Planificación anual por trimestre – Técnico en Construcciones Civiles / Informática Personal y Profesional / Equipos e Instalaciones Electromecánicas

ESPACIO CURRICULAR:	Seguridad Informática
CURSO:	5 “E” y “F”
DOCENTE:	Kolb, Mariela Elizabeth – Martínez, Silvia Natalia

FUNDAMENTACIÓN

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas.

Esta materia es transversal a todas las demás materias de la orientación.

PROPÓSITOS

Este espacio es relevante para que el futuro técnico en informática personal y profesional adquiera destrezas sobre la privacidad y protección de datos de las empresas y las organizaciones para hacer frente a los ciberataques.

OBJETIVOS

- Comprender los conceptos básicos de seguridad informática
- Describir los principales problemas de seguridad informática con los que se enfrentan los usuarios de computadoras.
- Conocer los conceptos de Integridad, confiabilidad y disponibilidad de la información.
- Conocer los factores de riegos.

- Reconocer e interpretar la seguridad lógica y física.
- Conocer los mecanismos de seguridad informática existentes.
- Concientizar sobre los riesgos a los que las organizaciones y usuarios de computadoras se enfrentan en materia de seguridad de la información.
- Ampliar o enriquecer los conocimientos acerca de la seguridad informática

COMPETENCIAS

A) **BÁSICAS**

- RELACIONA las temáticas abordadas en la materia de Seguridad Informática con las situaciones del contexto del sistema informático organizacional a partir de la bibliografía analizada en la clase.
- COMPRENDE situaciones del ámbito laboral para conocer el trabajo que realizará de acuerdo a su perfil profesional, analizando las necesidades del mercado.

B) **ESPECIFICAS**

- VALORA la importancia de la seguridad informática en el ámbito informático.
- DESARROLLA medidas o estrategias de seguridad informática.

CONTENIDOS

PRIMER TRIMESTRE	CAPACIDADES	ACTIVIDADES	INDICADORES/ EVIDENCIAS DE DESEMPEÑO
▪ Sistema de información y sistemas informático. ▪ Seguridad ▪ Análisis de riesgos ▪ Control de riesgos ▪ Herramientas de análisis y riesgos. ▪ Seguridad activa, pasiva, física y lógica. ▪ Seguridad en el entorno físico.	▪ Distingue entre sistema de información y entre sistema informático. ▪ Comprende significado de seguridad en el concepto de sistema de información y de sistema informático. ▪ Conoce cuales son la propiedad de un sistema seguro. ▪ Entiende conceptos de activo, amenaza, riesgo,	▪ Estudio de la seguridad de una empresa: ▪ Enumerar activos del sistema de información de la asesoría. ▪ Responder si se ha producido algún ataque y cuál ha sido. ▪ Investigar si existen medios para evitar picos de corriente que dañen equipos de un SI.	○ Argumenta los conceptos de sistema informático y sistema de información. ○ Identifica el significado de Activo, Amenaza, Riesgo, Vulnerabilidad, Ataque e Impacto mediante situaciones de la vida real. ○ Tiene predisposición para el trabajo en grupo. ○ Identifica sistemas de control de acceso mediante

▪ Sistema de control de accesos. ▪ Integración y centralización de sistemas de control de acceso.	vulnerabilidad, ataque e impacto. ▪ Entiende que es un servicio, mecanismo y herramienta de seguridad. ▪ Comprende la importancia de la seguridad en el entorno físico de un SI. ▪ Conoce algunos sistemas de control de acceso a personas al recinto. ▪ Conoce el riesgo del agua y del fuego y detecta si se han aplicado las medidas de seguridad activa y pasiva.		investigación en lugares de su vida cotidiana.
SEGUNDO TRIMESTRE	**CAPACIDADES**	**ACTIVIDADES**	**INDICADORES/ EVIDENCIAS DE DESEMPEÑO**
• Seguridad activa. • Seguridad pasiva. • Racks y armarios ignífugos. • Vulnerabilidad del software y la información. • Intrusismo informático. • Recursos de seguridad del sistema operativo. • Seguridad del software.	▪ Comprende la importancia de mantener una alimentación eléctrica ininterrumpida. ▪ Conoce las diferencias de aplicación y de resultados entre SAID, regleta y grupo electrógeno. ▪ Conoce distintos modos de monitorizar el hardware. ▪ Aprecia la importancia del uso de componentes homologados de buena	▪ Mediante caso práctico: ▪ Describir cómo funciona un grupo electrógeno. ▪ Evaluar ventajas y desventajas en utilizar monitorización de hardware mediante software. ▪ Explicar por qué utilizar un rack.	○ Diferencia cómo actúa un SAID, regleta y un grupo electrógeno, mediante situación práctica. ○ Reconoce los distintos modos de monitorización de hardware y los mecanismos existentes de tolerancia a fallos.

