1.- DATOS DE LA ASIGNATURA

Nombre de la asignatura:	**Seguridad Informática**
Carrera:	**Ingeniería en Sistemas Computacionales**
Clave de la asignatura:	**SIi-1601**
(Créditos) SATCA:	**3-4-7**

2.- PRESENTACIÓN

Caracterización de la asignatura.

Esta materia aporta al perfil del profesionista la visión de los aspectos que influyen en la seguridad informática. También proporcionará los conocimientos básicos de seguridad para el desarrollo de proyectos de tecnologías de información.

Se inicia dando una introducción de la historia de la computación en épocas de cuando estaba casi inexistente la seguridad Informática. Así se introducen conceptos como Seguridad informática, objetivos, misión y evolución. Temas como normatividad, esquemas y servicios de seguridad son detallados a fondo

En la unidad siguiente es dedicado completamente a los conceptos de Amenazas y Vulnerabilidades físicas y lógicas a los sistemas informáticos.

En la tercera unidad se da seguimiento a los conceptos de la segunda unidad mediante la identificación de ataques y técnicas de intrusión.

La segunda y tercera unidad hace hincapié a la identificación de problemas de la seguridad informática, sin embargo en la cuarta unidad se enfoca en profundizar en el tema de Políticas de Seguridad Informática en las Organizaciones, que implementaran mecanismos contra amenazas y vulnerabilidades.

La quinta y sexta unidad se basan en realizar análisis de riesgos de costo-beneficio al aplicar políticas Informática contra amenazas y vulnerabilidades o seguir simplemente los conceptos de ética informática.

3.- COMPETENCIAS A DESARROLLAR

Competencias Específicas	**Competencias genéricas**
Desarrollar soluciones para problemas de seguridad informática, analizando el tipo de vulnerabilidades, proponiendo soluciones tanto teóricas como prácticas e implementando políticas de calidad como herramientas de seguridad.	**Competencias instrumentales:** • Capacidad de análisis y síntesis • Capacidad de organizar y planificar • Comunicación oral y escrita • Habilidad para buscar y analizar • información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. **Competencias interpersonales:** • Capacidad crítica y autocrítica • Capacidad de trabajar en equipo • Capacidad de comunicar sus ideas • Capacidad de liderazgo **Competencias sistémicas:** • Capacidad de aplicar los conocimientos en la práctica • Habilidades de investigación • Capacidad de aprender • Capacidad de adaptarse a nuevas situaciones • Capacidad de generar nuevas ideas (creatividad) • Liderazgo • Habilidad para trabajar en forma autónoma • Preocupación por la calidad

4.- HISTORIA DEL PROGRAMA

Lugar y Fecha	Participantes	Evento
Instituto Tecnológico de Tláhuac, México D.F. 18 de Mayo de 2012 Instituto Tecnológico de Tláhuac, CDMX. 11 de Abril de 2016.	Academia de Sistemas y Computación	Revisión y actualización de contenidos temáticos del programa de estudios para esta especialidad.

5.- OBJETIVO(S) GENERAL(ES) DEL CURSO (competencias específicas a desarrollar).

El alumno comprenderá y aplicará los métodos y elementos que le permitan planificar el desarrollo de una arquitectura de seguridad, con base en la identificación y análisis de amenazas, ataques y vulnerabilidades en los sistemas y redes de cómputo, enmarcados en una base ética.

6.- COMPETENCIAS PREVIAS

Tener el conocimiento de conceptos sobre temas como el manejo de sistemas operativos, Bases de datos, Sistemas de Información y Redes de Telecomunicaciones. Específicamente los temas de Capas del modelo OSI y Técnicas de Conmutación TCP/IP.

