



UNIVERSIDAD DE GUADALAJARA

Centro Universitario de los Lagos

División de Estudios de la Biodiversidad e Innovación Tecnológica

Departamento de Ciencias Exactas y Tecnología

1. IDENTIFICACIÓN DEL CURSO

Nombre de la materia

Seguridad en Tecnologías de la Información

Clave de la materia:	Horas de teoría:	Horas de práctica:	Total de Horas:	Valor en créditos:
I5643	40	40	80	8

Tipo de curso: (Marque con una X)

C= curso	<input type="checkbox"/>	P= practica	<input type="checkbox"/>	CT = curso-taller	<input checked="" type="checkbox"/>	M= módulo	<input type="checkbox"/>	C= clínica	<input type="checkbox"/>	S= seminario	<input type="checkbox"/>
----------	--------------------------	-------------	--------------------------	-------------------	-------------------------------------	-----------	--------------------------	------------	--------------------------	--------------	--------------------------

Nivel en que ubica: (Marque con una X)

L=Licenciatura	<input checked="" type="checkbox"/>	P=Posgrado	<input type="checkbox"/>
----------------	-------------------------------------	------------	--------------------------

Prerrequisitos formales
(Materias previas establecidas en el Plan de Estudios)

Prerrequisitos recomendados (Materias sugeridas en la ruta académica aprobada)

Ninguno

Departamento:

Departamento de Ciencias Exactas y Tecnología (DCET)

Carrera:

Licenciatura en Tecnologías de la información (LTIN)

Área de formación:

Área de formación básica común obligatoria.	<input type="checkbox"/>	Área de formación básica particular obligatoria.	<input type="checkbox"/>	Área de formación básica particular selectiva.	<input type="checkbox"/>	Área de formación especializante obligatoria.	<input checked="" type="checkbox"/>	Área de formación optativa abierta.	<input type="checkbox"/>
---	--------------------------	--	--------------------------	--	--------------------------	---	-------------------------------------	-------------------------------------	--------------------------



UNIVERSIDAD DE GUADALAJARA

Centro Universitario de los Lagos

División de Estudios de la Biodiversidad e Innovación Tecnológica

Departamento de Ciencias Exactas y Tecnología



Historial de revisiones:

Acción: Revisión, Elaboración	Fecha:	Responsable
Elaboración		CUCEA
Revisión y Modificación	Julio 2015	L.I María del Rocío Ramírez Jiménez
Revisión	Enero 2016	L.I María del Rocío Ramírez Jiménez
Revisión	Julio 2016	Mtra. María del Rocío Ramírez Jiménez
Revisión	Enero 2017	Mtra. María del Rocío Ramírez Jiménez
Modificación	Enero 2019	Mtra. María del Rocío Ramírez Jiménez
Revisión	Enero 2020	Mtra. María del Rocío Ramírez Jiménez
Modificación	Enero 2021	Mtra. María del Rocío Ramírez Jiménez
Revisión	Enero 2023	Mtra. María del Rocío Ramírez Jiménez

Academia:

Cómputo

Aval de la Academia:

Marzo 2023		
Nombre	Cargo Presidente, Secretario, Vocales	Firma
Mtra. Larisa Elizabeth Lara Ramírez	Presidente	
Dra. Auria Lucia Jiménez Gutiérrez	Secretario	



UNIVERSIDAD DE GUADALAJARA

Centro Universitario de los Lagos

División de Estudios de la Biodiversidad e Innovación Tecnológica

Departamento de Ciencias Exactas y Tecnología

2. PRESENTACIÓN

El curso-taller de Seguridad Informática está caracterizado cubrir temas fundamentales de la Seguridad en las empresas.

3. OBJETIVO GENERAL

Conocer los conceptos sobre Seguridad Informática, revisando modelos existentes, aprendiendo sus fortalezas y sus debilidades. Además, podrán conocer las leyes su ámbito y aplicabilidad.

En este curso se pretende preparar profesionales capaces de dar respuesta a las distintas necesidades que se plantean en las sociedades modernas en el área de la seguridad en informática.

4. OBJETIVOS ESPECÍFICOS

1. Comprenderá los conceptos básicos de la seguridad sus diferentes tipos y propiedades a través de la implementación de actividades prácticas.
2. Implementará sus conocimientos sobre estrategias de seguridad de la información y las aplicará en el desarrollo fundamentando sus objetivos y pertinencia del mismo.
3. Tendrá conciencia de los sistemas de seguridad, la identificación, autenticación, el control de acceso y su aplicación e importancia dentro de los sistemas de información, así como también se abordará la importancia de conocer los riesgos que existen no solo determinados por su metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.
4. Reconocer los sistemas de detección de intrusos, así como los sistemas de protección, sus cualidades y cuando se pueden utilizar cada uno, además se hablará de la criptografía y como esta puede ser utilizada. De igual manera se abordarán temas sobre delitos informáticos y como esto puede impactar a la sociedad en general, se implementará un análisis hecho por los estudiantes para tener en claro la diversidad que existe en ellos y como combatirlos tomando como punto de referencia nuestro país.
5. Realización de un análisis completo de una empresa o institución en la cual se evaluarán los niveles de seguridad de sus datos, así como sus procesos informáticos, evaluando la situación actual de la misma y presentando un plan de seguridad eliminando la vulnerabilidad de pérdida de la información



5. CONTENIDO

Temas y Subtemas

MÓDULO I. CONCEPTOS DE SEGURIDAD

- 1.1 Introducción a la seguridad informática.
- 1.2 Conceptos de seguridad de la información.
 - 1.2.1 La criptografía
 - 1.2.2 Criptoanálisis
 - 1.2.3 Criptosistema
- 1.3 Fraudes y delitos informáticos
 - 1.3.1 Tipos de delitos informáticos
 - 1.3.1.1 Fraudes
 - 1.3.1.2 El sabotaje informático.
 - 1.3.1.3 El espionaje informático y el robo de software
 - 1.3.1.4 Gestión de seguridad
- 1.4 Administración eficaz de la seguridad informática.

