

Tecnológico Nacional de México

Instituto Tecnológico de Reynosa



Equipo conformado por:

Bermudez Dominguez Juan Carlos 19580585  
Castillo Jr Gregorio 19580589

Flores Acosta Sheila Lizeth 19580595

Morales Calixto Daniel Alexander 19580867

Gongora Raga Perla Elizabeth 19580603

Perez Romero Julio Alberto 19580633

Introducción a la administración de redes

# Índice

[Índice 1](#_Toc126593212)

[1.1 Definición de administración de redes 2](#_Toc126593213)

[1.2 Administración de redes por norma ISO 4](#_Toc126593214)

[1.3 Criptografía 7](#_Toc126593215)

[1.3.1 Criptografía simétrica 11](#_Toc126593216)

[1.3.2 Criptografía asimétrica 15](#_Toc126593217)

[1.3.3 Técnicas de HASH 17](#_Toc126593218)

[1.4 Rendimiento 19](#_Toc126593219)

[1.4.1 Análisis de fallas 22](#_Toc126593220)

[1.4.2 Análisis de contabilidad 24](#_Toc126593221)

[1.4.3 Análisis de seguridad 26](#_Toc126593222)

[Bibliografía 30](#_Toc126593223)

# Definición de administración de redes

**¿Qué es la administración de redes?**

La administración de redes suministra información a las organizaciones relacionada con rutas de recursos, redundancias inaceptables y recursos poco utilizados. La administración de redes correcta depende de la fiabilidad de la información de ruta.

También se puede definir como el proceso de administración de una red de los fallos y el rendimiento utilizando diversas herramientas y tecnologías para mantenerse al día con los requisitos empresariales. El objetivo de la administración de red es lograr una red libre de errores. En el entorno actual, se emplean múltiples herramientas de administración de red que hacen que todo el proceso sea complejo.

**Hay cuatro aspectos críticos de un software de administración de red:**

* [Identificación de fallos](https://www.manageengine.com/es/network-monitoring/network-management.html#fault-identification): El mayor desafío con las soluciones de administración de redes actuales es identificar fallos de manera proactiva antes de que afecte a los usuarios finales.
* [Administración del rendimiento](https://www.manageengine.com/es/network-monitoring/network-management.html#performance-management): La administración del rendimiento implica la resolución de fallos, ya sea a través de un enfoque manual o automatizado, de modo que el rendimiento de la red se restablezca a su estado original o mejorado.
* [Aprovisionamiento de red](https://www.manageengine.com/es/network-monitoring/network-management.html#network-provisioning): El aprovisionamiento de la red implica calcular la carga manejada por la red y las demandas futuras en función de la tendencia actual de la red. También implica mantener los recursos en reserva para que cuando surja una necesidad, sea más fácil de manejar.
* [Mantenimiento de QoS](https://www.manageengine.com/es/network-monitoring/network-management.html#maintaining-qos): Es común que el rendimiento de la red se degrade a medida que pasan los años. Por lo tanto, es esencial brindar servicios de TI de calidad a los usuarios finales que cumplen el SLA mes a mes.

**Objetivos de la administración de redes**

* Proporcionar herramientas automatizadas y manuales de administración de red para controlar posibles fallas o degradaciones en el desempeño de esta.
* Disponer de estrategias de administración para optimizar la infraestructura existente, optimizar el rendimiento de aplicaciones y servicios. Además, prever los crecimientos en la red esperados debido al cambio constante en la tecnología.

**¿Qué hace un administrador de red?**

El administrador de redes, en muchas de las empresas que hoy en día disponen de varios ordenadores o diverso software, realiza una función muy importante de gestión y coordinación de los distintos sistemas que interactúan en ellas y las redes que los unen. Este es el responsable de mantener la red informática actualizada y en continuo funcionamiento sin que existan problemas y, en caso de que los haya, poder solucionarlos de la forma más rápida y eficaz posible.

**Responsabilidades de un administrador de redes**

* **Instalar y mantener redes LAN, WAN, segmentos de red** y operaciones tanto de Internet como de Intranet.
* **Instalar y mantener varias aplicaciones**, incluyendo hardware y software.
* **Supervisar la efectividad de la red** y mantener medidas de seguridad eficaces.
* **Modificar el rendimiento de los sistemas de red** cuando sea necesario.
* **Supervisar las posibles actualizaciones, migraciones y reparaciones** para mejorar el funcionamiento del sistema.

**Trabajar con una serie de dispositivos**, como servidores, equipos de sobremesa y portátiles, enrutadores, impresoras, teléfonos móviles y tablets.

# 1.2 Administración de redes por norma ISO

**ISO 27001**

A medida que más personas y empresas se encuentran interconectadas entre sí, más información se intercambia, desde la que consideran trivial y desechable, hasta la que es mucho más sensible y necesaria para la vida de las personas y la supervivencia del negocio. La protección de esta información es gracias a la norma [ISO 27001](http://www.isotools.pe/normas/ntp-iso-27001).

