UD 1: Adopción de pautas de seguridad informática

Introducción a la seguridad informática

Indice

Introducción

¿Qué es un sistema de información?

¿Qué es un sistema informático?

¿Qué diferencias hay entre ellos?

Sistema de información

Un sistema de información (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos.

Los elementos de un SI son:

- Recursos: físicos y lógicos.
- Equipo humano.
- Información: datos.
- Actividades: que se realicen en la organización.

Sistema informático

Un sistema informático está constituido por un conjunto de elementos físicos (hardware, dispositivos, periféricos, y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos) y con frecuencia se incluyen también los elementos humanos (personal experto que maneja el software y el hardware).

¿Qué es la seguridad informática?

La seguridad informática es la disciplina que se ocupa de diseñar las normas, los procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Para conseguir que un sistema informático sea seguro tiene que cumplir con tres propiedades de seguridad que son los pilares fundamentales de la seguridad informática.

Pilares fundamentales de la seguridad informática

Integridad, confidencialidad y disponibilidad

Integridad

Garantiza que los datos no se alteren de forma no autorizada. Es decir, los datos deben permanecer inalterados y fiables desde el momento en que se crean o se transmiten hasta que se almacenan o reciben.

La integridad es critica en escenarios donde cualquier modificación puede tener consecuencias catastróficas.

Por lo tanto, garantiza la autenticidad y precisión de la información, es decir, que la información no ha sido alterada ni destruida de forma no autorizada.

Confidencialidad

Asegura que la información solo esté disponible para las personas autorizadas. Esto es esencial cuando se manejan datos sensibles, como información personal, datos financieros o secretos comerciales.

Por lo tanto, garantiza que la información o datos está disponibles solo para personal autorizado, en el momento autorizado.

Disponibilidad

Se refiere a que los sistemas, servicios y datos están accesibles cuando sea necesario. Si un sistema crítico no está disponible, incluso durante un breve período, puede causar grandes inconvenientes o pérdidas.

Por lo tanto, garantiza que la información esté disponible para los usuarios en el momento que la necesiten.

La paradoja de la seguridad

Uno de los principales desafíos al implementar seguridad en sistemas informáticos es encontrar un equilibrio entre tres factores: funcionalidad, usabilidad y seguridad. A menudo, al aumentar la seguridad se reduce la facilidad de uso del sistema o se limita la funcionalidad.

La seguridad también puede comprometer la funcionalidad si las restricciones impiden a los usuarios acceder a ciertas funcionalidades.

Las medidas de seguridad deben ser adecuadas a los recursos que se quieren proteger y los riesgos que se pueden sufrir.

Elementos vulnerables en el sistema informático

Hardware, software, datos y redes

Hardware

Se refiere a los componentes físicos del sistema, como servidores, estaciones de trabajo, routers y dispositivos de almacenamiento. Los daños físicos, como el desgaste pueden comprometer la funcionalidad del hardware, pero los ataques físicos directos como el robo de dispositivos, también representan un riesgo.

Software

Desde el sistema operativo hasta las aplicaciones instaladas, pueden contener vulnerabilidades que los atacantes utilizan.

Los errores de codificación, las configuraciones inseguras y las actualizaciones no aplicadas son las causas más comunes de vulnerabilidades de software.

Una vulnerabilidad crítica en un sistema operativo podría permitir que un atacante remoto obtenga acceso administrativo al sistema. Para evitar esto, es fundamental mantener el software actualizado y aplicar parches de seguridad regularmente.

Datos

Los datos son uno de los activos mas valiosos en cualquier sistema informático. Puede ser vulnerables tanto en el lugar donde se almacenan como cuando se envían o transmiten. Si no se cifran adecuadamente un atacante puede acceder a ellos y usarlos indebidamente.

Por ejemplo, en una empresa que gestiona datos financieros, la información de la tarjeta de crédito de los clientes debe estar cifrada tanto en las bases de datos como durante las transacciones. Sin cifrado, un atacante que acceda a la base de datos podría robar la información y usarla para cometer fraudes.

