

	Nombre del documento: Formato de Programa de Estudio de asignatura de Especialidad		Código: TecNM-AC-PO-007-02
			Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 1 de 13

1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad en la Ciencia de Datos.
Clave de la asignatura:	CDD-2503
SATCA¹:	2 – 3 – 5
Carrera:	Ingeniería en Sistemas Computacionales.

2. Presentación

Caracterización de la asignatura

La creciente dependencia de los datos en prácticamente todos los aspectos de la vida moderna ha puesto de manifiesto la importancia crítica de garantizar la seguridad. El programa de estudios en Seguridad en la Ciencia de Datos se enfoca en aportar al perfil de egreso del Ingeniero en Sistemas Computacionales con las habilidades necesarias para proteger la integridad, confidencialidad y disponibilidad de los datos, especialmente en el contexto de grandes volúmenes de información y análisis avanzados de la misma.

Así como las nuevas tecnologías juegan un papel importante como una herramienta en el manejo de información, también son las herramientas y técnicas apropiadas para mejorar la seguridad de la información para prevenir fraudes, robos de información e identidad, ataques cibernéticos y fallas en la infraestructura para el manejo y almacenamiento de los datos.

Los datos se han convertido en un activo valioso para las organizaciones, y su pérdida o corrupción puede tener consecuencias financieras y reputacionales significativas es por ello la importancia de analizar y estudiar las amenazas crecientes de los ciberataques se vuelven cada vez más sofisticados, y los científicos de datos son un objetivo atractivo para los atacantes.

Intención didáctica

Esta asignatura está organizada en cinco temas que proporcionan una visión clara de seguridad en la ciencia de datos, desde los conceptos básicos de la seguridad, hasta la gestión de riesgos y controles.

El primer tema aborda los fundamentos básicos de la ciberseguridad identificando las amenazas comunes como son los virus, malware, phishing, etc, así como los tipos de

¹ Sistema de Asignación y Transferencia de Créditos Académicos

	Nombre del documento: Formato de Programa de Estudio de asignatura de Especialidad		Código: TecNM-AC-PO-007-02
			Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 2 de 13

ataques cibernéticos identificando los ciber atacantes e implementar los principios básicos de la seguridad de la información.

En el segundo tema se estudia la mitigación de ataques y protección de las redes informáticas, de tal manera que el estudiante pueda identificar cada uno de los tipos de ataque de ingeniería social, a ataques a la red, ataques a las aplicaciones otros ataques, así como identificar las vulnerabilidades de Hardware y Software, y los exploits.

En el tercer tema se aborda la seguridad en la nube a través de los modelos de nube (IaaS, PaaS, SaaS), seguridad en la nube, así como los riesgos y mejores prácticas de seguridad en la nube.

En el cuarto tema se aborda la protección de datos, desde la privacidad de los datos, la Anonimización y pseudonimización, como el cumplimiento normativo (RGPD, CCPA). Así como la seguridad de redes, desde los protocolos de la red y seguridad de la misma, como los Firewalls y sistemas de detección de intrusiones hasta los VPNs y seguridad inalámbrica. Y la seguridad de las aplicaciones desde el desarrollo seguro de software, realizar pruebas de penetración y los gestores de vulnerabilidades.

Por último, en el quinto tema se analizan los gestores de riesgos y controles iniciando de análisis de riesgos, implementación de controles de seguridad y la implementación de planes de respuesta ante incidentes.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Zihuatanejo, Gro. del 20 mayo al 28 de octubre de 2024.	Instituto Tecnológico de la Costa Grande.	Reunión de Academia semanal e intersemestral.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Los objetivos principales de la asignatura son: • Análisis de riesgos: Identificar y evaluar las amenazas a la seguridad de los datos. • Diseño de sistemas seguros: Implementar medidas de seguridad en sistemas y aplicaciones.

	Nombre del documento: Formato de Programa de Estudio de asignatura de Especialidad		Código: TecNM-AC-PO-007-02
			Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 3 de 13

- Investigación de incidentes: Responder a incidentes de seguridad y realizar análisis forenses.
- Cumplimiento normativo: Asegurar que las prácticas de seguridad cumplan con las regulaciones aplicables.
- Comunicación: Explicar conceptos técnicos a audiencias no técnicas.

