Escuela de Ciencia y Tecnología
ECyT_UNSAM

Diplomatura en Seguridad de la Información

Febrero 2024

Contenido

1 Identificación de la formación

1.1 Denominación
Diplomatura en Seguridad de la Información

1.2 Ubicación
Escuela de Ciencia y Tecnología

1.3 Coordinación Académica
Pablo Russo

2 Fundamentación

Nos encontramos en una época de transformación digital a nivel global. Los servicios y dispositivos de sistemas de información y comunicaciones, el uso masivo de la Inteligencia Artificial, el Big Data y el Machine Learning, entre otras técnicas y disciplinas, han cambiado (y lo seguirán haciendo) las formas en que se desarrollan diversidad de actividades ya sean laborales o personales / sociales.

Esta realidad evidente se ha puesto en primer plano en el marco de la Pandemia de COVID-19, requiriendo el uso intensivo de las tecnologías de la información para brindar las herramientas que permitieran la continuidad laboral, educativa y de relaciones sociales y familiares.

Debido a esto, además, se ha incrementado la necesidad de las Organizaciones de abordar o profundizar procesos de transformación e innovación, incorporando soluciones de base tecnológica e incrementando sensiblemente la ya de por sí enorme generación de datos e información de todo tipo.

Todos estos procesos suelen estar direccionados y condicionados por objetivos de gestión y restricciones presupuestarias y de tiempos, impulsando un escenario en el cual las acciones relacionadas con la seguridad de la información no son consideradas o quedan relegadas a un segundo plano.

Las nuevas soluciones tecnológicas, pensadas para ambientes con mayor complejidad y que incluyen aplicaciones y bases de datos distribuidas, redes e infraestructura de Tecnología Informática (TI), se desarrollan e implementan sin un abordaje que considere las amenazas y riesgos en relación a la seguridad de la información, de activos y de personas.

3 Objetivos de la Diplomatura

3.1 Objetivos generales
- Proveer al personal de áreas de informática de los conocimientos fundamentales para una adecuada gestión de la seguridad de la información;
- Aportar a la profesionalización del personal que desarrolla, implementa y opera los sistemas y servicios de informática.

3.2 Objetivos específicos

- Proveer los fundamentos y marco general de la gestión, el gobierno y el rol de la seguridad de la información en las Organizaciones;
- Proveer los conocimientos fundamentales para el diseño e implementación de una Infraestructura Tecnológica que minimice los riesgos de seguridad;
- Brindar el conocimiento sobre las buenas prácticas en la seguridad de TI, como también información sobre el marco normativo y de estándares relacionados;
- Proveer conocimiento básico sobre técnicas, métodos y herramientas de Ethical Hacking;
- Proporcionar el conocimiento para la identificación y entendimiento de la posible explotación de vulnerabilidades;
- Brindar conocimientos iniciales en técnicas y métodos de análisis forense, que permitan identificar tanto soluciones a situaciones específicas como mejoras generales;
- Promover la incorporación de criterios de seguridad de la información en el diseño de soluciones y la contratación de proveedores de base tecnológica;

4 Certificación que otorga la formación

Diploma en Seguridad de la Información.

5 Destinatarios

La Diplomatura en Seguridad de la Información está orientada a todas aquellas personas que trabajan o han trabajado en áreas de Informática en Organizaciones (Gerencias, Direcciones, etc), que poseen conocimientos focalizados en distintas temáticas relacionadas con los Sistemas de Información (Gestión de Infraestructura Tecnológica, Desarrollo de Software, Microinformática, etc.) y que requieren incorporar la visión y conocimientos técnicos específicos de la Seguridad de la Información.

También se orienta a aquellas personas que busquen desarrollarse en las temáticas específicas de la Seguridad de la Información.

6 Requisitos de ingreso

Para el ingreso a la Diplomatura, los aspirantes deberán:

- Poseer antecedentes laborales en áreas de Informática;
- Presentar la documentación requerida por la normativa vigente.

7 Diseño y organización curricular

El plan de estudios de la Diplomatura en Seguridad de la Información consta de un total de 8 (ocho) asignaturas y un trabajo final integrador; con una carga horaria semanal de 10 horas, que se distribuye entre 2 actividades sincrónicas de 3 horas cada una y 4 horas de actividades asincrónicas.

La carga horaria total de la Diplomatura es de 122 horas.

La duración de la Diplomatura es trimestral.