Redes

Las redes conectan todos los componentes del sistema y permiten las comunicaciones entre ellos. Las redes vulnerables pueden ser un punto de entrada para los atacantes, que pueden interceptar datos, lanzar ataques de denegación de servicio o comprometer dispositivos en la red.

Un ataque de denegación de servicio distribuido (DDoS) puede dejar inoperativa una red al inundarla con tráfico malicioso. Para mitigar este tipo de amenazas, se pueden usar cortafuegos, sistemas de detección de intrusiones (IDS) y redes de distribución de contenidos (CDN).

Análisis de las principales vulnerabilidades de un sistema informático

Identificar y evaluar las debilidades en los sistemas informáticos. Las vulnerabilidades van desde configuraciones incorrectas hasta fallos de software

Elementos a estudiar en un análisis de riesgos

- Activos: recursos que pertenecen a un SI como el SW, HW, datos, instalaciones, personal, redes… Es decir, todo aquello que representa valor para la empresa.
- Amenazas: aquello que puede dañar a un activo (persona, cosa o suceso) produciéndole daños. (Ejemplo: Calor, lluvia…).
- Vulnerabilidad (Debilidad): debilidad de un activo que puede ser aprovechada por una amenaza. (Ejemplo: tenemos sistema de refrigeración, pero no contra inundaciones, somos vulnerables a inundaciones).
- Riesgo: posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. (Ejemplo: ¿inundación en el desierto?).
- Ataque: materialización de una amenaza. (Ejem.: se inunda el CPD).
- Impacto: consecuencias de que se llegue a producir un ataque.

Vulnerabilidades más comunes

Errores de programación: son errores cometidos durante el desarrollo del software. Pueden incluir desbordamientos de búfer, inyección de SQL o la falta de validación de entradas.

Configuraciones inseguras: las configuraciones por defecto de algunos sistemas son inseguras. Un administrador que no cambia la configuración puede dejar el sistema vulnerable. Un ejemplo clásico es el uso de la contraseña por defecto, que son fácilmente predecibles.

Vulnerabilidades no parcheadas: muchas vulnerabilidades conocidas ya tienen un parche disponible, pero si no se actualiza el sistema, el sistema sigue siendo vulnerable.

¿Qué herramientas de análisis de vulnerabilidades podemos usar?

Nessus: herramienta comercial que realiza escaneos completos para detectar vulnerabilidades en redes, servidores y aplicaciones. Genera informes detallados con recomendaciones para corregir vulnerabilidades.

OpenVAS: herramienta de código abierto que ofrece funciones similares a la herramienta anterior. Se utiliza para detectar vulnerabilidades en redes y servidores.

Nmap: herramienta que se conoce por el escaneo de puertos pero también puede detectar vulnerabilidades básicas en servicios y SO.

Amenazas

Tipos de amenazas

Amenazas físicas: afectan al hardware y a la infraestructura física del sistema. Estas amenazas incluyen incendios, inundaciones, fallos de energía, robos o daños intencionados a los equipos. Algunos ejemplos de amenazas físicas son:

- Incendios y desastres naturales
- Cortes de suministro eléctrico
- Robo de equipos

Amenazas lógicas: afectan el software, los datos y las redes. Estas amenazas incluyen virus, ataques de denegación de servicio, ransomware, spyware y phishing. Algunos ejemplos son:

- Virus y malware: programas maliciosos que infectan los sistemas, roban datos o corrompen la información.
- Ransomware: cifra los archivos del usuario y luego pide un rescate para liberarlo.
- Phishing: utiliza la ingeniería social para engañar a los usuarios y obtener información confidencial.

Ahora os toca trabajar a vosotros

- Busca estadísticas sobre amenazas de seguridad informática
- ¿Qué ataque se producen mas habitualmente?
- Valora cual es la causa por la que se producen esos ataques, como se producen y que impacto tienen sobre las compañías.

