

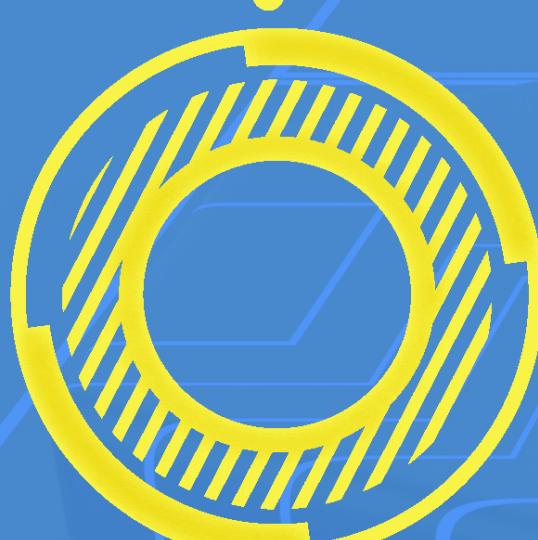
POR ARMENTA FABIAN Y NAYELI SIERRA

SEGURIDAD Y PROTECCIÓN EN SISTEMAS OPERATIVOS

INTRODUCCIÓN

Hoy en día, las tecnologías de la información han revolucionado al mundo y forman parte de nuestro día a día.

Es por esto que asegurar la confidencialidad, integridad y disponibilidad de los datos y recursos del sistema es fundamental en sistemas operativos, esto se logra mediante medidas de seguridad y protección.

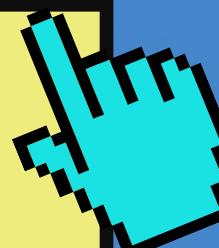


TIPOS DE SEGURIDAD EN SISTEMAS OPERATIVOS



Podemos encontrar varios tipos de seguridad para proteger los sistemas operativos y los datos almacenados en ellos, algunos de los más comunes en sistemas operativos modernos:

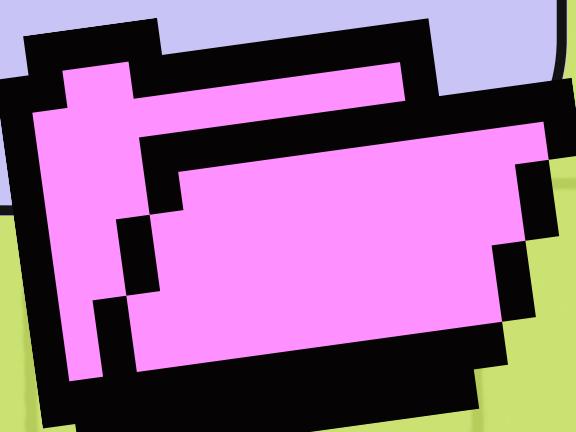
- Seguridad de autenticación y autorización
- Seguridad de control de acceso
- Seguridad de cifrado
- Seguridad de redes

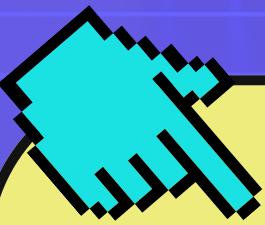




SEGURIDAD DE AUTENTICACIÓN Y AUTORIZACIÓN

La autenticación y autorización son elementos fundamentales en cualquier sistema de seguridad de la información, por lo que es importante aplicar medidas apropiadas para asegurar que los usuarios verificados solo accedan a los recursos necesarios para cumplir con sus responsabilidades.



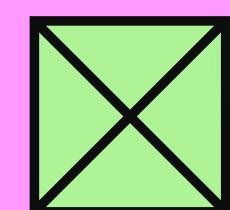


La autenticación consiste en garantizar que el usuario sea quien dice ser, es decir, verificar las credenciales brindadas por el mismo gracias a los factores de autenticación las cuales pueden ser:

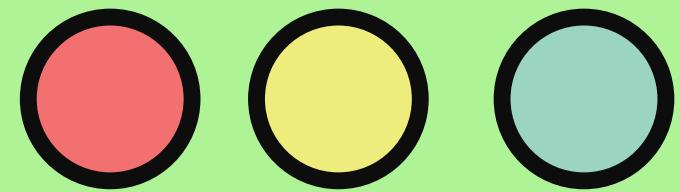
LAS CUALES PUEDEN SER:



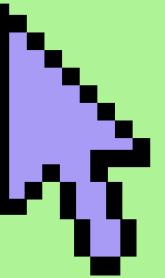
- Basada en información conocida.
- Basada en posesiones del usuario.
- Basada en datos biométricos.



