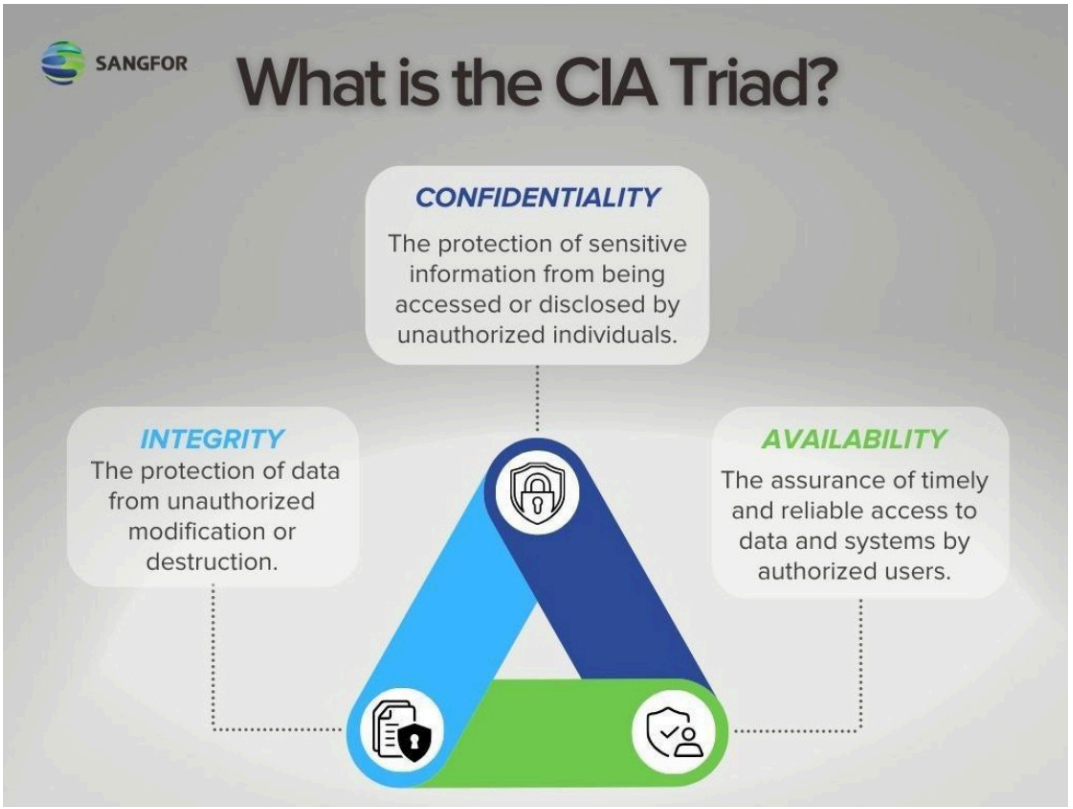
U1. Fundamentos de la seguridad informática

Descargar estos apuntes

Índice

Objetivos de la seguridad informática

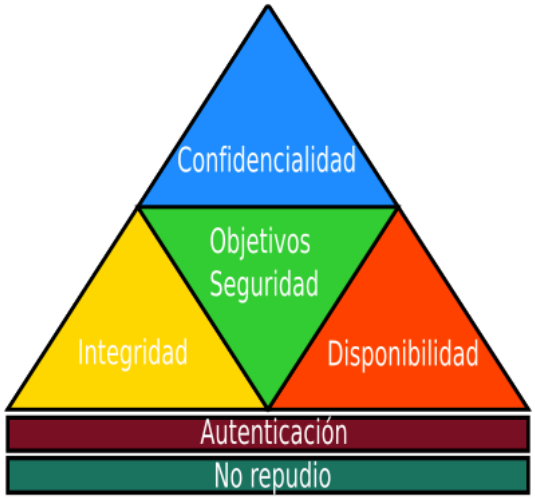
La seguridad informática tiene como objetivo crear un entorno seguro donde se mitiguen los riesgos y las organizaciones puedan operar con confianza, sabiendo que sus sistemas y datos están protegidos. Se centra en la protección de la **confidencialidad, integridad y disponibilidad** de la información. Otros aspectos importantes incluyen la **autenticación** y el **no repudio**.



