Universidad Metropolitana

PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN

Facultad:	Ingeniería	**Departamento:**	Gestión de Proyectos y Sistemas
Codigo:	FPTSP18	**Asignatura:**	Seguridad de la Información
Creditos:	3	**Tipo:**	X Obligatoria ___ Electiva
Carreras:	Ingeniería de Sistemas (IS)	**Trimestres:**	XI (IS)
Prerrequisito	Sistemas de Redes (FPTEN23)	**Modalidad:**	Virtual
Número de horas semanales			
En aula	**Prácticas supervisadas**	**Laboratorio**	**Aprendizaje Autónomo**
4			4
Coordinador:	Christian Guillén Drija	**Fecha de actualización**	Oct. 2025

1. ***Justificación:*** En un entorno de creciente dependencia tecnológica, esta asignatura es vital para proteger la confidencialidad e integridad de la información ante amenazas globales. Capacita al ingeniero de sistemas en el diseño de infraestructuras críticas y en la aplicación de técnicas de protección avanzadas. Así, el profesional garantiza la defensa de los activos digitales y el cumplimiento de las normativas de seguridad vigentes.

2. ***Propósito:*** Proporcionar una visión integral sobre amenazas y riesgos en informática y telecomunicaciones para desarrollar habilidades en la detección de vulnerabilidades. El curso busca que el estudiante implemente controles de seguridad, esquemas de cifrado y políticas de protección bajo estándares internacionales. Esto asegura la operatividad y resiliencia de los sistemas de información en las organizaciones actuales.

3. ***Objetivos***

- Conocer técnicas y mecanismos existentes que rigen la seguridad de la información en el ámbito empresarial.
- Analizar las situaciones de una red o un equipo que facilitan la penetración de intrusos y cuáles son los métodos de ataque que emplean los hackers. (Objetivo 1 de la carrera)
- Evaluar las condiciones de seguridad que imponen a las organizaciones los nuevos entornos de trabajo, tales como Internet, acceso remoto, teletrabajo y redes inalámbricas. (Objetivos 1 y 2 de la carrera)
- Implementar las medidas de seguridad para defenderse de las amenazas internas y externas a través de controles apropiados. (Objetivos 1 y 2 de la carrera)
- Administrar sistemas de seguridad tomando en cuenta las nuevas amenazas y riesgos que continuamente aparecen. (Objetivos 1 y 4 de la carrera)

4. ***Resultados de aprendizaje***

a) **RA8 - Resolución de problemas de ingeniería.** Capacidad para comprender, definir y resolver problemas de análisis de ingeniería en el campo de estudio pertinente, con el uso de conocimientos básicos y avanzados de métodos analíticos modernos.

5. ***Contenido***

Tema	Contenido	Herramientas técnicas y actividades (proyectos, trabajos, laboratorios)	Horas dedicadas
1	Introducción a la seguridad de la información.	Clase síncrona interactiva y discusión dirigida sobre fundamentos de seguridad.	5
2	Amenazas, vulnerabilidades y riesgo. Gestión de Vulnerabilidades y Parches. Inteligencia de Amenazas y Seguridad Proactiva.	Aprendizaje Basado en Problemas (ABP): Análisis de ciberataques reales. Simuladores (Cyber Range). Mapas de riesgo para estrategias de mitigación.	5
3	Medidas de protección y planes de seguridad. Seguridad en la Nube y Virtualización.	Estudio de casos: Creación de políticas de seguridad. Proyecto: Plan de seguridad empresarial. Software: Draw.io, Lucidchart, ISO 27001.	5
4	Criptografía y protección de la confidencialidad.	Vídeos asíncronos y clases síncronas. Práctica de cifrado/descifrado con entrega de informes técnicos.	5
5	Integridad y autenticidad de la información	Demostraciones prácticas y debates sobre banca online. Experimentos con archivos manipulados (Hash MD5/SHA) y	5

