1. Datos Generales de la asignatura

Nombre de la asignatura:	**Ciberseguridad en los negocios**
Clave de la asignatura:	
SATCA[1]:	**1-4-5**
Carrera:	**Ingeniería en Tecnologías de la Información y telecomunicaciones**

2. Presentación

Caracterización de la asignatura

Este curso abarca los conocimientos esenciales sobre todos los dominios de la ciberseguridad, incluidas la seguridad de la información, la seguridad de sistemas, la seguridad de la red, la ética y las leyes, y las técnicas de defensa y mitigación utilizadas en la protección de los negocios.

La asignatura permite que el estudiante amplíe y practique sus conocimientos y habilidades adquiridos en materias previas del área de redes.

Los riesgos y las amenazas de ciberseguridad siempre están presentes en nuestro mundo. La infraestructura de redes e Internet son cada vez más vulnerables a una amplia variedad de ataques físicos y cibernéticos, por lo cual los profesionales en el área de TI requieren conocimientos y habilidades para hacer frente a los retos actuales de seguridad que enfrentan las organizaciones.

Intención didáctica

La presente asignatura propone un enfoque práctico, en el que el docente aborde la teoría y posteriormente plantee situaciones en las que el estudiante deberá resolverlas mediante las herramientas sugeridas en cada tema.

La primera unidad aborda una introducción a los temas de confidencialidad, integridad y disponibilidad, así como el estado de los datos y el modelo de ciberseguridad de ISO.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

En la segunda unidad el estudiante reforzará y pondrá en práctica sus conocimientos sobre tipos y características de amenazas, vulnerabilidades y ataques.

La tercera unidad muestra el panorama actual de la criptografía y su aplicación en temas de seguridad informática.

En la cuarta unidad se explica cómo la integridad garantiza que nada ni nadie modifique los datos y que estos sean confiables durante su ciclo de vida completo.

La unidad cinco describe la importancia de contar con una alta disponibilidad en las organizaciones, con el objetivo de proporcionar un servicio prácticamente ininterrumpido a los usuarios.

La asignatura concluye con la unidad seis analizando las tecnologías, los procesos y procedimientos que los expertos en ciberseguridad utilizan para proteger los sistemas, dispositivos y datos que conforman la infraestructura de una red.

Se propone que en cada una de las seis unidades se realicen laboratorios en los cuales los estudiantes practiquen los temas abordados, además de la realización de un caso práctico final en el que se planteen situaciones que requieran aplicar las habilidades adquiridas en la asignatura.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Estudios Superiores de Zamora en Agosto de 2021.	Integrantes de las Academias de Ingeniería en Sistemas Computacionales e Ingeniería en Tecnologías de la Información y Comunicaciones.	Elaboración de las nuevas especialidades para los planes de estudio 2010.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Competencias específicas Desarrollar la capacidad de análisis, diseño y evaluación de sistemas usando

diferentes tecnologías de comunicaciones, dispositivos, y software de programación para ciberseguridad.

Competencias genéricas

Competencias instrumentales:
- Capacidad de abstracción, análisis y síntesis.
- Conocimiento sobre el área de estudio y la profesión.
- Capacidad de comunicación oral y escrita.
- Habilidades en el uso de las tecnologías de la información y de la comunicación.
- Habilidades para buscar, procesar y analizar información, procedente de fuentes
diversas.
- Capacidad para identificar, plantear y resolver problemas.
- Capacidad para tomar decisiones.

Competencias interpersonales:
- Capacidad crítica y autocrítica.
- Capacidad de trabajo en equipo
- Habilidades interpersonales.