MÓDULO II. DEFINICIÓN DE UN MODELO PARA LA SEGURIDAD

- 2.1 Alcance y estudio de la seguridad de información.
- 2.2 Estrategia de seguridad de información
- 2.3 Objetivos de la estrategia de seguridad de información.
- 2.4 Desarrollo de una estrategia de seguridad de información
- 2.5 Recursos de la estrategia.

MÓDULO III. DIAGNOSTICO INICIAL DE LA SEGURIDAD CON BASE EN LA NORMA ISO/IEC 27001

- 3.1 Cuestionario-entrevista de recolección de la información
- 3.2 Incidentes iniciales identificados (Hallazgos)
- 3.3 Definición de procedimientos en base a la norma ISO/IEC 27001
- 3.4 Implementación de medidas y procedimientos ISO/IEC 270001

MÓDULO IV. PROPUESTA DE SEGURIDAD INFORMÁTICA

- 4.1 Identificación de riesgos
- 4.2 Clasificación y valoración de magnitud de daño de los elementos de información
- 4.3 Valoración de probabilidad de amenaza
- 4.4 Definición de matriz de análisis de riesgos



6. TAREAS, ACCIONES Y/O PRÁCTICAS DE LABORATORIO

- a) Aprendizaje grupal y autogestivo.
- b) Investigación grupal e individual.
- c) Integración individual de productos de aprendizaje (reportes de lectura, ensayos, trabajos de investigación, exposición de temas, prácticas de algunos temas, portafolio, entre otros).
- d) Exposición por parte del maestro sobre los temas (pizarrón, diapositivas, etc.).

7. BIBLIOGRAFÍA BÁSICA (Preferentemente ediciones recientes, 5 años)

1	Seguridad cibernética: hackeo ético y programación defensiva. Gabriel Sánchez Cano. Ciudad de México. Alfaomega Grupo Editor. 2018
2	Introducción a la seguridad informática. Gabriel Baca Uribia. Primera edición. México D.F. Grupo editorial Patria. 2016
3	Hacking hardware y firmware. Antonio Ramos Varón, Carlos Alberto Barbero Muñoz, Yago Fernández Hansen, Yanko Vasilev Kóley, Raúl Sánchez Lorente. Madrid. RA MA. 2016
4	Gestión de incidentes de seguridad Informática. Esther Chicano Tejeda (2014). IC Editorial.

8. BIBLIOGRAFÍA COMPLEMENTARIA (Preferentemente ediciones recientes, 5 años)

1	Criptografía, protección de datos y aplicaciones. Guía para estudiantes y profesionales. Amparo Fuster Sabater, Luis Hernández Encinas, Agustín Martín Muñoz, Ernesto Montoya, Jaime Muñoz. (2013)
2	Redes y seguridad. Matiaz Katz. Alfaomega. (2013)
3	Computer Security, protecting digital resources. Robert C. Newman. Jones and Bartlett (2010)
4	Ethical Hacking, Un enfoque metodológico para profesionales
5	Ezequiel Sallis, Claudio Caracciolo, Marcelo Rodriguez(2010), Alfaomega.
6	Computación forense, descubrimiento los rastros informáticos. Jeimy J. Cano M (2009), Alfaomega.



UNIVERSIDAD DE GUADALAJARA

Centro Universitario de los Lagos

División de Estudios de la Biodiversidad e Innovación Tecnológica

Departamento de Ciencias Exactas y Tecnología

7	Ingeniería del Software Un enfoque práctico Pressman Roger S (2005) McGraw-Hill
8	Autoria Informatica Piattini M (2001) Alfaomega

9. CRITERIOS Y MECANISMOS PARA LA ACREDITACIÓN

Acreditación: Para tener derecho a examen ordinario el alumno deberá cumplir con un 80% de las asistencias.
Si el alumno llega a reprobar la materia por cuestiones de calificación, puede presentar examen extraordinario para poder aprobarla, de no ser así, tendrá que repetir curso.
Asimismo, esta materia puede ser acreditada por competencias para lo cual el alumno deberá registrar su solicitud en el departamento al cual pertenece la materia (Departamento de ciencias Exactas y Tecnología), de acuerdo con el calendario escolar vigente. Esta materia también puede ser sujeta a revalidación, acreditación o convalidación de acuerdo con la normatividad vigente.

10. EVALUACIÓN Y CALIFICACIÓN

Unidad de Competencia	Porcentaje
Proyecto final	25%
Examen Ordinario (2)	20%
Tareas	15%
Practicas	25%
Exposición, Foros	15%
Total	100%

11. ATRIBUTOS DEL EGRESADO RELACIONADOS CON EL PROGRAMA DE ESTUDIOS

1. Identificar, formular y resolver problemas de ingeniería aplicando los principios de las ciencias básicas e ingeniería.
2. Aplicar, analizar y sintetizar procesos de diseño de ingeniería que resulten en proyectos que cumplen las necesidades especificadas.
3. Reconocer la necesidad permanente de conocimiento adicional y tener la habilidad para localizar, evaluar, integrar y aplicar este conocimiento adecuadamente.
4. Trabajar efectivamente en equipos que establecen metas, planean tareas, cumplen fechas límite y analizan riesgos e incertidumbre