7.- TEMARIO

Unidad	Temas	Subtemas
1	Fundamentos teóricos	1.1 Introducción 1.1.1 Concepto de Seguridad Informática 1.1.3 Objetivos y misión de la Seguridad Informática 1.2 Normatividad de la Seguridad Informática 1.2.1 Normas de Seguridad a través de la Historia 1.2.1.1 TSEC / Libro Naranja 1.2.1.2 ITSEC 1.2.1.3 CTCPEC 1.2.1.4 FC-ITS 1.2.2 Criterios Comunes / ISO 15408 1.2.3 ISO 17799 1.2.4 Nuevas Tendencias 1.2.4.1 OCTAVE 1.3 Esquema de Seguridad basado en Criterios Comunes: Perfiles de Protección. 1.3.1 Definición y propósito 1.3.2 Estructura 1.3.2.1 Introducción 1.3.2.2 Descripción del objeto de evaluación 1.3.2.3 Entorno de Seguridad 1.3.2.4 Hipótesis 1.3.2.5 Amenazas 1.3.2.6 Políticas de la Organización 1.3.2.7 Nivel de Garantía general requerido 1.3.2.8 Objetivos de Seguridad 1.3.2.9 Requerimientos Funcionales y de Garantía 1.3.2.10 Justificación 1.4 Servicios de Seguridad 1.4.1 Confidencialidad 1.4.2 Autenticación 1.4.3 Integridad 1.4.4 No repudio 1.4.5 Control de acceso 1.4.6 Disponibilidad

2	Amenazas y vulnerabilidades	1.5 Ética informática 1.5.1 Concepto de Ética informática 1.5.2 Códigos Deontológico en Informática 1.5.3 Contenidos de la Ética Informática 1.5.4 Actualidad de la Ética Informática 1.5.5 Psicología del Intruso 2.1 Amenazas 2.1.1 Definición 2.1.2 Fuentes de amenaza 2.1.2.1 Factor humano 2.1.2.1.1 Tipos: ingeniería social, robo, fraude, sabotaje, intrusos, etc. 2.1.2.1.2 Hardware 2.1.2.1.3 Tipos: mal diseño, errores de fabricación, suministro de energía, etc. 2.1.2.2 Red de datos 2.1.2.2.1 Tipos: topología seleccionada, sistema operativo, sistema de administración, monitoreo, etc. 2.1.2.3 Software 2.1.2.3.1 Tipos: software de desarrollo, software de aplicación, código malicioso, virus, etc. 2.1.2.4 Desastres naturales 2.1.2.4.1 Tipos: inundaciones, Terremotos, fuego, viento, etc. 2.2 Tendencias en Ataques y Nuevos Problemas de Seguridad 2.2.1 SPAM 2.2.2 Malware 2.2.3 Exploits de Días Cero 2.2.4 Metasploits 2.2.5 Otros 2.3 Vulnerabilidades 2.3.1 Definición 2.3.2 Tipos de vulnerabilidades 2.3.2.1 Física 2.3.2.2 Natural 2.3.2.3 Hardware 2.3.2.4 Software 2.3.2.5 Red

3	Identificación de ataques y técnicas de intrusión	3.1 Reconocimiento y obtención de información. 3.1.1 Bases de datos públicas 3.1.2 WEB 3.1.3 DNS 3.1.4 Keyloggers 3.1.5 Ingeniería social 3.1.6 Otros 3.2 Identificación de vulnerabilidades 3.2.1 Ataques a redes telefónicas 3.2.2 Ataques a Telefonía Inalámbrica 3.2.3 Barrido de Puertos 3.2.4 Identificación de Firewalls 3.2.4.1 Interpretación de reglas y filtros 3.2.5 Identificación de Sistemas Operativos Fingerprinting. 3.2.5.1 Métodos de identificación 3.2.6 Escaneo a Redes Inalámbricas 3.2.7 Instalaciones Físicas 3.2.8 Configuración de Servicios y Servidores 3.2.9 Software 3.2.10 Otros 3.3 Explotación y obtención de acceso a Sistemas y Redes 3.3.1 Promiscuidad en Redes 3.3.2 Robo de identidad 3.3.3 Engaño a Firewalls y Detectores de intrusos 3.3.4 Vulnerabilidades en el Software 3.3.4.1 Buffer Overflows 3.3.4.2 Heap Overflows 3.3.4.3 Formato de Cadena 3.3.4.4 Race Conditions 3.3.4.5 SQL Injection 3.3.4.6 Cross-Site & Cross- Domain Scripting 3.3.4.7 Virus y gusanos 3.3.4.8 Otros 3.3.5 Ataques a contraseñas 3.3.6 Debilidad de los Protocolos de Red 3.3.7 Ataques a Servicios 3.3.8 Negación de Servicio 3.3.9 Ataques a Redes Inalámbricas

