Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

PROGRAMA ANALÍTICO DE ASIGNATURA

DEPARTAMENTO: Ingeniería en Sistemas de Información

CARRERA: Ingeniería en Sistemas de Información

NOMBRE DE LA ACTIVIDAD CURRICULAR: Seguridad en los Sistemas de Información

Año Académico: Plan 2023
Área: Gestión Ingenieril
Bloque: Tecnologías Aplicadas
Nivel: 5º
Tipo: Obligatoria
Modalidad: Cuatrimestral

Cargas horarias totales:

Horas reloj	*Horas cátedra*	*Horas cátedra semanales*
72	96	3

OBJETIVOS

- Aplicar modelos de referencia en la gestión de la seguridad de la información según las normativas vigentes
- Planificar controles de seguridad basados en la gestión de riesgo
- Desarrollar un plan de seguridad asegurando la continuidad del negocio
- Comprender el proceso de auditoría y tratamiento de evidencias

CONTENIDOS

Contenidos mínimos

- Seguridad de la Información
- Marco Normativo
- Gestión de Riesgos
- Sistemas de gestión de seguridad
- Auditoría de Sistemas de Información
- Peritaje informático forense

Contenidos analíticos

Unidad 1: Introducción a la Ciberseguridad

Conceptos introductorios. Ciberseguridad y Seguridad de la Información. Tríada de seguridad. Principios básicos: Defensa en profundidad. Mínimo privilegio (Least privilege). Necesidad de conocer (Need to know). Rotación de tareas y segregación de funciones. No repudio. Seguridad por defecto. Minimización de superficie de ataque. Simplicidad.

Unidad 2: Gobierno de la seguridad

Sistemas de gestión de seguridad. Estándares y marcos de referencia. Políticas, procedimientos, estándares y guías. Roles y dependencias organizacionales. Demanda laboral insatisfecha. Métricas (PKI, OKR). Alcance, roles y responsabilidades. Seguridad defensiva y ofensiva. CISO. Tipos de CISO. Competencias requeridas. Estructuras organizacionales. Cultura, ética y comportamiento. Ciberagilidad.

Unidad 3: Gestión de Riesgos

Conceptos de riesgo: activo, vulnerabilidad, amenaza, agente, impacto, probabilidad, exposición. Naturaleza de las amenazas. Fases de la gestión de riesgos. Cálculos cualitativos y cuantitativos. Valuación de Activos. Exposición y pérdida anualizada. Riesgo intrínseco y residual. Tipos de controles según enfoque. Estrategias de gestión de riesgo. Apetito de riesgo y tolerancia al riesgo. Metodologías y modelos de gestión de riesgo.

Unidad 4: Gestión de Identidades

Conceptos generales. Identificación, autenticación, autorización y auditoría. Autenticación de doble factor. Autenticación basada en comportamiento. Protección criptográfica. Federación. Identidad como servicio. Integración de servicios de identidad. Modelos de controles de acceso. Técnicas y tecnologías de control de acceso. Tipos de identidades. Modelo de Gobierno de identidades. Protocolos (SAML, Openid, OAuth). Tecnologías de Control de Acceso Corporativo. Gestión de cuentas privilegiadas. Gestión de identidades de terceros. Monitoreo y control. Identidad digital. Amenazas al control de acceso. Tendencias.

Unidad 5: Criptografía

Historia de la criptografía. Conceptos Generales: criptosistema, criptografía, criptoanálisis, criptología. Servicios provistos. Esteganografía. Tipos de cifrado. Sustitución y Transposición. Cifrado de bloque y flujo. Fortaleza de un algoritmo. Cifrado simétrico (DES, AES, RC4, etc). Cifrado asimétrico (RSA, Diffie-Hellman). Cifrado híbrido. Firma digital (MD4, MD5, SHA). Funciones de hash. Infraestructura de Clave pública. Certificados digitales. Protocolos (SSL, Https y otros). Ataques en criptografía.

