Universidad Estatal de Sonora
Secuencia Didáctica

Curso: SEGURIDAD E INTEGRIDAD DE LA INFORMACION **Clave:** COM31C1V	**Horas aula:** 0
Antecedentes:	**Horas plataforma:** 4

Competencia del área:	**Competencia del curso:** Emplear los sistemas de seguridad en redes, para la implementación y configuración de una red de datos que permitan enlazar las diferentes áreas de la organización, garantizando la seguridad de la información, utilizando estándares de organismos como ISO/ IEC y las normas RFCs (Request For Comments) con un sentido de innovación y trabajo en equipo.

Elementos de competencia:

1. Describir los algoritmos y protocolos de seguridad, para implementarlo en la configuración de una red de comunicación, considerando los protocolos y estándares de organismos internacionales como ISO/ IEC y las normas RFCs (Request For Comments) con una gran capacidad de análisis y toma de decisiones.
2. Implementar cortafuegos para garantizar la seguridad de la información en una red de comunicación, considerando los protocolos y estándares de organismos internacionales como ISO/ IEC y las normas RFCs (Request For Comments).

Perfil del docente:

Licenciatura en Informática, Ingeniero en Software o afín, preferentemente con Maestría en las áreas de Ingeniería de Software, Sistemas Computacionales o afín. Deberá contar con formación pedagógica en educación virtual; dominio de las tecnologías de información y comunicación para el uso en educación a distancia y en especial de las herramientas del entorno virtual o plataforma tecnológica; dominio de la educación por competencias; dominio de técnicas de aprendizaje activo y autorregulado, colaborativo y basado en problemas para centrar el aprendizaje en el estudiante; habilidad para motivar y guiar procesos de aprendizajes autónomos.

Elaboró: DEBORA BELTRAN VALENZUELA	Octubre 2021
Revisó: MTRO. JESÚS GONZÁLEZ ORNELAS	Noviembre 2021
Última actualización:	
Autorizó: UES Virtual	

Elemento de competencia 1: Describir los algoritmos y protocolos de seguridad, para implementarlo en la configuración de una red de comunicación, considerando los protocolos y estándares de organismos internacionales como ISO/ IEC y las normas RFCs (Request For Comments) con una gran capacidad de análisis y toma de decisiones.

Competencias blandas a promover: Capacidad de análisis, Creatividad, Toma de decisiones.

EC1 Fase I: Fundamentos de seguridad e integridad de la información y algoritmos criptográficos.

Contenido: Conceptos de seguridad, confidencialidad, integridad, disponibilidad, autenticidad de la información. Amenazas y vulnerabilidades, claves públicas, claves secretas, algoritmos DES, IDEA, RSA.

EC1 F1 Actividad de aprendizaje 1: Glosario sobre conceptos de seguridad de la información.

Elaborar un glosario de los siguientes conceptos sobre seguridad de la información**:**

Instrucciones:

1. Revisa el material incluido en el apartado de recursos, puedes apoyarte de otras fuentes con sustento académico.
2. Elabora un glosario que contenga al menos los siguientes conceptos: Seguridad de la información. Confidencialidad. Integridad. Disponibilidad. Autenticidad de la información. Control de acceso. Irrefutabilidad. Encriptación. Amenazas y vulnerabilidades.
3. En un documento en Word, elabora el glosario con el desarrollo de los conceptos mencionados, puedes incluir otros.
4. Deberás incluirle portada, introducción, desarrollo, conclusión y referencias bibliográficas.
5. Graba tu trabajo en pdf y súbalo a la plataforma educativa institucional.

5 hrs. Plataforma

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

Recursos:
- Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información?

Criterios de evaluación de la actividad:

Rubrica de Glosario

EC1 F1 Actividad de aprendizaje 2: Video Algoritmos criptográficos.

Leer los materiales incluidos en la sección de recursos e investigar en diferentes fuentes de información sobre el tema Algoritmos criptográficos:

- ¿Qué es un algoritmo de cifrado?.
- Técnicas de cifrado: asimétrico y simétrico.
- Clave secreta y clave pública. Explicar el concepto y su funcionamiento.
- Algoritmos: Simétricos: DES, Triple DES, IDEA, RC5 y AES, y asimétricos: RSA.

Instrucciones:

1. Analiza los materiales incluidos en la parte de

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

Recursos:
- Animoto
- Criptografía: Algoritmos de clave simétrica y asimétrica.

