Universidad Estatal de Sonora
Secuencia Didáctica

Curso: Seguridad e Integridad de la Información **Clave:** 061CP046	**Horas aula:** 2 **Horas virtuales:** 2
Antecedentes:	**Horas laboratorio:** 0 **Horas independientes:** 1

Competencia del área:	**Competencia del curso:**
Desarrollar software y servicios de soporte técnico y redes, con la finalidad de solucionar problemas y agilizar procesos en la toma de decisiones en empresas públicas y privadas, bajo estándares de calidad nacional e internacional, a través del análisis de problemas, comunicación, liderazgo e innovación.	Formular un sistema de gestión de seguridad de la información, aplicando normas y leyes sobre seguridad definidos por organismos e institutos como ISO y IETF para garantizar la confidencialidad, integridad y disponibilidad de la información de los sistemas informáticos utilizados dentro de las diferentes áreas de una organización demostrando dominio de estrés, manejo de relaciones interpersonales y liderazgo.

Elementos de competencia:

1. Identificar los métodos de cifrado, de autenticación y seguridad de la información para considerarlos al elaborar un sistema de gestión de seguridad de la información, aplicando normas y leyes sobre seguridad definidos por organismos e institutos como ISO y IETF dentro de las diferentes áreas de una organización demostrando manejo de relaciones interpersonales y liderazgo.
2. Describir un cortafuegos, red privada virtual, sistemas de detección de intrusos y los protocolos de seguridad en redes para considerarlos al elaborar un sistema de gestión de seguridad de la información, aplicando normas y leyes sobre seguridad definidos por organismos e institutos como ISO y IETF dentro de las diferentes áreas de una organización demostrando manejo de relaciones interpersonales y liderazgo.
3. Formular un sistema de gestión de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información dentro de las diferentes áreas de una organización, considerando las leyes y normas sobre la seguridad aplicándolas como lo definen los organismos e institutos como ISO y IETF, realizándolo con responsabilidad y enfoque a la calidad.

Perfil del docente:

Ingeniería en Sistemas, Licenciatura en Informática, Maestría en Ciencias Computacionales, Tecnologías de la Información y Comunicación o afín al Programa Educativo de Ingeniería en Software. Evalúa los procesos de enseñanza y de aprendizaje con un enfoque por competencias, con una actitud de cambio a las innovaciones pedagógicas. Construye ambientes para el aprendizaje autónomo y colaborativo con apoyo de las tecnologías.

Elaboró: MTRO. JOSE FRANCISCO BECERRA ARENAS	Octubre 2021
Revisó: DRA. CECILIA LÓPEZ CAMACHO	Octubre 2021
Última actualización:	

Autorizó: Coordinación de Procesos Educativos	Noviembre 2021

Elemento de competencia 1: Identificar los métodos de cifrado, de autenticación y seguridad de la información para considerarlos al elaborar un sistema de gestión de seguridad de la información, aplicando normas y leyes sobre seguridad definidos por organismos e institutos como ISO y IETF dentro de las diferentes áreas de una organización demostrando manejo de relaciones interpersonales y liderazgo.

Competencias blandas a promover: Manejo de relaciones interpersonales y liderazgo.

EC1 Fase I: Seguridad de la Información.

Contenido: Seguridad de la información, vulnerabilidades y amenazas de los sistemas de información. Principios de la seguridad. Sistema de Gestión de la Seguridad de la Información (SGSI). Proceso cíclico PHVA o circulo Deming de William Edwards Deming.