4	Control de la seguridad informática	3.3.9.1 Denegación de Servicio 3.3.9.2 Ataque de Hombre en Medio 3.3.9.3 ARP Poisoning 3.3.9.4 WEP key-cracking 3.3.9.5 Nuevos Métodos de Ataque en Redes inalámbricas 3.4 Mantener el acceso a Sistemas Comprometidos 3.4.1 Puertas traseras 3.4.2 Caballos de Troya 3.4.3 Rootkits 3.4.4 Otros 3.5 Eliminación de evidencias 3.5.1 Edición de Bitácoras 3.5.2 Ocultar información 3.5.3 Estenografía 3.5.4 Nuevos métodos 4.1 Auditoría de Red 4.1.1 Concepto de Auditoría sobre la Red 4.1.2 Herramientas de Auditoría 4.1.3 Mapeo de la Red 4.1.4 Monitoreo de Red 4.1.5 Auditoría a Firewalls 4.1.6 Pruebas de Penetración sobre redes 4.1.7 Análisis de información y resultados 4.2 Auditoría a Sistemas 4.2.1 Checklist de Seguridad 4.2.2 Baseline del Sistema 4.2.3 Auditoría a las políticas del sistema 4.2.4 Auditoría a usuarios 4.2.5 Comandos del sistema 4.2.6 Herramientas para realizar auditoría 4.2.7 Auditoría a los Registros y Bitácoras del Sistema

		4.2.8 Auditoría a la Capacidad de Recuperación ante desastres 4.2.9 Auditoría a la Configuración del Sistema 4.2.10 Análisis de la Información y Resultados 4.3 Análisis forense a sistemas de cómputo 4.3.1 Introducción al Análisis Forense en Sistemas de Cómputo 4.3.2 Obtención y Protección de la Evidencia 4.3.3 Análisis Forense sobre Sistemas 4.3.3.1 Imágenes en Medios de Almacenamiento 4.3.3.2 Revisión de Bitácoras 4.3.3.3 Revisión del Sistema de Archivos 4.3.3.3.1 Tiempos de modificación, acceso y creación 4.3.3.4 Revisión de procesos 4.3.3.5 Herramientas y técnicas del Análisis forense 4.3.4 Herramientas para obtener información de la Red 4.3.5 Análisis de la Información y Resultados 4.3.6 Sistemas de detección de intrusos 4.3.6.1 Aplicación de los SDI en la SI 4.3.6.2 Tipos de sistemas de DI 4.3.6.3 Nivel de interacción de los SDI 4.4 Respuesta y Manejo de Incidentes 4.4.1 Respuesta a Incidentes 4.4.2 Creación de un equipo de respuesta a Incidentes de Seguridad Informática
5	Análisis del riesgo	5.1 Terminología básica 5.1.1 Activos 5.1.2 Riesgo 5.1.3 Aceptación 5.1.4 Análisis del riesgo 5.1.5 Manejo del riesgo 5.1.6 Evaluación

		5.1.7 Impacto 5.1.8 Pérdida esperada 5.1.9 Vulnerabilidad 5.1.10 Amenaza 5.1.11 Riesgo residual 5.1.12 Controles 5.2 Análisis cuantitativo 5.3 Análisis cualitativo 5.4 Pasos del análisis de riesgo 5.4.1 Identificación y evaluación de los activos 5.4.2 Identificación de amenazas 5.4.3 Identificación de vulnerabilidades 5.4.4 Impacto de ocurrencia de una amenaza 5.4.5 Controles en el lugar 5.4.6 Riesgos residuales 5.4.7 Identificación de los controles adicionales 5.4.8 Preparación de un informe del análisis de Riesgo 5.5 Análisis costo-beneficio 5.6 Procedimientos y planes de contingencia 5.6.1 Procedimientos Preventivos 5.6.2 Procedimientos Correctivos 5.6.3 Planes de Contingencia 5.6.3.1 Objetivos y características de un plan de contingencias 5.6.3.2 Fases del plan de contingencia 5.6.3.2.1 Análisis y Diseño 5.6.3.2.2 Desarrollo de un plan de contingencias 5.6.3.2.3 Pruebas y Mantenimiento
6	Políticas de Seguridad Informática de la Organización	6.1 Políticas de seguridad informática 6.1.1 Objetivo de una política de seguridad 6.1.2 Misión, visión y objetivos de la organización 6.1.3 Principios fundamentales de las políticas de seguridad 6.1.4 Políticas para la confidencialidad 6.1.5 Políticas para la integridad 6.1.6 Modelos de seguridad: abstracto, concreto, de control de acceso y flujo de información

