Centro Universitario de Ciencias Exactas e Ingenierías.

Departamento para la integración ciber humana.

Sistemas operativos.

Becerra Velázquez Violeta Rocío.

SAUL EMANUEL YAÑEZ SALAZAR
220656484.

Ingeniería en computación.

D04

Seguridad

Jueves 1 de mayo. de 2025

Criptografia.

La criptografía es una disciplina esencial en la seguridad digital moderna, que se encarga de proteger la información mediante técnicas de codificación, asegurando que solo las personas autorizadas puedan acceder a ella. Esta ciencia ha evolucionado desde métodos antiguos de cifrado hasta complejos algoritmos utilizados en la actualidad.

¿Qué es la criptografía?

La criptografía transforma datos legibles en un formato cifrado, utilizando algoritmos matemáticos y claves, de modo que solo quienes posean la clave adecuada puedan descifrarlos. Este proceso garantiza la confidencialidad, integridad y autenticidad de la información. (TecnoDigital, 2025)

Usos actuales de la criptografía

La criptografía se aplica en diversos ámbitos para proteger la información y las comunicaciones:

1. Seguridad en las comunicaciones: Protege correos electrónicos, mensajes instantáneos y llamadas telefónicas mediante cifrado de extremo a extremo, asegurando que solo el emisor y el receptor puedan acceder al contenido.
2. Transacciones financieras y banca en línea: Garantiza la seguridad de las transacciones electrónicas, protegiendo los datos sensibles de los usuarios y previniendo fraudes.
3. Almacenamiento seguro de datos: Se utiliza para cifrar información almacenada en dispositivos o en la nube, protegiéndola contra accesos no autorizados.
4. Autenticación y control de acceso: Las contraseñas y sistemas de autenticación multifactor emplean técnicas criptográficas para verificar la identidad de los usuarios.
5. Firmas digitales: Permiten verificar la autenticidad de documentos y mensajes, asegurando que no han sido alterados y que provienen de una fuente confiable.
6. Criptomonedas y blockchain: Las monedas digitales como Bitcoin y Ethereum utilizan criptografía para asegurar las transacciones y controlar la creación de nuevas unidades.
7. Protección de derechos de autor: La criptografía ayuda a proteger la propiedad intelectual en el entorno digital, asegurando que los contenidos no sean copiados o distribuidos sin autorización. (Sanchez, 27)

Esteganografía

La esteganografía es el arte y la ciencia de ocultar información dentro de otro medio de manera que su existencia pase desapercibida. A diferencia de la criptografía, que cifra el contenido de un mensaje para hacerlo ininteligible a terceros, la esteganografía busca ocultar el hecho mismo de que se está transmitiendo un mensaje secreto.

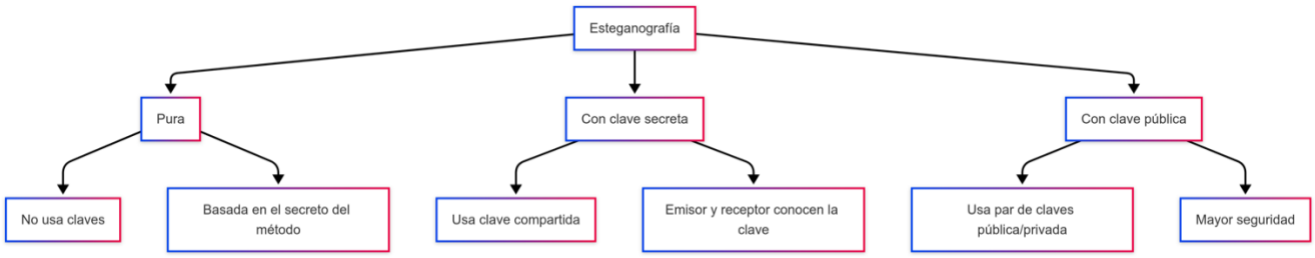
¿Cómo funciona?