Criterios de evaluación de la actividad:

Rubrica elaboración de video.

recursos. 2. En un documento de word, elabora el guion que te sirva como base para realizar tu video. Este documento deberá contar con una portada que tenga sus datos generales y referencias bibliográficas. 3. Debes elaborar el video utilizando algún programa especializado como como Animoto . 4. El video deberá tener una duración entre 3 y 5 minutos. 5. En el documento en el que hiciste tu guion, copia el enlace de tu vídeo. 6. Graba el documento en formato pdf y súbalo a la plataforma educativa institucional 5 hrs. Plataforma	
EC1 Fase II: Protocolos de Seguridad. **Contenido:** Protocolos IPSec, SSL, TLS y HTTPS.	
EC1 F2 Actividad de aprendizaje 3: Presentación multimedia Protocolos de seguridad. Elabora una presentación multimedia sobre Protocolos de Seguridad. Para cada protocolo, presentar la siguiente información: • Definición. • Significado de sus siglas. • Funcionamiento • Beneficios • Ejemplo de su utilización. Instrucciones: 1. Con base en la información revisada en la sección de recursos y/o apoyándote en otras fuentes con sustento académico identifica: Protocolos de seguridad: IPSec, SSL, TLS, HTTPS. 2. Con la información anterior, elabora una presentación en PowerPoint o Prezi. 3. La presentación deberá tener un mínimo de 10 diapositivas o *slides*. 4. Recuerda cuidar tu ortografía, no debe Incluir diapositivas saturadas de información y debe utilizar imágenes que sirvan como apoyo visual. 5. Incluirle a la presentación una portada y las referencias bibliográficas. 6. Graba tu archivo en formato pdf y súbelo a la plataforma educativa institucional.	**Tipo de actividad:** Aula ( ) Plataforma(X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes ( ) **Recursos:** • Protocolo IPSEC y acceso remoto **Criterios de evaluación de la actividad:** Rúbrica presentacion multimedia

5 hrs. Plataforma	
EC1 F2 Actividad de aprendizaje 4: Reporte de Practica Protocolo IPsec. Realizar el reporte de práctica configuración del protocolo IPSec. con evidencia en video y reporte. Instrucciones: 1. Siga los pasos detallados en la siguiente PRACTICA. 2. Deberá grabar un video con el desarrollo de cada uno de los pasos. 3. Se puede usar el dispositivo de preferencia para grabar el video: celular, tableta, computadora, etc. 4. Elaborar un reporte escrito de la práctica que contenga: portada, introducción, desarrollo y conclusión. Instrucciones de la entrega del video y reporte: 1. El video debe tener un mínimo de tiempo de 5 a 10 min. 2. Súbelo a YouTube o a un drive y compartir el link en el reporte escrito. 3. El reporte escrito sobre lo realizado en la práctica debe tener como mínimo 5 páginas. 4. Recuerda cuidar tu ortografía. 5. Una vez que hayas concluido el reporte, grábalo como archivo pdf y súbelo a la plataforma educativa institucional. 5 hrs. Plataforma	**Tipo de actividad:** Aula ( ) Plataforma(X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes ( ) **Recursos:** • CISCO Packet Tracer • MONGOOSE • Redes 179 VPN Protocolo IPSEC y acceso remoto **Criterios de evaluación de la actividad:** Rúbrica Reporte de Práctica
EC1 Fase III: Modelos de autenticación. **Contenido:** Certificados digitales, tarjetas inteligentes, kerberos, dispositivos de contraseña de uso únicos, métodos de autentificación y herramientas de protección de contraseñas.	
EC1 F3 Actividad de aprendizaje 5: Infografía Métodos de autenticación. Elabora una infografía de los diferentes métodos de autenticación: • Certificado digital. • Tarjetas inteligentes. • Dispositivos de contraseña de uso único DCU (token), • Métodos de autenticación versátil y autenticación contextual o de múltiples factores. • Herramientas de protección de contraseña (Anti-Keylogger). Instrucciones:	**Tipo de actividad:** Aula ( ) Plataforma(X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes ( ) **Recursos:** • Autenticación • CANVA **Criterios de evaluación de la actividad:** Rúbrica Infografia