Confidencialidad
Protección de la información para evitar que accedan a ella o la divulguen personas no autorizadas. Los métodos para garantizar la confidencialidad incluyen el cifrado de datos, la verificación de identidad o la autenticación multifactor

Integridad
Protección de los datos contra modificaciones o destrucciones no autorizadas.
Métodos: sumas de verificación, auditorías, controles de acceso.

Disponibilidad
Garantiza el acceso a tiempo y confiable a los datos por parte de usuarios autorizados. Algunas técnicas utilizadas para asegurar la disponibilidad incluyen el uso de SAI, RAID, copias de seguridad y redes SAN.



Autenticación
Es un proceso que garantiza y confirma la identidad del usuario. Algunos mecanismos de autenticación incluyen contraseñas, autenticación biométrica y autenticación multifactor.

No repudio
Proporciona prueba del origen, autenticidad e integridad de los datos. Garantiza al remitente que su mensaje ha sido entregado y ofrece al destinatario una prueba de la identidad del remitente. De esta manera, ninguna de las partes puede negar que un mensaje fue enviado, recibido y procesado. Las firmas digitales se utilizan ampliamente como mecanismos de no repudio.

Seguridad física y lógica

Los sistemas de seguridad informática funcionan de dos maneras: activa y pasiva.

Seguridad activa
Intenta prevenir un ataque o incidente antes de que ocurra, es decir, es proactiva. Estas medidas se centran en reducir la probabilidad de que ocurra una amenaza.

Seguridad pasiva
Se refiere a las medidas tomadas para responder a problemas de seguridad informática cuando ya han ocurrido, buscando una solución. Su objetivo es reducir el impacto de la amenaza.

Tipos de seguridad:

Seguridad física
Protege físicamente el sistema informático. Consiste en la protección del personal, el hardware, el software, las redes y los datos contra acciones y eventos físicos que puedan causar pérdidas o daños graves.

Seguridad lógica
Consiste en el uso de software y sistemas para controlar y limitar el acceso a los datos e información del sistema.

Centro de proceso de datos (CPD)

El centro de procesamiento de datos (CPD) es el lugar donde se concentran gran parte de los recursos necesarios para procesar la información de una organización. Así, los CPD suelen ubicarse en un edificio o una sala grande y albergan una gran cantidad de equipos informáticos.
El CPD es un punto particularmente vulnerable, ya que en él se concentran los recursos más importantes, por lo que es especialmente necesario considerar las amenazas físicas y ambientales a la hora de diseñarlos. Al seleccionar su ubicación, se recomienda minimizar el riesgo de incendios, inundaciones, terremotos, interferencias electromagnéticas, robos, etc. Un CPD suele contar con recursos específicos orientados a la seguridad

física, como sistemas de protección electrónica, sistemas de refrigeración, detección y extinción de incendios, y control de acceso biométrico. En cualquier caso, las decisiones de seguridad que se tomen dependerán del valor de los recursos a proteger y de su importancia para el negocio. Además de las características tecnológicas de seguridad, también son importantes otras medidas, como la capacitación adecuada del personal, la realización periódica de simulaciones de recuperación ante desastres y el diseño de planes de contingencia, entre otros.

Autenticación y autorización

La **autenticación** en el sistema operativo es un proceso mediante el cual un objeto (usuario, proceso, servicio, aplicación, etc.) verifica su identidad para obtener acceso a un sistema informático. Se pueden emplear diversos métodos de autenticación:

- **Conocimiento**: Algo que el usuario sabe, como una contraseña, un PIN o la respuesta a una pregunta de seguridad.
- **Posesión**: Algo que el usuario posee, como un teléfono móvil, una tarjeta inteligente o un certificado digital.
- **Características inherentes**: Algo que el usuario es, como una huella digital, reconocimiento de voz o facial.

> La **autenticación multifactor (MFA)** es un proceso de verificación de identidad que requiere el uso de al menos dos de los tres factores: conocimiento, posesión y características inherentes

La **autorización** determina qué puede hacer o a quién puede acceder un objeto autenticado (como usuarios o procesos) dentro del sistema. Para ello, utiliza mecanismos como políticas de usuario, grupos y permisos.

Listas de Control de Acceso (ACL)

Los objetos autenticados deben tener acceso únicamente a los recursos necesarios para su tarea y a ninguno más. Para gestionar este acceso, se utilizan herramientas como los grupos de usuarios y las listas de control de acceso (ACLs).

> Una **ACL** es un conjunto de reglas o permisos asociados a un archivo, directorio o recurso de red que define qué objetos pueden acceder y qué acciones están permitidas o denegadas.

