Universidad Tecnológica Nacional

Facultad Regional Resistencia

Tecnicatura Universitaria en Programación

Nombres y Apellidos		
• Galarza Pablo • Grossetti Ignacio • Hotchkyss Gersom Tomás • Quintero Camila		
Materia		
ARQUITECTURA Y SISTEMAS OPERATIVOS		
Comisión	**Tema**	
2	**SEGURIDAD EN SISTEMAS OPERATIVOS**	
Grupo	**Año**	**Nota**
2	**2025**	
Profesor		
Cuevas Carlos		

Índice:

Introducción:

La seguridad en los sistemas operativos es algo fundamental para que se pueda garantizar la integridad, confidencialidad y disponibilidad de toda la información. En este informe presentado, se mostrarán los mecanismos de protección que se implementan en los sistemas modernos, su objetivo, su correspondiente impacto en la seguridad informática y cuales son los desafíos actuales en la prevención de amenazas. Con una revisión de las herramientas que se usan para detectar malware.

¿Qué es un Sistema Operativo?

Podría considerarse el intermediario a través del cual interactuamos con la computadora y donde se ejecutan todas nuestras aplicaciones. Esta es la capa que interactúa con el hardware de la computadora. [1]

¿Qué es la seguridad y protección de los sistemas operativos?

Cuando hablamos de la seguridad en los sistemas operativos nos referimos a la funcionalidad de un sistema para proteger sus recursos, datos y funcionalidades de amenazas internas y externas, y para preservar la integridad, disponibilidad y confidencialidad de toda la información. La seguridad evoluciona con el tiempo a medida que la tecnología evoluciona y se adapta a nuevos escenarios.

El continuo avance de la informática ha estado dando lugar a sistemas digitales cada vez más complejos. Los microprocesadores, los sistemas operativos, las computadoras y las redes se han revolucionado en las últimas décadas para ofrecer más capacidades y opciones.

Sin embargo, este aumento de la complejidad también va generando más fallos y debilidades potenciales. Todo software es propenso a errores, y cuanto más complejo es el sistema, es mayor la probabilidad de que existan fallos que puedan comprometer su seguridad.

Para medir la seguridad de un sistema, es necesario realizar una evaluación general de la seguridad. Sin embargo, a medida que el sistema se va complejizando más, su evaluación se vuelve más difícil. El análisis, el diseño y la codificación de sistemas complejos están sujetos a un número en alza de fallos de seguridad, y las soluciones se vuelven cada vez más difíciles a medida que aumenta la complejidad. Cuanto más complejo es un sistema, más difícil es comprenderlo en su totalidad y el número de vulnerabilidades potenciales aumenta, por ejemplo, las interfaces usuario-máquina y la interacción interna del sistema, donde no es posible tener una visión completa de todo el sistema.[2]

Componentes de un Mecanismo de Seguridad en Sistemas Operativos

La seguridad en sistemas operativos se basa en varios mecanismos internos y externos que buscan proteger la integridad, confidencialidad y disponibilidad de toda la información del sistema.[2]

Seguridad Externa

Incluye medidas físicas y administrativas fuera del sistema operativo:

- **Seguridad Física**: Prevención ante desastres (incendios, inundaciones, temperatura, acceso físico) mediante controles como cerraduras, tarjetas o biometría.
- **Seguridad de Administración**: Control de acceso lógico mediante autenticación con usuario y contraseña, y prácticas seguras como el cambio frecuente de claves.
- **Criptografía**: Protección de datos mediante cifrado durante su transmisión.

Seguridad Interna

Opera dentro del sistema operativo para controlar el uso de recursos:

- **Procesador**: Usa modos protegido y usuario para limitar privilegios.
- **Memoria**: Impide accesos indebidos entre usuarios y asegura integridad con paridad o checksum.
- **Archivos**: Protege disponibilidad y privacidad con respaldos, archivos LOG y control de accesos.

Mecanismos Comunes de Protección

1. **Antivirus**: Detectan y eliminan software malicioso.
2. **Actualizaciones del SO**: Corrigen vulnerabilidades y refuerzan la seguridad.
3. **Firewalls**: Regulan el tráfico de red para evitar accesos no autorizados.
4. **Políticas de Acceso Seguro**: Asignan mínimos privilegios a los usuarios para reducir riesgos.

