

1. Datos Generales de la asignatura

Nombre de la asignatura:	Ciberseguridad empresarial
Clave de la asignatura:	CIF2604
SATCA¹:	3 -2 – 5
Carrera:	<ul style="list-style-type: none">• Ingeniería en Sistemas Computacionales• Ingeniería en Tecnologías de la Información y Comunicaciones• Ingeniería en Inteligencia Artificial• Ingeniería en Ciencia de Datos• Ingeniería en Desarrollo de Aplicaciones.• Ingeniería en Informática

2. Presentación

Caracterización de la asignatura

Esta asignatura proporciona las bases técnicas y conceptuales para la integración de los conocimientos y habilidades en materia de Ciberseguridad en entornos empresariales, con el propósito de asegurar el correcto funcionamiento y desempeño de los componentes que integran la infraestructura informática de la empresa mediante la prevención de ataques cibernéticos, apegándose a los principios éticos y de responsabilidad social.

El programa de la asignatura está diseñado para contribuir en la formación integral de las y los estudiantes del Tecnológico Nacional de México (TecNM), ya que proporciona las competencias necesarias para:

- Identificar los tipos de amenazas que ponen en riesgo la seguridad de los activos informáticos de la empresa, con alto sentido de la ética y de la responsabilidad.
- Implementar sistemas de seguridad perimetral en entornos tecnológicos empresariales para integrar soluciones de seguridad con responsabilidad social en las organizaciones.
- Realizar el monitoreo, análisis y control de la red empresarial utilizando las herramientas de ciberseguridad pertinentes, con perspectiva ética, de respeto por la persona, confidencialidad, privacidad y de responsabilidad social.
- Evaluar riesgos de seguridad y vulnerabilidad en la infraestructura de tecnologías de la información con apoyo de herramientas de vanguardia automatizadas de acuerdo con metodologías, normas y estándares de excelencia.
- Diseñar políticas de seguridad informática para establecer controles de seguridad pertinentes, capacitación de todos los miembros de la organización, simulacros y evaluación continua de la cultura de la ciberseguridad en la empresa, atendiendo los principios de no discriminación, Inclusión y equidad social.

¹ Sistema de Asignación y Transferencia de Créditos Académicos

La asignatura consiste en cinco temas, orientados a la implementación de políticas y seguimiento de buenas prácticas relacionadas con la gestión de la ciberseguridad en las empresas.

El primer tema tiene como objetivo abordar los principios de ciberseguridad en los entornos empresariales, así como conocer cuáles son los vectores de ataques más comunes que propician a una vulneración de los sistemas informáticos.

El segundo tema atiende los elementos correspondientes a la seguridad perimetral y su importancia dentro del esquema de seguridad de la empresa, asimismo se integra la configuración de seguridad de instancias en la nube.

El tercer tema se enfoca en la seguridad de redes inalámbricas, considerando que actualmente se tiene una alta preferencia por el uso de dispositivos móviles, dispositivos IoT, entre otros, que hacen uso de la tecnología inalámbrica y que representan potenciales puntos de ataque.

El cuarto tema atiende las necesidades de seguridad en los equipos que se encuentran dentro de la empresa, tales como computadoras, servidores y dispositivos de red, que forman parte fundamental de la infraestructura informática de la organización.

Esta materia se relaciona con las materias de:

Administración de redes

Taller de Sistemas Operativos

Fundamentos de Ciberseguridad

Intención didáctica

La asignatura se aborda desde un enfoque teórico-práctico en el cual el estudiante desarrollará los conocimientos y habilidades para evaluar, implementar y reforzar políticas que benefician a la seguridad de la información y de los equipos que integran la infraestructura informática de la empresa.

A través de las cinco unidades temáticas que componen el programa de la materia, el estudiante conocerá cuáles son los elementos básicos que componen la ciberseguridad en un entorno empresarial. De igual manera, conocerá cuáles son los tipos de ataques y riesgos de seguridad más comunes en las empresas y que representan posibles daños irreparables a la información y reputación de la organización. Además, de proponer, diseñar e implementar políticas que atiendan los requerimientos de ciberseguridad en las empresas.

Así también, se sugiere que en las prácticas se utilice software de diferentes plataformas que permita el desarrollo de la capacidad del estudiante de integrar soluciones con diferentes tecnologías, plataformas, dispositivos y elementos, basados en estándares utilizados ampliamente en los entornos comerciales.