5. Competencias previas

- Conceptos básicos de redes
- Configuración de dispositivos de red
- Manejo de comandos básicos en Linux
- Conceptos básicos en seguridad informática

6. Temario

No.	Temas	Subtemas

1	Las caras de la ciberseguridad	1.1 Introducción 1.2 Triada del CID (Confidencialidad, Integridad y Disponibilidad) 1.3 Estados de los datos 1.4 Contramedidas de ciberseguridad 1.5 Marco de trabajo 1.5.1 Modelo ISO
2	Amenazas, vulnerabilidades y ataques a la ciberseguridad	2.1 Introducción 2.2 Malware y código malicioso 2.3 Uso de trucos 2.4 Ataques 2.5 Laboratorio
3	Criptografía	3.1 Introducción 3.2 Criptografía 3.3 Controles de acceso 3.4 Ocultamiento de datos 3.5 Laboratorio
4	Garantía de integridad	4.1 Tipos de controles 4.2 Firmas digitales 4.3 Certificados 4.4 Integridad de la base de datos 4.5 Laboratorio
5	El reino de los cinco nueves	5.1 Alta disponibilidad 5.2 Medidas para mejorar la disponibilidad 5.3 Respuesta ante incidentes 5.4 Recuperación tras desastre 5.5 Laboratorio
6	Protección del negocio	6.1 Defensa de sistemas y dispositivos 6.2 Protección del servidor 6.3 Protección de la red 6.4 Seguridad física 6.5 Caso práctico

7. Actividades de aprendizaje de los temas

1. Las caras de la ciberseguridad	
Competencias	Actividades de aprendizaje
Específicas: ● Analiza el modelo de ciberseguridad	● Explorar la autenticación, autorización y auditoría realizando una práctica para agregar grupos, usuarios y

de ISO ● Identifica los principios de seguridad (CID) ● Identifica los tipos de almacenamiento de datos Genéricas: ● Capacidad de análisis y síntesis. ● Capacidad de organizar y planificar. ● Habilidad para buscar y analizar información proveniente de fuentes diversas. ● Solución de problemas. ● Toma de decisiones.	contraseñas en un sistema Linux. ● Explorar el cifrado de archivos y datos. ● Verificar la integridad de varios archivos mediante hashes para garantizar que los archivos no se hayan alterado usando los controles de integridad de datos y archivos.
2. Amenazas, vulnerabilidades y ataques a la ciberseguridad	
Competencias	Actividades de aprendizaje
Específicas: ● Identifica los tipos de amenazas, vulnerabilidades y ataques a la ciberseguridad. ● Aplica herramientas de escaneo de puertos y exploración de vulnerabilidades ● Configura protocolos de cifrado Genéricas: ● Capacidad de análisis y síntesis. ● Capacidad de organizar y planificar. ● Habilidad para buscar y analizar información proveniente de fuentes diversas. ● Solución de problemas. ● Toma de decisiones.	● Investigar los tipos de amenazas, vulnerabilidades y ataques a la ciberseguridad. ● Detectar amenazas y vulnerabilidades utilizando Nmap, un escáner de puertos y una herramienta de asignación de red en un sistema Linux. ● Configurar los protocolos WEP / WPA2 PSK / WPA2 RADIUS
3. Criptografía	
Competencias	Actividades de aprendizaje
Específicas: ● Identifica los tipos de encriptación y sus características ● Aplica software para uso de	● Investigar los tipos de encriptación, características, ventajas y desventajas. ● Emplear un programa de esteganografía de código abierto para ocultar los datos de distintos tipos de

esteganografía • Aplica y analiza técnicas de cifrado Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones.	archivos como archivos de audio y de imagen. • Observar la transferencia del tráfico FTP cifrado y no cifrado entre un cliente y un sitio remoto. • Configurar túneles VPN para observar la transferencia del tráfico FTP sin cifrar entre dos sitios geográficos. • Configurar un túnel VPN entre dos sitios geográficos y enviará el tráfico FTP cifrado.
4. Garantía de integridad	
Competencias	Actividades de aprendizaje
Específicas: • Identifica los tipos de controles de integridad de datos • Identifica el funcionamiento de la tecnología de firma digital • Aplica herramientas de recuperación de contraseñas • Aplica herramientas de uso y verificación de firmas digitales Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones.	• Utilizar una herramienta de decodificación de contraseñas para recuperar la contraseña de un usuario en un sistema Linux. • Utilizar herramientas que permitan comprender los conceptos detrás de una firma digital demostrar su uso y validación. • Comparar SSH y Telnet para acceder a un host remoto en un sistema Linux.
5. El reino de los cinco nueves	
Competencias	Actividades de aprendizaje
Específicas: • Identifica los puntos de falla únicos • Identifica la importancia de la redundancia en el logro de una alta	• Comprender los niveles de RAID (matriz redundante de discos independientes) mediante la