SEGURIDAD DE AUTENTICACIÓN Y
AUTORIZACIÓN



EJEMPLOS

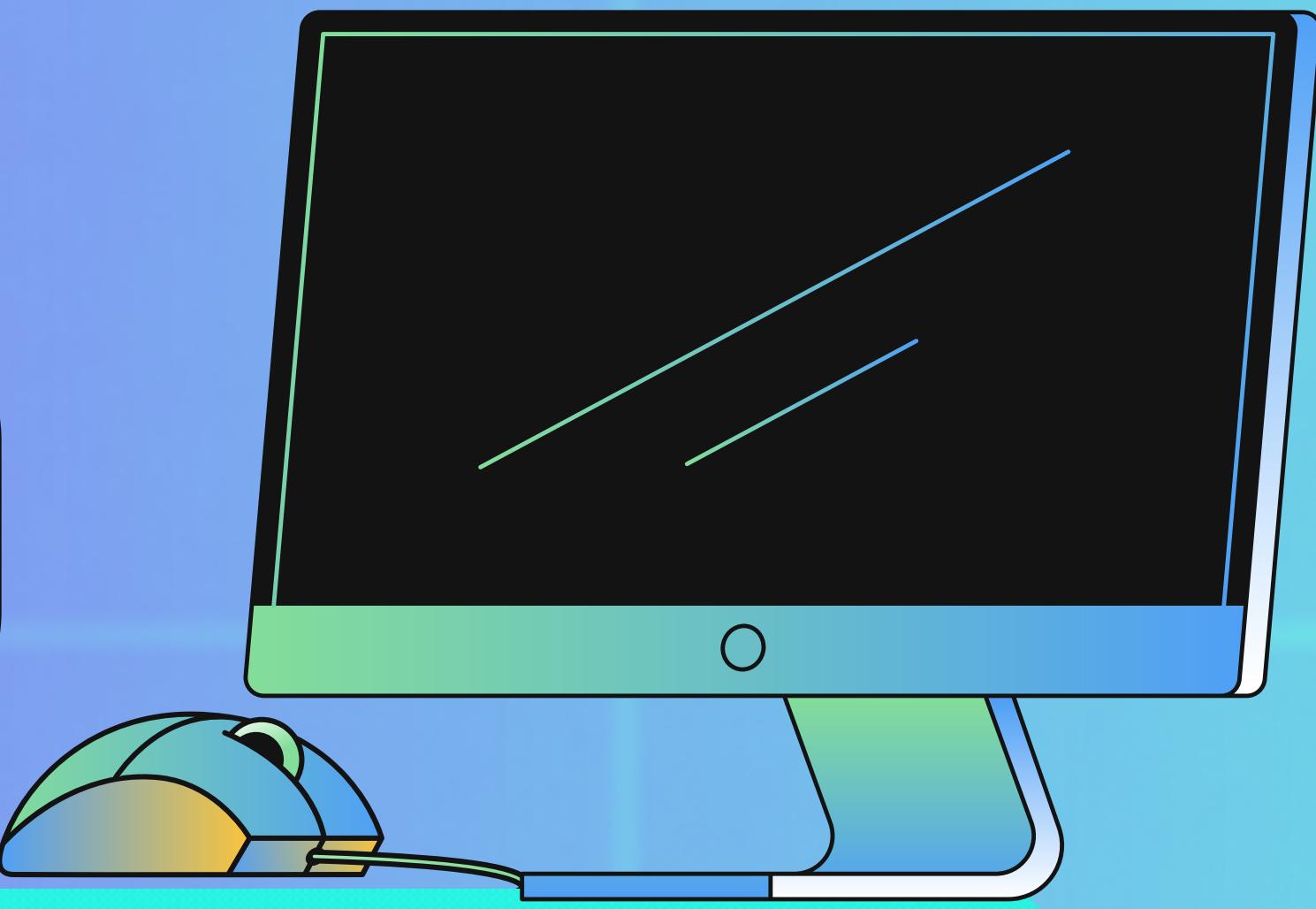


- ◆ Contraseñas seguras
- ◆ Autenticación multifactorial
- ◆ Políticas de control de acceso
- ◆ Registro y monitorización de eventos

SEGURIDAD DE CONTROL DE ACCESO

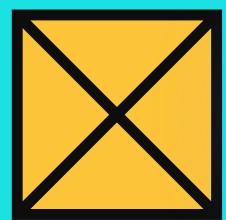
El control de acceso establece una política de seguridad que define qué usuarios o procesos tienen permiso para acceder a cada recurso del sistema y qué tipo de acceso se les permite.

Un mecanismo de control de acceso actúa como intermediario entre el usuario o proceso y los recursos del sistema



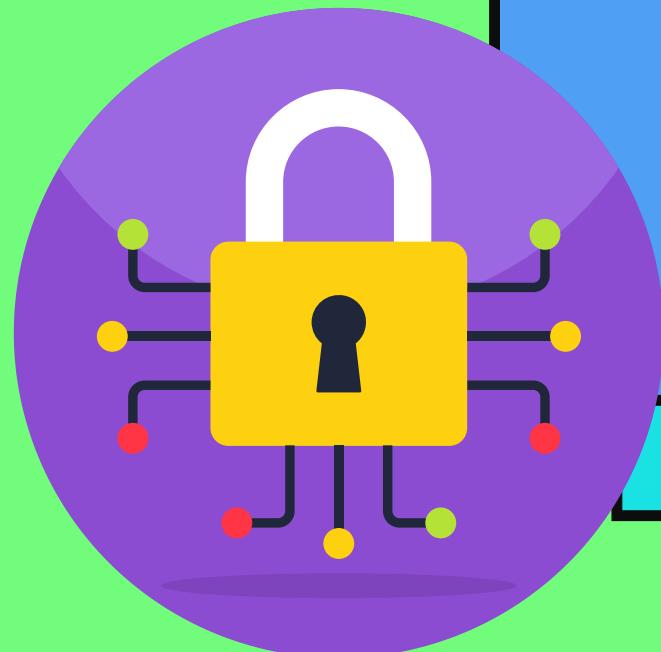
TIPOS

- Control de acceso basado en roles (RBAC)
- Control de acceso discrecional (DAC)
- Seguridad basada en políticas
- Control de acceso obligatorio (MAC)



SEGURIDAD DE CIFRADO

Seguridad de cifrado es la protección de información sensible o confidencial mediante la transformación de los mismos por medio de algoritmos matemáticos a un formato de cifrado de difícil comprensión



