## 1. Identificación del curso

| Seguridad en la información | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Programa educativo** | | | | **Departamento de adscripción** | | | |
| Ingeniería en Computación | | | | Departamento de Ingenierías | | | |
| **Área de formación** | | | | **Tipo de Unidad de Aprendizaje** | | | |
| Especializante obligatoria | | | | Curso - Taller | | | |
| **Carga horaria** | | | | | | **Créditos** | **Clave** |
| **Teoría** | 40 | **Práctica** | 40 | **Total** | 80 | 8 | IL368 |
| **Modalidad de Enseñanza - Aprendizaje** | | | | **Prerrequisito** | | | |
| Presencial | | | | *No aplica* | | | |
| **Academia** | | | | **Profesor responsable** | | | |
| Ciencias computacionales | | | | Francisco Javier Ulloa Cortez | | | |
| **Elaboró / Modificó** | | | | **Fecha de elaboración / modificación** | | | |
| Francisco Javier Ulloa Cortez / Horacio Gómez Rodríguez | | | | 15 de septiembre de 2024 | | | |

## 2. Competencias que abonan al perfil de egreso

| Transversal | Disciplinar | Profesional |
|---|---|---|
| Reconoce sus responsabilidades éticas y profesionales para actuar con rigor en su desarrollo como ingeniero;<br><br>Posee habilidades de trabajo en equipo que le permita desarrollarse como líder de proyectos en su campo profesional o integrarse a un grupo ya establecido;<br><br>Posee habilidades de aprendizaje autogestivo que le permita incrementar sus conocimientos en distintas áreas de interés; | Diseña y administra redes de computadoras y gestiona la garantía y seguridad de sistemas informáticos;<br><br>Posee capacidad de razonamiento crítico, lógico y matemático para resolver problemas dentro de su área de estudio a través de modelos abstractos que reflejen situaciones reales. | Diseña sistemas de software y de información, implementando arquitecturas, infraestructuras y características de seguridad, para dar solución a problemáticas reales<br><br>Implementa tecnologías de redes de computadoras, funcionalidades y estructuras para diseñar e integrar aplicaciones basadas en ellas.<br><br>Se forma con ética y responsabilidad, en búsqueda de la calidad y la innovación tecnológica en las organizaciones. |

## 3. Saberes previos

Ética y legislación, Cultura de la paz, Arquitectura de computadoras, Redes de computadoras, Administración de redes

## 4. Presentación de la unidad de aprendizaje

La asignatura Seguridad en la información pretende lograr que el estudiante de ingeniería en computación reconozca la importancia de la protección de los activos de información en una organización; que cuente con los conocimientos para identificar los riesgos de la seguridad de la información y que estos sean conocidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible y eficiente; lo anterior con la aplicación de una serie de políticas, procedimientos e instrucciones específicas para conservar la confidencialidad, integridad y disponibilidad de la información.

## 5. Objetivo de aprendizaje

El alumno es capaz de detectar, identificar y disminuir los riesgos y vulnerabilidades a los que se encuentran expuestos los activos de información de una organización; conoce y aplica las mejores prácticas y estándares internacionales relacionados con la seguridad de la información; todo lo anterior de forma ética y responsable.

## 6. Competencia general de la unidad de aprendizaje

SI.46 Comprender e implementar arquitecturas, infraestructuras y sistemas seguros.

**Valores y actitudes**

Asume una actitud positiva, participativa y proactiva en cuanto a los contenidos que va conociendo. Demuestra disposición y colaboración ante las actividades que le implica explicar la información que ha asimilado. Práctica los valores de orden, justicia, responsabilidad e integridad.

**8. Elementos de competencia**

| **Bloque No. I: Introducción a la seguridad de la información** | |
|---|---|
| **Sub-competencia** | Aprende los conceptos básicos de ciberseguridad para proteger la vida digital personal y obtiene información sobre los desafíos de seguridad a los que se enfrentan las organizaciones actualmente |
| **Cognitivos (Contenido)** | |
| Conoce y aplica:<br>• Concepto y evolución de la seguridad informática<br>• Importancia de la protección de los activos de información<br>• Normativa de la seguridad de la información<br>• Principios indispensables de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad | |
| **Procedimentales** | |
| Desarrolla habilidades:<br>• Prácticas<br>• Técnicas<br>• De investigación<br>Que le permitan adentrarse a las problemáticas cotidianas que pueden requerir la implementación de seguridad de la información. | |
| **Estrategias didácticas** | |
| • Indagación sobre conocimientos previos.<br>• Promoción de la comprensión mediante la organización de información.<br>• Análisis de casos.<br>• Exposición por parte del profesor.<br>• Participación del estudiante. | |

| **Criterios de desempeño** | **Producto esperado** | **Sesiones estimadas** |
|---|---|---|
| Participación en actividades individuales y grupales.<br>Presentación de organizadores gráficos de información.<br>Participación en sesiones presenciales o síncronas y actividades en plataforma. | Glosario de seguridad de la información, reportes escritos, documentaciones. | 20* |
| Área de conocimiento | Tecnologías de la información y comunicación, seguridad de la información | |

