Aprendizaje: SEGURIDAD EN LA INFORMACION

La seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras. 3Análisis de riesgos

OBJETIVO DE LA SEGURIDAD INFORMÁTICA

El objetivo de la segurida informática es mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por computadora

ELEMENTOS DE LA SEGURIDAD INFORMÁTICA

CONTROL: solo los usuarios autorizados deciden cuando y como permitir el acceso a la información

AUTENTICIDAD: definir que la información requerida es válida y utilizable en el tiempo, forma y distribución.

NO REPUDIO: Evita que cualquier entidad que envió o recibió información alegue que no lo hizo

AUDITORIA: determinar que, cuando, como y quien realiza acciones sobre el sistema.

SEGURIDAD FISICA:

Aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas ane amenazas a los recursos de información

AMENAZAS:	**CONTROLES**
• Incendios • Inundaciones • Terremotos • Trabajos no ergonómicos • Instalaciones eléctricas • Seguridad de equipamiento	• Sistemas de alarma • Control de personas • Control de vehículos • Barreras infrarrojas ultrasónicas • Control de hardware • Controles biométricos: huellas digitales, control de voz, patrones oculares y verificación de firmas

SEGURIDAD LOGICA

Aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permiatea acceder a ellos a las personas autorizadas para hacerlo.

IDENTIFICACION: El usuario se da a conocer al sistema

AUTENTICACION: Verificación del sistema ante la identificación

FORMAS DE AUTENTICACION-VERIFICACION

Algo que la persona conoce como **PASSWORD**

Algo que la persona es: HUELLA DIGITAL

Algo que la persona hace: FIRMAR

DELITO INFORMATICO:Cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el preprocesador automático de datos y/o transmisiones de datos.

Se realiza por medios informáticos y tienes como objeto a la información en si misma

Entre los delitos informáticos se destacan

FRAUDES

- Fraudes cometidos mediante manipulación de computadores.
- Daños a programas o datos almacenados
- Manipulación de datos de E/s
- Distribución de virus
- Espionaje
- Acceso no autorizados
- Reproducción y distribución de programas protegidos por la ley.

AMENAZAS HUMANAS

HACKER: Persona curiosa, “inconformista” y paciente que busca su superación continua aprovechando las posiblidades que le brinda los sistemas.

CRACKER: hacker dañino.

PHREAKER: Persona que engaña a las campañas telefónicas para su beneficio propio

PIRATA INFORMATICO: Persona que vende software protegido por las leyes copyright.

CREADOR DE VIRUS: Diseminadores de virus.

INSIDER: Personal inteno de una organización que amenaza de cualquier forma al sistema de la misma.

TECNICAS PARA ASEGURAR EL SISTEMA

Respaldo de información: La información constituye el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como hurtos, incendios, fallas de disco, virus y otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o *backups*. Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (solo se copian los ficheros creados o modificados desde la última copia de seguridad). Es vital para las empresas elaborar un plan de copia de seguridad en función del volumen de información generada y la cantidad de equipos críticos

6.2Protección contra virus

VIRUS

Un **virus** o **virus informático** es un *software* que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo producen molestias o imprevistos.

TIPOS DE VIRUS

- Sector de arranque
- Archivos ejecutables
- De e-mail
- Gusanos
- Caballos de Troya
- Armas digitales

ANTIVIRUS

Sirve para evitar o combatir las infecciones provocadas por un virus.

PASSWORDS	**NORMAS DE GESTION DE PASSWORDS**
• No utilizar contraseñas que sean palabras • Mezclar caracteres alfanuméricos • Longitud mínima de 7 caracteres • Contraseñas distintas en diferentes sistemas • Ser fáciles de recordar	• No permitir cuentas sin contraseña • No compartirlas • No escribir, enviar o decir la contraseña • Cambiarlas periódicamente.

RESPONDER DE ACUERDO A LA LECTURA

1. En los elementos de la seguridad informática hay uno que dice: Evita que cualquier entidad que envió o recibió información alegue que no lo hizo CUAL ES?
2. Diferencias entre seguridad física y lógica
3. En las amenazas explicar el trabajo no ergonómico y la seguridad de equipamiento
4. En los controles explicar a que se refiere: **Barreras infrarrojas ultrasónicas**
5. Qué es un delito informático
6. Mencionar y explicar 4 FRAUDES INFORMATICOS
7. Con sus palabras establecer la diferencia entre HACKER Y CRAKER
8. Qué es un INSIDER

Con sus palabras

10- Que se necesita para respaldar la información del computador

11-Medios mas comunes que se pueden infectar la información del computador o celular

CONSULTAR

1. Que es criptografia y cual es la utilidad
2. Que es firewalls
3. Que es un bastion
4. Que es un screened subnet
5. En que consiste el metodo de cesar
6. **Sanitización**;