SEGURIDAD DE CIFRADO

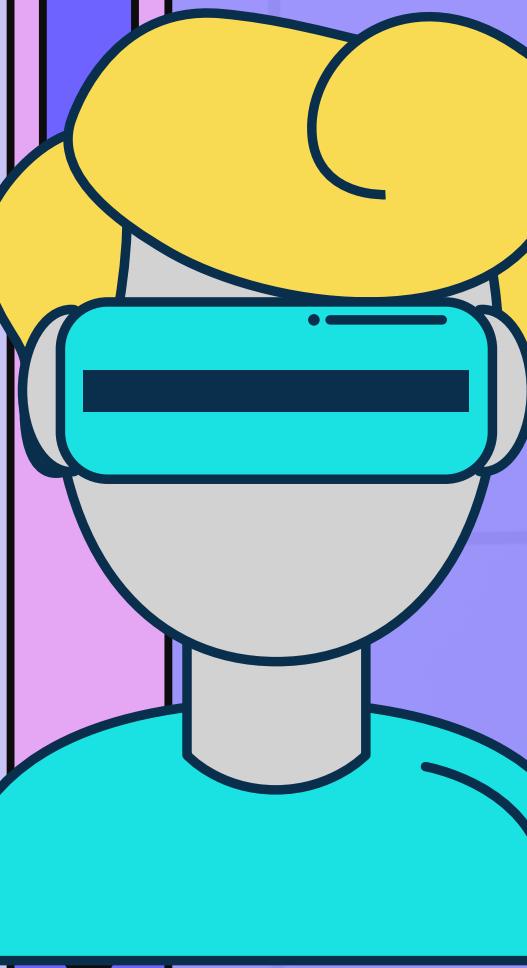
Los dos tipos de cifrado pueden ser:

1. Simétricos
2. Asimétricos

Es importante elegir un algoritmo de cifrado seguro y confiable, gestionar adecuadamente las claves de cifrado y proteger la privacidad y la confidencialidad de la información mediante técnicas de cifrado adecuadas.

Ejemplos:

- Comunicación en línea (protocolo HTTPS)
- Protección de datos almacenados



SEGURIDAD DE REDES



La seguridad de redes es un conjunto de medidas y técnicas diseñadas para proteger los sistemas informáticos y los datos que se transmiten a través de las redes.

La seguridad de redes es fundamental para proteger los sistemas y los datos que se transmiten a través de ellas. Por lo tanto es de utilidad implementar medidas de seguridad adecuadas, como:

- Autenticación y autorización
- Actualizaciones de software
- Gestión de contraseñas
- Políticas de seguridad

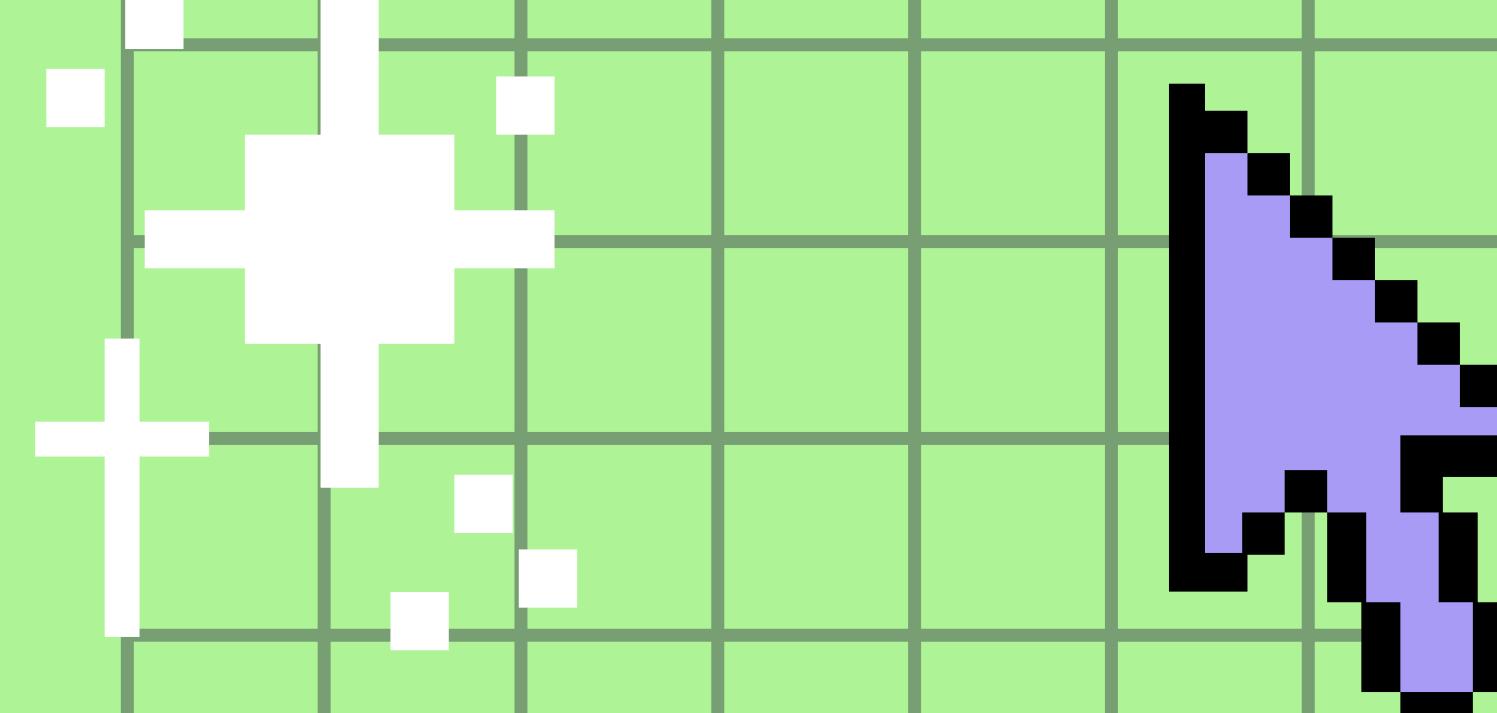


VPN (Redes Privadas Virtuales): Las VPN se utilizan para proteger la privacidad de las comunicaciones en línea y la seguridad de la red.