EC1 F1 Actividad de aprendizaje 1: Wiki: Glosario de términos sobre los principios de seguridad. Elaborar de manera individual, un glosario de términos con definiciones y ejemplos sobre los principios de la seguridad: confidencialidad, integridad, disponibilidad, autenticidad, no repudio, control de acceso e irrefutabilidad, Seguridad de la información, vulnerabilidades y amenazas de los sistemas de información. Investigar con base en la información proporcionada en el aula, en la sección de recursos, utilizando la bibliografía sugerida y otras fuentes con sustento académico. Integrar la información en el wiki de la plataforma, de acuerdo con las indicaciones del facilitador y exponer responsablemente en el aula. 2 hrs. Aula 2 hrs. Virtuales 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes (X) **Recursos:** • Costas Santos, J. (2015). Seguridad y alta disponibilidad . Capítulo I. • Baca Urbina, G. (2016). Introducción a la seguridad informática . Capítulo I. **Criterios de evaluación de la actividad:** • Rúbrica de glosario • Rúbrica de Wiki
EC1 F1 Actividad de aprendizaje 2: Exposición sobre Sistema de Gestión de la Seguridad de la Información. Exponer en equipo de forma responsable en el aula, sobre el Sistema de Gestión de la Seguridad de la Información (SGSI), fortaleciendo las relaciones interpersonales, con base en la información proporcionada en el aula, los recursos sugeridos para la actividad u otras fuentes con sustento académico. Identificar y valorar los activos, identificación de los riesgos de seguridad de la información, evaluación de los riesgos, tratamiento de los riesgos y planes de acción, seguimiento y evaluación del SGSI. 2 hrs. Aula 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales ( ) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes (X) **Recursos:** • Fernández Rivero, P. P. y Gómez Fernández, L. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad . Capítulos 1 y 2. • Diseño de un SGSI (Archivo en PDF). **Criterios de evaluación de la actividad:** Rúbrica de exposición oral
EC1 F1 Actividad de aprendizaje 3: Mapa mental	**Tipo de actividad:**

sobre el proceso cíclico PHVA. Elaborar de manera individual, un mapa mental sobre el Proceso cíclico PHVA o circulo Deming de William Edwards Deming, con base en la información proporcionada en el aula, en la sección de recursos, utilizando la bibliografía sugerida y otras fuentes con sustento académico. Presentar en aula para su evaluación y retroalimentación. 2 hrs. Aula 2 hrs. Virtuales 1 hr. Independiente	Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes (X) **Recursos:** Fernández Rivero, P. P. y Gómez Fernández, L. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad . Capítulos 1 y 2. **Criterios de evaluación de la actividad:** Rúbrica de mapa mental
EC1 Fase II: Criptografía y Métodos de Autenticación. **Contenido:** Criptografía, algoritmo de cifrado. Cifrado moderno: Simétrico, Asimétrico. Métodos de Autenticación. Aplicaciones de autenticación. Funciones HASH, SHA-2, SALT, Funciones de derivación de claves (Bcrypt, scrypt, PBKDF2 y Argon2). Firma electrónica y firma digital. Certificados digitales.	
EC1 F2 Actividad de aprendizaje 4: Mapa conceptual sobre Criptografía y cifrado moderno. Elaborar de manera individual, un mapa conceptual sobre la definición de criptografía, historia de la criptografía y el cifadro moderno, con base en la información proporcionada en el apartado de recursos u otras fuentes de sustento académico. Hacer uso de alguna aplicación online o en su software de preferencia y exponer responsablemente en el aula. 2 hrs. Aula 2 hrs. Virtuales 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes (X) **Recursos:** • Costas Santos, J. (2015). Seguridad y alta disponibilidad . Capítulo 5. • Escrivá Gascó, G. (2013). Seguridad informática . Capítulos 4 y 5. **Criterios de evaluación de la actividad:** Rúbrica de mapa conceptual
EC1 F2 Actividad de aprendizaje 5: Exposición sobre criptografía y cifrado moderno. Realizar en equipo, una exposición oral sobre los siguientes temas: Que es un algoritmo de cifrado, cifrado moderno: DES, T.DES, CAST, IDEA, AES Y RC5, asimétrico RSA e Híbridos SSL y TLS, con base en la información proporcionada en el aula, el apartado de recursos u otras fuentes confiables. 2 hrs. Aula 2 hrs. Virtuales	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes ( ) **Recursos:** Costas Santos, J. Seguridad y alta disponibilidad . Capítulo 5. **Criterios de evaluación de la actividad:** Rúbrica de exposición oral

EC1 F2 Actividad de aprendizaje 6: Investigación sobre métodos de autenticación.

Realizar una investigación en equipo, sobre Métodos de Autenticación; Autenticación en redes, elementos de la autenticación y métodos de autenticación, con base en la información proporcionada en el apartado de recursos u otras fuentes confiables.

Investigar los sistemas basados en algo conocido (contraseñas), tarjeta inteligente, biométrica, dispositivos de contraseña de uso único (Token o OPT), Autenticación contextual o de múltiples factores. Aplicaciones de autenticación; Funciones HASH, SHA-2, SALT, Funciones de derivación de claves (Bcrypt, scrypt, PBKDF2 y Argon2). Firma electrónica, firma digital y certificados digitales.