Seguridad física y ambiental

Medidas que se adoptan para prevenir daños o robos, así como medidas ambientales para que se produzcan deterioros por condiciones adversas

Ubicación y protección física de los equipos y servidores

Los servidores y equipos deben ubicarse en un lugar que sea tanto accesible para el personal autorizado como seguro frente a amenazas físicas. Idealmente, se deben instalar en centros de datos que cumplan con los estándares de seguridad física y operativa.

Las medidas mas comunes de seguridad física son las siguientes:

- Controles de acceso: el acceso a los servidores debe estar limitado al personal autorizado mediante el uso de biometría, tarjetas de identificación con chip o códigos PIN.
- Videovigilancia: las cámaras de seguridad deben estar presentes en todos los puntos de entrada y dentro de los centros de datos para monitorizar cualquier actividad sospechosa.
- Protección contra incendios: los centros de datos deben contar los sistemas de detección y supresión de incendios, como rociadores automáticos y extintores. Además, es importante usar sistemas de detección de humos de alta sensibilidad.

Sistemas de alimentación ininterrumpida (SAI)

Es un dispositivo esencial para garantizar que los servidores y sistemas críticos sigan funcionado durante un corte de energía. El SAI proporciona energía temporal para permitir un apagado o mantener en funcionamiento los sistemas hasta que se restablezca el suministro eléctrico.

Seguridad lógica

Medidas implementadas en el software y los datos para protegerlos de acceso no autorizados, alteraciones o destrucción.

Criptografía I

Es una técnica fundamental en la seguridad informática, ya que permite asegurar la confidencialidad e integridad de los datos mediante el uso de algoritmos matemáticos que transforman la información en un formato ilegible para cualquier persona no autorizada.

Existen 3 tipos de criptografía:

- Cifrado simétrico: se utiliza una clave única para cifrar y descifrar la información. Este tipo de cifrado es más rápido y eficiente, pero tiene el inconveniente de que la clave debe ser compartida de forma segura entre las partes.
- Cifrado asimétrico: utiliza dos claves, una clave pública para cifrar los datos y una clave privada para descifrarlos. Este tipo de cifrado es mas seguro para la transmisión de datos a través de las redes públicas, ya que solo el destinatario con la clave privada puede descifrar la información.

Criptografía II

- Criptografía híbrida: combina lo mejor del cifrado simétrico y asimétrico. En este esquema los datos se cifran con una clave simétrica, pero dicha clave se transmite cifrada utilizando un algoritmo asimétrico, lo que garantiza que solo el destinatario correcto puede acceder a la clave simétrica.

Para comprobar como funcionan estas criptografías vamos a utilizar el servicio web CyberChef (https://gchq.github.io/CyberChef/).

Tienes una tarea en el aula virtual para realizar y entregar que será evaluable en la que tienes que explicar el funcionamiento de la herramienta con ejemplos de criptografía simétrica, asimétrica e híbrida.

Listas de control de acceso (ACL)

ACL (Access Control List) es un conjunto de reglas que determinan que usuarios o sistemas tienen permitido acceder a ciertos recursos en sistema informático y que acciones pueden realizar. Las ACL pueden aplicarse tanto a archivos, carpetas, dispositivos como a conexiones de red.

Son una herramienta esencial para mantener la confidencialidad, integridad y disponibilidad de los datos.

Cada entrada de la lista se llama ACE (Access Control Entry)

Los principales sistemas operativos (Windows, Linux y macOS) tienen ACL y se pueden gestionar por los administradores para dar los permisos pertinentes a cada usuario y grupos de usuarios .

Establecimiento de política de contraseñas

Una de las principales defensas contra el acceso no autorizado es una política robusta de contraseñas.

Es una medida de control de acceso basada en el conocimiento.

Las contraseñas débiles o repetidas facilitan que los atacantes puedan realizar ataques de fuerza bruta o de diccionario para comprometer cuentas.