		6.1.7 Desarrollo de políticas orientadas a servicios de seguridad 6.1.8 Publicación y difusión de las políticas de seguridad 6.2 Legislación Mexicana 6.2.1 Acceso Ilícito a Sistemas 6.2.2 Código Penal 6.2.3 Derechos de Autor 6.2.4 Actualidad de la legislación sobre delitos informáticos

8.-SUGERENCIAS DIDÁCTICAS (desarrollo de competencias genéricas)

El profesor debe: Ser competente en la disciplina que está bajo su responsabilidad y aplicar los conceptos de la asignatura. Desarrollar la capacidad para coordinar y trabajar en equipo; orientar el trabajo del estudiante y potenciar en él la autonomía, el trabajo cooperativo y la toma de decisiones.
Tomar en cuenta el conocimiento de los estudiantes como punto de partida y como obstáculo para la construcción de nuevos conocimientos.

- Propiciar actividades de búsqueda, selección y análisis de información en distintas fuentes y explicarlo mediante un mapa conceptual, mental o cuadro sinóptico.
- Proponer un caso de estudio de seguridad física y lógica, en el cual el estudiante determine las diferentes fases del mismo, para discutirlo en grupos de trabajo y proponer soluciones.
- Fomentar la participación del estudiante mediante tormenta de ideas, exposiciones que permita que propicie el uso adecuado de conceptos, y de terminología de la seguridad Informática.
- Proponer problemas que permitan al estudiante la integración de contenidos de la asignatura y entre distintas asignaturas, para su análisis y solución.
- Propiciar en el estudiante la lectura y reflexión de artículos relacionados con la asignatura.
- Proporcionar al estudiante la relación de los contenidos de temáticos con el desarrollo de cuestionarios de investigación y ensayos sobre el estado de arte en los temas de este programa de estudio.
- Exponer los proyectos finales.

9.-SUGERENCIAS DE EVALUACIÓN

Se sugiere que el estudiante proponga en cada unidad realice trabajos de investigación, ensayos y/o casos de estudio reales sobre los temas en esa unidad. Se recomienda que los trabajos sean desarrollados por equipos de trabajo cuidando la participación activa de cada uno de los integrantes. También debe de fomentarse y evaluarse la investigación e incluir los resultados de las mismas como sustento en la toma de decisiones en el desarrollo del proyecto. La evaluación debe ser continua y formativa por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Ponderar tareas.
- Participación y desempeño del alumno en el aula
- Dar seguimiento al desempeño integral de alumno en desarrollo de programa (dominio de los conceptos, capacidad de la aplicación de los conocimientos en problemas reales en los laboratorios).
- Dar valor a la participación del alumno (exposición, mesas redondas y debates).
- Exámenes.

10.-UNIDADES DE APRENDIZAJE

UNIDAD 1.- Fundamentos teóricos

Competencia específica a desarrollar	Actividades de Aprendizaje
Conocer los conceptos, objetivos y antecedentes históricos de la Seguridad Informática, así como el de los modelos de seguridad que le permitan adoptar los Estándares destinados a planificar un esquema de seguridad en una organización.	Panel sobre la importancia de la seguridad informática Investigación de los conceptos básicos Exposición del profesor de algunos ejemplos sobre la importancia de la seguridad informática Ensayo sobre técnicas, normatividad, esquemas y servicios de la seguridad informática.

UNIDAD 2.-Amenazas y vulnerabilidades

Competencia específica a desarrollar	Actividades de Aprendizaje
Conocer, identificar y explicar los diferentes tipos de amenazas y vulnerabilidades así como las fuentes que las ocasionan.	Realizar un plan de seguridad en alguna empresa o institución. Exposición por parte de los alumnos sobre el plan de seguridad realizado. Investigación de las consideraciones técnicas para la seguridad

	física. Comentar en clase sobre términos como SPAM, las amenazas en la actualidad, Malware, etc.

UNIDAD 3.-Identificación de ataques y técnicas de intrusión

Competencia específica a desarrollar	Actividades de Aprendizaje
Conocer, identificar y explicar los métodos y técnicas de ataque e intrusión a redes y sistemas.	Realizar un plan de seguridad en alguna empresa o institución. Exposición por parte de los alumnos sobre el plan de seguridad realizado. Investigación de las consideraciones técnicas para la seguridad lógica.