Diseñar una presentación en una aplicación en línea como Powtoon, Prezi, Google Slides u otra, que integre la información investigada y exponer fortaleciendo las relaciones interpersonales en el aula.

2 hrs. Aula
2 hrs. Virtuales
1 hr. Independiente

Tipo de actividad:
Aula (X) Virtuales (X) Laboratorio ( )
Grupal ( ) Individual ( ) Equipo (X)
Independientes (X)

Recursos:

- Costas Santos, J. (2015). Seguridad y alta disponibilidad . Capítulo 5.
- Escrivá Gascó, G. (2013). Seguridad informática . Capítulos 5.

Criterios de evaluación de la actividad:

- Rúbrica de Investigación de Conceptos
- Rúbrica de exposición oral

Evaluación formativa:

- Glosario de términos sobre los principios de seguridad.
- Exposición sobre Sistema de Gestión de la Seguridad de la Información.
- Mapa mental sobre el proceso cíclico PHVA.
- Mapa conceptual sobre Criptografía y cifrado moderno.
- Exposición sobre criptografía y cifrado moderno.
- Investigacción sobre métodos de autenticación.

Fuentes de información

1. Baca Urbina, G. (2016). Introducción a la seguridad informática. Grupo Editorial Patria. https://elibro.net/es/ereader/ues/40458?page=19
2. Costas Santos, J. (2015). Seguridad informática. RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/62452
3. Costas Santos, J. (2015). Seguridad y alta disponibilidad. RA-MA Editorial. https://elibro.net/es/ereader/ues/62477?page=11
4. Díaz, G. (2004). Seguridad en las comunicaciones y en la información. UNED - Universidad Nacional de Educación a Distancia. https://elibro.net/es/lc/ues/titulos/48351
5. Escrivá Gascó, G. (2013). Seguridad informática. Macmillan Iberia, S.A. https://elibro.net/es/lc/ues/titulos/43260
6. Fernández Rivero, P. P. y Gómez Fernández, L. (2018). Cómo implantar un SGSI según UNE-EN

ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. AENOR - Asociación Española de Normalización y Certificación. https://elibro.net/es/lc/ues/titulos/53624

7. Flores Salgado, L. (2015). Derecho informático. Grupo Editorial Patria. https://elibro.net/es/lc/ues/titulos/39404
8. Gómez Vieites, Á. (2015). Seguridad en equipos informáticos. RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/62466
9. Ortega Candel, J. M. (2018). Seguridad en aplicaciones Web Java. RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/106511
10. Salcedo Cifuentes, M. Ortíz Gómez, Y. y Hincapie Saldarriaga, A. F. (2018). La calidad del dato en los sistemas de información de convivencia y seguridad ciudadana. Programa Editorial Universidad del Valle. https://elibro.net/es/lc/ues/titulos/131607

Elemento de competencia 2: Describir un cortafuegos, red privada virtual, sistemas de detección de intrusos y los protocolos de seguridad en redes para considerarlos al elaborar un sistema de gestión de seguridad de la información, aplicando normas y leyes sobre seguridad definidos por organismos e institutos como ISO y IETF dentro de las diferentes áreas de una organización demostrando manejo de relaciones interpersonales y liderazgo.

Competencias blandas a promover: Manejo de relaciones interpersonales y liderazgo.

EC2 Fase I: Cortafuegos.

Contenido: Definición y funcionamiento de un cortafuego. Tipos de cortafuegos. Instalación y configuración de un cortafuego.

EC2 F1 Actividad de aprendizaje 7: Mapa conceptual sobre cortafuegos. Elaborar de manera individual, un mapa conceptual sobre definición y funcionamiento de un cortafuego, tipos de cortafuegos, ejemplos y como se instala y configura un cortafuegos, con base en la información proporcionada en el aula, los recursos recomendados u otras fuentes de sustento académico. Diseñar en alguna aplicación online o en un software de su preferencia y exponer responsablemente fortalenciendo las relaciones interpersonales en el aula. 1 hr. Aula 2 hrs. Virtuales 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes (X) **Recursos:** • Costas Santos, J. (2015). Seguridad y alta disponibilidad . Capítulo 7. • Baca Urbina, G. (2016). Introducción a la seguridad informática . Capítulo 5. **Criterios de evaluación de la actividad:** Rúbrica de mapa conceptual
EC2 F1 Actividad de aprendizaje 8: Practica sobre instalación y configuración de un cortafuego. Realizar en equipo, la práctica de instalación y configuración de un cortafuegos en una computadora, tomar evidencia (impresión de pantalla) para elaborar el reporte de práctica en el formato indicado por el facilitador. Participar en el aula en la revisión del tema. 2 hrs. Aula 2 hrs. Virtuales 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes (X) **Recursos:** Documento realizado en la actividad 7. **Criterios de evaluación de la actividad:** Rúbrica de reporte de práctica

EC2 Fase II: Redes Privadas Virtuales.

