

PROGRAMA DE LA MATERIA

SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA DE SISTEMAS

1. IDENTIFICACIÓN

Facultad: Facultad de Ciencias Económicas, UNICEN

Plan de Estudios: Cincuentenario

Nombre de la Materia: Seguridad de la información y auditoría de sistemas

Ubicación: Cuarto Año

Carga Horaria: 40 horas

2. EQUIPO DOCENTE

El equipo docente estará integrado por:

- MBA. Oscar Nielsen. Coordinador de la materia.
- Dra. Sandra González Cisaro
- Ing. Norma Montero

3. CANTIDAD DE ALUMNOS

Se prevé hasta 50 alumnos organizados en una comisión.

4. MARCO REFERENCIAL

Ubicación en el Plan de Estudios: Carrera Licenciatura en Gestión Tecnológica. Cuarto Año. Ciclo Profesional (Resolución de Consejo Académico Nro. 176/2018).

Relación con materias anteriores, posteriores y simultáneas: Por la temática a abordar en el curso de la Asignatura, tiene como materia correlativa a L4005 Gobernanza de Tecnología de la Información.

Contenidos mínimos previstos en el Plan de Estudios:

Seguridad en los sistemas de información. Evaluación y gestión de riesgo. Activos de información. Gestión de la seguridad de la información. Auditoría de sistemas. Metodología de auditoría de sistemas. Normativa y buenas prácticas. Técnicas de auditoría asistidas por computadora (CAAT). Prevención y detección de fraude digital.

Conocimientos y habilidades, mínimos y básicos que debiera poseer el alumno para cursar la asignatura:

El alumno deberá conocer los aspectos de infraestructura tecnológica que sustentan los sistemas de información y la problemática relacionada con la adquisición e implementación de tecnologías de la información dentro de una organización. Además conocer los procesos básicos y la estructuración de una organización. A esta altura se prevé también que el alumno posea un razonable dominio de las herramientas informáticas y también del idioma inglés que le permite acceder a contenidos de carácter tecnológico.

Aportes a la formación del futuro profesional:

Conocer las principales vulnerabilidades y amenazas de los sistemas de información.

Conocer estrategias y herramientas disponibles para proteger los activos de información de las organizaciones.

5. OBJETIVOS

Se espera que el alumno pueda:

- Comprender las vulnerabilidades y amenazas propias de los sistemas de información, y su impacto en los negocios.
- Conocer las principales tecnologías y herramientas para proteger los recursos de la información.
- Comprender las buenas prácticas disponibles para una adecuada gestión de la seguridad de la información.
- Adquirir el lenguaje técnico de los conceptos básicos y avanzados que le permitan al estudiante una comunicación efectiva con los profesionales de seguridad y auditoría informática.

6. PROPUESTA DE CONTENIDOS

Unidad 1. Fundamentos de seguridad de la información

Vulnerabilidad de los sistemas de información. Riesgos y amenazas. Activos de información. Valor de negocios de la seguridad y el control. Controles de los sistemas de información. Evaluación de Riesgos. Principios de la seguridad de la información. Delitos informáticos. Ciberseguridad. Diferencia entre Seguridad de la información y ciberseguridad.

Unidad 2. Tecnologías y herramientas para proteger recursos de información

Herramientas de la administración de la seguridad. Defensas de seguridad. Seguridad física. Seguridad lógica. Seguridad humana. Criptografía. Infraestructura de clave pública. La seguridad de la información en los procesos de desarrollo de software.

Unidad 3. Gestión de la Seguridad de la Información

Organización y estructura del área de Seguridad: áreas, funciones y responsabilidades, perfiles, criterios de organización. Métricas y performance. Análisis y gestión del riesgo. Planificación de recuperación de desastres y planificación de continuidad de negocios

Unidad 4. Política de seguridad de la información

Política de seguridad. Organización de la seguridad. Clasificación y control de activos. Seguridad del Personal. Principales procesos cubiertos por una política de seguridad. Frameworks aplicables.

Unidad 5. Auditoría de SI/TI

Auditoría en General: Definición y objetivo de la auditoría. Riesgo y control interno. Principios fundamentales de la auditoría. Tipos de auditoría.

Auditoría de Sistemas de Información/Tecnologías de la Información (TI): Definición y alcance. Objetivos específicos. Fases generales. El informe de Auditoría.

Tipos de Sistemas de Información/Tecnologías de la Información (TI). Áreas de Aplicación en un Contexto Organizacional. Objetivos de la Auditoría en Sistemas de Información/TI.

Metodologías y estándares para la auditoría de seguridad de la información.

Unidad 6. Prevención y detección de fraude digital

Fraude. Proceso del defraudador. Perfil del defraudador. Programas de prevención y detección de fraude. Técnicas de análisis digital. Evidencia digital.

Unidad 7. Tendencias tecnológicas e impacto en la seguridad de la información

Principales tendencias tecnológicas. Riesgos. Impacto en la seguridad de la información. Tratamiento.

7. PROPUESTA METODOLÓGICA

Esquema de dictado:

3 (tres) horas semanales divididas en 1 bloque de 2 (dos) horas presenciales, cumplimentando la carga horaria restante con 1 (una) hora, a desarrollarse a través del entorno virtual.