5. Competencias previas

- Relaciona la ética con el desarrollo de la ciencia y la tecnología para determinar sus implicaciones sociales.
- Instala, configura y administra un gestor de base de datos para el manejo de la información de una organización, optimizando la infraestructura computacional existente.
- Configura y administra servicios de red para el uso eficiente y configurable de la infraestructura tecnológica de la organización.
- Conoce diferentes modelos de arquitectura y recomienda aplicaciones para resolver problemas de su entorno profesional.
- Desarrolla aplicaciones web dinámicas del lado del cliente y del servidor, considerando la conectividad a orígenes de datos, la interconectividad entre aplicaciones y computo en la nube.
- Aplica los paradigmas de diseño de los sistemas operativos actuales y emergentes, para el manejo de los recursos del sistema.

6. Temario

No.	Temas	Subtemas
1	Fundamentos de la Ciberseguridad.	1.1 Conceptos básicos de seguridad informática. 1.2 Amenazas comunes (virus, malware, phishing, etc.). 1.2.1 Tipos de Ataques Cibernéticos 1.2.1.1 Malware 1.2.1.2 Virus 1.2.1.3 Gusanos 1.2.1.4 Troyanos 1.2.1.5 Rootkits

	Nombre del documento: Formato de Programa de Estudio de asignatura de Especialidad	Código: TecNM-AC-PO-007-02
	Referencia a la Norma ISO 9001:2015 8.3, 8.3.1	Revisión: 0
		Página 4 de 13

		1.2.1.6 Spyware 1.3 Ciberatacantes 1.3.1 Tipos de atacantes 1.4 Principios de seguridad de la información.
2	Mitigación de ataques y protección de redes.	2.1 Ataques de Ingeniería Social 2.1.1 Phishing 2.1.2 Spear Phishing 1.2.2.3 Vishing 2.2 Ataques a la Red 2.2.1 DDoS (Ataque de Denegación de Servicio Distribuido) 2.2.2 Man-in-the-Middle 2.2.3 BootNet 1.2.4 Ataques a Aplicaciones 1.2.4.1 Inyección SQL 1.2.4.2 XSS (Cross-Site Scripting) 1.2.4.3 Ransomware 1.2.5 Otros Ataques 1.2.5.1 Ataques de fuerza bruta 1.2.5.2 Ataques de diccionario 1.2.5.3 Ataques de día cero 1.3 Vulnerabilidades y exploits 1.3.1 Vulnerabilidades de Hardware 1.3.2 Vulnerabilidades de Software
3	Seguridad en la Nube	3.1 Modelos de nube (IaaS, PaaS, SaaS). 3.2 Seguridad en la nube (IAM, encriptación, etc.). 3.3 Riesgos y mejores prácticas.
4	Protección de Datos	4.1 Privacidad de datos. 4.2 Anonimización y pseudonimización. 4.3 Cumplimiento normativo (RGPD, CCPA). 4.4 Seguridad de Redes: 4.4.1 Protocolos de red y seguridad. 4.4.2 Firewalls y sistemas de detección de intrusiones. 4.4.3 VPNs y seguridad inalámbrica. 4.4.4 Seguridad en Puertos por MacAddress 4.5 Seguridad de Aplicaciones: 4.5.1 Desarrollo seguro de software. 4.5.2 Pruebas de penetración. 4.5.3 Gestión de vulnerabilidades.

	Nombre del documento: Formato de Programa		Código: TecNM-AC-PO-007-02
	de Estudio de asignatura de Especialidad		Revisión: 0
	Referencia a la Norma ISO 9001:2015 8.3, 8.3.1		Página 5 de 13

5	Gestión de Riesgos y Controles	5.1 Análisis de riesgos. 5.2 Implementación de controles de seguridad. 5.3 Planes de respuesta a incidentes.
---	--------------------------------	--

	Nombre del documento: Formato de Programa		Código: TecNM-AC-PO-007-02
	de Estudio de asignatura de Especialidad		Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 6 de 13

