UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

TEMARIO

- Introducción a la seguridad de la información y el mercado profesional: se presenta la seguridad como servicio y los temas relacionados con la demanda de profesionales en las empresas y organizaciones.

- Gestión de la seguridad de la información: identificación de los activos de una organización y desarrollo, documentación e implementación de políticas, estándares, procedimientos y guías.

- Arquitectura y Modelos de Seguridad: conceptos, principios, estructuras y estándares empleados para diseñar, monitorizar y asegurar sistemas, equipos, redes, aplicaciones y controles usados para reforzar los diversos niveles de la disponibilidad, integridad y confidencialidad.

- Sistemas y Metodología de Control de Acceso: Conjunto de mecanismos que permiten crear una arquitectura segura para proteger los activos de los sistemas de información.

- Seguridad en el Desarrollo de Aplicaciones y Sistemas: Define el entorno donde se diseña y desarrolla el software y engloba la importancia crítica del software dentro de la seguridad de los sistemas de información:
    - Definiciones.
    - Amenazas y metas de seguridad.
    - Ciclo de vida.
    - Arquitecturas seguras.
    - Control de cambios.
    - Medidas de seguridad y desarrollo de aplicaciones.
    - Bases de datos y data warehousing.
    - Knowledge-basedsystems.

- Seguridad de las Operaciones: Usado para identificar los controles sobre el hardware, medios y los operadores y administrador con privilegios de acceso a algún tipo de recurso.

- Criptografía: principios, medios y métodos de protección de la información para asegurar su integridad, confidencialidad y autenticidad.

- Seguridad Física: componentes y técnicas de protección de instalaciones, incluyendo los recursos de los sistemas de información y su gestión.

- Seguridad en Internet, Redes y Telecomunicaciones: incluye dispositivos de red, métodos de transmisión, formatos de transporte, medidas de seguridad y autenticación.

- Recuperación ante Desastres y Planificación de la Continuidad del Negocio: dirige la preservación del negocio en el caso de producirse situaciones de parada para la restauración de las operaciones.

- Leyes, investigaciones y Ética: Engloba las leyes y regulaciones de los crímenes informáticos, las técnicas y medidas de investigación, recuperación de evidencias y códigos éticos.

- Cibercrimen: contexto mundial de la ciber delincuencia, activismo informático y operaciones ilegales, incluyendo aspectos técnicos y no técnicos.
    - Fundamentos y funcionamiento
    - Malware y Botnets
    - Deep Web
    - Phishing y Spam
    - Operaciones internacionales
    - Casos de estudio
    - Prevención y acciones

- Evaluaciones de seguridad: determinación de la necesidad de procesos de evaluación de la seguridad en organizaciones, detalles de su contratación y ejecución.

CRONOGRAMA DE CLASES

Clase 1
- Introducción
    - La seguridad como servicio
    - El mercado de la seguridad de la información
    - Certificaciones profesionales
    - Perfiles profesionales y trabajo
    - Educación en seguridad
    - Eventos y congresos especializados
    - Recursos y referencias
    - Bibliografía y lecturas complementaria

Clase 2
- Gestión de la Seguridad
    - Conceptos y definiciones
    - Gestión del riesgo
    - Procedimientos y políticas

  - Clasificación de la información
  - Responsabilidades y roles
  - Planes de concientización
  - Fuga de información
  - Ingeniería social

Clase 3

- Arquitectura y Modelos de Seguridad
  - Conceptos de control y seguridad
  - Modelos de seguridad
  - Criterios de evaluación
  - Seguridad en entornos cliente/servidor y host
  - Seguridad y arquitectura de redes
  - Arquitectura de la seguridad IP

Clase 4

- Sistemas de Control de Acceso
  - Conceptos y tópicos
  - Identificación y autenticación
  - Sistemas single sign-on
  - Centralización del acceso
  - Metodologías de control
  - Monitorización y tecnologías

Clase 5

- Seguridad en el Desarrollo de Aplicaciones y Sistemas
  - Definiciones y conceptos
  - Amenazas y metas de seguridad
  - Ciclo de vida
  - Arquitecturas seguras
  - Control de cambios
  - Medidas de seguridad y desarrollo de aplicaciones
  - Bases de datos y data warehousing
  - Knowledge-basedsystems

Clase 6

- Seguridad de las Operaciones
  - Recursos
  - Privilegios
  - Mecanismos de control
  - Abusos potenciales
  - Controles apropiados
  - Principios

Clase 7

- Criptografía (I)
  - Historia y definiciones
  - Aplicaciones y usos

  - Conceptos y elementos
  - Protocolos y estándares
  - Tecnologías básicas
  - Sistemas de cifrado
  - Criptografía simétrica y asimétrica

Clase 8

- Criptografía (II)
  - Firma digital
  - Seguridad en el correo electrónico
  - Protección de datos locales y en tránsito
  - Criptografía enInternet
  - Publickeyinfrastructure (PKI)
  - Esteganografía y esteganálisis
  - Ataques y criptoanálisis
  - Aspectos legales

Clase 9

- Seguridad física y ambiental
  - Componentes de seguridad física
  - Tipos de amenazas
  - Gestión de las instalaciones
  - El plan de seguridad física
  - Seguridad del personal
  - Defensa en profundidad
  - Perímetro e interiores
  - Protecciones en datacenters
  - Sistemas de vigilancia y detección
  - Accesos físicos
  - Trashing y dumpsterdiving
  - Sistemas de suministro
  - Detección y supresión de incendios

Clase 10

- Seguridad en Internet, Redes y Telecomunicaciones (I)
  - Gestión de las comunicaciones
  - Redes de datos
  - Tecnologías de comunicaciones
  - Protocolos de red
  - Internet y Web

Clase 11

- Seguridad en Internet, Redes y Telecomunicaciones (II)
  - Firewalls
  - Sistemas de detecciónde intrusos (IDS)
  - Honeypots
  - Conexiones a escritorios remotos

- Redes virtuales:VPN y VLAN
- Tecnología inalámbrica

Clase 12

- Recuperación ante Desastres y Continuidad del Negocio
  - Conceptos de recuperación ante desastres y de negocio
  - Procesos de planificación de la recuperación
  - Gestión del software
  - Análisis de Vulnerabilidades
  - Desarrollo, mantenimiento y testing de planes
  - Prevención de desastres

Clase 13

- Cibercrimen
  - Fundamentos y funcionamiento
  - Malware y Botnets
  - Deep Web
  - Phishing y Spam
  - Operaciones internacionales
  - Casos de estudio
  - Prevención y acciones

Clase 14

- Leyes, investigaciones y ética
  - Legislación y regulaciones
  - Gestión de incidentes
  - Respuesta ante incidentes
  - Conducción de investigaciones
  - Análisis forense informático
  - Ética y seguridad
  - Códigosde ética

Clase 15

- Evaluaciones de seguridad
  - Servicios de evaluación
  - Marco legal de un test
  - Alcances y tipos de pruebas
  - Testing funcional y auditorías
  - Ethical Hacking y PenetrationTesting
  - Metodologías de evaluación
  - Etapas del proceso
  - Vulnerabilityresearch
  - Herramientas y software
  - Informes y entregables

Clase 16

- Evaluación final

UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Debate y devolución de resultados