1. Para cada concepto, presentar la siguiente información: Definición, Funcionamiento, beneficios, Ejemplo de su utilización. 2. Ingresa a alguna aplicación para crear infografías, por ejemplo, Canva. 3. La infografía deberá contener imágenes representativas del tema y un diseño atractivo, usando fuentes y colores diversos. 4. Deberás incluir tus datos generales y referencias bibliográficas. 5. Descargar tu infografía y súbela a la plataforma institucional. 5 hrs. Plataforma	
EC1 F3 Actividad de aprendizaje 6: Foro Programas para encriptación y desencriptación. Participar activamente en el foro puesto en plataforma sobre los diferentes programas que existen para la encriptación y desencriptación, así como sus ventajas y desventajas y haciendo referencia a los diferentes algoritmos de encriptación como: AES, Triple DES, Rijandel, Blowfish, DESX, Cast 128, Gost, Serpent entre otros. Instrucciones: 1. Para resolver esta actividad deberás dar lectura al recurso "Encriptación y Seguridad" el cual se encuentra en el apartado de recursos. 2. Una vez que hayas revisado el material, deberás redactar un párrafo donde menciones los diferentes programas que existen para la encriptación y desencriptación, asi como sus ventajas y desventajas. 3. Tu comentario debe tener una extensión de al menos 100 palabras (puedes usar el contador de palabras del Word). 4. La respuesta deberá tener un sustento lógico de acuerdo con tu opinión personal. 5. Recuerda cuidar tu ortografía. 6. Realiza tu participación en el foro copiando y pegando la respuesta que redactaste. 7. Analiza con profundidad las opiniones que expresan los compañeros logrando identificar las ideas generales, así como los argumentos poco sólidos. 8. Así mismo, deberás comentar o retroalimentar los comentarios de 2 de tus compañeros. 5 hrs. Plataforma	**Tipo de actividad:** Aula ( ) Plataforma(X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes ( ) **Recursos:** • Biblioteca Digital de UES • Encriptación y Seguridad **Criterios de evaluación de la actividad:** Rubrica participación en Foro

Evaluación formativa:

- Glosario Conceptos seguridad de la información.
- Exposición en video Algoritmos criptográficos.
- Presentación multimedia Protocolos de seguridad.
- Reporte de Práctica Protocolo IPsec.
- Infografía Métodos de autenticación.
- Foro Programas para encriptación y desencriptación.

Fuentes de información

1. Andrew, S.; Tanenbaum &David J. Wetherall (2011).*Computer networks.* 5th edition. USA: Pearson Education, publishing as Prentice Hall. http://index-of.es/Varios-2/Computer%20Networks%205th%20Edition.pdf
2. *Free video maker.* (2006). Animoto. https://animoto.com/
3. *Biblioteca - UES.* (2013). Biblioteca UES. http://biblioteca.ues.mx/Default.aspx
4. *Inicio - Canva.* (2013). Canva. https://www.canva.com/
5. *Cisco Packet Tracer.* (1997). Cisco Networking Academy. https://www.netacad.com/es/courses/packet-tracer
6. *Cortafuegos*. (s. f.). © Copyright IBM Corp. 1999, 2013. Recuperado 9 de diciembre de 2021, de https://www.ibm.com/docs/es/i/7.2?topic=options-firewalls
7. 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
8. De Luz, S. (2021, 10 junio). *Mejora la seguridad de tu VPN con el protocolo IPsec. RedesZone.* https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/
9. *Encriptación | Seguridad de la información.* (s. f.). CryptoForge. Recuperado 9 de diciembre de 2021, de https://www.cryptoforge.com.ar/encriptacion-seguridad-de-la-informacion.htm
10. Gómez Vieites, Á. Enciclopedia de la seguridad informática (2a. ed.). Madrid: RA-MA Editorial, 2014. p. https://elibro.net/es/ereader/ues/106416?page=1
11. Garcia, R. (2019, 30 agosto). *Protocolo IPSEC en Windows - Seguridad y Alta disponibilidad.* https://sites.google.com/site/syadroberto/ .
12. López, A. (2021, 4 abril). *Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica. RedesZone*. https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/
13. *Mongoose*. (2004). Google Code Archive. https://code.google.com/archive/p/mongoose/
14. Arumadigital. (2014, 14 octubre). *Redes 179 VPN Protocolo IPSEC y acceso remoto* [Vídeo]. YouTube. https://www.youtube.com/watch?v=gQbxv-YnwUc&t316s
15. *Stream and listen to music online for free with soundcloud.* (2007). SoundCloud. https://soundcloud.com/
16. Toro, R. (2021, 18 febrero). *¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información?* PMG SSI - ISO 27001. https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

Elemento de competencia 2: Implementar cortafuegos para garantizar la seguridad de la información en una red de comunicación, considerando los protocolos y estándares de organismos internacionales como ISO/ IEC y las normas RFCs (Request For Comments).