Hay que tener en cuenta que si se pide cambiar con demasiada frecuencia las contraseñas al usuario van a escoger contraseñas más débiles para recordarlas mejor.

Ejercicio: Establecer una política de contraseñas seguras en Windows mediante el uso de la directiva de seguridad local. Debe tener:

- Al menos 12 caracteres
- Mayúsculas, minúsculas, números y caracteres especiales
- Cambiar la contraseña cada 90 días
- No se puede reutilizar contraseñas anteriores

Utilización de sistemas biométricos de identificación

Permiten una identificación más segura y eficiente mediante características físicas únicas del individuo, como la huella dactilar, el reconocimiento facial, la retina o el reconocimiento de voz.

Las ventajas de su utilización son:

- Difícil de falsificar: es muy difícil de copiar o robar.
- Conveniencia: no es necesario recordar contraseñas lo que facilita el acceso.

Las desventajas

- Consentimiento de identificación: se puede utiliza sin el consentimiento del usuario (p.e. cuando la persona está dormida)
- Resistencia al cambio: es difícil modificar las características biométricas si se roba o se hace un mal uso.

Políticas de almacenamiento

El almacenamiento seguro de los datos es otro aspecto crítico de la seguridad informática. Esto implica no solo cómo se almacenan los datos, sino también quien tiene acceso a ellos y cómo se gestionan las copias de seguridad y la redundancia.

Las características principales son:

- Especificar donde se deben guardar los datos sensibles
- Por cuanto tiempo
- Medidas de cifrado y acceso

Copias de seguridad e imágenes de respaldo

Las copias de seguridad son fundamentales para la recuperación ante desastres. Una copia de seguridad debe definir la frecuencia, el tipo y los medios de almacenamiento utilizados.

- Tipos de copias: Completa, incremental y diferencial
- Diferencia entre copia y tolerancia a fallos
  - La tolerancia a fallos implica sistemas redundantes que permiten seguir operando en caso de una falla (RAID)
  - La copia de seguridad tendrá que ser restablecida para poder volver a trabajar con los datos.
- Tolerancia a errores: RAID 0, 1 o 5
- Imágenes de respaldo: son copias completas de un sistema en un momento específico, permitiendo restaurar no solo archivos, sino también configuraciones y aplicaciones instaladas. (Ej. Clonezilla o Acronis)

Medios de almacenamiento

La elección del medio de almacenamiento y como se utilizan afecta a la integridad, disponibilidad y confidencialidad de los datos.

Cada medio tiene sus características y sus ventajas y desventajas. Dependiendo de la elección se implementarán diferentes estrategias de seguridad.

Ejercicio: Buscar los dispositivos de almacenamiento que existen y que se pueden utilizar en un sistema informático.

Recuperación de datos

Ejercicio: ¿Qué herramientas utilizarías si por error un malware te ha eliminado una carpeta con archivos críticos y necesarios para el correcto funcionamiento de tu organización?

Necesito herramientas tanto para Linux como para Windows porque en la empresa hay equipos con los dos Sistemas Operativos.

Realización de auditorías de seguridad

Son evaluaciones sistemáticas que buscan identificar vulnerabilidades y riesgos en un sistema informático. Estas auditorías pueden realizarse manualmente o con la ayuda de herramientas automatizadas que escanean el sistema en busca de posibles brechas de seguridad. Su objetivo es verificar que los controles de seguridad implementados sean eficaces y cumplan con las políticas de seguridad establecidas.

a)Auditorías de seguridad en Windows

b)Auditorías de seguridad en Linux

c)Auditorías de seguridad en macOS

d)Auditorías de seguridad en red

- Nmap: que es un escáner de puertos y servicios que permite identificar los servicios que se ejecutan en una red y detectan posibles vulnerabilidades.

- OpenVAS: escanea redes y sistemas en busca de fallo de seguridad conocidos

Análisis forense en sistemas informáticos

¿Qué es el análisis forense digital?