Se debe privilegiar el desarrollo de las prácticas en un ambiente de respeto, ética, confidencialidad y compromiso social, toda vez que la información que puede ser visible a través de los diversos sistemas de monitoreo y análisis puede estar protegida por legislaciones, reglamentos y políticas aplicables.

En el transcurso del desarrollo de la materia, el docente debe incentivar a que el estudiante se desenvuelva de manera proactiva y responsable, atendiendo el respeto a los valores éticos, la responsabilidad social y el trabajo en equipo.

Además, se debe fomentar el pensamiento crítico, la curiosidad, el entusiasmo y el interés en el desarrollo de las actividades y la retroalimentación positiva, que permita el reforzamiento de los conocimientos y habilidades adquiridas.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México, campus Tuxtla Gutiérrez del 18 septiembre al 26 de octubre de 2024	Representantes de los Institutos Tecnológicos de: Tuxtla Gutiérrez, Tapachula y Frontera Comalapa. Enrique Abel Sánchez Velázquez Ezequiel Cruz Wong Carlos Alberto López Escobar Brenda Guadalupe Pinto Vázquez	Foro Estatal Actualización Curricular para la Consolidación de Proyectos Estratégicos del TecNM en el Estado de Chiapas

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Diseña, configura e implementa políticas de seguridad de red para su aplicación en la organización.
Diseña e integra soluciones de seguridad a nivel de red para promover la protección de la infraestructura tecnológica de la organización.
Desarrolla propuestas relacionadas con la seguridad de la infraestructura tecnológica que contribuya al desarrollo de la protección de la información en la organización.

5. Competencias previas

Configura y administra servicios de red para el uso eficiente y confiable de la infraestructura tecnológica de la organización
--

Conoce, identifica, selecciona y administra diferentes sistemas operativos con el fin de resolver problemáticas reales, así como aplicar procedimientos de interoperabilidad entre diferentes sistemas operativos.

6. Temario

No.	Temas	Subtemas
1	Fundamentos de Ciberseguridad Empresarial	1.1 Impacto de la ciberseguridad en la empresa. 1.2 Tipos de ciberataques: ingeniería social, phishing, malware, ransomware, DDoS, MITM, exploits.
2	Seguridad perimetral	2.1 Implementación de sistemas de monitoreo y detección (Firewalls, IDS, IPS). 2.2 Control de acceso y autenticación. 2.3 Filtrado de contenidos 2.4 Políticas y privilegios de red. 2.5 VPNs 2.6. Seguridad perimetral en la nube
3	Seguridad de redes inalámbricas	3.1 Protocolos de cifrado en redes inalámbricas. 3.2 Autenticación en redes inalámbricas (radius, portal cautivo, 802.1x) 3.3 Configuración e implementación de redes inalámbricas
4	Seguridad de equipos	4.1 Antivirus y EDR 4.2 Hardening en servidores y estaciones de trabajo. 4.3 Hardening en dispositivos de red
5	Cultura Organizacional de Seguridad	5.1 Planes de recuperación ante desastres y continuidad del negocio (BCP, DRP). 5.2 Diseño de programas de capacitación y simulacros de ciberseguridad (phishing tests, simulaciones de ataques). 5.3 Evaluación continua de la cultura organizacional en seguridad. 5.4 Roles y responsabilidades de los empleados en la ciberseguridad.

7. Actividades de aprendizaje de los temas

1. Fundamentos de Ciberseguridad Empresarial	
Competencias	Actividades de aprendizaje
<p>Específica(s): Conocer la importancia de la ciberseguridad y su impacto en las actividades de la empresa.</p> <p>Genéricas: Capacidad de análisis y síntesis, Habilidad para buscar y analizar información proveniente de fuentes diversas, Trabajo en equipo, Capacidad de generar nuevas ideas.</p>	<ol style="list-style-type: none"> 1. Investigar el rol de la ciberseguridad en las empresas 2. Realizar una presentación sobre los tipos de amenazas informáticas y sus consecuencias para la organización. 3. Discutir en grupo incidentes recientes de alto impacto de seguridad informática en las empresas
2. Seguridad perimetral	
Competencias	Actividades de aprendizaje
<p>Específica(s): Implementar configuraciones y políticas de seguridad en la red perimetral de la organización.</p> <p>Genéricas: Capacidad de análisis y síntesis, Capacidad de organizar y planificar, Solución de problemas, Toma de decisiones, Trabajo en equipo, Capacidad de aplicar nuevos conocimientos, Habilidad para trabajar de forma autónoma, Búsqueda del logro, Apego a los valores éticos.</p>	<ol style="list-style-type: none"> 1. Evaluación de las distintas soluciones de seguridad perimetral que existen actualmente, tanto de software libre como software comercial. 2. Instalación, configuración y puesta en operación de firewall de software libre o de uso gratuito. 3. Diseño de políticas de seguridad de red perimetral que promuevan la mejora en la protección de los servicios de red. 4. Implementación de una VPN utilizando software libre. 5. Configuración de la red virtualizada en la nube utilizando las ofertas educativas disponibles de los proveedores de nube existentes.
3. Seguridad de redes inalámbricas	
Competencias	Actividades de aprendizaje
<p>Específica(s): Implementar configuraciones y políticas de seguridad en las redes inalámbricas de la organización.</p> <p>Genéricas: Capacidad de análisis y síntesis, Capacidad de organizar y</p>	<ol style="list-style-type: none"> 1. Evaluación de los distintos protocolos de cifrado de red inalámbrica disponibles y su aplicación correspondiente a las necesidades de la organización.