Objetivos de la Seguridad en Sistemas Operativos

La seguridad en sistemas operativos tiene como propósito principal proteger los recursos del sistema y la información que contiene. Sus objetivos fundamentales son:

- **Confidencialidad**: Asegurar que solo los usuarios autorizados puedan acceder a la información.
- **Integridad**: Garantizar que los datos y recursos no sean modificados sin autorización.
- **Disponibilidad**: Mantener el sistema y sus servicios accesibles para los usuarios legítimos.
- **Control de acceso**: Restringir el uso de recursos según los permisos definidos para cada usuario o proceso.
- **Prevención y detección de amenazas**: Evitar ataques internos y externos, y responder ante incidentes de seguridad.[1]

Políticas de Seguridad en Sistemas Operativos

Las políticas de seguridad en Sistemas Operativos son un conjunto de reglas que definen cómo se protege la información dentro del sistema. Su objetivo es establecer un marco de actuación frente a accesos, uso de recursos y prevención de amenazas. Entre las principales políticas se encuentran:

- **Política de control de acceso**: Define quién puede acceder a qué recursos, en qué condiciones y con qué permisos (lectura, escritura, ejecución).
- **Política de autenticación**: Establece los métodos para verificar la identidad de los usuarios (contraseñas, biometría, tokens).
- **Política de contraseñas**: Indica la longitud mínima, caducidad, complejidad y periodicidad del cambio de las contraseñas.
- **Política de copias de seguridad**: Asegura que los datos importantes se respalden periódicamente para evitar pérdidas ante fallos o ataques.

- **Política de actualización del sistema**: Establece que el sistema operativo y el software deben mantenerse actualizados para corregir vulnerabilidades.

- **Política de uso aceptable**: Determina el uso permitido del sistema y las conductas prohibidas por los usuarios (instalar software no autorizado, compartir contraseñas, etc.).

Estas políticas deben ser claras, aplicables y estar acompañadas de mecanismos técnicos (como firewalls o antivirus) para su cumplimiento.

Herramientas

¿Qué son?

Las herramientas son los recursos o programas qué utiliza el sistema operativo para poder defenderse de posibles virus o amenazas qué puedan afectar a la integridad de este.

Hay 3 herramientas principales, los antivirus, los firewall y los detectores.

Antivirus: Su objetivo es detectar y eliminar virus informáticos. han avanzado hasta conseguir bloquearlos, desinfectarlos, y prevenir infecciones. El primer antivirus documentado es el realizado por Omri y Rakvi, el cual fue creado para combatir un virus llamado virus Jerusalén.[3]

Firewalls: Un firewall es un dispositivo de seguridad de red diseñado para monitorear, filtrar y controlar el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas. El propósito principal de un firewall es establecer una barrera entre una red interna confiable y redes externas no confiables.[4]

Detectores: Un sistema de detección de intrusiones (IDS) es una aplicación que monitorea el tráfico de red y busca amenazas conocidas y actividad sospechosa o maliciosa. El IDS envía alertas a los equipos de TI y seguridad cuando detecta cualquier riesgo y amenaza de seguridad.[5]

Funcionamiento Del Antivirus

La forma qué utiliza el antivirus para funcionar es mediante un escaneo de todos los archivos del sistema, verificando su integridad, su origen, su tamaño y su composición.

1. **Firma de Virus:** Aquí se almacenan las firmas de virus, estos son los patrones de bytes qué componen a los virus de forma general.Se crea una lista con todos los conocidos para poder facilitar el hallazgo de estos. [6]

2. Análisis heurístico: Este método se basa en la descomposición del código analizándolo y comparándolo con otros virus conocidos. Si en la comparación se encuentran similitudes, se considera a dicho código como posible malware, aislandolo del resto. Otra forma de analizar el código, es mediante el Análisis heurístico dinámico, se basa en la ejecución del programa a analizar en una máquina virtual segura, observando cada proceso qué se lleva a cabo. [7]

Procesos de contingencia

Una vez qué el antivirus detecta un malware en el sistema tiene qué realizar una de las siguiente 2 acciones para pararlo.

1. Eliminación del programa: De forma automática, el sistema operativo decide eliminar el programa malicioso junto a los archivos relacionados a este, evitando así la posible infección del equipo.
2. Bloqueo del programa: Si se llega a detectar con antelación, el antivirus bloquea el archivo malicioso antes de qué pueda ser ejecutado. A veces el mismo antivirus permite al usuario habilitar el posible malware, pero únicamente con permisos de administrador.