Los IDS/IPS monitorean el tráfico de red para detectar patrones de actividad sospechosos y alertan a los administradores de la red para que tomen medidas de seguridad.

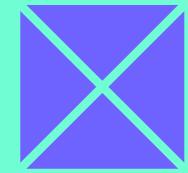


EJEMPLOS DE APLICACIÓN



New Tab

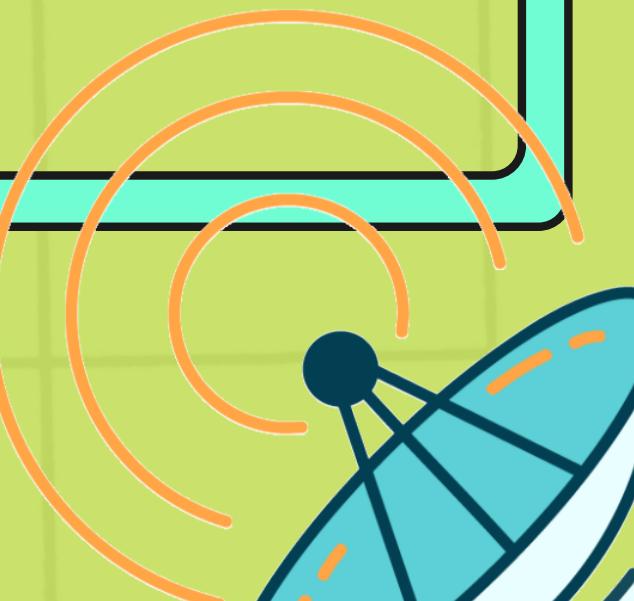
+



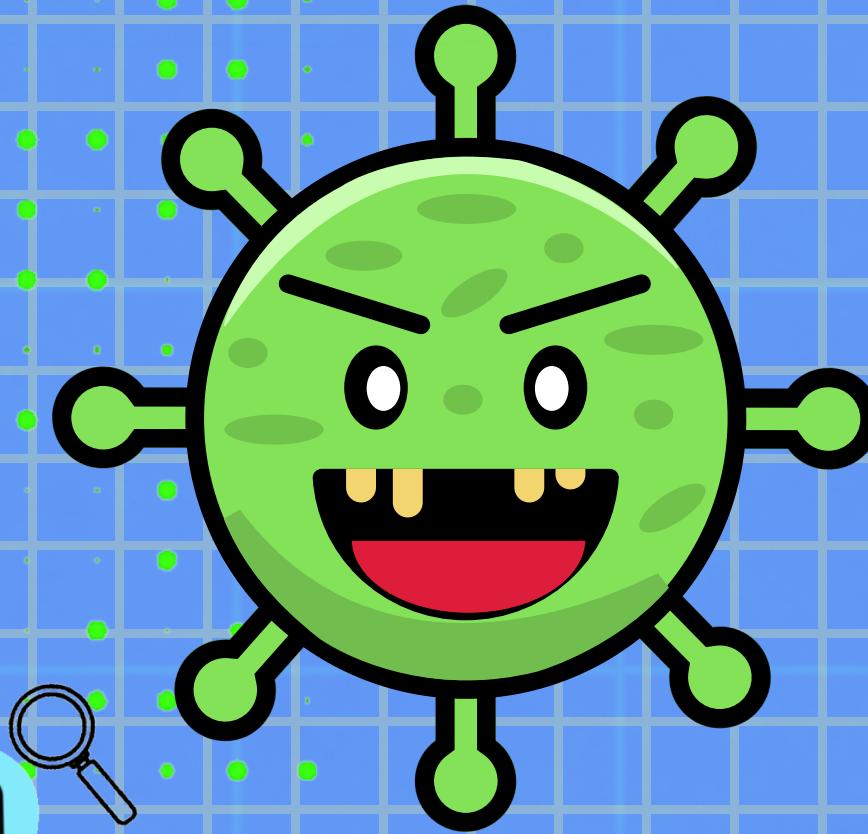
TÉCNICAS DE SEGURIDAD Y PROTECCIÓN EN SISTEMAS OPERATIVOS



Las técnicas de seguridad y protección en sistemas operativos son estrategias y medidas que se implementan para salvaguardar la integridad, confidencialidad y disponibilidad de los datos y recursos de un sistema operativo.