Competencias blandas a promover: Trabajo en equipo, capacidad de resolución de casos prácticos.

EC2 Fase I: Clasificación y administración de cortafuegos.

Contenido: Definición de cortafuego, funcionamiento, tipos, instalación y configuración de cortafuegos (FireWall).

EC2 F1 Actividad de aprendizaje 7: Trabajo escrito Cortafuegos.

Realizar un trabajo escrito sobre Cortafuegos (firewall).

Para poder realizar tu aportacion debes seguir el siguiente proceso:

1. Deberás dar lectura al recurso "Firewalls" el cual se encuentra en el apartado de recursos.
2. Una vez que hayas revisado el material, deberás redactar la definición, funcionamiento, tipos de cortafuegos, cuál es su uso y un ejemplo.
3. Deberás incluirle al trabajo una portada, introducción, desarrollo, conclusión y las referencias bibliográficas.
4. Recuerda cuidar tu ortografía.
5. Grábalo en formato pdf y súbelo a la plataforma educativa.

5 hrs. Plataforma

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

Recursos:
- Biblioteca Digital de UES
- Cortafuegos

Criterios de evaluación de la actividad:

Rubrica de Trabajo escrito

EC2 F1 Actividad de aprendizaje 8: Reporte de práctica Instalación de un cortafuego.

Realizar una instalación y configuración de un cortafuego; la selección del cortafuego queda a libertad del equipo. Deberán descargarlo, instalarlo y configurarlo.

Realizar la práctica de la instalacion y configuracion de un cortafuego con evidencia en video y reporte.
Instrucciones de la práctica:

1. Detallar los pasos para la realización de la práctica.
2. Deberá grabar un video con el desarrollo de cada uno de los pasos.
3. Se puede usar el dispositivo de preferencia para grabar el video: celular, tableta, computadora. etc.
4. Elaborar un reporte escrito de la práctica que contenga: portada, introducción, desarrollo y conclusión.

Instrucciones de la entrega del video y reporte:

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

Recursos:
- Bibliotecas digitales o repositorios academicos en Internet
- Biblioteca Digital de UES

Criterios de evaluación de la actividad:

Rubrica Reporte de Prácticas.

1. El video debe tener un mínimo de tiempo de 5 a 10 min. 2. Súbelo a youtube o a un drive y compartir el link en el reporte escrito. 3. El reporte escrito sobre lo realizado en la práctica debe tener como mínimo 5 páginas. 4. Recuerda cuidar tu ortografía. 5. Una vez que hayas concluido el reporte, grábalo como archivo pdf y súbelo a la plataforma educativa institucional. 6. Para todo lo anterior deben presentar las evidencias correspondientes, para lo cual pueden utilizar videos y/o imágenes. 5 hrs. Plataforma	
EC2 Fase II: Configuración de Proxy. **Contenido:** Proxy hardware y software, servidor NAT, configuración de proxy.	
EC2 F2 Actividad de aprendizaje 9: Wiki Proxys. Participar en el wiki sobre el tema Proxys: Para su participación, considere los siguientes aspectos: 1. Consulta el recurso ¿Qué es un proxy? el cual se encuentra en el apartado de recursos. 2. Una vez que haya revisado el material, deberá redactar un párrafo con la definición, funcionamiento, tipos de proxys su uso y ejemplos. 3. Su comentario debe tener una extensión de al menos 60 palabras (puede usar el contador de palabras del Word). 4. Su participacion debera incuir por lo menos una imagen relacionada al tema. 5. No olvide incuir su nombre comleto. 6. Así mismo, deberá comentar o retroalimentar los comentarios de 2 de tus compañeros. 7. Recuerde cuidar su ortografía. 5 hrs. Plataforma	**Tipo de actividad:** Aula ( ) Plataforma(X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes ( ) **Recursos:** • Video ¿Qué es un proxy? **Criterios de evaluación de la actividad:** Rubrica de participación en la Wiki
EC2 F2 Actividad de aprendizaje 10: Reporte de práctica Instalación y configuración de un proxy. Realizar una instalación y configuración de un Proxy: Realizar la práctica de la instalacion y configuracion de un proxy con evidencia en video y reporte. Instrucciones de la práctica:	**Tipo de actividad:** Aula ( ) Plataforma(X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo (X) Independientes ( ) **Recursos:** • Bibliotecas digitales o repositorios academico en Internet • Biblioteca Digital de UES **Criterios de evaluación de la actividad:**

