Carrera INGENIERIA EN INFORMATICA		
Asignatura 3650 - Seguridad de la Información		
Trayecto Calidad y Seguridad de la Información		
Año académico 2023		
Responsable / Jefe de catedra Mg. Ing. Jorge Esteban Eterovic		
Carga horaria semanal 4 hs.	**Carga horaria total** 64 hs.	**Créditos ----**
Modalidad: Presencial		
Correlativas anteriores: REDES DE COMPUTADORAS – ARQUITECTURA DE COMPUTADORAS - TOPICOS DE PROGRAMACION	**Correlativas posteriores** AUDITORIA Y LEGISLACION - GESTION DE PROYECTOS	
Conocimientos necesarios Programación básica. Conceptos fundamentales de informática. Arquitectura de Redes de Computadoras.		

Descripción de la asignatura

La materia está orientada a que el alumno pueda comenzar a desarrollar sus capacidades en los diferentes dominios de la Seguridad de la Información y la Ciberseguridad, brindando un amplio abanico de conocimientos teóricos y prácticos. Se enfoca en que el alumno pueda comprender las diversas estándares, metodologías y funcionalidades para enfrentar las necesidades de las organizaciones en materia de seguridad de la información, alineados con las mejores prácticas del mercado y posibilitando implementar sistemas de gestión de seguridad de la información alineados con el contexto de riesgo de la organización y articulados para protegerse de riesgos emergentes. La gran cantidad de infraestructura y servicios interconectados, cada vez más distribuidas, plantea un importante desafío de como garantizar la seguridad de la información, siendo la información uno de los activos más importantes que poseen las organizaciones. En este contexto es primordial que los alumnos comprendan la importancia de prevenir y evitar los ataques informáticos y de la definición y puesta en marcha de planes de protección de todos los activos informáticos y sus correspondientes datos.

Metodología de enseñanza

La metodología de enseñanza se focaliza en clases teóricas con la ejemplificación de la aplicación de los mismos en escenarios, de manera de lograr que el alumno obtenga un conocimiento equilibrado de los componentes teóricos y aplicación de los mismos en escenarios reales.

A modo complementario se llevan a cabo diferentes trabajos prácticos orientados a desarrollar alguna actividad práctica ya sea aplicando alguna metodología o estándar o utilizando herramientas específicas.

Las clases serán dictadas a través de distintos métodos, como explicaciones a través de definiciones, ejemplos, ejercicios, lectura individual dirigida, actividades grupales de análisis, transferencia, validación colectiva y exámenes. Determinados contenidos temáticos serán presentados a los alumnos a través de proyecciones y videos.

Se desarrollarán diferentes prácticos individuales y/o grupales aplicando los contenidos dados en las diferentes unidades temáticas, para poder fijar los conocimientos de forma práctica. Se fomentará al alumno al trabajo en grupo.

El proceso de enseñanza y de aprendizaje de carácter teórico-práctico, permanente e integral, propone a los alumnos la adquisición de conocimientos, el desarrollo de actitudes y la detección de aptitudes, el aumento de la destreza y las habilidades para comprender y encontrar información relevante, y la resolución de las situaciones nuevas que se le presenten, utilizando un enfoque hacia la resolución de problemas.

El alumno debe mostrar al finalizar el curso un nivel mínimo de destreza en los conceptos y las tecnologías específicas asociadas a la materia.

Las diversas actividades teórico-prácticas planteadas favorecen la investigación, el desarrollo, el trabajo en equipo y la fijación de conocimientos.

Considerando que la adaptación a las nuevas tecnologías supone un reto fundamental actual, se le facilitará al alumno la posibilidad y los medios necesarios para que puedan acceder, conocer e investigar todos los instrumentos que las nuevas y últimas tecnologías ofrecen.

Metodología de Clases Teóricas

- Las clases teóricas están orientadas a introducir a los alumnos en los diferentes conceptos teóricos conceptuales de la materia.
- Cada tema teórico es abordado en clase brindando el profesor ejemplos de aplicación.
- La metodología de trabajo alternará entre clases expositivas donde los profesores explicarán los temas y otras haciendo participar a los alumnos mediante exposición dialogada.