Funcionamiento Del Firewall

Los firewalls vienen en formas de hardware y software, y funcionan inspeccionando paquetes de datos y determinando si los permiten o bloquean en función de un conjunto de reglas. Las organizaciones pueden configurar estas reglas para permitir o denegar el tráfico en función de varios criterios, como direcciones IP de origen y destino, números de puerto y tipo de protocolo. [4]

¿Qué hace un firewall?

Los firewalls protegen contra el tráfico malicioso. Están estratégicamente posicionados en el borde de la red o en un centro de datos, lo que les permite monitorear de cerca cualquier cosa que intente cruzar este límite.

Esta visibilidad también permite a un firewall de red inspeccionar y autenticar glandularmente los paquetes de datos en tiempo real. Esto implica verificar el paquete de datos con criterios predefinidos para determinar si representa una amenaza. Si no cumple con los criterios, el firewall le impide entrar o salir de la red.

Los firewalls regulan el tráfico entrante y saliente, protegiendo la red de:

- **Amenazas externas** como virus, puertas traseras, correos electrónicos de suplantación de identidad y ataques de denegación de servicio (DoS). Los firewalls filtran los flujos de tráfico entrantes, evitando el acceso no autorizado a datos sensibles y frustrando posibles infecciones de malware.

- **Amenazas internas** como actores maliciosos conocidos o aplicaciones riesgosas. Un firewall puede aplicar reglas y políticas para restringir ciertos tipos de tráfico saliente, lo que ayuda a identificar actividades sospechosas y mitigar la exfiltración de datos.

Comparación entre firewall y antivirus

¿Cuál es la diferencia entre el firewall y el software antivirus? Los firewalls se enfocan en controlar el tráfico de red y prevenir el acceso no autorizado. Por el contrario, los programas antivirus se dirigen y eliminan las amenazas a nivel de dispositivo. Más específicamente, sus diferencias clave incluyen:

- **Alcance:** El software antivirus es principalmente una solución de endpoint, lo que significa que se instala en un dispositivo individual. Los firewalls se implementan principalmente a nivel de red, pero algunas organizaciones instalan firewalls alojados directamente en un endpoint para obtener protección adicional.

- **Funcionalidad:** Los firewalls monitorean el tráfico, bloqueando los datos maliciosos antes de que ingresen a la red (o endpoint). Las herramientas antivirus escanean el entorno local en busca de signos de malware, ransomware y otros ataques infecciosos.

Las empresas normalmente implementan tanto firewalls como programas antivirus. Como soluciones complementarias, cada una proporciona capas de protección esenciales para proteger los activos comerciales.[4]

Funcionamiento de los Detectores

La mayoría de las soluciones de IDS simplemente monitorean e informan sobre la actividad y el tráfico sospechosos cuando detectan una anomalía. Sin embargo, algunos pueden ir un paso más allá al tomar medidas cuando detectan actividad anómala, como bloquear tráfico malicioso o sospechoso.

Las herramientas IDS generalmente son aplicaciones de software que se ejecutan en el hardware de las organizaciones o como una solución de seguridad de red. También hay soluciones IDS basadas en la nube que protegen los datos, recursos y sistemas de las organizaciones en sus implementaciones y entornos en la nube.[5]

¿Qué es una intrusión en ciberseguridad?

La respuesta a "qué es una intrusión" generalmente es un atacante que obtiene acceso no autorizado a un dispositivo, red o sistema. Los cibercriminales utilizan técnicas y tácticas cada vez más sofisticadas para infiltrarse en organizaciones sin ser descubiertos. Esto incluye técnicas comunes como:

1. **Suplantación de direcciones:** la fuente de un ataque se oculta mediante servidores proxy falsificados, mal configurados y mal protegidos, lo que dificulta que las organizaciones descubran atacantes.
2. **Fragmentación:** los paquetes fragilizados permiten a los atacantes eludir los sistemas de detección de las organizaciones.
3. **Evasión de patrones:** los hackers ajustan sus arquitecturas de ataque para evitar los patrones que las soluciones de IDS utilizan para detectar una amenaza.
4. **Ataque coordinado:** una amenaza de escaneo de red asigna numerosos hosts o puertos a diferentes atacantes, lo que dificulta que el IDS resuelva lo que sucede.[5]

¿Cómo avanzo la seguridad en sistemas operativos durante los años?