En la esteganografía digital, la información se incrusta en archivos aparentemente inocuos, como imágenes, audios, videos o documentos de texto. Por ejemplo, en una imagen, se pueden modificar los bits menos significativos de los píxeles para insertar datos sin que haya cambios perceptibles a simple vista. Este proceso permite que el archivo portador mantenga su apariencia original, evitando levantar sospechas. (ARIELMCORG, 2024) (Wikipedia Authors, 28)

Aplicaciones comunes

- Protección de la privacidad: Permite a activistas, periodistas y disidentes comunicarse de forma segura en entornos hostiles.
- Seguridad informática: Se utiliza para ocultar información sensible en archivos digitales, protegiéndola de accesos no autorizados.
- Protección de derechos de autor: Las marcas de agua digitales emplean técnicas esteganográficas para identificar la autoría de contenidos multimedia.
- Ciberdelincuencia: Desafortunadamente, también puede ser utilizada para ocultar malware o coordinar actividades ilícitas sin ser detectadas.

Tipos.



¿Cómo aplican ambos?

La criptografía y la esteganografía tienen aplicaciones fundamentales tanto en los sistemas operativos como en las redes informáticas, aunque con enfoques distintos.

Aplicaciones en Sistemas Operativos

Criptografía

Cifrado de archivos y discos

Los sistemas operativos modernos implementan criptografía para cifrar el disco completo o archivos individuales, protegiendo así los datos en caso de pérdida o robo del equipo.

Gestión segura de contraseñas

Las contraseñas no se almacenan en texto plano. Se utilizan algoritmos de hash (como SHA-256 o bcrypt) para almacenar sus huellas digitales de forma segura.

Autenticación de usuarios

En la autenticación mediante certificados, claves públicas/privadas garantizan la identidad del usuario o del sistema.

Integridad del sistema

Se usan firmas digitales para verificar que los archivos del sistema o actualizaciones no han sido alterados.

Esteganografía

Ocultamiento de datos internos o logs

Aunque no es común en implementaciones oficiales, algunos mecanismos maliciosos pueden usar esteganografía para ocultar datos dentro de archivos aparentemente inofensivos, dificultando su detección.

Protección contra ingeniería inversa

Algunos sistemas pueden emplear técnicas esteganográficas para proteger información sensible sobre el software o algoritmos internos.

Mecanismos de DRM

En algunos entornos operativos, los sistemas de gestión de derechos digitales pueden usar marcas de agua digitales (una forma de esteganografía) para rastrear el uso de medios.

Aplicaciones en Redes Informáticas

Aplicaciones en redes.

Criptografía

Cifrado de comunicaciones

Protocolos como TLS/SSL, SSH, IPsec, y VPNs utilizan criptografía para asegurar que la comunicación entre dispositivos sea confidencial e íntegra.

Certificados digitales

Se utilizan para verificar la identidad de servidores (como en HTTPS) mediante una infraestructura de clave pública (PKI).

Firmas digitales y autenticación

Los mensajes en protocolos seguros pueden incluir firmas digitales para garantizar que provienen de fuentes auténticas y no han sido alterados.

Esteganografía

Canales encubiertos

En redes, la esteganografía puede ocultar mensajes dentro de protocolos aparentemente legítimos, lo cual puede ser usado tanto para fines legítimos como maliciosos.

Exfiltración de datos

Los atacantes pueden usar técnicas esteganográficas para sacar información confidencial de una red sin ser detectados por sistemas de seguridad tradicionales.

Comunicaciones encubiertas entre malware

Algunas botnets usan imágenes o videos subidos a redes sociales que contienen comandos ocultos mediante esteganografía, evadiendo así los sistemas de detección.

Seguridad y protección en el sistema operativo.

La seguridad y protección dentro del sistema operativo constituye uno de los pilares fundamentales en el ámbito de la informática moderna, ya que su función es velar por la integridad, confidencialidad y disponibilidad de los datos y procesos que se ejecutan dentro de un entorno computacional. A medida que las tecnologías avanzan y los sistemas se vuelven más interconectados, también crece el espectro de amenazas a las que están expuestos, por lo que se vuelve imprescindible implementar mecanismos robustos y eficaces para mitigar los riesgos y asegurar el correcto funcionamiento del sistema. En este contexto, el sistema operativo no solo actúa como un intermediario entre el hardware y el software de usuario, sino que también desempeña el rol de primer defensor frente a cualquier intento de acceso no autorizado, manipulación maliciosa o fallo inesperado que pueda comprometer el entorno de ejecución.