Es por eso que la infraestructura de red de hoy en día es tan importante, y tan atractiva para los piratas informáticos. Por lo tanto, para asegurarnos del rendimiento de la red y evitar que se generen situaciones en las que la información que lleva se vea comprometida, es necesario tomar medidas de seguridad.

**¿Qué es la gestión de seguridad de la red?**

Se puede definir la gestión de la seguridad de red siendo un proceso diseñado para proteger una red y los datos que fluyen mediante los riesgos en cuanto al acceso no autorizado, mal utilización, mal funcionamiento, modificación, destrucción o divulgación indebida, al tiempo que permite que se establezcan ordenadores autorizados, usuarios y aplicaciones para llevar a cabo las actividades. Si empresa puede contar con una red interna y externa.

Mediante los administrativos, físicos y controles tecnológicos, la gestión de la seguridad de la red busca generar un entorno seguro basado en capas de componentes protectores que apoyan y se complementan entre sí para incrementar la seguridad en general.

**Gestión de red de acuerdo con la norma ISO 27001**

Al igual que cualquier sistema de gestión, la norma ISO 27001 se basa en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar), que se integra de forma perfecta con el enfoque de gestión de seguridad de la red.

En cuanto a las actividades de planificación de gestión de red, es necesario definir los objetivos de seguridad de la red para que sea protegida y administrada. Una vez que se definen los objetivos de seguridad de la red, es necesario definir todos los controles que se deben realizar, sobre la base de los riesgos más relevantes que existen en el contexto de la organización.

La aplicación de los controles de seguridad se puede utilizar dentro del plan de tratamiento del riesgo definido para la aplicación de todos los controles del Sistema de Gestión de Seguridad de la Información. De acuerdo a la norma ISO 27002, los controles de gestión de la seguridad de red deben ser considerados como:

* Controles de red: un conjunto de controles generales deben aplicarse, como la definición de las responsabilidades y procedimientos para la gestión de equipos de red, la separación de funciones entre las redes y los ordenadores, la utilización de las soluciones de cifrado para proteger los datos en tránsito e interconectado sistemas, supervisando y registrando las actividades de la red que se llevan a cabo, la autenticación y otros medios para que se restrinja el acceso y la utilización de los recursos de la red.
* Seguridad de los servicios de red: las soluciones de red que se esperan, y los niveles de rendimiento y seguridad deben ser definidos e incluso en los acuerdos de nivel de servicio, así como el medio por el cual la empresa puede verificar si se está cumpliendo con todos los niveles de servicio. Estos acuerdos de servicio deben ser considerados de forma interna y externa.
* La segregación de las redes: los servicios, los sistemas de información, los usuarios, las estaciones de trabajo y los servidores deben encontrase por separado en distintas redes, según los criterios que han sido definidos como la exposición al riesgo y el valor de negocio, y un estricto control de flujo de datos entre estas redes debe estar establecida.

**Los beneficios de la seguridad de la red**

Existen muchos beneficios de una empresa puede lograr mediante la adopción de la gestión de seguridad de la red:

* Aumentar la productividad, como resultado de una red mucho más fiable y menos interrupciones en el negocio.
* Mantenimiento del cumplimento de la normativa, ya que la seguridad de la red es un punto común en muchas regulaciones.
* Reducir el riesgo de las acciones legales, ya que los esfuerzos que se realizan para proteger los datos de los clientes muestran la debida diligencia de la empresa y el debido cuidado.
* Incremento de la reputación de la organización, debido a los esfuerzos realizados para proteger los datos de los clientes muestran el compromiso de la empresa para controlar la seguridad.

# 1.3 Criptografía

La criptografía es una práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas. La información puede estar en reposo (como un archivo ubicado en un disco duro), en tránsito (una comunicación electrónica intercambiada entre dos o más partes) o en uso (mientras se ejecutan operaciones de computación con los datos). La criptografía tiene cuatro objetivos principales:

* Confidencialidad: poner la información únicamente a disposición de usuarios autorizados.
* Integridad: asegurar que la información no se ha manipulado.
* Autenticación: confirmar la autenticidad de la información o de la identidad de un usuario.
* No repudio: evitar que un usuario deniegue compromisos o acciones previas.

La criptografía utiliza varios algoritmos criptográficos de bajo nivel para lograr uno o más de dichos objetivos de seguridad de la información. Estas herramientas incluyen algoritmos de cifrado, algoritmos de firma digital, algoritmos de hash y otras funciones.

**¿Para qué se utiliza la criptografía?**

La criptografía tiene sus raíces en el envío de información sensible entre militares y políticos. Los mensajes podían encriptarse para que parecieran texto aleatorio a cualquiera que no fuera el destinatario.

