

Centro Universitario de Ciencias Exactas e Ingenierías.

Ciencias de la computación

Seminario de Uso, Adaptación y Explotación de Sistemas Operativos, Becerra Velázquez Violeta del Rocío

Becerra Velázquez Violeta del Rocío

Hernandez Lomelí Diego Armando

219750396

INNI- Ingeniería en informática

D02

Actividad de aprendizaje 16

(3.3 Seguridad)

2023/11/30

Tabla de contenido

[Seminario de Uso, Adaptación y Explotación de Sistemas Operativos, Becerra Velázquez Violeta del Rocío 1](#_Toc152181569)

[Introducción: 2](#_Toc152181570)

[Objetivo: 2](#_Toc152181571)

[Instrucciones. 2](#_Toc152181572)

[Ilustración 1 principales elementos para la seguridad de un sistema operativo 2](#_Toc152185366)

Introducción:

La seguridad es parte fundamental en sistemas operativos, de ahí la importancia de esta investigación.

# Objetivo:

El estudiante investigara la importancia de la seguridad en la red.

# Instrucciones.

## Realizar una investigación sobre la seguridad y protección en sus diferentes aspectos.

1. Sistema operativo

La seguridad dentro de un sistema operativo tiene como finalidad proteger la información que se almacena en el mismo equipo.

Los principales elementos para proteger la seguridad de un sistema son:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ilustración 1 principales elementos para la seguridad de un sistema operativo

Un sistema puede ser muy vulnerable si se explotan las capacidades de un sistema o si su manera de protegerse es débil, hasta ahora hablamos de cifrados fácilmente decodificables, protección en el uso de recursos (overflow forzado, por ejemplo), etc. hoy en día los sistemas operativos se mantienen en constante evolución para afrontar los peligros y evitar problemas de seguridad que se descubren día con día. Algunas estrategias que se implementan son cifrados avanzados, seguridad de red y actualizaciones constantes del sistema operativo.

La seguridad de un sistema como Windows, se puede dividir en categorías diferentes.

* **Seguridad del sistema.**

Permitiendo al equipo operar con configuraciones de confianza desde que arranca, acceso protegido a recursos del sistema, configuración de directivas, entre otros.

Están fuertemente ligados al hadware y al acceso a la información.

* **Protección contra virus y amenazas.**

Utiliza diferentes herramientas para proteger al equipo generalmente incluidas en el sistema operativo (se pueden instalar más a conveniencia del usuario), con su uso se pueden hacer diferentes comprobaciones de comportamiento e identificación de identidad según la capa del sistema en la que se esté actuando, también son de gran utilidad para prevenir al usuario de acciones que puedan abrir un apertura de seguridad, ya sea descargando archivos infectados o entrando a webs maliciosas de robo de datos o suplantación de identidad.

* **Protección y cifrado de datos**

Está categoría se enfoca en la comunicación entre componentes y red, cifra los datos de forma que incluso siendo interceptados, no puedan ser accedidos, especialmente útiles para evitar el robo de datos ya sea por una sustracción o eliminación no adecuada o en el envío de información por la red.

Un sistema operativo moderno debe contar con las herramientas mínimas para evitar que los usuarios fuera del contexto informático caigan víctimas de ataques fácilmente y ayudar quien esté experimentado a detectar fácilmente problemas existentes en el equipo

1. Red

Protege a los usuario de cualquier comportamiento inusual en el tráfico de red, existen diferentes implementaciones para esta capa de seguridad, el hardware suele ser el protagonista y aunque existen implementaciones para equipos personales, llega a ser más efectivo implementar la seguridad directamente en los dispositivos encargados de hacer posible la comunicación en la red, los firewalls, segmentación de red analisis de comportamiento y otros, son algunas estrategias a nivel hardware.

A nivel de software también existen algunas opciones similares a las anteriores, pero en su lugar protegen solo al dispositivo configurado y no a toda la red. Algunas medidas son la protección del correo electrónico, seguridad de operaciones VPN, etc.

La seguridad de red tiene como propósito:

* Estar adaptada a diferentes amenazas.
* Evitar que amenazas entren y/o se propaguen por la red.
* Administrar el acceso a la red.

Su **funcionalidad** combina diferentes capaz que implementan diferentes medidas y políticas cada una, y debe garantizar acceso a usuarios autorizados y negarlo a los maliciosos o que no están identificados.

Con su implementación se garantiza protección e integridad a los usuarios y sus datos, además, como organización puede proteger su reputación al público general.

1. Usuario

La seguridad no solo va por lo automático, un sistema informático debe ser capaz de proteger medidas de seguridad a los usuario para su uso frecuente, un usuario puede ser capaz de generar una brecha de seguridad inintencionalmente y la seguridad para usuario sigue de cerca los movimientos del usuario. Para asegurar el uso legítimo de un sistema.

Para acceso a datos importantes y aplicaciones o sistemas se pueden implementar:

* Especificación de contraseñas a nuevos usuarios.

Se deben asignar claves de seguridad y formas de comunicación o contacto con los usuarios, de este modo se puede asociar un perfil a un usuario para visualizar sus acciones y también estos datos permiten el cambio de contraseña dependiendo de los motivos que existan.

* Generación de grupos de seguridad

Da permisos a usuarios para garantizar que cuente con permisos iguales a otros usuario con la misma capacidad

* Desconexión y boqueo de usuarios.

Gestionar la capacidad de un usuario a un sistema es importante, gracias a ello se puede permitir a un usuario acceder y denegar su acceso si hace falta hacer el cambio.

## Genere una conclusión sobre lo aprendido en esta actividad.

En la actualidad la información de los usuario de sistemas computacionales se ve constantemente comprometida por terceros tratando de obtenerla para sus propios beneficios. Siendo datos de navegación por la red hasta datos personales o financieros los que buscan ser obtenidos malintencionadamente, es importante de vital importancia contar con herramientas especializadas para mejorar la eficiencia de la protección en todos los niveles de comunicación posibles y sobre todo, es importante que los usuarios conozcan estas medidas para fortalecer su propia seguridad en la navegación.

# Bibliografía

(s.f.). Obtenido de Cisco: https://www.cisco.com/c/es\_mx/products/security/what-is-network-security.html

(12 de Abril de 2021). Obtenido de IBM: https://www.ibm.com/docs/es/aix/7.2?topic=administration-operating-system-security

(3 de Marzo de 2021). Obtenido de IBM: https://www.ibm.com/docs/es/control-desk/7.6.1?topic=users-implementing-security

Vinay Pamnani, P. M. (Octubre de Febrero de 2023). Obtenido de Microsoft: https://learn.microsoft.com/es-es/windows/security/operating-system-security/