La seguridad en un sistema operativo puede abordarse desde diversas dimensiones, comenzando por el control de acceso, que garantiza que los usuarios solo puedan interactuar con los recursos del sistema conforme a los privilegios que les han sido asignados. Este control se implementa mediante políticas que definen claramente quién puede hacer qué con qué recurso. Los sistemas operativos modernos emplean esquemas como listas de control de acceso, modelos basados en capacidades e incluso en contextos más complejos, incluso políticas de control obligatorio, como las que se encuentran en sistemas de alta seguridad. Además, los permisos a nivel de archivos y procesos son una medida básica pero eficaz que evita que los usuarios ejecuten acciones que puedan comprometer la estabilidad o privacidad del sistema.

Una parte crucial en términos de seguridad es la autenticación de usuarios, que consiste en verificar la identidad de los individuos que intentan acceder al sistema. Los métodos tradicionales como el uso de contraseñas están siendo complementados (y en algunos casos, se son cambiados) por mecanismos más avanzados como la autenticación dos factores (donde los usuarios usan otro dispositivo para poder ingresar), la biometría o el uso de certificados digitales. Estos sistemas fortalecen significativamente la seguridad, ya que dificultan el acceso por parte de actores malintencionados incluso si han obtenido credenciales válidas por otros medios, dado que estos factores siempre se encargarán de buscar un método de autenticación valido que permita realmente solo dar acceso al usuario deseado, haciéndose preguntas o demostrando su identidad, con partes como:

- Algo que es el usuario
- Algo que sabe el usuario.

Por otra parte, la protección contra malware (o en casos más “naturales” conocidos como “*virus”*) también es una responsabilidad compartida entre el sistema operativo y las aplicaciones de seguridad instaladas en el sistema. Los sistemas operativos modernos integran mecanismos como el sandboxes, que permite aislar la ejecución de programas para

evitar que uno pueda afectar a los demás, y el uso de firmas digitales para asegurar que los archivos ejecutables no hayan sido alterados. Además, la implementación de firewalls, tanto a nivel de red como de host, es esencial para filtrar el tráfico y bloquear actividades sospechosas o no autorizadas.

La gestión de vulnerabilidades es otro componente clave. Todos los sistemas operativos contienen, por su propia naturaleza, errores y debilidades que pueden ser explotados por atacantes. Por ello, la actualización constante mediante parches de seguridad se vuelve una tarea indispensable. La mayoría de sistemas actuales, como Windows, macOS y las distintas distribuciones de Linux, cuentan con sistemas de actualización automática que permiten corregir fallos y cerrar brechas de seguridad en cuanto estas son detectadas.

Un elemento frecuentemente subestimado pero crítico es el registro y monitoreo de actividades, que permite a los administradores del sistema realizar auditorías, identificar patrones inusuales de comportamiento y tomar decisiones informadas en caso de incidentes de seguridad. Los sistemas de registro recogen información sobre accesos, cambios en archivos críticos, intentos fallidos de autenticación y otra clase de eventos que pueden indicar una posible intrusión o mal uso del sistema.

Por último, pero menos importante, la seguridad en el sistema operativo no es una función aislada ni una tarea que se realiza una sola vez, sino un proceso continuo que involucra tanto a los desarrolladores del sistema como a los administradores y usuarios finales. La concientización, la capacitación en buenas prácticas y la implementación de políticas estrictas de uso también forman parte integral de una estrategia efectiva de protección, no tiene un caso útil hacer el sistema más seguro si el mayor problema de seguridad se encuentra entre la computadora y la silla, y así es, me refiero al usuario.

El sistema operativo, como núcleo de cualquier infraestructura computacional, debe estar diseñado y configurado con un enfoque claro en la seguridad. Desde el control de acceso hasta la actualización de vulnerabilidades, pasando por la autenticación robusta, la defensa contra malware y el monitoreo constante, todos estos elementos conforman un entramado complejo pero necesario para garantizar que los datos y recursos permanezcan protegidos frente a un entorno cada vez más amenazante. La seguridad y la protección en el sistema operativo, por tanto, no son opcionales ni accesorios, sino una exigencia crítica en la era digital contemporánea.