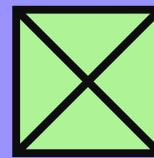
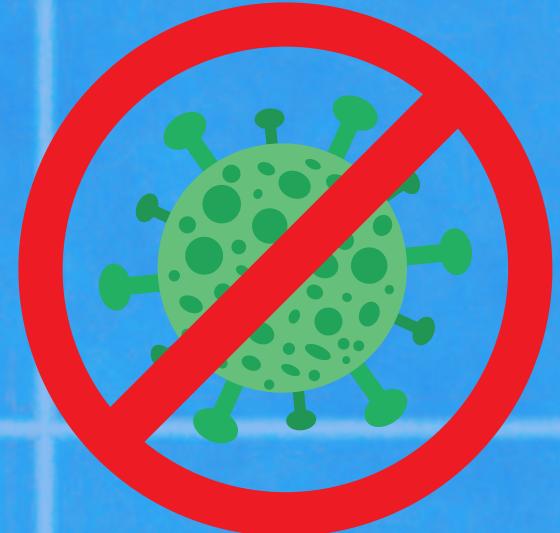


SOFTWARE ANTIVIRUS



Entendemos por software antivirus como aplicaciones o programas diseñados para proteger un sistema informático contra virus, malware y más amenazas informáticas

SOFTWARE ANTIVIRUS



Su funcionamiento se basa en varios pasos para detectar y eliminar todo tipo de malware:

1. Escaneo de archivos y directorios
2. Análisis heurístico
3. Eliminación del malware
4. Actualización de virus



¿S.O? ¿ANTIVIRUS?

El Sistema Operativo llama al antivirus para cada archivo u otro objeto que maneja mediante la integración de una funcionalidad conocida como escaneo en tiempo real o protección en tiempo real.

Cuando se habilita la protección en tiempo real en un antivirus, el software se integra en el sistema operativo y monitorea continuamente todos los archivos y objetos que se acceden o modifican en el sistema.

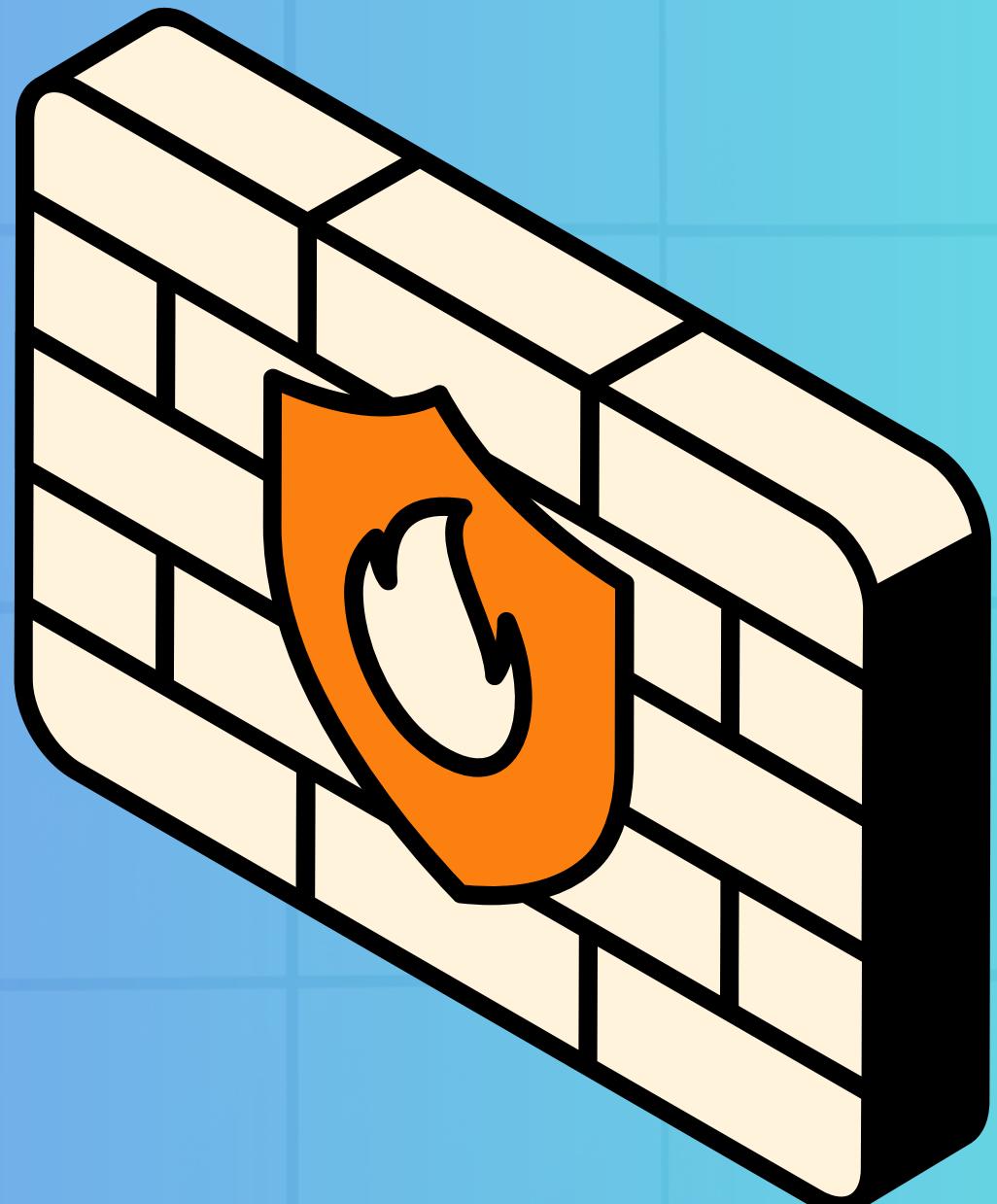
Los fabricantes suelen desarrollar controladores de dispositivo especiales que se instalan en el S.O.