7.1 Estructura del plan de estudios

Asignatura	Carga horaria
Introducción a la Seguridad de la Información	1,5
Gobierno de la Seguridad de la Información	9
Seguridad de la infraestructura de TI	30
Criptografía	10
Ethical Hacking	21
Informática Forense	18
Aspectos Legales	12
Seguridad en el desarrollo de software	10
Trabajo Final Integrador	10,5
Carga horaria total	122

8 Modalidad de evaluación

Para la obtención del Diploma deberán realizarse los trabajos prácticos de las asignaturas y aprobarse el Trabajo Final Integrador.

9 Contenidos mínimos de las asignaturas

Introducción a la Seguridad de la Información:

- Estructura de la Diplomatura. Perfil profesional.
- Conceptos generales de Seguridad.
- Evolución de la seguridad de la información. Situación actual.
- La triada CID: Confidencialidad, Integridad, Disponibilidad
- Características adicionales al CID: Autenticidad y Confianza, No repudio, Privacidad, Auditabilidad, Responsabilidad.

Gobierno de la Seguridad de la Información

- Sistema de Gestión de la Seguridad de la Información (SGSI)
- Gestión de Riesgos en Seguridad
- Políticas de Seguridad
- Planificación e Implementación de un SGSI
- Marcos Normativos

Seguridad de la Infraestructura IT

- **Seguridad de equipos de usuarios**
    - Gestión de usuarios

- Cifrado de discos
- Gestión de contraseñas
- Dispositivos I/O
- Equipos móviles
- Herramientas básicas de seguridad

- **Seguridad en servidores**
  - Gestión de accesos
  - Contingencia (backups, snapshots)
  - Firewall / IPS / IDS
  - Alta disponibilidad y replicación de la infraestructura
  - Buenas prácticas
- **Seguridad en redes**
  - Segmentación de redes departamentales
  - Gestión de permisos y autenticación de red (PROXY, RADIUS)
  - Configuración segura de equipos de red.
  - Conexiones seguras (VPN, SSH, etc)
  - Protocolos seguros (SSL, TLS, etc)
  - Seguridad WIFI

Ethical Hacking

- Tipos de ataques
- Ingeniería Social
- Introducción a OSINT
- Reconocimiento
- Escaneo.
- Vulnerabilidades
- Metasploit.
- Test de intrusión
- Deep Web.
- Ataques a dispositivos móviles.
- Ataques WIFI.

Criptografía

- Introducción a la criptografía
- Algoritmos
  - Cifrado simétrico (AES)
  - Resumen de mensaje – HASH (SHA-1, SHA-2, SHA-3)
  - Código de mensaje autenticado – MAC (HMAC, CMAC, GCM)
  - Cifrado asimétrico (RSA, Diffie-Hellman)
  - Establecimiento de Claves (generación, transporte, acuerdo, derivación)
- Aplicaciones
  - Cifrado de almacenamiento
  - Firma Digital
  - Infraestructura de clave pública
  - Protocolos de comunicación

Informática Forense

- Introducción a la Informática Forense
- Adquisición Forense/Evidencia Digital
- Validación de la prueba digital, Hashes, Cadena de Custodia
- Medios de Almacenamiento, Sistemas Operativos, Sistemas de Archivos
- Live Forensics / Dead Box Forensics
- Auditoría e informes
- Datos Volátiles, adquisiciones en vivo
- File carving / Data carving
- DFIR / TRIAGE
- Detección de artefactos, cabeceras de archivos, firmas.-
- Análisis de Logs / Análisis de Correos electrónicos
- Last activity view (línea de tiempo del uso del ordenador)

Aspectos Legales

- Legislación vigente sobre correos electrónicos
- Ley 26388
- Convenio de Budapest y su aplicación en delitos transnacionales.
- Evolución legislativa argentina respecto del avance informático
- Ley de protección de datos
- Colaboración y legislación internacional

Seguridad en el desarrollo de software

- Políticas de Desarrollo Seguro (Responsables, lineamientos de desarrollo seguro, vigencia y versionado)
- Seguridad en el Ciclo de Vida (requerimientos, arquitectura, desarrollo, prueba, despliegue y mantenimiento, gestión de la configuración y gestión de fallas)
- Control de roles y privilegios
- Buenas prácticas en el desarrollo de software
- Base de datos de vulnerabilidades

Trabajo Final Integrador (TFI)

- Definición de una Política de Seguridad de la Información que integre las temáticas de la diplomatura.