Metodología de Clases Prácticas

- Las clases prácticas se referirán a cada núcleo temático de la materia o podrán integrar conceptos de diferentes unidades.

Trabajos Prácticos

- Para poder realizar un seguimiento progresivo del aprendizaje, se asocian a determinadas unidades temáticas trabajos prácticos en la que los alumnos podrán aplicar lo aprendido.
- Se desarrollarán trabajos prácticos donde se hará hincapié en algún concepto fundamental o combinación de los mismos, para luego comprender los resultados en base a los procedimientos aplicados.
- Estos trabajos prácticos posibilitan la resolución de problemas por unidad temática o integrando varias unidades, con objetivos específicos. Consisten en planteos de problemas y actividades referentes a los diversos contenidos de la asignatura.
- Los trabajos prácticos serán seleccionados con un criterio que pondere lo conceptual y lo estratégico en lugar de la mecanización de procedimientos.
- Los trabajos prácticos pueden variar en cada cuatrimestre, considerando además los avances tecnológicos y de contenido de la materia.

- Se plantearán trabajos prácticos obligatorios y complementarios. Los docentes corregirán cada trabajo práctico entregado por los alumnos y darán una devolución personalizada.
- Esto trabajos estarán destinados a aplicar y medir el grado de comprensión de los temas teóricos expuestos en clase y el manejo de las definiciones y propiedades en contextos prácticos para comprobar que realmente se han incorporado los conceptos y no memorizado o mecanizado definiciones, procedimientos y demostraciones presentadas en las clases .
- Los trabajos tienen como finalidad generar la capacidad necesaria para saber interpretar claramente los objetivos del problema y poder resolverlo, aplicando una adecuada estrategia en la resolución.
- El docente irá evaluando el progreso de cada alumno en cada entrega de los diferentes prácticos (sean grupales o individuales).
- Los alumnos deberán ir realizando entregas parciales de avances establecidas por el docente durante la cursada.

Plataforma y Materiales Didácticos

- La materia cuenta con apuntes teórico-prácticos desarrollados por los profesores de la cátedra. También se utilizan los libros detallados en la sección de Bibliografía.
- Se motiva a los estudiantes el uso de la plataforma MIEL para acceder al material, usar el foro, para comunicaciones con la cátedra y para la resolución de dudas tanto de conceptos teóricos como prácticos.

Objetivos de aprendizaje

- Comprender los conceptos y términos fundamentales relacionados a la seguridad de la información.
- Comprender los principios, tecnologías, metodologías y diversos estándares empleados para asegurar la integridad, disponibilidad y confidencialidad de la información.
- Identificar, prevenir y resolver situaciones o eventos vinculados a ataques a la seguridad de la información.
- Proponer medidas de protección de seguridad físicas, lógicas y procedimentales contra eventos que pudieran llevar a la adquisición y transferencia indebida de datos, modificación o distribución ilegítima de los mismos o bloqueo de los sistemas.
- Aplicar mecanismos y técnicas de control de acceso.
- Conocer las técnicas y mecanismos de protección de instalaciones físicas.
- Comprender los principios de administración de red segura, distinguir y diferenciar elementos y componentes de una red, así como implementar y utilizar protocolos comunes.
- Comprender qué es un Sistema de Gestión de la Seguridad de la Información (SGSI)
- Fundamentar la aplicación de normas para la gestión de la seguridad de la información.
- Aplicar estrategias para la gestión de los activos de información.
- Aplicar metodologías de administración de riesgos de seguridad de la información.
- Describir las metodologías para asegurar la continuidad del negocio de las organizaciones en el caso de producirse situaciones críticas que pudieran detener la operación normal de la misma.

- Explicar los conceptos y mejores prácticas referentes a la gestión de servicios TI (tecnologías de la información).
- Introducir los conceptos generales relacionados con la criptografía y su aplicación.