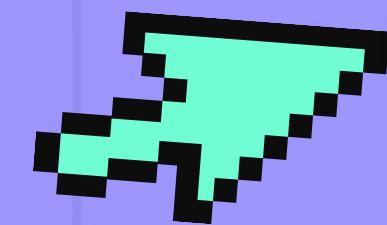
Estos interactúan directamente con el núcleo del sistema operativo para monitorear los archivos y objetos a medida que se acceden o modifican

FIREWALLS

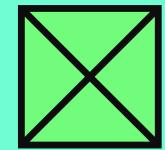
En los sistemas operativos, un firewall representa un componente de seguridad el cual examina y filtra el tráfico de red, el cual entra y sale del sistema.

Un firewall es una forma en la que una computadora especializada está conectada con sistemas que no están dentro de la red, y tiene las medidas de seguridad necesarias para poder proteger la información importante

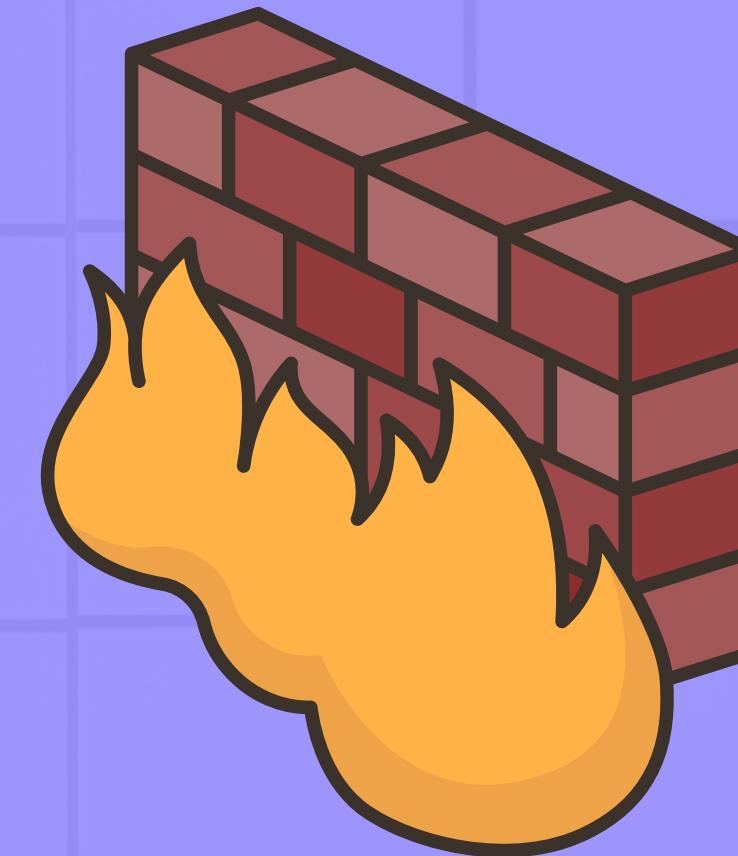




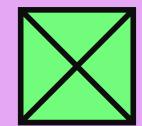
FIREWALL



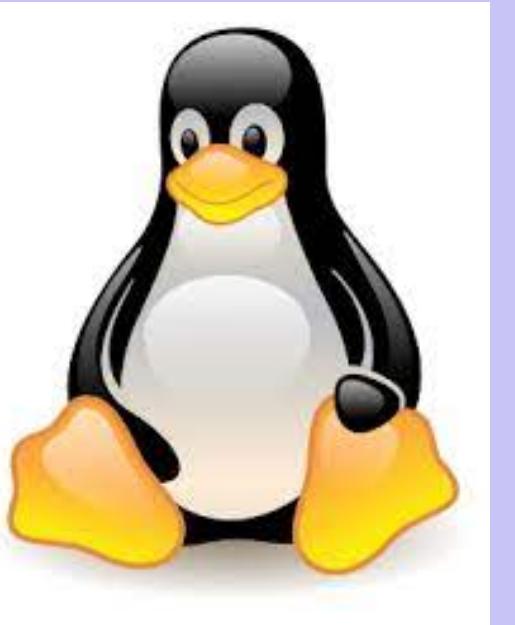
¿Por qué resulta efectivo un firewall?



El firewall resulta ser efectivo debido a que funciona como una barrera de seguridad entre el sistema local y una red externa