Hoy en día, las técnicas originales de encriptación no funcionan. Tanto es así que solo se encuentran en las secciones de enigmas de algunos periódicos. Afortunadamente, el campo ha hecho grandes avances en materia de seguridad, y los algoritmos que se utilizan hoy en día se basan en un análisis riguroso y en las matemáticas para su seguridad.

A medida que la seguridad avanza, el campo de la criptografía se amplía para incluir una gama más amplia de objetivos de seguridad. Entre ellos se encuentran la autenticación de mensajes, integridad de los datos, cálculo seguro, etc.

La criptografía está en la base de la sociedad moderna. Es la base de innumerables aplicaciones de Internet a través del protocolo seguro de transferencia de hipertexto (HTTPS), de la comunicación segura de texto y voz, e incluso de las monedas digitales.

**¿Qué es el cifrado?**

Un algoritmo de cifrado es un procedimiento que convierte un mensaje de texto plano en un texto cifrado. Los algoritmos modernos utilizan matemáticas avanzadas y una o varias claves de cifrado. Esto hace que sea relativamente fácil cifrar un mensaje, pero prácticamente imposible descifrarlo sin conocer las claves.

Las técnicas de cifrado se dividen en dos categorías, simétricas y asimétricas, según el funcionamiento de sus claves.

**Técnicas de criptografía**

La criptografía está estrechamente relacionada con las disciplinas de la criptología y el criptoanálisis. Incluye técnicas como micro puntos, fusión de palabras con imágenes y otras formas de ocultar información almacenada o en tránsito.

Sin embargo, en el mundo actual centrado en la informática, la criptografía se asocia con mayor frecuencia con la codificación de texto sin formato (texto ordinario, a veces denominado texto sin cifrar) en texto cifrado (un proceso llamado cifrado) y nuevo (conocido como descifrado). Las personas que practican este campo se conocen como criptógrafos.

La criptografía moderna se preocupa por los siguientes cuatro objetivos:

Confidencialidad: la información no puede ser entendida por nadie para quien no fue intencionada

Integridad: la información no se puede alterar en el almacenamiento o tránsito entre el remitente y el destinatario previsto sin que se detecte la alteración

Sin rechazo: el creador / remitente de la información no puede negar en una etapa posterior sus intenciones en la creación o transmisión de la información.

Autenticación: el remitente y el receptor pueden confirmar la identidad del otro y el origen / destino de la información

Los procedimientos y protocolos que cumplen con algunos o todos los criterios anteriores se conocen como criptosistemas. A menudo se piensa que los criptosistemas se refieren únicamente a procedimientos matemáticos y programas informáticos. Sin embargo, también incluyen la regulación del comportamiento humano, como elegir contraseñas difíciles de adivinar, cerrar la sesión de sistemas no utilizados y no discutir procedimientos sensibles con personas externas.

**Funciones de la criptografía**

¿Qué problemas resuelve la criptografía? Un sistema seguro debe proporcionar varias garantías, como confidencialidad, integridad y disponibilidad de los datos o autenticidad. Cuando se usa correctamente, la criptografía ayuda a proporcionar estas garantías.

La criptografía puede garantizar la confidencialidad e integridad tanto de los datos en tránsito como de los datos en reposo. También puede autenticar a remitentes y destinatarios entre sí y proteger contra el repudio.

Los sistemas de software suelen tener varios puntos finales, normalmente varios clientes y uno o más servidores de servicios de fondo. Estas comunicaciones cliente / servidor tienen lugar a través de redes en las que no se puede confiar. La comunicación se produce a través de redes públicas abiertas como Internet o redes privadas que pueden verse comprometidas por atacantes externos o personas internas malintencionadas.

Puede proteger las comunicaciones que atraviesan redes que no son de confianza, hay dos tipos principales de ataques que un adversario puede intentar llevar a cabo en una red.

**Tipos de ataques**

Ataques pasivos

Involucran a un atacante que simplemente escucha en un segmento de la red e intenta leer información confidencial mientras viaja. Pueden ser online (en los que un atacante lee el tráfico en tiempo real) u offline (en los que un atacante simplemente captura el tráfico en tiempo real y lo ve más tarde, tal vez después de pasar algún tiempo descifrándolo).

Ataques activos

Involucran a un atacante que se hace pasar por un cliente o servidor, intercepta las comunicaciones en tránsito y ve y / o modifica los contenidos antes de pasarlos a su destino previsto (o dejarlos por completo).

Las protecciones de confidencialidad e integridad que ofrecen los protocolos criptográficos como SSL / TLS pueden proteger las comunicaciones de escuchas y manipulaciones maliciosas. Las protecciones de autenticidad brindan garantía de que los usuarios se están comunicando realmente con los sistemas según lo previsto. Por ejemplo, ¿envías tu contraseña de banca online a tu banco o a otra persona?