disponibilidad en los sistemas de una organización • Identifica los niveles de RAID • Aplica el diseño de recuperabilidad de un sistema Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones.	comparación de los mismos. • Realizar práctica de laboratorio para observar una conmutación por falla de la red con routers y switches redundantes. • Realizar práctica de laboratorio de recuperabilidad del router y switch, fortalecer la configuración de IOS, activar la función de configuración de recuperabilidad de Cisco IOS.
6. Protección del negocio	
Competencias	Actividades de aprendizaje
Específicas: • Identifica los requerimientos para la protección de un host • Identifica los requerimientos para la protección de dispositivos móviles e inalámbricos • Aplica herramientas de auditoría de seguridad • Empleo de firewalls y ACLs Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones.	• Analizar los requerimientos para la protección de un host • Analiza los requerimientos para la protección de dispositivos móviles e inalámbricos • Realizar práctica de laboratorio para el fortalecimiento de un sistema Linux mediante el uso de una herramienta de auditoría de seguridad. • Realizar práctica empleando firewalls del servidor y ACL del router

8. Práctica(s)

- Explorar los procesos de autenticación, autorización y auditoría
- Explorar el cifrado de archivos y datos

- Uso de controles de integridad de datos y archivos
- Configuración de protocolos de encriptación
- Detección de amenazas y vulnerabilidades
- Uso de esteganografía
- Decodificación de contraseñas
- Uso de firmas digitales

9. Proyecto de asignatura

Esta actividad final incluye las habilidades adquiridas en este curso. Debe configurar un router inalámbrico, cargar y descargar archivos con el FTP, se conectará de forma segura a un sitio remoto mediante una VPN y protegerá el router Cisco IOS.

10. Evaluación por competencias

La evaluación de la asignatura se hará con base en siguiente desempeño:

- Reportes escritos de las observaciones hechas durante las actividades, así como de las conclusiones obtenidas de dichas observaciones.
- Información obtenida durante las investigaciones solicitadas plasmada en documentos escritos.
- Exámenes para comprobar el manejo de aspectos teóricos - declarativos y de habilidades y destrezas.
- Resolución de tareas, trabajos prácticas relacionadas con el tema en cuestión, haciendo uso del cómputo en la nube.
- Participaciones y actitudes del estudiante (responsabilidad, cumplimiento en tiempo y forma, trabajo en equipo, exposición de temas, etc.)
- Integración del portafolio de evidencias del curso (tareas, trabajos, prácticas, exámenes, entre otros).
- Desarrollo de proyectos de aplicación real debidamente documentado que describa la experiencia concreta y conclusiones obtenidas, para ser

expuesto ante el grupo.

11. Fuentes de información

1. Arboledas, D. (2014). Backtrach 5: Hacking de redes inalámbricas. (A. Grupo, Ed.) (Primera ed). 2. Carballar, J. (2006). Firewall- la seguridad de la banda ancha. (A. Grupo, Ed.) (Primera ed).

3. Gómez, Á. (2011). Enciclopedia de la seguridad informática. (A. Grupo, Ed.) (Segunda ed).

4. Picouto, F., Lorente, I., García-Morán, J., & Ramos, A. (2008). Hacking y seguridad en internet. (A. Grupo, Ed.) (Primera ed).

5. Zemánek, J. (2005). Cracking sin secretos- ataque y defensa de software. (A. Grupo, Ed.) (Primera ed).

6. L. Joyanes Aguilar, Industria 4.0-la cuarta revolución industrial. Alfaomega, 2017