planificar, Solución de problemas, Toma de decisiones, Trabajo en equipo, Capacidad de aplicar nuevos conocimientos, Habilidad para trabajar de forma autónoma, Búsqueda del logro, Apego a los valores éticos.	<p>2. Implementación de servidores de autenticación para los dispositivos que se conectan de manera inalámbrica a la red.</p> <p>3. Configuración de redes inalámbricas con base a las necesidades de la organización.</p>
4. Seguridad de equipos	
Competencias	Actividades de aprendizaje
<p>Específica(s): Implementar configuraciones y políticas de seguridad en los equipos informáticos de la organización.</p> <p>Genéricas: Capacidad de análisis y síntesis, Capacidad de organizar y planificar, Solución de problemas, Toma de decisiones, Trabajo en equipo, Capacidad de aplicar nuevos conocimientos, Habilidad para trabajar de forma autónoma, Búsqueda del logro, Apego a los valores éticos.</p>	<p>1. Comparar las soluciones de seguridad existentes y sus diferentes enfoques en materia de protección de estaciones de trabajo y servidores.</p> <p>2. Evaluar e implementar configuraciones adicionales que mejoren la seguridad en sistemas operativos de escritorio y de servidor.</p> <p>3. Evaluar e implementar configuraciones adicionales que mejoren la seguridad de los dispositivos de red de la organización.</p>
5. Cultura Organizacional de Seguridad	
Competencias	Actividades de aprendizaje
<p>Específica(s): Implementar políticas que fortalezcan la cultura de la ciberseguridad en el personal de la organización.</p> <p>Genéricas: Capacidad de análisis y síntesis, Capacidad de organizar y planificar, Solución de problemas, Toma de decisiones, Trabajo en equipo, Capacidad de aplicar nuevos conocimientos, Habilidad para trabajar de forma autónoma, Búsqueda del logro, Apego a los valores éticos.</p>	<p>1. Investigar y comparar los marcos de trabajo actuales en materia de recuperación de desastres posteriores a los incidentes de ciberseguridad.</p> <p>2. Diseñar estrategias que permitan una mejora en la cultura de la ciberseguridad dentro de la organización.</p> <p>3. Implementar simulacros de ataques comunes a los miembros de todos los niveles de la organización.</p>

8. Práctica(s)

Análisis de incidentes históricos: Estudio de casos reales de ataques cibernéticos a grandes corporaciones, así como el análisis de los vectores de ataque utilizados, software implementado y consecuencias del ataque, así como la evaluación de las respuestas aplicadas.

Configuración e implementación de sistemas de ciberseguridad: Aplicación de herramientas de software y hardware para la detección y prevención de amenazas en una infraestructura simulada y generación de políticas de configuración que fortalezcan la seguridad de la información en la organización.

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 comunitario, 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.

10. Evaluación por competencias

A continuación, se especifica para cada competencia a formar las evidencias y métodos de evaluación que se sugiere utilizar para cada una competencia:

Competencia 1: Diseña, configura e implementa políticas de seguridad de red para su aplicación en la organización.