UNIDAD 4.- Control de la Seguridad Informática

Competencia específica a desarrollar	Actividades de Aprendizaje
Conocer los métodos y herramientas para el análisis forense en informática, así como mantener el control sobre redes y dispositivos	Realizar investigación sobre los distintos tipos de auditorías, que se aplican en los controles de la seguridad informática, tomando en cuenta prácticas en cada una de ellas.

UNIDAD 5.-Análisis del riesgo

Competencia específica a desarrollar	Actividades de Aprendizaje
Conocer, identificar, seleccionar y aplicar las técnicas y métodos que le permitan llevar a cabo actividades concernientes a la evaluación de riesgos dentro de una organización.	Investigar los conceptos básicos y debatir en clase los diferentes análisis, tanto cualitativos como cuantitativos, identificación de amenazas.

UNIDAD 6.- Políticas de seguridad informática de la organización

Competencia específica a desarrollar	Actividades de Aprendizaje
Entender, explicar, valorar y adquirir la capacidad para desarrollar políticas de seguridad informática así como los procedimientos y planes de contingencia que le permitan mantener el control de la seguridad de una organización.	Investigar las diferentes políticas de seguridad que se aplican en la informática y debatir en clase las mismas. Estructurar planes de contingencia para mantener la seguridad en los datos.

11.-FUENTES DE INFORMACIÓN

- ANONYMOUS, Maximun Security, 4rd. Edition, U.S.A., Sams Publishing, 2003. FACCIN, Stefano, et al., IP in Wireless Networks, U.S.A., Prentice Hall, 2003.
- FLICKENGER, Rob, Linux Server Hacks, U.S.A., O'Reilly, 2003.
- GARFINKEL, Simson, SCHWARTZ, Alan, SPAFFORD, Gene., Practical UNIX & Internet Security, 3rd. Edition, U.S.A., O'Reilly, 2003.
- KING, Todd, Security + Training Guide, U.S.A., Que, 2003.
- SUMMERS, Rita, Secure Computing, Threats and Safeguards, U.S.A., McGraw Hill, 1997.
- LOPEZ, Jaquelina y QUEZADA, Cintia, Apuntes de Seguridad Informática, México, Facultad de Ingeniería – UNAM, 2005.
- McCARHY, Linda, IT security: risking the corporation, U.S.A., Prentice Hall, 2003.
- BHASKAR, K., Threats and countermeasures, England, NCC Blackwell, 1993.
- ELEGIDO M,. Juan, Fundamentos de Ética de Empresa, México, IPADE, 1998.
- FACCIN, Stefano, et al., IP in Wireless Networks, U.S.A., Prentice Hall, 2003.
- FOGIE, Seth; PEIKARI, Cyrus, Maximum Wireless Security, U.S.A., Sams Publishing, 2002.

12.-PRÁCTICAS PROPUESTAS

UNIDAD I. FUNDAMENTOS TEÓRICOS.

- Cuestionario
  1. ¿Por qué es importante proteger la información?
  2. ¿Cuáles son los objetivos de la seguridad informática?
  3. ¿Cuáles son las amenazas a los sistemas informáticos y en qué consisten?
  4. ¿Qué son los criterios Comunes?

5. ¿Qué son los perfiles de protección y cuál es su propósito?
6. ¿Cuáles son las clasificaciones de los servicios de seguridad?
7. ¿Qué es ética informática?
8. ¿Cuáles son los objetivos de la ética informática?
9. ¿Qué es un código deontológico?
10. Mencione cuáles temas son tratados frecuentemente en la ética informática.
11. Describa en qué consiste cada tema mencionado en la pregunta anterior.
12. Mencione qué problemas se enfrenta actualmente la ética informática.

- Mapa de Ideas con los conceptos: Seguridad Informática, objetivos, amenazas y perfiles de protección.
- Ensayo sobre la Seguridad Informática.
- Mapa de ideas sobre Códigos y ética Informática.
- Ensayo de ideas sobre Códigos y ética Informática.

UNIDAD II. AMENAZAS Y VULNERABILIDADES

- Cuestionario.
  1. ¿Qué es una amenaza?
  2. ¿Qué es una vulnerabilidad?
  3. ¿Cuál es la diferencia entre una vulnerabilidad y una amenaza?
  4. ¿Cómo se clasifican las vulnerabilidades?
  5. ¿Cuáles son las amenazas de origen humano?
  6. ¿Cuáles son las amenazas de hardware?
  7. ¿Cuáles son las amenazas de Software?
  8. Explique en qué consiste la vulnerabilidad de factor humano.
- Mapa de ideas con los conceptos: Amenazas, vulnerabilidades y tipos de amenazas
- Estudio sobre la seguridad Informática en el Instituto, identificando amenazas y vulnerabilidades en las áreas: SITE, red de datos física, red de datos inalámbrica, , sala de computo, red de energía.