Contenido: Definición y tipos de redes privadas virtuales (VPN). Protocolos utilizados en una VPN. Instalación y configuración de una VPN.

EC2 F2 Actividad de aprendizaje 9: Mapa conceptual sobre redes privadas virtuales (VPN).	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( )

Elaborar de manera individual, un mapa conceptual sobre las redes privadas virtuales (VPN), protocolos utilizados y pasos para instalar y configurar una VPN, con base en la información proporcionada en el apartado de recursos u otras fuentes de sustento académico. Diseñar en alguna aplicación online u otra de su preferencia y exponer responsablemente, fortaleciendo las relaciones interpersonales en el aula. 2 hrs. Aula 2 hrs. Virtuales 1 hr. Independiente	Independientes (X) **Recursos:** Costas Santos, J. Seguridad y alta disponibilidad . Capítulo 6. **Criterios de evaluación de la actividad:** Rúbrica de mapa conceptual
EC2 F2 Actividad de aprendizaje 10: Practica sobre instalación y configuración de una VPN. Realizar en equipo, la práctica de instalación y configuración de una red privada virtual, el cliente VPN y el servidor VPN, tomar evidencia (impresión de pantalla) para elaborar el reporte de práctica en el formato indicado por el facilitador. Participar en el aula en la revisión del tema. 2 hrs. Aula 1 hr. Virtual 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes (X) **Recursos:** Documento realizado en la actividad 9. **Criterios de evaluación de la actividad:** Rúbrica de reporte de práctica
EC2 Fase III: Protocolos de Seguridad en las Redes y Sistemas de Detección de Intrusos (SDI). **Contenido:** IPSec. SSL. TLS. SSH. HTTPS. Definición, arquitectura general de un SDI, funcionamiento y tipos. Mecanismo de detección. Implementación de un sistema de detección de intrusos.	
EC2 F3 Actividad de aprendizaje 11: Exposición sobre protocolos de seguridad en las redes. Realizar en equipo, una exposición oral sobre los protocolos de seguridad de redes, con base en la información proporcionada en el apartado de recursos u otras fuentes confiables. Considerar los temas: protocolos de seguridad de redes de datos: IPSec, SSL, TLS, SSH y HTTPS. Diseñar presentación en el software de su preferencia y exponer, fortaleciendo las relaciones interpersonales en el aula. 2 hrs. Aula 2 hrs. Virtuales 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes (X) **Recursos:** Díaz, G. (2004). Seguridad en las comunicaciones y en la información . Unidad 3. **Criterios de evaluación de la actividad:** Rúbrica de exposición oral

EC2 F3 Actividad de aprendizaje 12: Practica sobre protocolo IPSec. Realizar en equipo, una práctica de configuración del protocolo IPSec, seguir los pasos descritos en el material disponible en la sección de recursos, tomar evidencia (impresión de pantalla) para elaborar el reporte de práctica en el formato indicado por el facilitador. Participar en el aula en la revisión del tema. 2 hrs. Aula 1 hr. Virtual 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes (X) **Recursos:** Documento realizado en la actividad 11. **Criterios de evaluación de la actividad:** Rúbrica de reporte de práctica
EC2 F3 Actividad de aprendizaje 13: Infografía sobre sistemas de detección de intrusos. Elaborar de manera individual, una infografía sobre los sistemas de detección de intrusos: Definición, arquitectura general de un SDI, funcionamiento, tipos y mecanismo de detección, con base en la información proporcionada en el apartado de recursos u otras fuentes de sustento académico. Diseñar en alguna aplicación online o en su software de preferencia y exponer fortaleciendo las relaciones interpersonales en el aula. 1 hr. Aula 2 hrs. Virtuales 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes (X) **Recursos:** Costas Santos, J. (2015). Seguridad y alta disponibilidad . Capítulo 6. **Criterios de evaluación de la actividad:** Rúbrica de infografía

Evaluación formativa:

- Mapa conceptual sobre cortafuegos.
- Practica sobre instalación y configuración de un cortafuego.
- Mapa conceptual sobre redes privadas virtuales (VPN).
- Practica sobre instalación y configuración de una VPN.
- Exposición sobre protocolos de seguridad en las redes.
- Practica sobre protocolo IPSec.
- Infografía sobre sistemas de detección de intrusos.