También se puede utilizar para proteger los datos en reposo. Los datos de un disco extraíble o de una base de datos se pueden cifrar para evitar la divulgación de datos confidenciales en caso de pérdida o robo.

Además, también puede proporcionar protección de la integridad de los datos en reposo para detectar manipulaciones maliciosas.

**Tipos de criptografías**

Criptografía de clave simétrica

Tanto el remitente como el receptor comparten una única clave. El remitente utiliza esta clave para cifrar texto sin formato y enviar el texto cifrado al receptor. Por otro lado, el receptor aplica la misma clave para descifrar el mensaje y recuperar el texto sin formato.

Criptografía de clave pública

Este es el concepto más revolucionario de los últimos 300-400 años. En criptografía de clave pública se utilizan dos claves relacionadas (clave pública y privada). La clave pública se puede distribuir libremente, mientras que su clave privada emparejada permanece en secreto. La clave pública se utiliza para el cifrado y para el descifrado se utiliza la clave privada.

Funciones hash

No se utiliza ninguna clave en este algoritmo. Se calcula un valor hash de longitud fija según el texto sin formato que hace que sea imposible recuperar el contenido del texto sin formato. Muchos sistemas operativos también utilizan las funciones hash para cifrar contraseñas.

## 1.3.1 Criptografía simétrica

Entre los primeros métodos empleados para el cifrado de información está la criptografía simétrica. También conocida como [criptografía](https://academy.bit2me.com/que-es-criptografia/) de clave secreta o criptografía de una clave. Su nombre se debe a que este método emplea la misma clave tanto para el cifrado como el descifrado de un mensaje. Por lo que el emisor y el receptor deben estar previamente de acuerdo y en conocimiento de la clave a utilizar.

En la criptografía simétrica, toda la seguridad está centrada en la clave. Por lo que debe ser secreta y que no sea fácil de adivinar por una tercera persona. Sin embargo, con la tecnología que disponemos hoy en día, el proceso de comunicación o distribución de la clave se volvió el punto débil de este método. Ya que al comunicarse (el emisor y el receptor) para definir y acordar la clave, un tercero puede interceptar dicha comunicación, hacerse con la clave y acceder a la información contenida en el mensaje.

**¿Quién la desarrollo?**

La criptografía se desarrolló hace muchísimos años. Se estima que desde los tiempos del Antiguo Egipto y el Imperio Romano se empleaba la criptografía simétrica de manera muy básica. Sin embargo, esta se desarrolló y fue ampliamente utilizada durante la Segunda Guerra Mundial. Fue durante este conflicto bélico, que los ejércitos emplearon y desarrollaron poderosos sistemas criptográfico simétricos. Todo con el fin de codificar los mensajes y protegerlos de los enemigos.

Luego de estos sucesos, la era de la criptografía simétrica moderna sufrió toda una revolución hasta llegar a lo que conocemos hoy en día. Todo gracias al trabajo de investigadores y científicos dedicados a este campo. Sin embargo, un nombre destaca sobre todos los demás, el de [Claude Shannon](https://es.wikipedia.org/wiki/Claude_Elwood_Shannon). Shannon es conocido como el padre de la criptografía matemática.

Los trabajos de Shannon se desarrollaron a partir de 1949, cuando publicó un artículo llamado [Communication Theory of Secrecy Systems](https://www.cs.virginia.edu/~evans/greatworks/shannon1949.pdf" \t "_blank). En este artículo se describe la modernización de las técnicas de encriptado conocidas hasta ese entonces, con procesos matemáticos avanzados que le brindaban un mayor nivel de complejidad y seguridad. Más tarde escribió un libro con el informatólogo, [Warren Weaver](https://es.wikipedia.org/wiki/Warren_Weaver). Todo este conjunto de trabajos realizados, se convirtieron en las bases de la criptografía simétrica moderna.

**Métodos: Algoritmos de cifrado simétrico**

Desde el nacimiento de los ordenadores, la criptografía sufrió grandes cambios. En los que pasó de realizarse de forma clásica y manual, para integrar complejos problemas matemáticos. Hoy en día existen muchos algoritmos de cifrado que son empleados en los correos, en las bases de datos e incluso en los discos duros. Veamos algunos de los más conocidos y ampliamente utilizados.

**Data Encryption Standard (DES)**

Fue el primer método de cifrado informático desarrollado por la compañía IBM en 1975. Este algoritmo trabaja en bloques y emplea una clave simétrica de 64 bits de longitud que es sometida a 16 interacciones. De los 64 bits, 56 bits son utilizados para el encriptado. Y los 8 bits restantes son usados para paridad y para la detección de errores, y luego son descartados. Por lo que la longitud real de la clave es de 56 bits.