7. Actividades de aprendizaje de los temas

1. Fundamentos de la Ciberseguridad.	
Competencias	Actividades de aprendizaje
Específica(s): Conocer los fundamentos básicos de la ciberseguridad identificando las amenazas comunes, y los tipos de ataques cibernéticos. 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. ● Trabajo en equipo. ● Capacidad de aplicar los conocimientos. ● Habilidades de investigación. ● Capacidad de generar nuevas ideas. ● Liderazgo. ● Habilidad para trabajar en forma. ● Autónoma. ● Búsqueda del logro.	● Investigar los conceptos clave de la seguridad informática: confidencialidad, integridad, disponibilidad, autenticación y no repudio. Elaborar un reporte de investigación con ejemplos de cada concepto y la importancia de la seguridad informática. ● Elaborar un cuadro comparativo de los diferentes tipos de amenazas cibernéticas (virus, malware, phishing, etc.) y clasifica cada uno según sus características y objetivos. Realizar una presentación visual y exponer en plenaria. ● Investigar los diferentes tipos de malware, virus, gusanos, troyanos, rootkits, spyware, sus características y cómo se propagan. Realizar un cuadro sinóptico donde se informe también sobre la prevención y mitigación de cada uno. ● Investigar el concepto de ciberatacantes, los tipos de atacantes y sobre los principios de seguridad de la información. Realizar un resumen con una presentación visual y exponer en plenaria.
2. Mitigación de ataques y protección de redes.	
Competencias	Actividades de aprendizaje
Específica(s): Aprender a mitigar los ataques de ingeniería social, a ataques a la red, ataques a aplicaciones y otros ataques, así como conocer las vulnerabilidades de hardware y software. Genéricas:	● Realizar un cuadro comparativo sobre los ataques de ingeniería social donde se identifiquen las características, señales de advertencia y protección de phishing, spear phishing, y vishing. ● Investigar sobre los ataques a la red: DDoS, y man-in-the-middle en que consisten, su impacto en las infraestructuras y cómo defenderse ante estos ataques, así como la implementación

	Nombre del documento: Formato de Programa		Código: TecNM-AC-PO-007-02
	de Estudio de asignatura de Especialidad		Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 7 de 13

● 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. ● Trabajo en equipo. ● Capacidad de aplicar los conocimientos. ● Habilidades de investigación. ● Capacidad de generar nuevas ideas. ● Liderazgo. ● Habilidad para trabajar en forma. ● Autónoma. ● Búsqueda del logro.	de firewalls y otras técnicas. Realizar reporte de la investigación. ● Investigar y realizar ejemplos de casos prácticos sobre ataques a aplicaciones, que incluya lo siguiente: Donde se puedan identificar y mitigar vulnerabilidades de inyección SQL en una base de datos web. Casos donde se encuentren y reparen vulnerabilidades XSS en una aplicación web, y un ejercicio en el que se simulen un ataque ransomware, analizar cómo proteger sus sistemas y datos mediante copias de seguridad y otras medidas preventivas. Realizar presentación visual y exponer por equipos en plenaria. ● Realizar un cuadro comparativo sobre un ataque de fuerza bruta, ataque de diccionario, vulnerabilidades de día cero recientes, analizar las estrategias para protegerse ante ellas, como el uso de parches y actualizaciones de seguridad, detallar las características de cada uno de estos. ● En equipo de trabajo los estudiantes analizan los principios fundamentales de la seguridad de la información (confidencialidad, integridad, disponibilidad) y cómo se aplican en diferentes escenarios (ej. protección de datos en redes sociales, bancos, etc.). Elaboran y discuten políticas de seguridad de la información dentro de una empresa ficticia. Los estudiantes deben desarrollar un conjunto de reglas para asegurar los sistemas y datos de la empresa. Realizar presentación visual y exposición en plenaria.
3. Seguridad en la Nube	
Competencias	Actividades de aprendizaje

	Nombre del documento: Formato de Programa de Estudio de asignatura de Especialidad		Código: TecNM-AC-PO-007-02
			Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 8 de 13