Fuentes de información

1. Baca Urbina, G. (2016). Introducción a la seguridad informática. Grupo Editorial Patria. https://elibro.net/es/ereader/ues/40458?page=19
2. Costas Santos, J. (2015). Seguridad informática. RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/62452
3. Costas Santos, J. (2015). Seguridad y alta disponibilidad. RA-MA

Editorial. https://elibro.net/es/ereader/ues/62477?page=11
4. Díaz, G. (2004). Seguridad en las comunicaciones y en la información. UNED - Universidad Nacional de Educación a Distancia. https://elibro.net/es/lc/ues/titulos/48351
5. Escrivá Gascó, G. (2013). Seguridad informática. Macmillan Iberia, S.A. https://elibro.net/es/lc/ues/titulos/43260
6. Fernández Rivero, P. P. y Gómez Fernández, L. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. AENOR - Asociación Española de Normalización y Certificación. https://elibro.net/es/lc/ues/titulos/53624
7. Flores Salgado, L. (2015). Derecho informático. Grupo Editorial Patria. https://elibro.net/es/lc/ues/titulos/39404
8. Gómez Vieites, Á. (2015). Seguridad en equipos informáticos. RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/62466
9. Ortega Candel, J. M. (2018). Seguridad en aplicaciones Web Java. RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/106511
10. Salcedo Cifuentes, M. Ortíz Gómez, Y. y Hincapie Saldarriaga, A. F. (2018). La calidad del dato en los sistemas de información de convivencia y seguridad ciudadana. Programa Editorial Universidad del Valle. https://elibro.net/es/lc/ues/titulos/131607

Elemento de competencia 3: Formular un sistema de gestión de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información dentro de las diferentes áreas de una organización, considerando las leyes y normas sobre la seguridad aplicándolas como lo definen los organismos e institutos como ISO y IETF, realizándolo con responsabilidad y enfoque a la calidad.

Competencias blandas a promover: Responsabilidad y enfoque a la calidad

EC3 Fase I: Seguridad en los Sitios Web.

Contenido: Definición, vulnerabilidades más comunes, medidas preventivas. Comercio electrónico, seguridad en las transacciones comerciales. Infraestructura de clave pública (PKI). Infraestructura de gestión de privilegios (PMI).

EC3 F1 Actividad de aprendizaje 14: Mapa conceptual sobre seguridad en sitios Web. Elaborar de manera individual, un mapa conceptual la seguridad de los sitios web: Definición, vulnerabilidades más comunes, configuraciones en sitios y/o navegadores web, medidas preventivas; Comercio electrónico, seguridad en las transacciones comerciales; Infraestructura de clave pública (PKI); Infraestructura de gestión de privilegios (PMI), con base en la información proporcionada en el apartado de recursos u otras fuentes de sustento académico. Diseñar en alguna aplicación online o en su software de preferencia y exponer responsablemente en el aula. 1 hr. Aula 2 hrs. Virtuales 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes (X) **Recursos:** • Baca Urbina, G. (2016). Introducción a la seguridad informática . Capítulo 3. • Video: Cómo configurar las opciones de privacidad en los principales navegadores . **Criterios de evaluación de la actividad:** Rúbrica de mapa conceptual
EC3 F1 Actividad de aprendizaje 15: Practica sobre seguridad en sitios web. Realizar en equipo, una práctica de configuración de seguridad en los diferentes navegadores web, seguir los pasos descritos en el material disponible en la sección de recursos y tomar evidencia (impresión de pantalla) para elaborar el reporte de practica en el formato indicado por el facilitador. 1 hr. Aula 1 hr. Virtual 1 hr. Independiente	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes (X) **Recursos:** • Documento realizado en la actividad 14. • Video: Cómo configurar las opciones de privacidad en los principales navegadores . **Criterios de evaluación de la actividad:** Rúbrica de reporte de práctica

EC3 Fase II: Normas, leyes y regulación de los delitos informáticos.

Contenido: Delito informático. Tipo de delitos. Leyes Mexicanas e internacionales sobre delitos informáticos. Ética profesional y Manejo de incidentes. Norma ISO 27001, Norma UIT-T X.509 ISO/CEI 9594-8.