Seguridad en la red.

Por otro lado, la seguridad y protección en la red es un aspecto absolutamente esencial en el mundo digital actual, especialmente considerando el crecimiento exponencial de las interconexiones, la computación en la nube, los servicios web y el uso intensivo de dispositivos inteligentes. En este contexto interconectado, donde la información fluye de un punto a otro a velocidades aceleradas, las amenazas también se han vuelto más sofisticadas

y constantes, lo que hace imprescindible establecer medidas de seguridad robustas que protejan los datos en tránsito, los dispositivos conectados y la infraestructura de red en su conjunto. A grandes rasgos, la seguridad en la red tiene como objetivo principal garantizar la confidencialidad, la integridad y la disponibilidad de la información, además de asegurar la autenticación y el no repudio de las comunicaciones entre los distintos actores que participan en una red.

Para comenzar a comprender la complejidad y profundidad de la seguridad en redes, primero hay que entender los múltiples vectores de ataque que pueden existir. Entre los más comunes se encuentran los ataques de denegación de servicio, los cuales se basan en interrumpir el servicio sobresaturando el origen principal (Cloudflare, s.f.) , la interceptación de paquetes o sniffing, el spoofing de direcciones IP y MAC, la suplantación de identidades, las inyecciones de código en protocolos de comunicación, y los accesos no autorizados por medio de vulnerabilidades en los dispositivos de red, como routers, switches, firewalls, y servidores. Estos ataques pueden tener consecuencias devastadoras, desde la interrupción del servicio hasta la pérdida o robo de información sensible, pasando por el control remoto de dispositivos y el sabotaje de operaciones empresariales o gubernamentales.

Uno de los pilares fundamentales de la protección en redes es el uso de firewalls, dispositivos o software que actúan como una barrera entre una red interna confiable y una externa potencialmente peligrosa, como Internet. Los firewalls pueden configurarse con reglas específicas para permitir o denegar el tráfico en función de direcciones IP, puertos, protocolos o contenido de los paquetes, lo que permite establecer políticas de seguridad estrictas y adaptadas a las necesidades del entorno. Existen firewalls perimetrales, que protegen toda la red, y firewalls de host, que protegen individualmente a cada dispositivo.

Además, otro elemento crucial son los sistemas de detección y prevención de intrusiones, los cuales monitorizan de manera constante el tráfico de red para identificar patrones sospechosos o conocidos como maliciosos, y en el caso de los IPS, tomar medidas automáticamente para mitigar el impacto del ataque, como cortar conexiones o bloquear direcciones. Estos sistemas funcionan basándose en firmas de ataques conocidos o mediante el análisis del comportamiento del tráfico, lo que permite detectar amenazas tanto conocidas como emergentes.

La encriptación es igualmente vital en la protección de las redes, ya que asegura que los datos transmitidos no puedan ser leídos por terceros en caso de ser interceptados. Protocolos como SSL/TLS (usados comúnmente en HTTPS), IPsec (para conexiones a nivel de red), y VPN (redes privadas virtuales) emplean algoritmos criptográficos para cifrar la información y garantizar su integridad. Así, aunque un atacante logre capturar los paquetes transmitidos, no podrá descifrar su contenido sin las claves adecuadas. Esta

práctica es indispensable en entornos corporativos, gubernamentales y personales donde se maneje información confidencial.

La autenticación y el control de acceso también juegan un rol protagónico. Mediante mecanismos como RADIUS, LDAP o Kerberos, los administradores pueden verificar la identidad de los usuarios y determinar qué recursos pueden o no utilizar dentro de la red. Además, el uso de redes segmentadas mediante VLANs y la implementación de listas de control de acceso permiten limitar el alcance de los usuarios, restringiendo su capacidad de moverse libremente por toda la red, lo cual es esencial para minimizar el impacto de posibles intrusiones.