Específica(s): Conocer e identificar la seguridad en la nube a través de los modelos de nube (IaaS, PaaS, SaaS), seguridad en la nube, así como los riesgos y mejores prácticas de seguridad en la nube. 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. • Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma. • Autónoma. • Búsqueda del logro.	• Los estudiantes investigan casos de uso reales de cada modelo de nube en diferentes industrias. • Los estudiantes debaten sobre las ventajas y desventajas de cada modelo de nube en diferentes escenarios. • IaaS (Infraestructura como Servicio). Los estudiantes crean y configuran máquinas virtuales en un proveedor de IaaS (AWS, Azure, Google Cloud). Aprenden a instalar sistemas operativos, configurar redes y administrar el almacenamiento. • PaaS (Plataforma como Servicio). Los estudiantes crean una aplicación web utilizando un framework popular (Node.js, Python, Java) y la despliegan en una plataforma PaaS (Heroku, AWS Elastic Beanstalk, Google App Engine). • SaaS (Software como Servicio). Los estudiantes trabajan en un proyecto en equipo utilizando herramientas SaaS como Google Workspace o Microsoft 365. • Los estudiantes utilizan herramientas SaaS de análisis de datos (Google Analytics, Tableau Public) para analizar conjuntos de datos y extraer conclusiones.
4. Protección de Datos	
Competencias	Actividades de aprendizaje
Específica(s): Conocer y aplicar la protección de datos, desde la privacidad de los datos, la Anonimización y pseudonimización, Así como la seguridad de redes, desde los protocolos de la red y seguridad de la misma, como los Firewalls y sistemas de	• Los estudiantes investigan y comparan las definiciones de anonimización y seudonimización, analizando ejemplos prácticos de cómo se aplican en diferentes contextos (salud, finanzas, redes sociales). • Objetivo: Conocer los principios clave del RGPD y la CCPA, sus similitudes y diferencias. Actividad: Los estudiantes

	Nombre del documento: Formato de Programa		Código: TecNM-AC-PO-007-02
	de Estudio de asignatura de Especialidad		Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 9 de 13

detección de intrusiones hasta los VPNs y seguridad inalámbrica. Y la seguridad de las aplicaciones desde el desarrollo seguro de software, realizar pruebas de penetración y los gestores de vulnerabilidades. 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. ● Trabajo en equipo. ● Capacidad de aplicar los conocimientos. ● Habilidades de investigación. ● Capacidad de generar nuevas ideas. ● Liderazgo. ● Habilidad para trabajar en forma. ● Autónoma. ● Búsqueda del logro.	investigan los derechos de los interesados (acceso, rectificación, supresión, portabilidad, etc.), las obligaciones de los responsables y encargados del tratamiento, los conceptos de "datos personales", "tratamiento", "consentimiento", etc. Comparan las disposiciones del RGPD y la CCPA, identificando puntos en común y divergencias. ● Objetivo: Comprender el funcionamiento de los protocolos de red más comunes (TCP/IP, UDP, HTTP, HTTPS, DNS, etc.). Actividad: Los estudiantes investigan cómo funcionan estos protocolos, sus características, ventajas y desventajas. Pueden utilizar herramientas de análisis de tráfico de red (Wireshark) para observar cómo se intercambian paquetes de datos entre dispositivos. ● Objetivo: Identificar y comprender los principales tipos de ataques y vulnerabilidades en redes (ataques de denegación de servicio, ataques de intermediario, inyección SQL, cross-site scripting, etc.). Actividad: Los estudiantes investigan cómo se llevan a cabo estos ataques, qué vulnerabilidades explotan y cuáles son sus posibles consecuencias. Pueden realizar ejercicios prácticos simulando algunos ataques en entornos controlados (máquinas virtuales). ● Objetivo: Conocer y aplicar diferentes mecanismos de seguridad para proteger las redes (firewalls, sistemas de detección de intrusiones, VPN, cifrado, autenticación, autorización, etc.). Actividad: Los estudiantes investigan cómo funcionan
---	--