Autenticación centralizada

Los sistemas operativos y las aplicaciones suelen tener sistemas de autenticación independientes, lo que obliga a los usuarios a recordar múltiples nombres de usuario, contraseñas y claves. Sin embargo, los sistemas operativos implementan métodos de gestión centralizada de usuarios.
En un sistema centralizado, se utiliza una única base de datos de usuarios y grupos, y todos los dispositivos de la red verifican las credenciales de los usuarios contra esa base de datos.

En Windows

Active Directory (AD) es una plataforma centralizada para la gestión de usuarios y grupos. Los **dominios** son contenedores lógicos que organizan y administran usuarios, grupos y equipos dentro de la red. La base de datos de usuarios, que almacena información como nombres de usuario y contraseñas, se guarda en servidores llamados **controladores de dominio**.

En Linux

PAM (Pluggable Authentication Modules) permite que diferentes aplicaciones y servicios utilicen un sistema de autenticación común. Admite varios métodos de autenticación, como contraseñas, biometría o tarjetas inteligentes.
PAM se combina con **LDAP** (Lightweight Directory Access Protocol) para lograr una autenticación centralizada de usuarios. LDAP actúa como la base de datos central donde se almacenan las cuentas de usuario (nombres de usuario, contraseñas, etc.), mientras que PAM configura las políticas de autenticación para las aplicaciones..

Sistema de alimentación ininterrumpida (SAI)

Un **SAI** (Sistema de Alimentación Ininterrumpida) es un dispositivo que proporciona energía de respaldo mediante baterías cuando falla el suministro eléctrico. La mayoría también incluyen componentes eléctricos que estabilizan el voltaje de salida cuando la tensión de la red eléctrica sube o baja fuera de unos niveles aceptables.

Los **SAI pequeños** ofrecen energía durante unos minutos, lo suficiente para apagar el equipo de forma segura, mientras que los **SAI de mayor capacidad** pueden suministrar energía durante varias horas.

Factores a considerar al elegir un SAI

- **Potencia máxima**: Medida en vatios (W) o voltamperios (VA).

- **Tiempo de autonomía**: Depende del número de baterías, la carga conectada y la potencia suministrada.

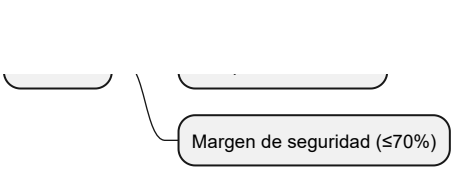
Requisitos de potencia

La potencia del SAI se expresa en voltio-amperios (VA), que es una medida de la potencia eléctrica total consumida por el dispositivo.
Según la ley de Ohm, en un sistema de corriente continua (CC) la potencia (en vatios) es igual a la intensidad de corriente (en amperios) multiplicada por la tensión (en voltios), **W = I x V**. En un circuito de corriente alterna (CA), para equiparar vatios (W) a voltios-amperios (VA) hay que considerar el pico máximo de potencia. Así, la potencia aparente (VA) se calcula como $VA = Wx1,4$
Al seleccionar un SAI, se deja un margen de potencia sin utilizar para evitar sobrecargas.

> **Tip**
>
> Una recomendación habitual es no superar el 70% de la capacidad del SAI con los dispositivos conectados.

Mapa mental


U1. Fundamentos de la Seguridad Informática
Objetivos de la Seguridad
Confidencialidad
Integridad
Disponibilidad
Autenticación
No repudio
Seguridad Física y Lógica
Seguridad física
Ubicación de equipos
Protección física
Seguridad lógica
Control de acceso
Políticas de usuario
CPD (Centro de Proceso de Datos)
Amenazas físicas
Seguridad ambiental
Control de acceso
Planes de contingencia
Autenticación y Autorización
MFA (Autenticación multifactor)
Conocimiento
Posesión
Características inherentes
Autorización
Grupos y permisos
Listas de Control de Acceso (ACL)
Autenticación Centralizada
Windows - Active Directory
Dominios
Controladores de dominio
Linux - PAM y LDAP
Gestión de usuarios
Políticas comunes
Sistema de Alimentación Ininterrumpida (SAI)
Tipos de SAI
Pequeños
Alta capacidad
Selección
Potencia (W/VA)
Tiempo de autonomía


Margen de seguridad (≤70%)