EC3 F2 Actividad de aprendizaje 16: Investigación sobre delitos informáticos.	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X)

Realizar en equipo, una investigación sobre delitos informáticos, definición y ejemplos, descripción y ejemplos de tipos de delitos, relacionados con el contenido, con infracciones de los derechos de autor, con la informática y contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, con base en la información proporcionada en el apartado de recursos u otras fuentes confiables. Participar en la retroalimentación en el aula. 1 hr. Aula 1 hr. Virtual 1 hr. Independiente	Independientes (X) **Recursos:** Flores Salgado, L. Derecho informático . Unidad 3 y 4. **Criterios de evaluación de la actividad:** Rúbrica de investigación de conceptos
EC3 F2 Actividad de aprendizaje 17: Resumen sobre leyes mexicanas e internacionales acerca de delitos informáticos. Realizar en equipo, un resumen sobre las Leyes Mexicanas e internacionales acerca de delitos informáticos; identificar en que artículos se mencionan y qué tipos de delitos informáticos existen, con base en la información proporcionada en el apartado de recursos u otras fuentes confiables. Participar responsablemente en la retroalimentación en el aula. 1 hr. Aula 1 hr. Virtual	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes ( ) **Recursos:** Diseño de un SGSI (Archivo en PDF). **Criterios de evaluación de la actividad:** Rúbrica de resumen
EC3 F2 Actividad de aprendizaje 18: Resumen sobre normas referente a delitos informáticos. Realizar en equipo, un resumen sobre las normas ISO 27001, UIT-T X.509 y ISO/CEI 9594-8, con base en la información proporcionada en el apartado de recursos u otras fuentes confiables. Participar responsablemente en la retroalimentación en el aula. 1 hr. Aula 1 hr. Virtual	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes ( ) **Recursos:** • Flores Salgado, L. (2015). Derecho informático . Unidad 3 y 4. • Fernández Rivero, P. P. y Gómez Fernández, L. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad . Capítulos 1. **Criterios de evaluación de la actividad:** Rúbrica de resumen
EC3 F2 Actividad de aprendizaje 19: Diseñar un sistema de gestión de la seguridad	**Tipo de actividad:** Aula (X) Virtuales (X) Laboratorio ( )

Realizar en equipo, el diseño de un sistema de gestión de la seguridad de la información para una empresa o para una área o departamento, ejerciendo un enfoque a la calidad, considerar las leyes y normas analizadas con anterioridad. Entregar diseño en un documento considerando las indicaciones del facilitador y exponer responsablemente en el aula. 1 hr. Aula 2 hrs. Virtuales	Grupal ( ) Individual ( ) Equipo (X) Independientes ( ) **Recursos:** • Fernández Rivero, P. P. y Gómez Fernández, L. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad . Capítulos 1 y 2. • Diseño de un SGSI (Archivo en PDF). **Criterios de evaluación de la actividad:** • Rúbrica de práctica general • Rúbrica de exposición

Evaluación formativa:

- Mapa conceptual sobre seguridad en sitios Web.
- Práctica sobre seguridad en sitios web.
- Investigación sobre delitos informáticos.
- Resumen sobre leyes mexicanas e internacionales sobre delitos informáticos.
- Resumen sobre normas referente a delitos informáticos.
- Disen~ar un sistema de gestio´n de la seguridad

Fuentes de información

1. Baca Urbina, G. (2016). Introducción a la seguridad informática. Grupo Editorial Patria. https://elibro.net/es/ereader/ues/40458?page=19
2. Costas Santos, J. (2015). Seguridad informática. RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/62452
3. Costas Santos, J. (2015). Seguridad y alta disponibilidad. RA-MA Editorial. https://elibro.net/es/ereader/ues/62477?page=11
4. Díaz, G. (2004). Seguridad en las comunicaciones y en la información. UNED - Universidad Nacional de Educación a Distancia. https://elibro.net/es/lc/ues/titulos/48351
5. Escrivá Gascó, G. (2013). Seguridad informática. Macmillan Iberia, S.A. https://elibro.net/es/lc/ues/titulos/43260
6. Fernández Rivero, P. P. y Gómez Fernández, L. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. AENOR - Asociación Española de Normalización y Certificación. https://elibro.net/es/lc/ues/titulos/53624
7. Flores Salgado, L. (2015). Derecho informático. Grupo Editorial Patria. https://elibro.net/es/lc/ues/titulos/39404
8. Gómez Vieites, Á. (2015). Seguridad en equipos informáticos. RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/62466
9. Ortega Candel, J. M. (2018). Seguridad en aplicaciones Web Java. RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/106511
10. Salcedo Cifuentes, M. Ortíz Gómez, Y. y Hincapie Saldarriaga, A. F. (2018). La calidad del dato en los sistemas de información de convivencia y seguridad ciudadana. Programa Editorial Universidad del Valle. https://elibro.net/es/lc/ues/titulos/131607