En el contexto actual, donde el uso del Internet de las Cosas y dispositivos móviles se ha masificado, la superficie de ataque se ha incrementado significativamente, ya que cada nuevo dispositivo conectado a una red representa un punto potencial de vulnerabilidad. Por ello, la seguridad debe extenderse a cada nodo, asegurando no solo los servidores y computadoras tradicionales, sino también sensores, cámaras, asistentes virtuales, impresoras y cualquier otro dispositivo que pueda conectarse a la red. Aquí se vuelve indispensable aplicar políticas de seguridad de red basadas en Zero Trust, donde no se confía automáticamente en ningún dispositivo ni usuario, independientemente de su ubicación dentro o fuera del perímetro de la red.

Snowden.

La epica historia del hombre que en 2013 puso en jaque a los EE.UU. Cuando Edware J. Snowden desvelo los documentos del programa de vigilancia secreto de la NSA, abrió los ojos del mundo y cerro las puertas de su propio futuro. Se vio obligado a renunciar a su carrera, a su novia de toda la vida y a su patria. (Filmaffimity, s.f.) x

Resumen.

Snowden narra la historia del exanalista de la Agencia de Seguridad Nacional (NSA), quien filtró a la prensa una serie de documentos clasificados que revelaban cómo el gobierno de los Estados Unidos espiaba masivamente a ciudadanos, tanto dentro como fuera del país, mediante el acceso indiscriminado a correos electrónicos, llamadas telefónicas, mensajes de texto e incluso cámaras de dispositivos móviles. Este suceso marcó un punto de inflexión global en la percepción de la privacidad digital y la seguridad informática, exponiendo al mundo los límites difusos entre proteger una nación y violar los derechos fundamentales de las personas.

Lo interesante de esta película es que no se limita únicamente a mostrar los aspectos técnicos de la ciberseguridad, como el uso de firewalls, sistemas operativos encriptados, redes privadas y técnicas de evasión de rastreo, sino que profundiza en las implicaciones humanas, éticas y legales del uso (y abuso) del poder tecnológico. A lo largo de la trama, el espectador se sumerge en un entorno donde los equipos de cómputo se convierten en herramientas tanto de protección como de vigilancia, y donde los expertos en seguridad informática no solo luchan contra hackers externos, sino también contra decisiones políticas y estructuras burocráticas que manipulan la tecnología con fines oscuros.

Además, Snowden pone en evidencia cómo incluso los sistemas más sofisticados pueden ser vulnerables si quienes los operan pierden de vista los principios éticos. La película resalta cómo el conocimiento técnico, en manos de individuos sin un fuerte sentido de responsabilidad, puede utilizarse tanto para proteger como para oprimir. Esto nos recuerda que la seguridad no es solo una cuestión de software o hardware, sino también de personas, valores y decisiones.

Conclusiones.

La seguridad es el pilar de todas las tecnologías que nos rodean, nos permite sentirnos seguros en lugar donde todas las personas buscan alguna manera de obtener mas que el otro, pero la seguridad no solo depende de las empresas productoras de estos aparatos, si no que es conjunto de reglas que tanto como empresas como usuarios debemos seguir, además, al tener acceso a los datos sensibles, las empresas deben expresar y asegurarse que estos datos esten seguros en donde sea que ellos los almacenen.

Bibliografía

Cloudflare. (s.f.). *What's a DDoS?* Obtenido de Cloudflare: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

ARIELMCORG. (6 de julio de 2024). *¿Que es la esteganografia?* . Obtenido de Infosertec: https://infosertecla.com/2024/07/06/ciberseguridad-que-es-la-esteganografia-como-funciona/

Filmaffimity. (s.f.). *Snowden*. Obtenido de Filmaffimity: https://www.filmaffinity.com/mx/film892502.html

Sanchez, L. (2024 de febrero de 27). *Criptografia: que es, cuales son sus usos y por qué es tan importante.* . Obtenido de DeltaProtet: https://www.deltaprotect.com/blog/criptografia-definicion-usos-e-importancia

TecnoDigital. (24 de marzo de 2025). *¿Que es la criptografia?* . Obtenido de TecnoDigital: https://informatecdigital.com/que-es-criptografia/

Wikipedia Authors. (2025 de febrero de 28). *Estenografia - Wikipedia*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Esteganografía