Para realizar el encriptado, este algoritmo aplica una serie de permutaciones y sustituciones. Con lo que modifica inicialmente la secuencia de los bits y escribe el resultado en bloques diferentes de un tamaño determinado. Que luego son cifrados de forma independiente. El proceso consta de 16 rondas de cifrado y una vez realizadas, se agrupan los resultados en un bloque de tamaño de 64 bits que también es sometido a otra permutación. El texto final que resulta de todo este proceso es el mensaje cifrado.

DES posee 4 modos de operación: el Electronic Codebook Mode (ECB) que se emplea para mensajes cortos de longitud menor a 64 bits. El Cipher Block Chaining Mode (CBC) empleado para mensajes largos. El Cipher Block Feedback (CFB) utilizado para cifrar bit por bit, o byte por byte. Y por último el Output Feedback Mode (OFB) que tiene el mismo uso, pero además evita la propagación de errores.

Sin embargo, aunque este algoritmo al momento de su creación fue un gran avance y sentó las bases para la criptografía moderna que conocemos actualmente. Hoy en día ya no es utilizado debido a que su clave es demasiado corta y ya no es segura a los ataques de fuerza bruta. Como se demostró en 1999 cuando fue roto.

**Triple Data Encryption Standard (3DES)**

El algoritmo 3DES es el mismo que el algoritmo DES, sólo que como su nombre indica, se aplica 3 veces. Dependiendo de las claves que se utilicen, se puede generar un sistema más robusto. Por ejemplo, si se emplean 3 claves se puede generar una de 168 bits; si se emplean sólo 2 claves se puede generar una de 112 bits.

**Advanced Encryption Standard (AES)**

Este nuevo algoritmo fue el sustituto de DES y es el empleado actualmente debido a que su método de cifrado se adapta mejor a las necesidades del siglo XXI. El cifrado de AES puede ser empleado tanto en software como en hardware y el tamaño fijo del bloque es de 128 bits. Mientras que las claves pueden ser elegida a voluntad entre 128, 192 y 256 bits. Siendo la longitud de 128 bits un estándar. E igual que su antecesor, aplica el cifrado por bloques.

El resultado de cifrar con este método genera una matriz de 4 filas por 4 columnas. A la que luego se le aplica una serie de rondas de cifrado que están basadas en operaciones matemáticas según la longitud de sus claves. Para una clave de 128 bits se aplican 10 rondas de cifrado, para una clave de 192 bits se aplican 12 rondas, y para una clave de 256 bits son necesarias 14 rondas.

Y aunque es un algoritmo ampliamente usado en la actualidad, muchos criptógrafos comienzan a dudar de su seguridad. Ya que se han registrado la posibilidad de ataques en un número de rondas de cifrado muy cercanas al número de rondas necesarias para el cifrado.

**¿Qué tan segura es la criptografía simétrica?**

En términos de seguridad, el cifrado simétrico no es tan confiable por el hecho de que se debe compartir la clave privada para descifrarlo. En este tipo de cifrado, toda la seguridad está reflejada en la clave. Por lo que compartirla representa una gran vulnerabilidad si no se emplean los sistemas de comunicación adecuados. Sin embargo, cuando se emplea este método se deben cumplir dos parámetros esenciales para que se considere seguro, los cuales son:

Después de encriptar una información, no se puede obtener la clave usada para el cifrado y descifrado. Ni la información contenida en el mensaje cifrado.

El costo de descifrar una información debe ser más alto que la misma información contenida en el mensaje cifrado.

**Ventajas y desventajas**

Este tipo de criptografía presenta varias ventajas. Por ejemplo, la rapidez, ya que requiere de menor poder computacional debido a la longitud de sus claves que es de 64 bits, mientras que en el algoritmo AES van desde 128 a 256 bits. Además, posee una infraestructura sencilla y sólo requiere de una clave, por lo que es muy fácil de emplear para el cifrado de archivos que contengan datos personales.

Por otro lado, el cifrado simétrico garantiza la privacidad y la integridad en las comunicaciones vía telefónica o por internet, como el caso del correo electrónico.

Sin embargo, su mayor desventaja está en el intercambio o distribución de la clave. Debido a que ésta debe distribuirse a todo aquel que necesite acceder a la información encriptada. Y en ese intercambio, un tercero puede interceptar la clave en un medio de comunicación no seguro y hacerse con la información contenida en el mensaje.

Igualmente, la criptografía simétrica es vulnerable a los ataques de fuerza bruta. En teoría, la ruptura de este cifrado es posible mediante el criptoanálisis lineal y el criptoanálisis diferencial, pero en la práctica estos ataques no han tenido éxito. Sin embargo, si es posible romperlo con un ataque de fuerza bruta que pruebe todas las combinaciones posibles hasta hallar la clave correcta.