Unidad 6: Amenazas y vulnerabilidades

Conceptos: amenaza, vulnerabilidad, control. Parche. Zero Day. Exploit. Bug Bounty. Amenazas y vulnerabilidades en el host y en la red. Fases de un ataque. Indicadores de Compromiso. Código malicioso. Virus. Gusano. Troyanos. Spyware. Adware. Keyloggers. Backdoors. Phishing. Spearphishing. BEC. Pharming. Tipos de pharming. Aplicaciones potencialmente indeseadas. Botnets. Ramsonware. Amenazas persistentes avanzadas (APTs). Antivirus. Sandboxing.

Unidad 7: Aspectos legales, regulaciones, certificaciones y Compliance.

Principales aspectos en materia de Ciberseguridad y Seguridad en los sistemas de Información. Diferencias de alcance y obligatoriedad entre ley, regulación, metodologías y certificaciones. Compliance corporativo. Desafíos. Programa de integridad.

Leyes: Ley N° 26.388 "Delitos informáticos". Tipificación de delitos. Convención de Budapest. Grooming, Sexting, Sextorsión y Porno-venganza, adolescentes (pornografía infantil). Ley N°25326 "Protección de Datos Personales". Ley N° 25506 "Firma Digital". Sarbanes Oxley SOX. COBIT. Regulaciones: PCI[1], HIPAA[2], BCRA 4609, BCRA A7266[3].

Metodologías y estándares: OSSTMM, ISO 2700X, Cloud Security Alliance, Orange Book, OWASP. Certificaciones: ISO 2700X, CISSP, CCSP, CISM, CEH, entre otras.

Unidad 8: Informática forense

Investigación Criminal de los delitos informáticos. Territorialidad. Criminología. Criminalística. Evidencia Digital. Funciones. Características de las evidencias. Cadena de custodia. Principios Forenses: Principio de legalidad, Fruto del árbol envenenado. Proceso de Preservación, Colección, Análisis y Presentación de evidencia digital. Tipos de Análisis. Protocolos y Guías de Buenas Prácticas en el tratamiento de la evidencia digital nacionales e internacionales. ISO/IEC 27037.

Unidad 9: Seguridad en el desarrollo de aplicaciones

El nuevo perímetro. Problemática y desafíos en las organizaciones. Principios generales. Autenticación y autorización. Manejo de información sensible. Auditoría y trazabilidad. Participación en el Ciclo de Seguridad: Seguridad en el desarrollo, en la construcción, en el despliegue, testing y seguridad en la operación. Evolución de prácticas modernas de desarrollo. Modelado de amenazas. OWASP Top 10. Vulnerabilidades comunes y estrategias de mitigación. Modelo de madurez de seguridad en aplicaciones. Revisión estática y dinámica de código. Despliegue continuo. DevSecOps. Agilidad en el desarrollo.

Unidad 10: Seguridad en las operaciones

Procesos de seguridad y roles en áreas de seguridad. Seguridad defensiva y ofensiva. Gestión de vulnerabilidades y control de estándares. Monitoreo y detección. Gestión de Incidentes de Seguridad: detección, respuesta, mitigación, reporte, recuperación y remediación. Evento e incidente. Centro de Operaciones de Seguridad (SOC- CSIRT-SOAR). Modelos de madurez. Herramientas y tecnologías. Frameworks reconocidos: NIST ATTACK, MITRE, Controles CIS, NIST Security Framework. Ciber-resiliencia.

Unidad 11: Inteligencia, Espionaje e Ingeniería Social – La brecha humana

Tipos de ingeniería social. Principios tácticos y psicológicos. Factor humano, sus vulnerabilidades. Principios básicos de la Ingeniería Social. Vectores de ataque. Técnicas de manipulación y persuasión. Sesgos mentales. El lenguaje corporal. Usos y objetivos. Técnicas de Inteligencia (OSINT, HUMINT, SIGINT, etc.). Técnicas de Ingeniería Social (físicas y digitales). Agregar e inferir. Búsqueda de información en fuentes abiertas. Hacking en buscadores.

Metabuscadores. Deep web. Privacidad y anonimato. Programas de Concientización. Estrategias y desarrollo de capacidades.

Unidad 12: Auditorías y revisiones de seguridad

Introducción a los Procesos de Evaluación. Auditoría Técnica de Sistemas: Generalidades. Análisis de brecha. Marco legal de un test. Alcances y tipos de pruebas: Escaneo de vulnerabilidades. Pruebas de penetración. Hackeo ético. Posicionamiento y visibilidad. Fases de una prueba: reconocimiento, enumeración, acceso, mantenimiento y eliminación de rastros. Investigación y reporte de vulnerabilidades. Herramientas y software. Informes y entregables.