** Una sesión equivale a una hora*

| **Bloque No. II Amenazas, vulnerabilidades y ataques a los activos de información** | |
|---|---|
| **Sub-competencia** | Conoce los tipos de amenazas y vulnerabilidades a la seguridad de la información más comunes, algunos métodos para su detección, control y herramientas para evitarlos. |
| **Cognitivos (Contenido)** | |
| Conoce e identifica:<br>• Fuentes y tipos de amenazas<br>• Naturaleza y tipos de vulnerabilidades<br>• Métodos y técnicas de ataques e intrusión a redes y sistemas<br>• Mecanismos y herramientas para la protección de los datos | |
| **Procedimentales** | |
| Aplica procedimientos de:<br>• Detección<br>• Análisis<br>• Identificación<br>Que le permitan establecer elementos de protección de amenazas para prevenir y mitigar posibles ataques | |
| **Estrategias didácticas** | |
| • Exposición por parte del profesor.<br>• Participación del estudiante. | |

- Resolución de prácticas de laboratorio
- Exploración de recursos multimedia en línea

| Criterios de desempeño | Producto esperado | Sesiones estimadas |
|---|---|---|
| Participación en actividades individuales y grupales.<br>Realización correcta de prácticas de laboratorio<br>Resolución de ejercicios y casos prácticos | Reportes de prácticas de laboratorio<br>Reportes de resolución de ejercicios | 30* |
| Área de conocimiento | Tecnologías de la información y comunicación, seguridad de la información | |

** Una sesión equivale a una hora*

| Bloque No. III: Políticas, lineamientos y controles de seguridad de la información | |
|---|---|
| **Sub-competencia** | Conoce e implementa un conjunto de buenas prácticas orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información que maneja una organización |

**Cognitivos (Contenido)**

Conoce y aplica:

- Políticas generales
- Gestión de los activos de información
- Seguridad física y del entorno
- Control de accesos
- Seguridad en las operaciones
- Seguridad en las comunicaciones
- Infracciones a las Políticas de seguridad

**Procedimentales**

Aplica procedimientos de:

- Comprensión
- Organización de información
- Identificación de riesgos
- Mejora continua

Que le permitan implementar buenas prácticas relacionadas con la seguridad de la información en las organizaciones.

**Estrategias didácticas**

- Exposición por parte del profesor.
- Participación del estudiante.
- Resolución de prácticas de laboratorio
- Selección y aplicación de controles de seguridad

| Criterios de desempeño | Producto esperado | Sesiones estimadas |
|---|---|---|
| Participación en actividades individuales y grupales.<br>Realización correcta de prácticas de laboratorio<br>Resolución de ejercicios y casos prácticos | Política general de la seguridad de la información base<br>Inventario de activos de la información típicos en una organización | 30* |
| Área de conocimiento | Tecnologías de la información y comunicación, seguridad de la información | |

** Una sesión equivale a una hora*

## 9. Recursos requeridos

- Computadora, proyector
- Bibliografía básica
- Herramientas y recursos públicos en la Web
- Plataforma LMS
- Recursos electrónicos
- Prácticas y laboratorios

10. **Evaluación y acreditación de la unidad de aprendizaje**

- Actividades individuales 20%
- Actividades en equipo 20%
- Prácticas de laboratorio 30%
- Exámenes 30%

11. **Referencias (APA)**

**Básica**

Moisés, T. P. (2018). Administración y Seguridad en Redes de Computadoras. Ciudad de México: Alfaomega.

Velasco, M. A. C., Lerma, L. B., & Serrano, D. C. (2023). Ciberseguridad paso a paso. Anaya Multimedia.

**Complementaria**

Organización Internacional de Normalización (2022) *Seguridad de la Información, ciberseguridad y protección a la privacidad (*ISO 27001:2022). https://www.iso.org/standard/27001

Normalización y Certificación NYCE, S.C. (2015) Tecnologías de la información, técnicas de seguridad, Sistemas de Gestión de Seguridad de la información (NMX-I-27001-NYCE-2015). https://estandaresnyce.com.mx/producto/nmx-i-27001-nyce-2015-tecnologias-de-la-informacion-tecnicas-de-seguridad-sistemas-de-gestion-de-seguridad-de-la-informacion-requisitos-cancela-a-la-nmx-i-27001-nyce-2009/

Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la Información y comunicación, y la seguridad de la información en la administración pública federal, Presidencia de la Republica; Estados Unidos Mexicanos; DOF 06/09/2011; [consultado el 15 de mayo del 2024]; disponible en versión HTML en internet: https://www.dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021

**Sitios web**

Cisco Networking Academy https://skillsforall.com/es/

12. **Campo de aplicación profesional**

El profesional en esta materia se puede desempeñar como gerente de la seguridad de la información de la organización o bien como parte del grupo estratégico de seguridad de la información; se encarga de establecer, cumplir y hacer cumplir las políticas de seguridad de la información, y proporcionar apoyo especializado al personal de la institución.

13. **Perfil docente**

El docente de esta materia deberá ser un profesionista con formación en las áreas de la computación, comunicaciones o informática; capaz de motivar a la investigación y la resolución de problemas, con dominio de hardware y software, habilidades para transmitir sus conocimientos y enseñar de forma interactiva propiciando en los alumnos el autoaprendizaje.

CENTRO UNIVERSITARIO DE LOS ALTOS
DIVISIÓN DE CIENCIAS AGROPECUARIAS E INGENIERÍAS
DEPARTAMENTO DE INGENIERÍAS

| | |
|---|---|
| **Dr. Alejandro Pérez Larios**<br>Jefe de departamento de ingenierías | **Mtro. Fernando Cornejo Gutiérrez**<br>Presidente de academia |