1. Detallar los pasos para la realización de la práctica. 2. Deberá grabar un video con el desarrollo de cada uno de los pasos. 3. Se puede usar el dispositivo de preferencia para grabar el video: celular, tableta, computadora. etc. 4. Elaborar un reporte escrito de la práctica que contenga: portada, introducción, desarrollo y conclusión. Instrucciones de la entrega del video y reporte: 1. El video debe tener un mínimo de tiempo de 5 a 10 min. 2. Súbelo a youtube o a un drive y compartir el link en el reporte escrito. 3. El reporte escrito sobre lo realizado en la práctica debe tener como mínimo 5 páginas. 4. Recuerda cuidar tu ortografía. 5. Una vez que hayas concluido el reporte, grábalo como archivo pdf y súbelo a la plataforma educativa institucional. 6. Para todo lo anterior deben presentar las evidencias correspondientes, para lo cual pueden utilizar videos y/o imágenes. 5 hrs. Plataforma	Rubrica reporte de práctica.
EC2 Fase III: Red privada virtual, cliente/servidor **Contenido:** Definición, características, tipos y protocolos, instalación y configuración de la red privada virtual.	
EC2 F3 Actividad de aprendizaje 11: Quiz VPN. Contestar el quiz incluido en la plataforma de forma individual, en base a las siguientes instrucciones: Repasar todos los temas que se vieron en el elemento de competencia mediante los materiales incluidos en los apartados de recursos. 1. Accese al quiz en la plataforma educativa institucional. 2. En base a la pregunta, eligir la respuesta que considers correcta. 3. Avanza hasta concluir todas las preguntas. 4. Tendras un tiempo limite de 30 min. 5. Envialo para su revision. 6. Solo tendrás una oportunidad para contestarlo. 5 hrs. Plataforma	**Tipo de actividad:** Aula ( ) Plataforma(X) Laboratorio ( ) Grupal ( ) Individual (X) Equipo ( ) Independientes ( ) **Recursos:** • Recursos del elemento de competencia. • Biblioteca Digital de UES **Criterios de evaluación de la actividad:** Cantidad de aciertos en relacion a la cantidad de preguntas.
EC2 F3 Actividad de aprendizaje 12: Reporte de práctica Instalación y configuracion de una VPN.	**Tipo de actividad:** Aula ( ) Plataforma(X) Laboratorio ( ) Grupal ( ) Individual ( ) Equipo (X) Independientes ( )

Realizar la práctica de configuración de instalación y configuración de red privada virtual: Servidor VPN y cliente VPN, con evidencia en video y reporte. Instrucciones: 1. Siga los pasos detallados en la siguiente PRACTICA. 2. Deberá grabar un video con el desarrollo de cada uno de los pasos. 3. Se puede usar el dispositivo de preferencia para grabar el video: celular, tableta, computadora, etc. 4. Elaborar un reporte escrito de la práctica que contenga: portada, introducción, desarrollo y conclusión. Instrucciones de la entrega del video y reporte: 1. El video debe tener un mínimo de tiempo de 5 a 10 min. 2. Súbelo a YouTube o a un drive y compartir el link en el reporte escrito. 3. El reporte escrito sobre lo realizado en la práctica debe tener como mínimo 5 páginas. 4. Recuerda cuidar tu ortografía. 5. Una vez que hayas concluido el reporte, grábalo como archivo pdf y súbelo a la plataforma educativa institucional. 5 hrs. Plataforma	**Recursos:** • Bibliotecas digitales o repositorios académicos en Internet • Biblioteca Digital de UES **Criterios de evaluación de la actividad:** Rubrica Reporte de práctica

Evaluación formativa:

- Trabajo escrito Cortafuegos.
- Reporte de práctica Instalación de un cortafuego.
- Wiki Proxys.
- Reporte de práctica Instalación y configuración de un proxy.
- Quiz VPN.
- Reporte de práctica Instalación y configuracion de una VPN.