Unidad 13: Privacidad y Protección de Información

El valor de la privacidad y los datos personales. GDPR (Reglamento General Europeo de Protección de Datos personales): su impacto en la región. Gobierno. Desarrollo de la estrategia. Frameworks de control (ISO 27701, NIST SP 800-53, NIST SP 800-122, NIST Privacy Framework). Controles de seguridad y privacidad para Organizaciones y sistemas de información. Roles y responsabilidades. Gestión de Riesgos de Privacidad. Arquitectura de la privacidad. Privacidad por diseño. Privacidad por defecto.

Ciclo de Vida de la información. Conceptos (data protection, data leak, data breach). Clasificación de la información. Implementación de un programa de protección. Paradigmas de protección (repositorio, perímetro, contenido y etiquetado). Enmascaramiento y Ofuscación. Retención y backup. Enfoque de protección basado en estado (uso, transporte, reposo) . Tecnologías de protección. Impacto de una brecha de información. Responsabilidades sobre gestión de terceras partes.

Unidad 14: Seguridad en la Nube y Tendencias en tecnología

Conceptos. Estándar NIST 800-145. Características. Modelos de despliegue. Modelos de servicio. Actores. Ecosistema de actores Cloud. Modelo de responsabilidad compartida. Retos y desafíos. Seguridad en los datos, en la arquitectura y las aplicaciones. Compliance. Amenazas en la nube. Amenazas globales actuales. Tendencias nacionales e internacionales. BYOD (Bring your own device). APT (Advanced Persistent Threats). Big Data. Transformación Digital. Nuevos paradigmas (Zero Trust, etc). Ciber-agilidad. DevSecOps.

BIBLIOGRAFÍA OBLIGATORIA

- Belapurkar, Abhijit (2009). Distributed Systems Security. Ed. Willey.
- Bell, Luara et al (2016). Agile Application Security. O'Reilly Media
- Bennet, Steven y Genung, Jordan. (2021). Certified Chief Information Security Officer (CCISO). Ed. Mc Graw Hill Education.
- Calashian, Tara (2008). Google Hacks. O'Reilly & Associates, Inc
- Carnegie, Dale (1964). How to win Friends and influence people. Ed. Simon and Schuster
- Harris, Shon (2019). CISSP Exam Guide. Ed. Mc Graw Hill Education.
- Hsu, Tony (2018). Hands-On Security in DevOps. Ed. Packt Publishing.

- Jara, Hector y Pacheco, Federico (2012). Ethical Hacking 2.0. Ed. Red Users.
- Kahn, David (1967). The Codebreakers. Ed. The Macmillan Company
- Kim, Gene et al (2016). The DevOps Handbook. Ed. IT Revolution Press
- Kim, Behr y Spafford. (2013). The Phoenix Project. Ed. IT Revoluton Press
- McDonald, Malcom (2020). Web Security for Developers. Ed. No Starch Press
- Madden, Neil (2020). API Security in Action. Ed. Manning
- Mitnick, Kevin y Simon, William (2005). The art of intrusion. Ed. Wiley Publishing, Inc.
- Peter H., G. (2021). Certified Data Privacy Solutions Engineer (CDPSE) Exam Guide. Ed. Mc Graw Hill Education.
- Saccani, Raúl et al (2018). Tratado De Compliance 2 tomos. Ed. La Ley.
- Spade, Daniel. (2019). How to analize people. 13 laws about the Manipulation of the Human Mind. Ed. Spade, Daniel.
- Walker, Matt (2019). Certified Ethical Hacker (CEH). Ed. Mc Graw Hill Education.
- Williams, James (2018). How to analyze people – Dark Phsychology. Ed. SD Publishing.
- Zalewski, Michal (2012). The Tangled Web. Ed. No Starch Press.

CORRELATIVAS

Para cursar y rendir

- Cursadas:
    - Redes de Datos
    - Administración de Sistemas de Información (Integradora)
- Aprobadas:
    - Desarrollo de Software
    - Comunicación de Datos