	Nombre del documento: Formato de Programa de Estudio de asignatura de Especialidad	Código: TecNM-AC-PO-007-02
		Revisión: 0
	Referencia a la Norma ISO 9001:2015 8.3, 8.3.1	Página 10 de 13

	estos mecanismos, sus ventajas y desventajas, y cómo se configuran. Pueden realizar ejercicios prácticos configurando firewalls, VPNs y otros dispositivos de seguridad.
5. Gestión de Riesgos y Controles	
Competencias	Actividades de aprendizaje
Específica(s): Conocer los gestores de riesgos y controles iniciando de análisis de riesgos, implementación de controles de seguridad y la implementación de planes de respuesta ante incidentes. 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. • Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma. • Autónoma. • Búsqueda del logro.	• Crear un cuadro sinóptico con tipos de riesgos y sus impactos. • Investigar diferentes controles de seguridad (firewalls, autenticación, etc.). Actividad: Realizar un resumen de los controles de seguridad más comunes y sus beneficios. • Objetivo: Conocer los conceptos clave relacionados con la respuesta a incidentes, como "incidente", "vulnerabilidad", "amenaza", "riesgo", etc. Actividad: Los estudiantes investigan y definen estos conceptos, analizando ejemplos prácticos de incidentes de seguridad que han ocurrido en el pasado. • Objetivo: Aprender a crear un plan de respuesta a incidentes efectivo. Actividad: Los estudiantes trabajan en grupos para elaborar un plan de respuesta a incidentes para una organización ficticia o real (con autorización). Deben definir los roles y responsabilidades, los procedimientos de detección, análisis, contención, erradicación y recuperación, así como los canales de comunicación. • Simulación de incidentes. Objetivo: Poner a prueba el plan de respuesta a incidentes mediante simulaciones. Actividad: Los estudiantes participan en simulaciones de incidentes de seguridad, donde se enfrentan a diferentes escenarios y deben aplicar los procedimientos establecidos en el plan. • Comunicación y coordinación. Objetivo: Aprender a comunicarse y coordinarse durante un incidente de seguridad. Actividad: Los

	Nombre del documento: Formato de Programa de Estudio de asignatura de Especialidad		Código: TecNM-AC-PO-007-02
			Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 11 de 13

	estudiantes practican la comunicación con diferentes partes interesadas (equipos técnicos, dirección, clientes, autoridades, etc.) durante un incidente de seguridad.
--	---

8. Práctica(s)

● Investigar y realizar ejemplos de casos prácticos sobre ataques a aplicaciones, que incluya lo siguiente: Donde se puedan identificar y mitigar vulnerabilidades de inyección SQL en una base de datos web. Casos donde se encuentren y reparen vulnerabilidades XSS en una aplicación web, y un ejercicio en el que se simulen un ataque ransomware, analizar cómo proteger sus sistemas y datos mediante copias de seguridad y otras medidas preventivas. ● Crear un grafo visualizando relaciones de un ataque cibernético utilizando herramientas como Gephi o Python (NetworkX).
--

	Nombre del documento: Formato de Programa de Estudio de asignatura de Especialidad		Código: TecNM-AC-PO-007-02
			Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 12 de 13

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) de la asignatura, considerando las siguientes fases:

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.
- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitaria, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.
- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y específicas a desarrollar.
- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

	Nombre del documento: Formato de Programa de Estudio de asignatura de Especialidad		Código: TecNM-AC-PO-007-02
			Revisión: 0
	Referencia a la Norma ISO 9001:2015	8.3, 8.3.1	Página 13 de 13

10. Evaluación por competencias

Son las técnicas, instrumentos y herramientas sugeridas para constatar los desempeños académicos de las actividades de aprendizaje.

11. Fuentes de información

1. Salomon, D. (2006). *Privacidad y seguridad de los datos: Encriptación y protección del contenido digital*. Springer.
2. Gupta, B. B., & Sharma, S. (2020). *Ciencia de datos para ciberseguridad*. Wiley.
3. Bertino, E. (Ed.). (2017). *Seguridad y privacidad en la gestión de datos*. Springer.
4. Fernández Isabel, Alberto - Diego, Isaac Martín DE. *Ciencia de datos para la ciberseguridad*. RA-MA Editorial 2020 ISBN: 9788418551192
5. Urcuqui L., Christian Camilo - García P., Melisa - Osorio Q., José Luis. *Ciberseguridad: un enfoque desde la ciencia de datos*. Editorial Universidad Icesi. ISBN: 9781512973891, 9789588936550
6. Guerra Soto, Mario, *Ciberinteligencia de la amenaza en entornos corporativos*, RA-MA Editorial Ed. 2023, ISBN: 9788419857460