EJEMPLOS

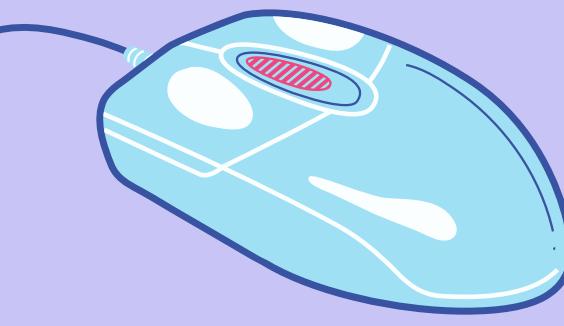


- ZoneAlarm
- Comodo Firewall
- TinyWall

- Little Snitch
- Lulu
- Radio Silencio

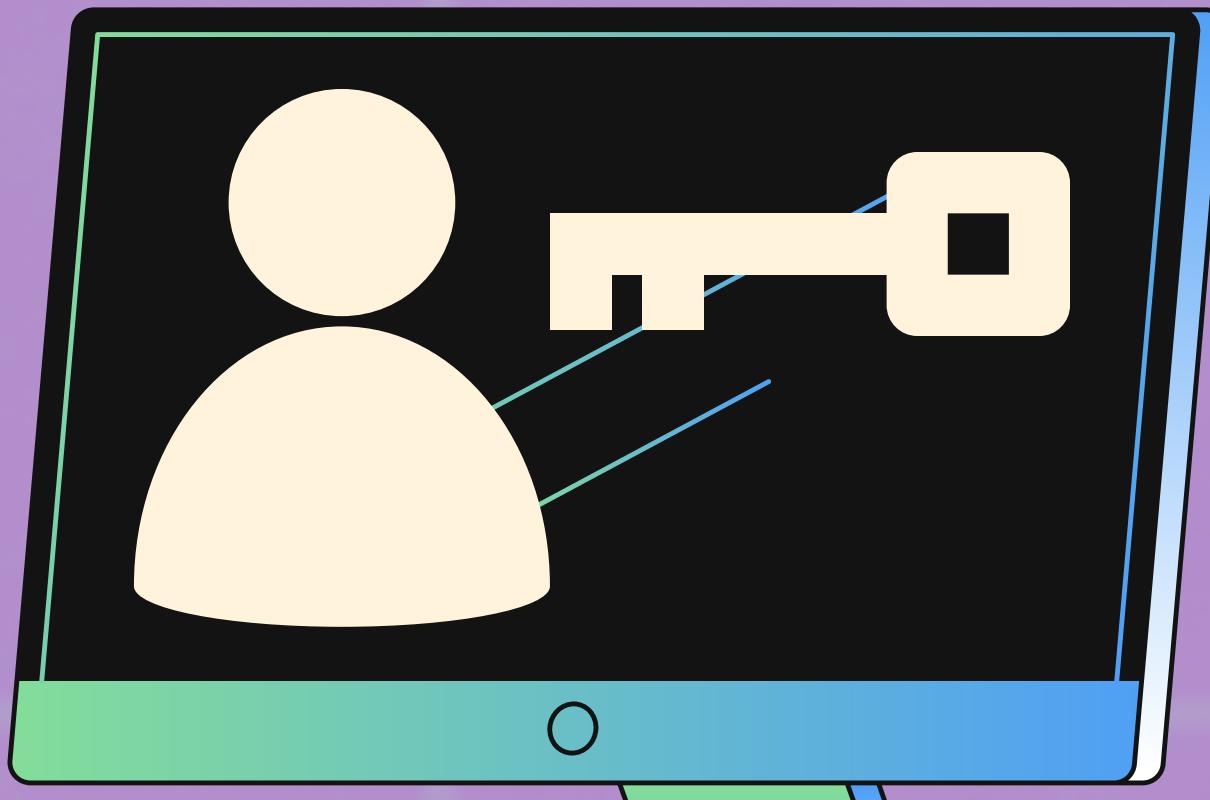
- IPCop Firewall
- Iptables
- Shorewall

- NetGuard
- Karma Firewall
- Mobiwol



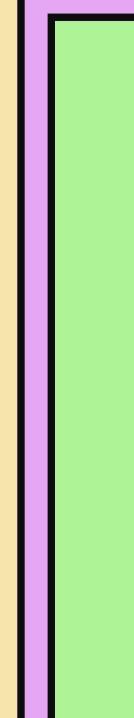
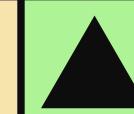
Los privilegios mínimos se implementan mediante la asignación de permisos o derechos de acceso a nivel de usuario o cuenta, esto significa que los usuarios solo tienen acceso a los recursos y acciones necesarios para realizar su trabajo, y no tienen permisos innecesarios que podrían ser utilizados de forma inapropiada.

PRIVILEGIOS MÍNIMOS





Su implementación se puede hacer en diferentes niveles, como el diseño de sistemas, la configuración de permisos de usuarios y la asignación de roles y privilegios.



Algunas de las aplicaciones prácticas son

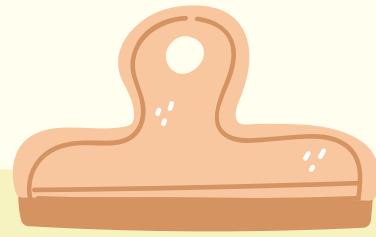
- Asignación de roles y permisos
- Restricción de privilegios de sistema
- Separación de tareas
- Auditoría y monitoreo
- Defensa en profundidad

APLICACIONES



Asignación de roles y permisos:

Los usuarios y programas deben tener solo los roles y permisos necesarios para llevar a cabo sus funciones específicas, reduciendo el riesgo de que los usuarios realicen acciones no autorizadas.



Restricción de privilegios de sistema:

Los sistemas operativos y aplicaciones deben configurarse con los privilegios más bajos posibles para llevar a cabo sus funciones, limitando la capacidad de los programas maliciosos.



Separación de tareas:

Los usuarios y procesos deben tener roles claramente definidos y limitados a las tareas específicas que necesitan realizar, reduciendo la posibilidad de errores o acciones malintencionadas.