Otra desventaja es que este tipo de cifrado no permite autenticar la identidad del emisor. Como sí ocurre en la [criptografía asimétrica](https://academy.bit2me.com/que-es-criptografia-asimetrica/), ya que el emisor firma digitalmente el mensaje.

## 1.3.2 Criptografía asimétrica

La Criptografía de clave pública o asimétrica, también denominada RSA por las siglas de los apellidos de sus inventores Rivest Shamir y Adelman, es por definición aquella que utiliza dos claves diferentes para cada usuario, una para cifrar que se llama clave pública y otra para descifrar que es la clave privada. El nacimiento de la Criptografía asimétrica ocurrió como resultado de la búsqueda de un modo más práctico de intercambiar las llaves simétricas

El esquema propuesto en RSA se explica así:

Mediante un programa de cómputo cualquier persona puede obtener un par de números, matemáticamente relacionados, a los que se denominan llaves. Una llave es un número de gran tamaño, que usted puede conceptualizar como un mensaje digital, como un archivo binario, o como una cadena de bits o bytes. Las llaves, públicas y privadas, tienen características matemáticas, su generación se produce siempre en parejas, y se relacionan de tal forma que, si dos llaves públicas son diferentes, entonces, las correspondientes llaves privadas son diferentes y viceversa. En otras palabras, si dos sujetos tienen llaves públicas diferentes, entonces sus llaves privadas son diferentes. La idea es que cada individuo genere un par de llaves: pública y privada. El individuo debe de mantener en secreto su llave privada, mientras que la llave pública la puede dar a conocer.

El procedimiento de firma de un documento digital, por ejemplo, implica que, mediante un programa de cómputo, un sujeto prepare un documento a firmar y su llave privada (que sólo él conoce). El programa produce como resultado un mensaje digital denominado firma digital. Juntos, el documento y la firma, constituyen el documento firmado.

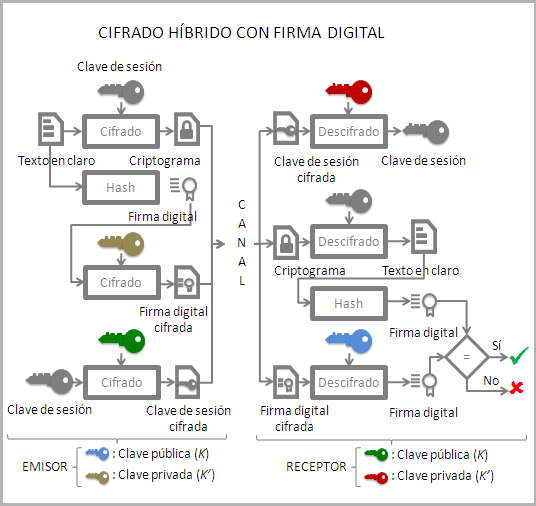
Es conveniente señalar que, a diferencia de la firma autógrafa, si dos documentos son diferentes entonces la firma digital también es diferente. En otras palabras, la firma digital cambia de documento a documento, si un sujeto firma dos documentos diferentes producirá dos documentos firmados diferentes. Si dos sujetos firman un mismo documento, también se producen dos documentos firmados diferentes.

El proceso de autentificación se efectúa de la siguiente forma:

Dos puntos I y II mantienen comunicación, conociendo I la llave pública de II. Desde el punto II, se envía un documento firmado digitalmente y un criptograma asociado que sólo es posible hacerse utilizando su clave privada. Entonces I, utilizando la llave pública de II genera un criptograma reflejo, compara ambos criptogramas y, si son iguales, el documento es auténtico.  
Si alguna parte del documento o parte de la firma se modifica, aunque sea ligeramente, entonces, el procedimiento de autentificación indicará que el documento no es auténtico. Si una llave pública autentifica un documento firmado, entonces el documento fue firmado con la correspondiente llave privada, es decir, si un individuo tiene asociada la llave pública que autentifica el documento, entonces, el documento fue efectivamente firmado por ese individuo.

A diferencia de la firma autógrafa, que es biométrica, y efectivamente prueba el acto personal de firma, la firma digital sólo prueba que se utilizó la llave privada del sujeto y no necesariamente el acto personal de firma. En consecuencia, no es posible establecer con total seguridad que el individuo firmó un documento, sino que sólo es posible demostrar que es el individuo es el responsable de que el documento se firmara con su llave privada. En otras palabras, si un documento firmado corresponde con la llave pública de un sujeto, entonces el sujeto, aunque no lo haya hecho, debe de reconocer el documento como auténtico.

Por lo tanto, el sujeto debe cuidar de mantener su llave privada en total secreto y no revelársela a nadie, porque de hacerlo es responsable de su mal uso.