Contenidos mínimos

Conceptos de Seguridad Informática. Amenazas. Vulnerabilidades. Riesgos. Políticas de seguridad informática. Normas Aplicables. Protección de datos. Seguridad Lógica. Seguridad Física. Seguridad en Redes. Mecanismos criptográficos aplicados a la seguridad informática.

Competencias a desarrollar

Genéricas

- Actuación profesional ética y responsable.
- Aprendizaje continuo.
- Identificación, formulación y resolución de problemas de ingeniería en sistemas de información/informática.
- Gestión, planificación, ejecución y control de proyectos de ingeniería en sistemas de información / informática.
- Utilización de técnicas y herramientas de aplicación en la ingeniería en sistemas de información / informática.
- Evaluación y actuación en relación con el impacto social de su actividad profesional en el contexto global y local.
- Desarrollo de una actitud profesional emprendedora.
- Desempeño en equipos de trabajo.
- Comunicación efectiva.

Especificas

- Proyecto y dirección en lo referido a seguridad informática.
- Procedimientos y certificaciones del funcionamiento, condición de uso o estado de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software.
- Dirección y control de la implementación, operación y mantenimiento de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software.
- Especificación, proyecto y desarrollo de sistemas de información.
- Especificación, proyecto y desarrollo de sistemas de comunicación de datos.

Programa Analítico

Unidad 1	**Introducción a la Seguridad de la Información** Fundamentos de la seguridad de la información. Conceptos básicos. Importancia de la información para las organizaciones. La seguridad en la actualidad. Pilares de la seguridad de la información. Evolución de la seguridad informática. Estadísticas. Políticas de seguridad de la información. Definición de conjunto de políticas de seguridad de la información. Organización de seguridad de la información. Seguridad de

	los recursos humanos. Amenazas. Vulnerabilidades. Detección y gestión de Vulnerabilidades. Tipos de intrusiones. Mecanismos y tecnologías de prevención. Estrategias de seguridad. Concientización, capacitación y educación. Normas aplicables.
Unidad 2	**Ataques de Ciberseguridad** Conceptos y funciones de la ciberseguridad. Tipos de ciberataques. Modalidades de ataques. Ataques a contraseñas. Ataques por Ingeniería Social. Ataques a las conexiones. Ataques de denegación de servicio. Ataques por suplantación de identidad. Ataques por malware. Ataques a aplicaciones. Ransomware. Aplicaciones maliciosas. Prevención de ataques. Recomendaciones y soluciones frente ataques. Importancia de la seguridad en el ciclo de vida de desarrollo de software.
Unidad 3	**Seguridad Lógica** Definiciones básicas de la seguridad lógica. Gestión de identidades y accesos. Control de acceso. Mecanismos y técnicas de control de acceso. Registros de accesos (Accountability). Mecanismos de identificación. Métodos de autenticación. Métodos de autorización. Administración de accesos. Protocolos y soluciones.
Unidad 4	**Seguridad Física** Aspectos generales y fundamentos de la seguridad física. Controles y mecanismos de prevención, detección y respuesta. Diseño y construcción de sitios seguros. Componentes de la seguridad física. Medidas de seguridad y ambientales. Protección Perimetral. Controles de acceso físico a las instalaciones. Sistemas de vigilancia y detección. Requerimientos de un centro de cómputos. Prevención, detección y supresión de incendios. Control de inventarios.
Unidad 5	**Introducción a la Seguridad en Redes** Definiciones de seguridad en redes. Principales riesgos y tipos de ataques en redes. Diseño seguro de redes. Componentes de una red. Tipos de redes. Topología de redes. Protocolos de red. Seguridad de perímetro. Seguridad en el canal. Seguridad de acceso. Seguridad aplicada a la nube.
Unidad 6	**Sistema de Gestión de la Seguridad de la Información (SGSI)** Definición de SGSI. Principios fundamentales. Introducción a los estándares de seguridad de la Información. Entidades de normalización. Normas BS. Normas de Criterios Comunes (CC, Common Criteria). Estándares del NIST. Marco de Ciberseguridad del NIST. Normas ISO, serie 27.000 y su evolución. Otros estándares de seguridad de la información.
Unidad 7	**Normas ISO Serie 27.000** Norma IRAM-ISO/IEC 27001. Términos y definiciones. Alcance y campo de aplicación de la norma. Estructura de la norma. Dominios de la norma. Objetivos de control y controles. Aspectos cubiertos por la norma. Modelo P-H-V-A aplicado a los procesos del SGSI. Fases del SGSI. Implementación. Metodología de Certificación. Buenas Prácticas en la