11. You Tube. (S.f). www.youtube.com

Políticas	Metodología	Evaluación
Para un adecuado desarrollo de las actividades del curso, quedan definidas las políticas para los estudiantes, que estarán vigentes durante el curso; para las situaciones no contempladas en esta secuencia, se aplicará la decisión tomada entre facilitador y alumnos durante las sesiones y si se presentará algún caso especial, con las autoridades académicas de la UES. El trato entre compañeros y facilitador, deberá ser con el debido respeto, y las clases se impartirán en un ambiente de armonía, participación y excelente actitud. El manejo de la plataforma educativa es indispensable para tomar este curso. Entrar diariamente al curso en la plataforma y revisar el calendario de actividades a desarrollar. El facilitador proporcionará las actividades en un tiempo razonable para consultar, desarrollar y cumplir en tiempo y forma con la entrega de las mismas.	Es responsabilidad del estudiante gestionar los procedimientos necesarios para alcanzar el desarrollo de las competencias del curso. El curso se desarrollará combinando sesiones presenciales y virtuales, así como prácticas presenciales en laboratorios, campos o a distancia en congruencia con la naturaleza de la asignatura. Los productos de las actividades de aprendizaje deberán ser entregados en formato PDF en la plataforma institucional, de acuerdo con los criterios establecidos por el facilitador.	La evaluación del curso se realizará de acuerdo al Reglamento Escolar vigente que considera los siguientes artículos: ARTÍCULO 27. La evaluación es el proceso que permite valorar el desarrollo de las competencias establecidas en las secuencias didácticas del plan de estudio del programa educativo correspondiente. Su metodología es integral y considera diversos tipos de evidencias de conocimiento, desempeño y producto por parte del alumno. ARTÍCULO 28. Las modalidades de evaluación en la Universidad son: I. Diagnóstica permanente, Entendiendo esta como la evaluación continua del estudiante durante la realización de una o varias actividades; II. Formativa, siendo esta, la evaluación al alumno durante el desarrollo de cada elemento de competencia; III. Sumativa es la evaluación general de todas y cada una de las actividades y evidencias de las secuencias didácticas sólo los resultados de la evaluación sumativa tienen efectos de acreditación y serán reportados al departamento de registro y control escolar. ARTÍCULO 29. La evaluación sumativa será realizada tomando en consideración de manera conjunta y razonada, las evidencias del desarrollo de las competencias y los aspectos relacionados con las actitudes y valores logradas por el alumno. ARTÍCULO 30. Los resultados de la evaluación expresarán el grado

		de dominio de las competencias, por lo que la escala de evaluación contemplará los niveles de: I. Competente sobresaliente; II. Competente avanzado; III. Competente intermedio; IV. Competente básico; y V. No aprobado. El nivel mínimo para acreditar una asignatura será el de competente básico. Para fines de acreditación los niveles tendrán un equivalente numérico conforme a lo siguiente: Competente sobresaliente 10 Competente avanzado 9 Competente intermedio 8 Competente básico 7 No aprobado 6 ARTÍCULO 31. Para lograr la acreditación de las competencias comprendidas en las secuencias didácticas de las asignaturas del programa educativo, el alumno dispondrá de los siguientes medios: I. La evaluación sumativa, mínimo 7, competente básico; II. La demostración de competencias previamente adquiridas; III. Por convalidación, revalidación o equivalencia. ARTÍCULO 32. Los resultados de la evaluación sumativa serán dados a conocer a los alumnos, en un plazo no mayor de cinco días hábiles después de concluido el proceso. ARTÍCULO 33. En caso de que el alumno considere que existe error u omisión en el registro de evaluación sumativa, podrá

		presentar solicitud por escrito ante el director de la unidad académica dentro de los cinco días hábiles siguientes contados a partir de la fecha de publicación de los resultados, quien en igual termino emitirá una respuesta.