## 1.3.3 Técnicas de HASH

Las técnicas hash se establecen como métodos que mediante una ecuación fueron creados para generar posiciones en una tabla (arreglo) que será la que contendrá datos. Surge, por tanto, la necesidad de comprender las diferentes funciones como: SHA-1, SHA-3, SHA-256

Dentro del mundo de las estructuras de datos existe un sinfín de temas que conllevan diferentes métodos, funciones y aplicaciones para explotar en el contexto de programación; con el objetivo de innovar con soluciones que den soluciones a actividades de la cotidianidad

Al hablar de hashing estamos refiriéndonos a una tabla que almacena tanto registros como objetos, para después realizar una búsqueda de la cual su prioridad es tener un constante tiempo de recuperación en base a 0 y 1 sin tomar en cuenta qué cantidad de elementos puedan están dentro de una table

La manera correcta para poder lograr ese objetivo es crear una tabla de gran medida para abarcar cada elemento que se pueda almacenar y luego guardar cada objeto dentro de una posición con el valor clave del objeto.

Las técnicas hashing o tablas de dispersión se han creado para crear mediante una ecuación y una clave de entrada, como parte fundamental, un dato que será una posición en un arreglo

La función hash cumple con una operación fundamental y es que, si queremos buscar el objeto que guardamos en “x posición”, mediante la clave y la ecuación, podremos obtener el archivo guardado, sin importar si los elementos en arreglo están ordenados o no, y sin importar cuál sea el tamaño del arreglo, ya que las técnicas hashing son unos de los métodos de búsqueda más rápido, lo cual es una gran ventaja. Es posible que ocurra que a la hora de generar una posición en el arreglo o a la hora de buscar un elemento, la posición generada ya existe o nos devuelva un dato no deseado, en caso de la búsqueda, esto se conoce como colisiones. Importante conocer que dada dos claves diferentes k1 y k2 nos deberían dar resultados diferentes.