	calidad para protección del hw. ▪ Conoce los mecanismos de tolerancia a fallos.		
TERCER TRIMESTRE	**CAPACIDADES**	**ACTIVIDADES**	**INDICADORES/ EVIDENCIAS DE DESEMPEÑO**
• Redes seguras. • Políticas de almacenamiento y resguardo de la información. • Legislación sobre la seguridad informática y protección de los datos.	▪ Comprende que la red es un medio cambiante. ▪ Resuelve el problema de la interceptación de información por parte de intrusos o malware. ▪ Comprende la importancia de la adecuada política de copias de seguridad. ▪ Conoce la normativa que rige los datos. ▪ Aplica técnicas legales sobre seguridad informática para realizar auditoria.	▪ Investigar sobre la vulnerabilidad del software y de la información. ▪ Opinar sobre las advertencias durante (mensajes) la navegación. ▪ Explicar el significado de: scareware, ingeniería social, adware y malware.	Mediante estudio de caso: • Elabora una lista de políticas *anti spam* para la protección de datos. • Aplica técnicas legales sobre seguridad informática para realizar una auditoría en el lugar propuesto.

PROPUESTA METODOLÓGICA PARA LA ENSEÑANZA

La enseñanza de la Seguridad Informática, como asignatura, se orienta a través de un enfoque práctico. Por lo tanto, se trabajará con estudios de casos de la vida cotidiana para fijar el aprendizaje de los contenidos propuestos. Mediante la utilización de recursos audiovisuales y planteo de situaciones reales producidas en el ambiente cotidiano, el alumno utilizará todo recurso tecnológico, de software y hardware, para desarrollar actividades en clase y hogar.

INSTRUMENTOS DE EVALUACIÓN

Se utilizarán como instrumentos de evaluación:

- T.P.O.s: Realización de Trabajos Prácticos obligatorios
- Exposición Oral,
- Cuestionario Escrito.

FIRMA DEL DOCENTE

PROGRAMA

Unidad Didáctica Nº 1: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Sistema de información y sistemas informático. Seguridad. Análisis de riesgos. Control de riesgos. Herramientas de análisis y riesgos.

Unidad Didáctica Nº 2: SEGURIDAD EN EL ENTORNO FÍSICO

Seguridad activa, pasiva, física y lógica. Seguridad en el entorno físico.

Unidad Didáctica Nº 3: CONTROL DE ACCESO EN EL ENTORNO FÍSICO

Sistema de control de accesos. Integración y centralización de sistemas de control de acceso.

Unidad Didáctica N° 4: SEGURIDAD DEL HARDWARE

Seguridad activa. Seguridad pasiva. Racks y armarios ignífugos.

Unidad Didáctica Nº 5: AMENAZAS AL SOFTWARE

Vulnerabilidad del software y la información. Intrusismo informático.

Unidad Didáctica Nº 6: SEGURIDAD DEL SOFTWARE

Recursos de seguridad del sistema operativo. Seguridad del software.

Unidad Didáctica N° 7: REDES SEGURAS. POLITICAS DE RESGUARDO DE LA INFORMACION. PROTECCIÓN DE LOS DATOS

Redes seguras. Políticas de almacenamiento y resguardo de la información. Legislación sobre la seguridad informática y protección de los datos.

BIBLIOGRAFÍA

Aguilera, P. (2010). *Seguridad Informática.* Pozuelo de Alarcón – España: EDITEX.

Ramió J./ Muñoz A., *http://www.criptored.upm.es*. España.