Fuentes de información

1. Andrew, S.; Tanenbaum &David J. Wetherall (2011).Computer networks. 5th edition. USA: Pearson Education, publishing as Prentice Hall. http://index-of.es/Varios-2/Computer%20Networks%205th%20Edition.pdf
2. Animoto https://animoto.com/
3. *Cortafuegos*. (s. f.). © Copyright IBM Corp. 1999, 2013. Recuperado 9 de diciembre de 2021, de https://www.ibm.com/docs/es/i/7.2?topic=options-firewalls
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. De Luz, S. (2021, 10 junio). *Mejora la seguridad de tu VPN con el protocolo IPsec*. RedesZone. https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/
6. *Encriptación | Seguridad de la información*. (s. f.). CryptoForge. Recuperado 9 de diciembre de 2021, de https://www.cryptoforge.com.ar/encriptacion-seguridad-de-la-informacion.htm
7. Gómez Vieites, Á. Enciclopedia de la seguridad informática (2a. ed.). Madrid: RA-MA Editorial, 2014. p. https://elibro.net/es/ereader/ues/106416?page=1
8. Garcia, R. (2019, 30 agosto). *Protocolo IPSEC en Windows - Seguridad y Alta disponibilidad*. https://sites.google.com/site/syadroberto/ .
9. López, A. (2021, 4 abril). *Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica*. RedesZone. https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/
10. *Redes 179 VPN Protocolo IPSEC y acceso remoto*. (2014, 14 octubre). [Vídeo]. YouTube. https://www.youtube.com/watch?v=gQbxv-YnwUc&t316s
11. Toro, R. (2021, 18 febrero). *¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información?* PMG SSI - ISO 27001. https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

Políticas

Al inicio del curso el facilitador establecerá los horarios y las vías de comunicación, considerando al menos una vía alterna a la plataforma educativa.

El profesor publicará los Lineamientos de entrega de actividades y evaluación, en donde quedará establecido el calendario semanal que tendrán para subir las actividades a la plataforma, así como las fechas de cierre de plataforma. ES RESPONSABILIDAD DEL ALUMNO LEER LOS LINEAMIENTOS.

El alumno deberá ingresar diariamente al curso en plataforma y realizar las actividades de acuerdo con el calendario establecido por el profesor.

Cualquier duda que tenga el alumno al realizar la actividad, es obligación solicitar asesoría al facilitador mediante la plataforma educativa institucional o el medio que el mismo haya dispuesto.

El facilitador deberá dar retroalimentación oportuna de las actividades elaboradas por el alumno.

En caso de no entregar a tiempo alguna evidencia, se penalizará con un porcentaje de la calificación.

En caso de que la plataforma no esté disponible, deberá reportarlo al correo: uesvirtual@ues.mx. El facilitador deberá ofrecer un plan alterno para la realización de las actividades.

Metodología

El curso se llevará mediante la plataforma educativa que la institución designe.

El curso será intensivo, por lo que se deberán realizar un determinado número de actividades cada semana.

La dinámica del curso consiste en dar seguimiento a cada tema establecido en la secuencia didáctica a través de diversos tipos de actividades destinadas a ejecutarse, en su mayoría, en forma individual, a través de la plataforma educativa institucional.

Se deberá participar en al menos un foro en cada elemento de competencia. donde el facilitador lanzará un tema o pregunta y los alumnos deberán aportar sus ideas propias y deberán retroalimentar al menos a 2 de sus compañeros.

Se contestará al menos un quiz en cada elemento de competencia.

Se participará en la construcción de al menos una wiki de forma colaborativa con el resto de los miembros del grupo.

Se debe elaborar un Proyecto Final integrador.

Se proporcionará una explicación de cada uno de los temas con material y herramientas apropiadas para su mejor comprensión y para un adecuado desarrollo de cada una de las actividades.

Evaluación

La evaluación del curso se realizará de acuerdo con el 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:

1. Diagnóstica permanente, entendiendo esta como la evaluación continua del estudiante durante la realización de una o varias actividades;
2. Formativa, siendo esta, la evaluación al alumno durante

En caso de plagio en alguna de las actividades, el alumno no obtendrá la competencia en la evaluación correspondiente y su calificación será como si la actividad no la hubiese entregado.	La plataforma educativa se cerrará en 2 cortes en el transcurso del módulo. El docente les proporcionará un calendario de elaboración de actividades, que contemple las fechas específicas de entrega de cada actividad. En caso no entregar las actividades de acuerdo con el calendario establecido por el facilitador, si podrán entregarlas fuera de tiempo (siempre y cuando no esté cerrada la plataforma), sin embargo, se penalizará con el 20% de la calificación por la entrega tardía de la misma. Podrán entregar actividades siempre y cuando la plataforma se encuentre abierta, una vez que se cierre, ya no se aceptarán actividades.	el desarrollo de cada elemento de competencia; y 3. 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: 1. Competente sobresaliente; 2. Competente avanzado; 3. Competente intermedio; 4. Competente básico; y 5. 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: 1. Competente sobresaliente= 10 2. Competente avanzado= 9 3. Competente intermedio= 8 4. Competente básico= 7 5. No aprobado= 6