		simuladores de firmas electrónicas.	
6	Autenticación, autorización y control de acceso.	Resolución de problemas: Configuración de roles y permisos. Plataformas: OpenLDAP, Auth0 y diagramas de control de acceso.	5
7	Defensa contra intrusos y barreras de protección. Pentesting y Técnicas de Hacking Ético.	Simuladores de firewall (Sense, Snort lab). Escenarios de intrusión y defensa con informe de práctica y cuestionario de repaso.	5
8	Seguridad en redes y en Internet.Ciberseguridad en Aplicaciones Web.Seguridad en voz sobre IP y telefonía por Internet.	Taller de análisis de tráfico (Wireshark). Configuración de sistemas VoIP seguros (3CX, Asterisk, Zoiper). Análisis de capturas de red reales.	5
9	Análisis Forense y Respuesta a Incidentes.	Aprendizaje Basado en Retos (CBL): Simulación de intrusión. Uso de Autopsy, FTK Imager, Wireshark y Volatility (RAM).	5
10	Tendencias Emergentes	Vigilancia tecnológica (Gartner/Google Trends). Análisis de malware con IA (ChatGPT/Claude). Simulación en Cisco Packet Tracer.	3

6. ***Métodos de aprendizaje:*** **Participación activa:** En clases virtuales síncronas se fomentará la participación de los estudiantes a través de chats en vivo donde puedan plantear dudas y comentarios. **Aprendizaje basado en problemas (ABP):** Presentación de distintos casos reales a los estudiantes con el fin de analizar en clase las lecciones aprendidas. **Aprendizaje Invertido (Flipped Classroom):** el docente propiciará la revisión del material teórico (lecturas, videos) antes de la clase. **Aprendizaje autónomo:** revisión de vídeos cortos y materiales de lectura como documentos PDF, artículos y presentaciones como complemento a las clases virtuales, fomentando la lectura y la investigación.

7. ***Métodos de evaluación:***

Aprendizaje en contacto con el docente (45%)	Aprendizaje práctico experimental (55%)	Aprendizaje autónomo (0%)
Exposiciones, Participación en clases, Debates, Exámenes escritos u orales, Talleres, Defensa de proyectos, entre otros.	Resolución de problemas prácticos, Prácticas de laboratorio, Salidas de campo o visitas técnicas, Manejo de software especializado, Prototipado técnico, Estudios de caso técnicos, entre otros.	Elaboración de informes, Resolución de problemas y ejercicios, Ensayos de investigación, Creación de mapas conceptuales, Participación en foros, entre otros.

8. ***Referencias***

Obligatoria:

- Briceño, E. V. (2025). Seguridad de la información: Fundamentos, amenazas y soluciones. Editorial Académica Española.
- Lucena López, M. (2007). *Criptografía y seguridad en computadores.* Universidad de Jaén.
- Stallings, W. (2023). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson Educación.
- Pfleeger, C. P., & Pfleeger, S. L. (2022). *Security in Computing* (6th ed.). Prentice Hall.

Adicional:

- Bertino, E., et al. (2010). *Security for web services and service oriented architecture.* Springer-Verlag.
- Canal, V. A. (2022). *Seguridad de la información: Expectativas, riesgos y técnicas de protección*. Limusa/Noriega Editores.
- Copper-Royer, B. (2023). *Hacking ético y ciberseguridad.* De Vecchi.
- Joshi, J., et al. (2008). *Network security: Know it all. Morgan Kaufmann.*
- Kizza, J. M. (2009). *A guide to computer network security.* Springer-Verlag.
- Pfleeger, C. P. (2006). *Security in computing.* Prentice Hall.
- Senft, S., & Gallegos, F. (2009). *Information technology control and audit.* CRC Press.
- Stallings, W. (2005). *Cryptography and network security*. Prentice-Hall.
- Vacca, J. R. (2024). *Los secretos de la seguridad en internet.* Anaya Multimedia.