- **1950-1960:** Los primeros sistemas operativos no tenían características de seguridad robustas. Sin embargo, con la introducción de Unix en la década de 1960, se implementaron mecanismos de autenticación y autorización de usuarios, lo que marcó el comienzo de la seguridad en sistemas operativos.
- **1970-1980:** En la década de 1970, comenzaron a desarrollarse herramientas de seguridad básicas, como antivirus primitivos. En la década de 1980, se popularizaron los firewalls y el software de detección de virus, lo que mejoró la seguridad en sistemas operativos personales.
- **1990:** La llegada de los sistemas operativos de código abierto, como Linux, permitió a los desarrolladores revisar y mejorar el código, lo que llevó a una mayor seguridad y estabilidad en los sistemas operativos.
- **2000:** Con el auge de los sistemas operativos móviles, como Android e iOS, la seguridad se centró en la protección de la información personal y la prevención de malware.

- **Actualidad:** En la actualidad, la seguridad en sistemas operativos se enfoca en la detección y prevención de amenazas avanzadas, utilizando tecnologías como la inteligencia artificial y el aprendizaje automático.[8]

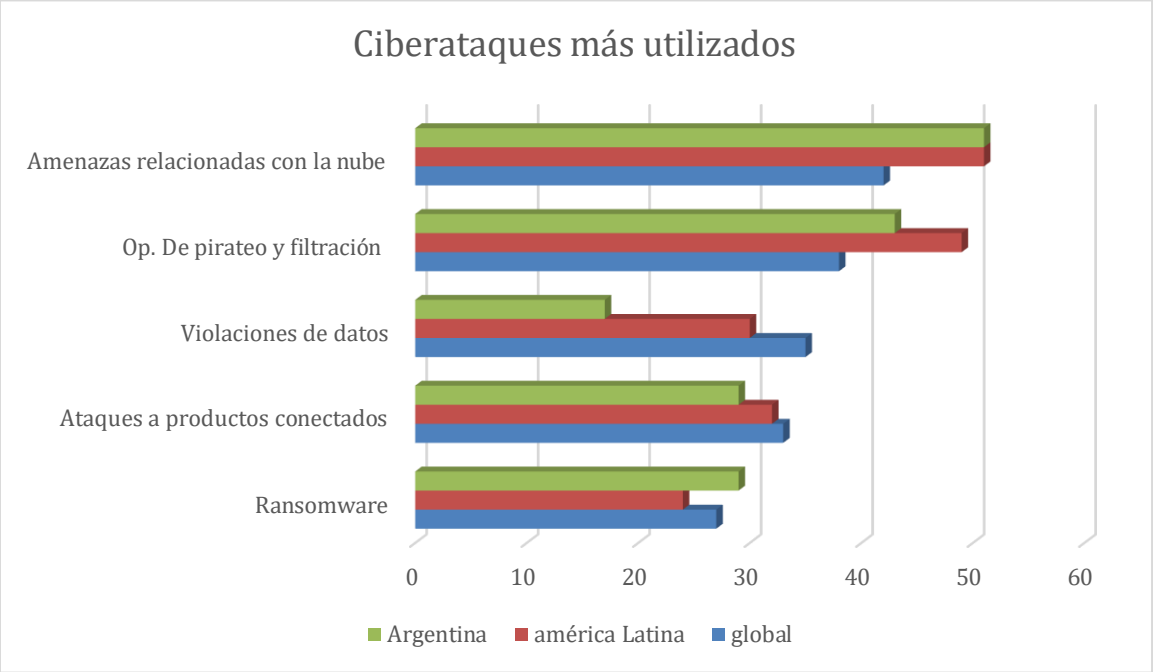
¿Cuáles son los ataques más comunes que podemos conocer relacionados a la seguridad en sistemas operativos?

