información. Presentar metodologías concretas para la gestión de riesgos y gestión de incidentes. Se abarcarán los principales conceptos en torno a la familia de normas ISO/IEC 27000.

ÉTICA Y CONDUCTA PROFESIONAL
Objetivos de la materia: Introducir a los estudiantes en las principales cuestiones y elementos de la conducta profesional. Comprende entre otros las cuestiones sociales, legales, códigos de ética y conducta profesional.