1. Datos Generales de la asignatura

Nombre de la asignatura:	**Ciberseguridad**
Clave de la asignatura:	SIC-2508
SATCA[1]:	2-2-4
Carrera:	Ingeniería en Tecnologías de la Información y Comunicaciones

2. Presentación

Caracterización de la asignatura

Aporta el perfil del egresado las siguientes habilidades:

• Dirige el monitoreo, análisis y control de la información utilizando herramientas y marcos de referencia, con perspectiva ética, de respeto por la persona y de responsabilidad social.
• Evalúa riesgos de seguridad y vulnerabilidad en aplicaciones o instalaciones de tecnologías de la información con apoyo de herramientas de vanguardia automatizadas de acuerdo con metodologías, normas y estándares de excelencia.
• Diseña políticas de seguridad informática para establecer controles de seguridad pertinentes atendiendo los principios de no discriminación, Inclusión y equidad social.
• Gestiona incidentes y eventos de seguridad de informática para reducir la afectación negativa de la seguridad de la información y dar continuidad a las operaciones de la organización, atendiendo los principios de no discriminación, Inclusión y equidad social.
• Emplea métodos criptográficos para establecer protocolos de seguridad en el transporte de datos seguros a nivel de aplicación, usando herramientas de seguridad basadas en dichos protocolos integrando excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.
• Propone soluciones para proteger la transmisión y almacenamiento de información sensible dentro de un área funcional o técnica, a partir de marcos de referencia con excelencia, vanguardia e innovación social aplicando mejores prácticas del mercado.
• Aplica procedimientos y técnicas de auditoría informática para detectar si se protegen los activos y recursos de la organización, si se mantiene la integridad de los datos, si se utiliza eficientemente los recursos, si se atienden los principios de no discriminación, Inclusión y equidad social y si se cumple con las leyes y regulaciones establecidas.
• Implementa soluciones metodológicas y controles de seguridad en el ciclo de vida del desarrollo de software que permitan la reducción de vulnerabilidades y la inclusión de mejores prácticas de seguridad, con una perspectiva de responsabilidad social.

Los egresados construyen tecnologías que mantienen segura la arquitectura informática. Su responsabilidad es anticiparse a las vulnerabilidades de la red, lo que requiere crear firewalls, ejecutar programas de encriptación y actualizar el software.

Intención didáctica

Este programa de estudios se sugiere eminentemente práctico, es decir, el docente propone el planteamiento de un problema y el estudiante deberá resolverlo mediante diversas técnicas, por mencionar algunas: herramientas de modelado y codificación; con el monitoreo del docente.

El tema uno, introduce a un campo fundamental en la tecnología moderna, que abarca un conjunto de prácticas, políticas, herramientas y tecnologías diseñadas para proteger los sistemas informáticos, redes, programas y datos contra ataques, accesos no autorizados, daños o robos. A medida que la tecnología se integra más profundamente en nuestra vida diaria, la protección de la información y los sistemas se ha vuelto una prioridad tanto para individuos como para organizaciones a nivel mundial.
En el segundo tema, se enfoca en la protección de la información mediante el uso de técnicas matemáticas. Su objetivo principal es garantizar la confidencialidad, integridad, autenticidad y no repudio de los datos en su transmisión o almacenamiento. En otras palabras, la criptografía se utiliza para asegurar que la información solo sea accesible para las partes autorizadas, que no se altere sin ser detectada y que se pueda verificar su origen.
El tema tres, se enfoca en la identificación, recolección, análisis e interpretación de datos y evidencia digital con el objetivo de apoyar investigaciones legales o criminales. Este campo combina técnicas avanzadas de análisis de datos con principios legales, y su propósito es ayudar a resolver crímenes o disputas mediante la recuperación de información almacenada en dispositivos electrónicos, redes y sistemas informáticos.
El tema cuatro, ciber inteligencia es el proceso de recolectar, analizar y utilizar información relacionada con amenazas cibernéticas para proteger activos, prevenir ataques y apoyar decisiones estratégicas en el ámbito de la ciberseguridad. En un mundo cada vez más digitalizado, las organizaciones, gobiernos y empresas se enfrentan a un panorama de amenazas cibernéticas cada vez más complejo y sofisticado.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Evento
Instituto Tecnológico Superior de Puruándiro, 6 de septiembre al 10 octubre 2024	Docentes de la Academia Ingeniería en Tecnologías de la Información y Comunicaciones.	Propuesta inicial.
Instituto Tecnológico Superior de Puruándiro, 15 de noviembre al 22 noviembre 2024	Docentes de la Academia Ingeniería en Tecnologías de la Información y Comunicaciones.	Reunión en academia para la revisión de los temas de la asignatura.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
El estudiante será capaz de identificar, evaluar y gestionar los riesgos cibernéticos en diferentes entornos organizacionales, proponiendo soluciones de seguridad apropiadas para mitigar las vulnerabilidades detectadas.