- Proceso de investigar sistemas informáticos para recopilar y preservar evidencias en casos de delitos informáticos.
- Implica el estudio de discos duros, registros del sistema. Archivos y cualquier otro rastro digital que pueda servir como evidencia en una investigación.
- Los objetivos principales son:
  - Descubrir como se produjo el incidente
  - Identificar a los responsables
  - Restaurar los sistemas infectados.
  - Recopilar evidencias para que puedan ser utilizados en un juicio.

Recogida y análisis de evidencia

Es el comienzo del proceso. Es fundamental que la evidencia sea capturada sin alterarla de ninguna manera, para que pueda ser presentada a un tribunal si es necesario.

Se consigue mediante la ceración de imágenes forenses de los discos duros y otros dispositivos de almacenamiento que son copias exactas de los datos, incluyendo sectores marcados como vacíos o eliminados.

Procedimientos clave:

- Asegurar la escena: aislar todos los sistemas afectados, desconectándolos de la red y garantizando que no se manipulen hasta que no llegue el equipo forense
- Crear una imagen forense: se usa software especializado para hacer una copia bit a bit del disco duro o sistema de almacenamiento. (Imager o dd)
- Verificación: después de crear la imagen se genera un hash (cadena única de caracteres basada en los datos) tanto de la original como de la imagen para garantizar una copia idéntica-
- Análisis de la imagen: se utilizan herramientas especializadas como Autopsy que no modifiquen la copia original.

Herramientas del análisis I

- Para Windows
  - FTK (Forensic ToolKit) Imager: herramienta gratuita qu permite la creación de imágenes forenses de discos duros y otros dispositivos. También permite recuperar archivos eliminados.
  - En Case: herramienta comercial muy utilizada por investigadores que sirve para capturar imágenes forenses, analizar registros del sistema y recupera archivo ocultos o eliminados.
  - Volatility: permite extraer información de una captura de la RAM como procesos en ejecución o conexiones de red activa. Se pueden detectar procesos que estaban activos durante el ataque e identificar cual de ellos era malicioso y que conexiones de red estaban abiertas durante el incidente.

Herramientas del análisis II

- Linux
  - The Sleuth Kit (TSK): conjunto de herramientas de línea de comandos que permiten analizar particiones y sistemas de archivos para buscar archivos eliminados y particiones perdidas.
  - Autopsy: interfaz gráfica de la anterior que facilita la investigación de discos duros y sistemas de archivos. Examina archivos, permite recuperar datos eliminados y analizar registros de eventos.
  - Dd: herramienta básica pero muy potente para hacer copias de discos duros bit a bit. Es escial para crear imágenes forenses de dispositivos de almacenamiento.

Herramientas del análisis III

- macOs
  - MacQuisition: se utiliza para capturar imágenes forenses de sistemas macOs sin modificar el sistema. Permite la extracción de datos y la captura de imágenes de sistemas en vivo.
  - BlackLight: herramienta especializada para análisis forense de dispositivos macOs. Permite analizar archivos específicos de macOs, examinar correos electrónicos y recuperar archivos eliminados.

En conclusión

- Pilares fundamentales de la SI son:
  - Confidencialidad
  - Integridad
  - Disponibilidad
- Elementos vulnerables en el SI son:
  - Hardware
  - Software
  - Datos
  - Redes
- Análisis de las principales vulnerabilidades.
- Amenazas pueden ser físicas o lógicas
- Seguridad física y ambiental

En conclusión

- Seguridad lógica
  - Criptografía
  - Listas de control de acceso
  - Contraseñas
  - Sistemas biométricos
  - Políticas de almacenamiento
  - Copias de seguridad e imágenes de respaldo
  - Almacenamiento
  - Recuperación de datos
  - Auditorías
- Análisis forense
  - Objetivo del análisis
  - Recogida y análisis de evidencias
  - Herramientas del análisis