	Gestión de la Seguridad de la Información. Norma IRAM-ISO/IEC 27002. Estructura de los objetivos de control. Dominios de la norma IRAM-ISO/IEC 27002.
Unidad 8	**Gestión de activos de información, de riesgos de seguridad de la Información y de incidentes** Activos de información. Inventario de activos. Propietarios. Clasificación de activos de información. Administración de activos. Amenazas. Vulnerabilidades. Riesgos. Incidentes de Seguridad. Importancia de la gestión de riesgos de seguridad de la información. Mejores prácticas y normas vinculadas. Norma ISO/IEC 27005. Política de gestión de riesgos. Proceso de administración de riesgos. Evaluación de riesgos. Análisis de riesgos cuantitativos y cualitativos. Técnicas de tratamiento de riesgos. Plan de tratamiento de riesgos. Mejora continua. Indicadores y métricas. Gestión de incidentes de Seguridad.
Unidad 9	**Gestión de la Continuidad del Negocio** Fundamentos de la continuidad del negocio. Plan de continuidad del negocio (BCP). Análisis de Impacto de negocio (BIA). Plan de recuperación ante desastres (DRP).
Unidad 10	**Introducción a las buenas prácticas ITIL.** Fundamentos y principios de las buenas prácticas de ITIL. Alineación de TI con el negocio. Gestión de servicios de tecnologías de información. Funciones, Procesos y Roles ITIL. Indicadores claves de desempeño. Mediciones para poder gestionar. Definición del ciclo de vida por ITIL.
Unidad 11	**Introducción a la Criptografía** Conceptos generales. Criptografía clásica. Criptografía moderna. Algoritmos simétricos. Algoritmos asimétricos. Conexiones seguras por cifrado. Firma electrónica. Firma Digital. Infraestructura de clave pública. Algoritmos de Hash. Estenografía. Introducción a criptomonedas.

Planificación de actividades					
Semana	**Clase**	**Actividad**	**Tipo**	**Duración estimada**	**Unidad/des**
Semana 1	Introducción a la Seguridad de la Información.	Presentación	Teoría	4 horas	Unidad 1
Semana 2	Introducción a la Seguridad de la Información. Ataques de Ciberseguridad.	Presentación	Teoría	4 horas	Unidad 1/2
Semana 3	Ataques de Ciberseguridad.	Presentación/ Práctica	Teoría/ Práctica	4 horas	Unidad 2

Semana 4	Seguridad Lógica	Presentación	Teoría	4 horas	Unidad 3
Semana 5	Seguridad Lógica. Seguridad Física.	Presentación	Teoría	4 horas	Unidad 3/4
Semana 6	Seguridad Física	Presentación	Teoría	4 horas	Unidad 4
Semana 7	Int. a la Seguridad en Redes	Presentación/ Práctica	Teoría/ Practica	4 horas	Unidad 5
Semana 8	PARCIAL Sistema de Gestión de la Seguridad de la Información (SGSI)	PARCIAL Presentación	Evaluación Teoría	2 horas 2 horas	 Unidad 6
Semana 9	Sistema de Gestión de la Seguridad de la Información (SGSI). Normas ISO Serie 27.000.	Presentación	Teoría	4 horas	Unidad 6/7
Semana 10	Gestión de activos de información, de riesgos de seguridad de la Información y de incidentes.	Presentación	Teoría	4 horas	Unidad 8
Semana 11	Gestión de activos de información, de riesgos de seguridad de la Información y de incidentes.	Presentación/ Práctica	Teoría/ Práctica	4 horas	Unidad 8
Semana 12	Gestión de la Continuidad del Negocio	Presentación	Teoría	4 horas	Unidad 9
Semana 13	Buenas prácticas ITIL.	Presentación	Teoría	4 horas	Unidad 10
Semana 14	Introducción a la Criptografía.	Presentación/ Práctica	Teoría/ Práctica	4 horas	Unidad 11
Semana 15	PARCIAL	PARCIAL	Evaluación	4 horas	
Semana 16	RECUPERATORIO	RECUPERATORIO	Evaluación	4 horas	