5. Competencias previas

Utiliza el razonamiento lógico utilizando sistemas de cómputo, conceptos avanzados relacionados con la protección de sistemas informáticos, redes y datos.

6. Temario

No.	Temas	Subtemas
1	**Introducción a la ciberseguridad.**	1.1. Antecedentes históricos y aplicaciones. 1.2. Ataques y profesionales de la ciberseguridad. 1.2.1. Perfil del atacante cibernético. 1.2.2. Tipos de atacantes. 1.3. Guerra cibernética. 1.3.1. Qué es la guerra cibernética. 1.3.2. Propósito de la guerra cibernética. 1.4 Aspectos legales éticos y sociales en ciberseguridad.
2	**Criptografía**	2.1. Conceptos básicos de la criptografía. 2.2. Algoritmos criptográficos de cifrado simétrico. 2.3. Algoritmos de cifrado asimétrico. 2.4. Funciones de HASH y firmas digitales. 2.5. Protocolos criptográficos.

		2.6. Criptografía en la seguridad informática. 2.7. Aplicaciones de la criptografía.
3	**Computo forense**	3.1. Concepto de cómputo forense. 3.2. El modelo de diamante del análisis de intrusiones. 3.3. Marco legal. 3.4. Manejo de evidencia. 3.5. Análisis Forense. 3.5.1. Análisis de metadatos de archivos. 3.5.2. Análisis forense de Windows. 3.5.3. Análisis forense de Linux y Mac. 3.5.3. Análisis forense de teléfonos móviles. 3.5.4. Análisis forense de correo electrónico.
4	**Ciber inteligencia**	4.1. Importancia y aplicaciones en la seguridad cibernética. 4.2. Principales vectores de ataque en el ciberespacio. 4.3. Ciberseguridad en empresas e instituciones. 4.4. Inteligencia aplicada al cibercrimen. 4.5. Técnicas, herramientas y procedimientos de recopilación de información. 4.6. Técnicas de análisis. 4.6.1. Monitoreo de conversaciones y tendencias.

7. **Actividades de aprendizaje de los temas**

1. Introducción a la ciberseguridad.	
Competencias	**Actividades de aprendizaje**
Específica(s): Conocer los conceptos sobre la ciberseguridad informática. Genérica(s): ● Capacidad para identificar, plantear y resolver problemas. ● Capacidad para trabajar en equipo interdisciplinario. ● Capacidad crítica y autocrítica. ● Habilidades interpersonales. ● Capacidad de aplicar los conocimientos en la práctica. Transversal(es): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. ● Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrano aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	● Investigar las diferencias fundamentales y específicas de la seguridad informática para una comunicación confiable. ● Asociar el funcionamiento de los componentes básicos del contemplados en la ciberseguridad. ● Buscar y seleccionar información sobre los diferentes modelos de transición en la comunicación de redes. ● Debate sobre Amenazas Cibernéticas y su Impacto. ● Mapa de Riesgos Cibernéticos. ● Simulación de Phishing.
2. Criptografía	
Competencias	**Actividades de aprendizaje**

Específica(s): Entender los principios y aplicaciones de los algoritmos de cifrado simétrico y asimétrico y aplicar funciones hash y firmas digitales. Genérica(s): ● Capacidad de análisis y síntesis. ● Capacidad de organizar y planificar. ● Habilidad para buscar y analizar información proveniente de fuentes diversas. ● Capacidad de aplicar los conocimientos. ● Capacidad de investigación y Autoaprendizaje. Transversal(es): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. ● Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	● Lectura de capítulos seleccionados sobre la historia y evolución de la criptografía, seguida de una discusión en clase para profundizar en los conceptos. ● Análisis de casos históricos de criptografía, como el Enigma alemán durante la Segunda Guerra Mundial. ● Investigación sobre diferentes tipos de ataques criptográficos y sus mecanismos. ● Implementación de algoritmos de cifrado simétrico (como AES) y asimétrico (como RSA) en un lenguaje de programación. ● Realización de prácticas de laboratorio para implementar y utilizar funciones hash (como SHA-256) y firmas digitales. ● Comparar y contrastar diferentes algoritmos de cifrado en términos de seguridad y eficiencia. ● Implementación y simulación de protocolos de autenticación y cambio de clave en un entorno controlado. ● Configuración práctica de protocolos como SSL/TLS y SSH en servidores y clientes. ● Estudio y análisis de cómo funcionan los protocolos de seguridad en la web, como PGP y otros. ● Desarrollo de proyectos que integren criptografía en la seguridad informática y sistemas de almacenamiento. ● Configuración y prueba de sistemas de comunicación segura utilizando criptografía. ● Investigación y análisis del uso de criptografía en blockchain y criptomonedas. ● Simulación de transacciones electrónicas

	seguras utilizando criptografía.