1. Phishing: un tipo de ataque que implica el envío de correos electrónicos genéricos o personalizados que parecen legítimos, con el objetivo de robar información privada del usuario.
2. Malware: software malicioso diseñado para dañar o infiltrarse en sistemas informáticos sin el consentimiento del usuario.
3. Ataques DDoS (Denegación de Servicio Distribuido): un ataque que busca inhabilitar un servidor o servicio mediante la saturación del ancho de banda o agotamiento de recursos del sistema.
4. Inyección de SQL: un ataque que manipula bases de datos mediante la inyección de declaraciones SQL maliciosas en aplicaciones que tienen bases de datos relacionales.
5. Ransomware: un tipo de malware que cifra archivos importantes y exige un rescate para descifrarlos. [9]

[1] *"Clasificación de los delitos"*, imagen. [Online]. Disponible: [https://www.argentina.gob.ar/sites/default/files/cofemod_comisionciberseguridad_el_panorama_de_la_ciberseguridad_en_numeros_12-08-16.pdf]. [Acceso: 17-Jun-2024].

CIBERSEGURIDAD EN ARGENTINA

En Argentina, las amenazas cibernéticas más preocupantes para las organizaciones incluyen los ataques a la nube, las infracciones de terceros y los ataques a productos conectados. Sin embargo, estos mismos riesgos son los que los ejecutivos de seguridad se sienten menos preparados para enfrentar, lo que evidencia una brecha significativa en la resiliencia cibernética del país.[10]



[2] *"Ciberataques más utilizados"*, imagen. [Online]. Disponible: [https://www.elseguroenaccion.com.ar/los-ataques-ciberneticos-ya-son-la-principal-preocupacion-en-una-de-cada-dos-empresas-y-en-argentina-persiste-la-falta-de-preparacion-para-evitarlos/#:~:text=preparaci%C3%B3n%20para%20evitarlos-,Los%20ataques%20cibern%C3%A9ticos%20ya%20son%20la%20principal%20preocupaci%C3%B3n%20en%20una,falta%20de%20preparaci%C3%B3n%20para%20evitarlos&text=Buenos%20Aires%2C%2020%20de%20marzo,para%20fortalecer%20su%20resiliencia%20cibern%C3%A9tica]. [Acceso: 17-Jun-2024].

BIBLIOGRAFÍA:

[1]- Universidade da Coruña - “Seguridad en Sistemas Operativos”
http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/03%20-%20Seguridad%20en%20Sistemas%20Operativos.pdf

[2]- “Protección y Seguridad en Sistemas Operativos: qué es y cómo se compone”
https://ciberseguridadtips.com/proteccion-seguridad-sistemas-operativos/#Que_es_Seguridad_y_Proteccion_en_Sistemas_Operativos

[3]-”Antivirus”
https://es.wikipedia.org/wiki/Antivirus

[4]-”¿Qué es un Firewall?”
https://www.fortinet.com/lat/resources/cyberglossary/firewall#:~:text=Un%20firewall%20es%20un%20dispositivo,y%20redes%20externas%20no%20confiables

[5]-”¿Qué es un sistema de detección de intrusiones (IDS)?”
https://www.fortinet.com/lat/resources/cyberglossary/intrusion-detection-system

[6]-”Understanding Anti-virus Software”
”https://www.cisa.gov/news-events/news/understanding-anti-virus-software”

[7]-”¿En qué consiste el análisis heurístico?”
https://www.kaspersky.es/resource-center/definitions/heuristic-analysis

[8]-” ¿Cómo avanzo la seguridad en sistemas operativos durante los años?“
https://www.incibe.es/empresas/blog/pasado-presente-y-futuro-de-la-seguridad-de-la-informacion

[9]-” ¿Cuáles son los ataques más comunes que podemos conocer relacionados a la seguridad en sistemas operativos?“
https://www.argentina.gob.ar/sites/default/files/cofemod_comisionciberseguridad_el_panorama_de_la_ciberseguridad_en_numeros_12-08-16.pdf

[10]-“ IA y CIBERSEGURIDAD”
https://www.elseguroenaccion.com.ar/los-ataques-ciberneticos-ya-son-la-principal-preocupacion-en-una-de-cada-dos-empresas-y-en-argentina-persiste-la-falta-de-preparacion-para-evitarlos/#:~:text=preparaci%C3%B3n%20para%20evitarlos-,Los%20ataques%20cibern%C3%A9ticos%20ya%20son%20la%20principal%20preocupaci%C3%B3n%20en%20una,falta%20de%20preparaci%C3%B3n%20para%20evitarlos&text=Buenos%20Aires%2C%2020%20de%20marzo,para%20fortalecer%20su%20resiliencia%20cibern%C3%A9tica