- **Evidencia 1:** Desarrollo de un proyecto de políticas de seguridad
 - **Descripción:** Los estudiantes diseñarán un conjunto de políticas de seguridad de red adaptadas a un caso empresarial específico. Incluirán controles de acceso, procedimientos de gestión de incidentes, y lineamientos de seguridad de redes inalámbricas.
 - **Criterios de Evaluación:** Coherencia de las políticas, claridad y aplicabilidad de los controles, alineación con los estándares de ciberseguridad.
- **Evidencia 2:** Configuración y simulación de seguridad en redes
 - **Descripción:** Mediante un entorno de simulación o red de laboratorio, los estudiantes implementarán configuraciones de seguridad, como firewalls y sistemas de detección de intrusos.
 - **Criterios de Evaluación:** Precisión en la configuración, efectividad de los controles en el entorno simulado, y capacidad para mitigar amenazas simuladas.

Competencia 2: Diseña e integra soluciones de seguridad a nivel de red para promover la protección de la infraestructura tecnológica de la organización.

- **Evidencia 1:** Propuesta de diseño de infraestructura de seguridad perimetral
 - **Descripción:** Los estudiantes presentarán un diseño de arquitectura de seguridad perimetral para una organización que contemple la segregación de redes, protección de equipos críticos, y aseguramiento de redes inalámbricas.
 - **Criterios de Evaluación:** Complejidad y adecuación de las soluciones, integración con la infraestructura de red, y justificación técnica de los componentes seleccionados.
- **Evidencia 2:** Prueba de concepto de solución de seguridad en redes inalámbricas
 - **Descripción:** Desarrollarán y probarán una propuesta de seguridad en redes inalámbricas que contemple controles de acceso, autenticación y cifrado para una organización simulada.
 - **Criterios de Evaluación:** Funcionalidad de los controles implementados, robustez de las configuraciones y mitigación de riesgos asociados a redes inalámbricas.

Competencia 3: Desarrolla propuestas relacionadas con la seguridad de la infraestructura tecnológica que contribuya al desarrollo de la protección de la información en la organización.

- **Evidencia 1:** Informe de análisis de vulnerabilidades en equipos y dispositivos
 - **Descripción:** Realizarán un análisis de vulnerabilidades en una infraestructura simulada, identificando áreas de riesgo y proponiendo mejoras específicas para proteger los equipos.
 - **Criterios de Evaluación:** Exhaustividad del análisis, identificación precisa de vulnerabilidades, y calidad de las propuestas de mitigación.

- **Evidencia 2:** Plan de Cultura Organizacional de Seguridad
 - **Descripción:** Diseñarán un plan para fomentar la cultura de seguridad en una organización ficticia, abordando la capacitación del personal y políticas de concienciación.
 - **Criterios de Evaluación:** Adecuación del plan a la organización simulada, propuestas realistas y sostenibles, y alineación con las mejores prácticas de ciberseguridad organizacional.

Métodos de Evaluación

- **Proyectos y entregables:** Se evaluarán mediante rúbricas detalladas para medir la coherencia, profundidad, y aplicabilidad de los diseños.
- **Simulaciones y prácticas de laboratorio:** Evaluación de desempeño en actividades prácticas de configuración y pruebas de seguridad.
- **Autoevaluación y coevaluación:** Refuerzan la competencia de trabajo en equipo y responsabilidad profesional en la implementación de políticas de ciberseguridad.

Estas sugerencias de evaluación por competencias permitirá a los estudiantes demostrar de manera integral su dominio de los contenidos temáticos y aplicarlos en un contexto empresarial, sin embargo queda a consideración del docente aplicarlos.

11. Fuentes de información

Deutsch, V. E. (2022). *Ciberseguridad para directivos: riesgos, control y eficiencia de las tecnologías de la información*: (1 ed.). LID Editorial España.

<https://elibro.net/es/ereader/ittuxtlagtz/269669>

Beltrán, M. (Coord.) & Sevillano, F. (Coord.). (2021). *Ciberseguridad industrial e infraestructuras críticas*: (1 ed.). RA-MA Editorial.

<https://elibro.net/es/lc/ittuxtlagtz/titulos/222659>

Arroyo Guardado, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). *Ciberseguridad*: (1 ed.). Los libros de la Catarata.

<https://elibro.net/es/lc/ittuxtlagtz/titulos/233122>

Gómez Hervás, N. D. C. (2021). *Normativa de Ciberseguridad*: (1 ed.). RA-MA Editorial.

<https://elibro.net/es/lc/ittuxtlagtz/titulos/222663>

National Institute of Standards and Technology (NIST), (2024), The NIST Cybersecurity Framework (CSF) 2.0, U.S. Department of Commerce:

<https://doi.org/10.6028/NIST.CSWP.29>