Metodología de dictado y Timeline de clase:

- La metodología contempla aspectos presenciales y virtuales
- Lectura previa o visualización de un video sobre la temática por parte de los alumnos. (se dejará disponible en la plataforma virtual). Se estima que esto le demandará unos 60 minutos por clase.
- Inicio: (15 primeros) Intercambio con estudiantes respecto de la lectura.
- Desarrollo: (45 - 60 minutos) exposición a cargo del docente
- Artículo: (30 minutos) lectura y actividad a partir de lectura periodística o de revista.
- Cierre: Elaboración de conclusiones sobre los contenidos analizados.
- Periódicamente se realizan actividades de repaso de temas desarrollados utilizando herramientas de gamificación (con plataformas como Kahoot o Quizizz) para su evaluación y puesta en común.

Actividad en CAMPUS Virtual

- Contenido disponible en la plataforma
- Actividad identificada por unidad temática (ej: preguntas de autoevaluación)

Actividades vivenciales

- Visitas a organizaciones para resolver problemas: empresas de Software, Municipio, Universidad, Ong´s, etc
- Invitados especializados en la temática.

Comunicación con los docentes

- Los docentes comunicarán las cuestiones relativas a la cursada durante el dictado de clases o mediante la utilización de Novedades de la Plataforma de Educación Virtual (CAMPUS VIRTUAL). Por esto se recomienda que mantenga actualizada su dirección de email en su perfil de usuario de dicha plataforma.
- Las consultas se realizan en clase o en los foros establecidos en la plataforma CAMPUS VIRTUAL. En caso que el alumno tenga alguna cuestión de tipo personal se podrá comunicar con el docente vía el email que él mismo le haya indicado.
- Si un alumno tuviera una situación particular que discutir con el docente lo podrá hacer mediante comunicación por email a la dirección que le hubiera dado el docente al comienzo de la cursada.

8. CONDICIONES DE APROBACIÓN DE LA MATERIA

Las condiciones de aprobación de la materia son las establecidas en la resolución del Consejo Académico 080/2017 con las modificaciones de la RCA 140/2019.

Como indica dicha resolución la condición de promoción o de regular se establece al final de la cursada de acuerdo al cumplimiento que el alumno haya obtenido a lo largo de la cursada.

Para poder promocionar:

Los alumnos deberán:

- Asistencia mínima obligatoria del 60%, computable sobre la totalidad de las clases efectivas.
- Aprobar el parcial con una nota promedio de 6 (seis) o más.
- Aprobar la parte práctica con 6 (seis) o más.
- Respecto de la práctica es fundamental la entrega en tiempo y forma de cada uno de los trabajos establecidos.
- Aprobar la evaluación integradora con 6 (seis) o más.

IMPORTANTE: Todos los alumnos en condición de promocionar deberán realizar la instancia integradora. Los alumnos que cumplan con todo lo previsto anteriormente promocionarán la materia.

Aquellos alumnos que hubieran sacado menos de 6 (seis) o no hubieran realizado la evaluación integradora accederán a rendir el final en carácter de alumnos regulares.

La posibilidad de rendir examen final (solo se evaluará la parte teórica) como alumno regular se pierde luego de 3 años de cursada la materia o luego de haber rendido dicho final en 4 (cuatro) oportunidades.

Condición de Regular:

Los alumnos que no hayan alcanzado a cumplimentar los requisitos para la cursada por promoción y tengan un promedio de 4 ó 5 continuaran bajo el régimen de cursada regular con examen final.

De todas formas deberán cumplimentar como mínimo lo siguiente.

- Asistencia mínima obligatoria del 60%, computable sobre la totalidad de las clases efectivas.
- Aprobar la parte práctica con 4 (cuatro) o más
- Tener 4 ó 5 de promedio en las evaluaciones parciales.

Recuperatorio Global:

Los alumnos que no hayan obtenido la nota suficiente o hayan tenido una ausencia sin justificación en los parciales deberán rendir un recuperatorio global y obtener 4 ó más para acceder a la condición de regular además de cumplimentar los requisitos de asistencia y de la práctica.

9. BIBLIOGRAFÍA

- Samaniego, E., Ponce, J. (2021) Fundamentos de seguridad informática. Editorial Grupo Compás.

- Costas Santos, Jesús. Gestión de la seguridad informática en la empresa. (2021). RA-MA Editorial.
- Silvia Clara Menéndez Arantes. Auditoría de seguridad informática: Curso práctico (2022). RA-MA Editorial.
- Seguridad Informática. Jesús Costas Santos. Editorial Ra-Ma. 2014
- Seguridad de la Información. Edgar Vega Briceño. Ed. 3 Ciencias. 2021
- Sistemas de Información Gerencial. Keneth Laudon & Jane P. Laudon. 12º Edición. Prentice Hall. Grupo Editorial Pearson Education. 2016.
- Cybersecurity Student Book. © 2014 ISACA.
- Information Security Governance: Guidance for Information Security Managers. IT Governance Institute. ISBN 978-1-933284-73-6. 2008
- Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking Edgar Vega Briceño. Ed. 3 Ciencias. 2020
- Ciberseguridad. Alejandro Corletti Estrada. 2017.

Material de los sitios:

- isaca.org
- campusvirtual.econ.unicen.edu.ar
- acfe.com
- ted.com
- youtube.com

Herramienta propuesta para traducción de textos en línea:

- <https://translate.google.com/?hl=es&sl=en&tl=es&op=docs>