APLICACIONES



Auditoría y monitoreo:

La aplicación también implica llevar a cabo una auditoría y monitoreo adecuado para identificar y detectar posibles violaciones de seguridad. Esto incluye la revisión regular de los roles y permisos de los usuarios,



Defensa en profundidad:

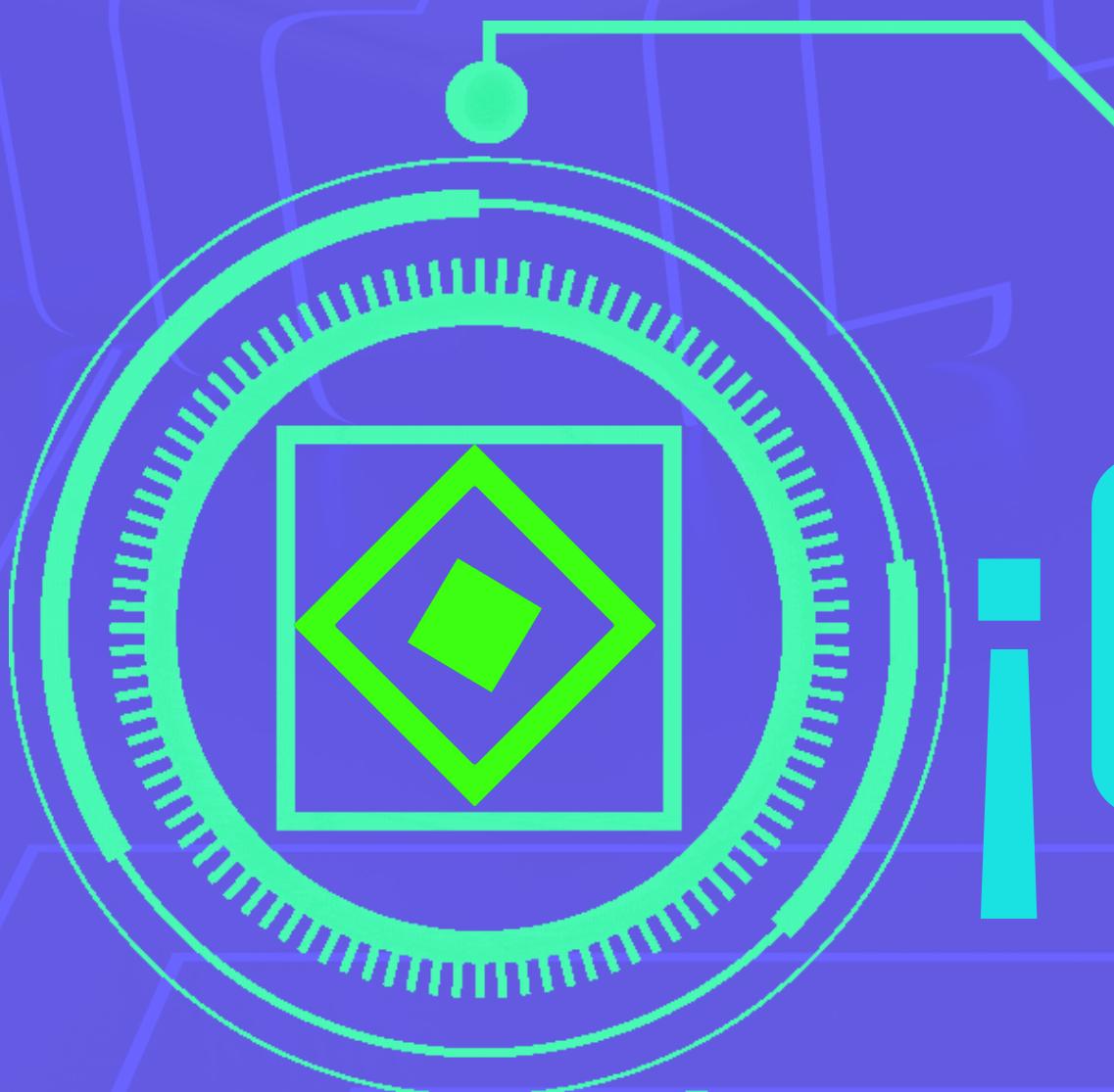
También se puede combinar con otras técnicas de seguridad, como la defensa en profundidad, que consiste en la aplicación de múltiples capas de seguridad para proteger un sistema o red



FUENTES DE CONSULTA

- [1]. FERNÁNDEZ, L. (2020, JUNIO 27). QUÉ SIGNIFICA AUTENTICACIÓN Y AUTORIZACIÓN. REDESZONE.
<HTTPS://WWW.REDESZONE.NET/TUTORIALES/SEGURIDAD/DIFERENCIAS-AUTENTICACION-AUTORIZACION/>
- [2]CIBERSEG1922. (2020, 17 SEPTIEMBRE). FIREWALL. CIBERSEGURIDAD.
<HTTPS://CIBERSEGURIDAD.COM/SERVICIOS/FIREWALL/>
- [3].STALLINGS, W. (2018). OPERATING SYSTEMS: INTERNALS AND DESIGN PRINCIPLES (9THED.). PEARSON.
- [4].¿QUÉ ES EL CIFRADO DE DATOS? DEFINICIÓN Y EXPLICACIÓN. (2022, FEBRERO 11). LATAM.KASPERSKY.COM.
<HTTPS://LATAM.KASPERSKY.COM/RESOURCE-CENTER/DEFINITIONS/ENCRYPTION>
- [5].FERNÁNDEZ, Y. (2019, 17 OCTUBRE). FIREWALL: QUÉ ES UN CORTAFUEGOS, PARA QUÉ SIRVE Y CÓMO FUNCIONA. XATAKA.
<HTTPS://WWW.XATAKA.COM/BASICS/FIREWALL-QUE-CORTAFUEGOS-SIRVE-COMO-FUNCIONA>
- [6].SECURITY ENGINEERING - A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS. (S.F.). <HTTPS://WWW.CL.CAM.AC.UK/%7ERJA14/BOOK.HTML>

POR ARMENTA FABIAN Y NAYELI SIERRA



iGRACIAS!