Evaluación

El proceso evaluativo se basa en dos exámenes parciales presenciales y un examen recuperatorio presencial (en el cual se puede recuperar uno de los dos parciales). Las evaluaciones serán escritas y prácticas, pudiendo la cátedra llevar a cabo evaluaciones orales y/o en la PC.

En el primer parcial se evaluarán las unidades 1 a la 8, por medio de preguntas teóricas y prácticas. El segundo parcial se evaluarán las unidades 9 a 16 utilizando una metodología similar, pero se agregan más ejercicios prácticos.

Además los alumnos deberán desarrollar los trabajos prácticos obligatorio durante el cuatrimestre, los cuales tendrá un seguimiento periódico quincenal.

En el caso que el alumno cumpla con los requisitos establecidos en el Régimen de Cursada pero no con los criterios de promoción, deberá rendir un examen final, los cuales se confeccionarán de manera de poder evaluar la parte teórica/práctica integral de la materia.

Para poder rendir el examen libre, el alumno deberá contactar al inicio del primer cuatrimestre o del segundo cuatrimestre a los docentes de la materia, a fin de solicitar el acceso al material actualizado y además el enunciado de los trabajos prácticos especiales que deberá entregar y aprobar, previo a rendir el final. Si el alumno no entregara y aprobara, previo al examen final libre, los trabajos prácticos especiales, no estará en condiciones de rendir el examen final libre.

Primera Evaluación	Semana 8	Evaluación Teórica	2 hs.
Segunda Evaluación	Semana 15	Evaluación Teórica	2 hs.
Recuperatorio	Semana 16	Evaluación Teórica	2 hs.

Bibliografía obligatoria

Titulo	Autor	Editorial	Edición	Año
Qué es la seguridad informática	Hugo D. Scolnik	PAIDOS	1era.	2012
Criptografía : desde los sistemas clásicos hasta el futuro de la privacidad	Pacheco, Federico	Fox Andina	2014	2014

Bibliografía complementaria recomendada

Titulo	Autor	Editorial	Edición	Año
CIBER SEGURIDAD DE	Israel Rosales	Ediciones Trilabs	1ra. edición	2020

LA INFORMACIÓN: Una Guía de Entrenamiento para el Profesional de Seguridad OSI				
Seguridad de la información: Ciberseguridad	Rajapraveen K. N.	Sciencia Scripts	1ra. Edición	2022

Otros recursos obligatorios [Videos, enlaces, otros. Incluir una fila por cada recurso]	
Nombre	
Apuntes de la cátedra	https://miel.unlam.edu.ar/
Marco para la mejora de la seguridad cibernética en infraestructuras críticas	https://doi.org/10.6028/NIST.CSWP.04162018es.
Security and Privacy Controls for Information Systems and Organizations	https://doi.org/10.6028/NIST.SP.800-53r5
An Introduction to Information Security	https://doi.org/10.6028/NIST.SP.800-12r1

Otros recursos complementarios [Videos, enlaces, otros. Incluir una fila por cada recurso]	
Nombre	
BCRA COMUNICACIÓN “A” 7319 Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de	https://www.bcra.gob.ar/pdfs/comytexord/A7319.pdf

información y recursos asociados para las entidades financieras. Adecuaciones.	