3. Computo forense	
Competencias	**Actividades de aprendizaje**
Específica(s): Aplicará los conceptos y técnicas avanzadas de análisis forense, incluyendo el análisis de sistemas de archivos, slack space, recuperación de archivos y particiones, identificando y documentando evidencias digitales relevantes de manera precisa y eficiente en el proceso forense. Genérica(s): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas) ● Capacidad de aprender ● Solución de problemas Transversal(es): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. ● Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación	● Estudio de conceptos fundamentales: los estudiantes pueden realizar lecturas y discusiones en clase sobre los conceptos fundamentales del análisis forense, incluyendo sistemas de archivos, slack space, recuperación de archivos borrados, recuperación de particiones eliminadas, file carving y data carving. Pueden estudiar casos prácticos y ejemplos para comprender cómo se aplican estos conceptos en situaciones reales. ● Prácticas de laboratorio: se pueden organizar prácticas de laboratorio donde los estudiantes aprendan a realizar análisis forenses en diferentes plataformas y dispositivos. Pueden practicar el análisis de metadatos de archivos, análisis forense de sistemas operativos como Windows, Linux y Mac, análisis forense de redes, bases de datos, correo electrónico, memoria, teléfonos móviles y entornos en la nube.

integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano	
4. Ciber inteligencia	
Competencias	**Actividades de aprendizaje**
Específica(s): ● Comprender y aplicar los conceptos y fundamentos de la ciberinteligencia, identificar su importancia y aplicaciones en la seguridad cibernética, gestionar el ciclo de inteligencia, implementar medidas de seguridad operativa (OPSEC), aplicar técnicas de ciberprotección y anonimización, y manejar identidades digitales (Sock Puppets), con el fin de fortalecer la capacidad de detección, análisis, protección y respuesta a amenazas y riesgos cibernéticos, y contribuir al desarrollo de estrategias y acciones efectivas en el ámbito de la ciberseguridad. Genérica(s): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas) ● Capacidad de aprender ● Solución de problemas Transversal(es): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. ● Diseña e implementa soluciones a problemas propios de ámbito de su área de	● Análisis de casos prácticos y estudios de caso relacionados con la aplicación de la ciberinteligencia en la detección, prevención, mitigación y respuesta a amenazas y ataques cibernéticos. ● Simulación de incidentes de seguridad en entornos empresariales e institucionales, donde los estudiantes deberán identificar, contener, mitigar y responder a los ataques cibernéticos. ● Investigación y análisis de amenazas cibernéticas, incluyendo ciberdelitos y ataques dirigidos a empresas, instituciones, infraestructuras críticas y sistemas gubernamentales. ● Análisis de casos de terrorismo cibernético, incluyendo incidentes de ciberterrorismo pasados y potenciales, así como las estrategias de inteligencia utilizadas para prevenir y responder a tales amenazas.

aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano	

8. Práctica(s)

- Simulación de un Ataque de Phishing y Análisis de Consecuencias
- Escaneo de Vulnerabilidades de una Red Local con Nessus
- Análisis Forense de un Equipo Infectado con Malware
- Configuración de un Sistema de Prevención de Intrusos (IPS/IDS)
- Implementación de un VPN para la Protección de la Información

9. Proyecto de asignatura

El objetivo principal del proyecto es integrar los conocimientos y habilidades adquiridos a lo largo del curso de **ciberseguridad** para diseñar, implementar y evaluar un sistema seguro, capaz de detectar, prevenir y mitigar amenazas cibernéticas en un entorno simulado o real. Los estudiantes deberán aplicar las mejores prácticas de seguridad, configurar medidas de protección, identificar vulnerabilidades y proponer soluciones efectivas para garantizar la integridad, confidencialidad y disponibilidad de la información en un sistema.

10. Evaluación por competencias

- Análisis de casos.
- Entrevistas a expertos
- Solución de problemas realizados en forma individual o en equipo.
- Discusiones y debates en equipos.
- Paneles de presentaciones de temas.
- Reportes de proyectos, investigaciones, trabajos, etc.
- Simulaciones y/o demostraciones.
- Esquemas gráficos (mapas conceptuales, mapas mentales, mapas
- Procedimentales, cuadros sinópticos, diagramas de flujo, etc.)

11. Fuentes de información

1. McClure, S., Scambray, J., & Kurtz, G. (2007). Hacking exposed: Network security secrets & solutions (6th ed.). McGraw-Hill
2. Navarro Isla, Jorge. (2005). Tecnologías de la información y de las comunicaciones: Aspectos legales (Primera edición). Editorial Porrúa.
3. Análisis de casos históricos de criptografía, como el Enigma alemán durante la Segunda Guerra Mundial.
4. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
5. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
6. Casey, E. (2014). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.
7. Gordon, S. (2015). The internet police: How crime went online, and the cops followed. Reaktion Books.
8. Casey, E. (2011). "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet." Academic Press.
9. Nelson, B., Phillips, A., & Steuart, C. (2017). "Guide to Computer Forensics and Investigations." Cengage Learning.
10. Sammons, J. (2014). "The basics of digital forensics: The primer for getting started in digital forensics." Syngress.