UNIDAD III. IDENTIFICACIÓN DE ATAQUES Y TÉCNICAS DE INTRUSIÓN

- Cuestionario.
  1. ¿Qué son las técnicas de intrusión y porqué es importante conocerlas?
  2. ¿En qué consiste la ingeniería social?
  3. ¿Cuáles son los métodos de fingerprinting y en qué consisten?
  4. ¿Qué métodos pueden usar los intrusos para escanear una red inalámbrica y qué información pueden obtener?
  5. ¿En qué consiste la seguridad física y a qué amenazas se enfrenta?
  6. ¿Qué es la explotación de sistemas?

7. Mencione cuatro formas comunes de explotación de sistemas y explique en qué consisten.
8. Mencione los métodos usados por los atacantes para mantener el acceso a un sistema.
9. Mencione los métodos usados por los atacantes para eliminar la evidencia de sus actividades en el sistema.

- Mapas mentales con los conceptos: la seguridad física, técnicas y métodos de intrusión.
- Ensayo sobre seguridad técnicas y métodos de intrusión.

UNIDAD IV. CONTROL DE LA SEGURIDAD INFORMÁTICA

- Cuestionario.
  1. ¿Qué es auditoría de red y qué herramientas se utilizan?
  2. ¿Qué es un análisis forense a un sistema de cómputo?
  3. ¿Qué es revisión de bitácoras?
  4. ¿Qué es revisión de archivos?
  5. ¿Cuáles son las herramientas para obtener información de red?
  6. ¿Qué es respuesta y manejo de incidentes en seguridad informática?
- Realizar el escaneo de una computadora conectada a una LAN utilizando software para verificar vulnerabilidades
- Aplicar monitoreo de tráfico a una red LAN
- Realizar un plan o programa de auditoria para un sistema informático que especificando herramientas, mecanismos y acciones para lograr el control de la seguridad informática
- Crear un esquema que indique las acciones que se deben llevar a cabo para respuesta a incidentes en seguridad informática

UNIDAD V. ANÁLISIS DE RIESGOS

- Cuestionario.
  1. ¿Qué es el análisis de riesgo?
  2. ¿Qué es la aceptación de riesgo?
  3. ¿Qué es el riesgo residual?
  4. ¿Qué son los controles?
  5. ¿Qué es el análisis cuantitativo?
  6. ¿Qué es el análisis cualitativo?
  7. ¿Cuáles son los pasos del análisis de riesgo?
  8. Explique brevemente qué actividades se desarrollan en cada paso del análisis de riesgo.
  9. ¿En qué consiste el análisis costo beneficio?
- Mapas de ideas con los conceptos de Análisis de riesgo.
- Estudio del Análisis de riesgos de la seguridad informática en el Instituto.

UNIDAD VI. POLÍTICAS DE SEGURIDAD INFORMÁTICA DE LA ORGANIZACIÓN

- Cuestionario.
  1. ¿Qué es una política de seguridad y cuál es su objetivo?
  2. ¿Cómo se define la visión, misión y objetivo de una organización?
  3. Mencione los principios fundamentales de una política de seguridad.
  4. ¿De qué se encargan las políticas para la confidencialidad?
  5. ¿De qué se encargan las políticas para la integridad?
  6. ¿Cuáles son los métodos de seguridad?
  7. ¿Qué son los procedimientos preventivos?
  8. ¿Qué son los procedimientos correctivos?
  9. ¿Qué es un plan de contingencia?
  10. ¿Cuáles son las fases del plan de contingencia?
  11. ¿Qué actividades se realiza en cada fase del plan de contingencia?
- Mapas de ideas con los conceptos: Políticas y métodos de seguridad, procedimientos preventivos y correctivos, y planes de contingencia.
- Ensayo sobre políticas y métodos de seguridad, procedimientos preventivos y correctivos, y planes de contingencia.
- Estudio sobre las políticas y métodos de seguridad, procedimientos y planes de contingencia implementados en el Instituto, aplicados en el SITE, red de datos física, red de datos inalámbrica, sala de cómputo y red de energía.