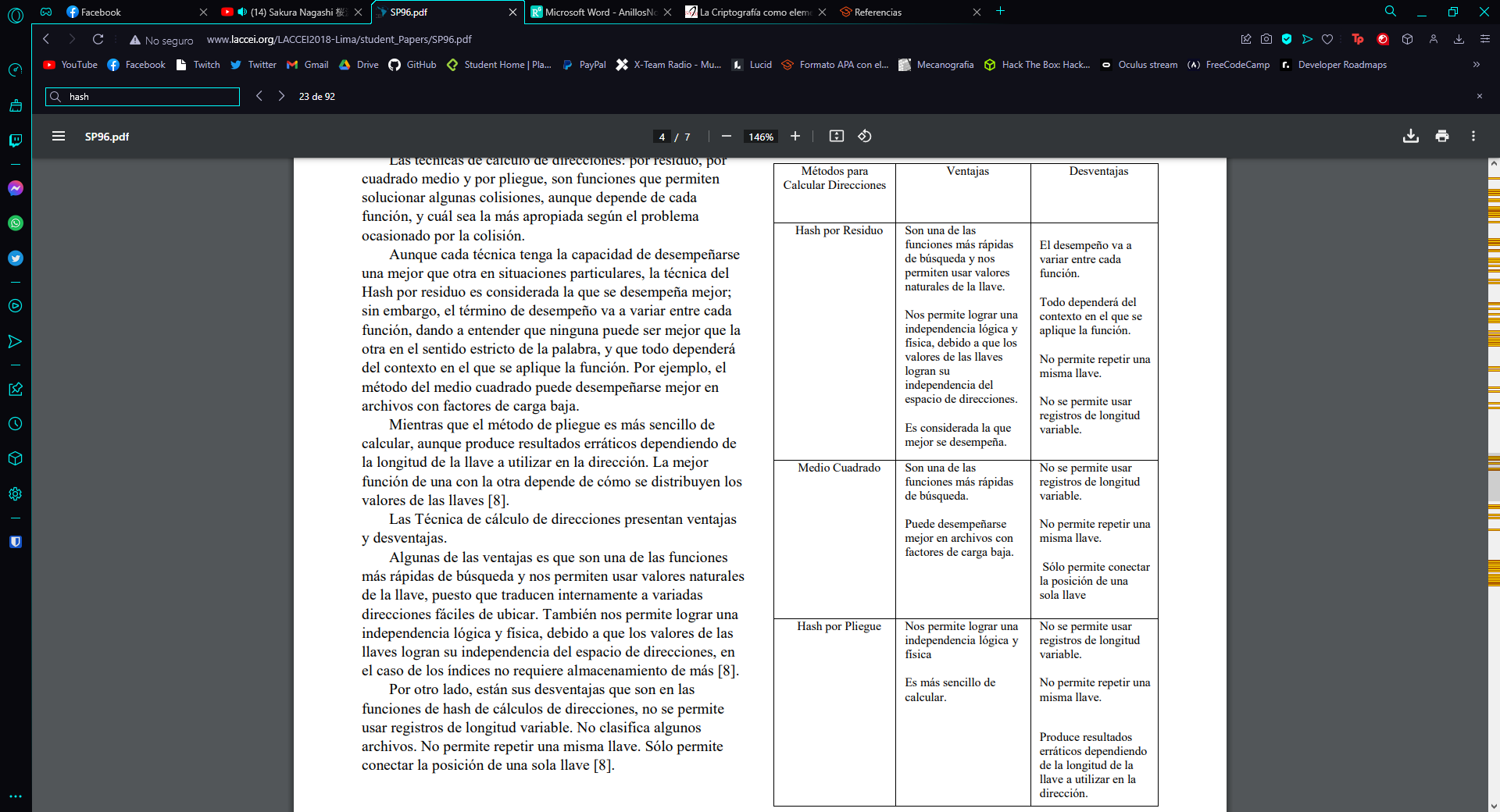
UTILIZACIÓN DEL HASH

Las diferentes funciones Hash que existen son utilizadas más que nada para resguardar la integridad de los archivos de grandes empresas, para certificación que las páginas web, proteger los derechos de autor de libros, películas, y otros contenidos que se encuentran en internet. Un ejemplo claro del uso de Hash es en las contraseñas, ciertos servicios en línea generan una función hash cuando el usuarios crean sus contraseñas, estos servicios en línea no guardan en texto plano las contraseñas de sus usuarios ya que esto significaría un problema grande en caso de que sufran de algún ataque a sus Base de Datos, generando una función Hash de la contraseña de los usuarios será más difícil de descifrar cuál será la contraseña en texto plano brindando mayor seguridad a los usuarios resguardando su información.

De acuerdo a lo analizado, las empresas que quieran mantener su información a salvo tendrán que cambiarse a las mejoras del SHA-1 que son: SHA-3 Y SHA-256.

SHA-3, SECURE HASH ALGORITM, fue creado a partir del SHA-2 como una actualización para solventar errores que se encontraban dentro de ese método. Debido a que los navegadores como Google Chrome, Internet Explorer entre otros utilizan el método SHA-1 tiene una baja seguridad que estos diseñadores demoraron solo 10 días en descubrir, Google informó que su navegador cambiaría a SHA3 durante el año 2017 y de igual manera lo realizan otras empresas como Microsoft

SHA 256, son nuevas funciones hash que utilizan palabras de 32 bits a 64 bits, la función SHA 256 pertenece a la familia del SHA-2. Esta función participa para la autenticación de software, y para la firma de mensajes



# 1.4 Rendimiento

¿Qué es el rendimiento en redes?

El rendimiento de la red es el análisis y la revisión de las estadísticas de la red colectiva, para definir la calidad de los servicios ofrecidos por la red informática subyacente.

Un proceso cualitativo y cuantitativo que mide y define el nivel de rendimiento de una red determinada. Guía a un administrador de red en la revisión, medición y mejora de los servicios de red.

Esto se logra a través de la monitorización continua y la optimización de los componentes de la red, incluyendo hardware, software y protocolos de comunicación. Algunos de los factores clave que afectan el rendimiento en la administración de redes incluyen la congestión del tráfico, la configuración inadecuada de los dispositivos, los ataques de seguridad y la obsolescencia de los equipos. Es importante tener en cuenta que el rendimiento en la administración de redes puede ser un desafío constante, ya que las redes evolucionan y crecen continuamente y los requisitos de los usuarios cambian con el tiempo.

Algunas medidas comunes del rendimiento en la administración de redes incluyen:

* Ancho de banda: la cantidad de información que se puede transmitir a través de una red en un período de tiempo determinado.
* Latencia: el tiempo que tarda un paquete de datos en viajar desde su origen hasta su destino.
* Tasa de paquetes perdidos: la cantidad de paquetes de datos que se pierden en la transmisión.
* Utilización del enlace: la cantidad de ancho de banda utilizado en un enlace en particular.
* Tiempo de disponibilidad: el tiempo que una red está disponible y en funcionamiento sin interrupciones.
* Velocidad de transmisión: la velocidad a la que se transmiten los datos a través de la red.
* Eficiencia de la red: la capacidad de la red para utilizar eficientemente su ancho de banda y recursos.

Estas medidas del rendimiento en la administración de redes se pueden monitorear y evaluar continuamente para garantizar que la red cumpla con los requisitos y objetivos de la organización.

Además de las medidas del rendimiento mencionadas anteriormente, también hay otros aspectos importantes en la administración de redes que contribuyen a un rendimiento óptimo:

* Topología de la red: la disposición física y lógica de los componentes de la red, incluyendo servidores, switches, routers y dispositivos de almacenamiento.
* Configuración de la red: la forma en que los componentes de la red están conectados y configurados para funcionar juntos.
* Protocolos de comunicación: los estándares y reglas que rigen la transmisión de datos a través de la red.
* Seguridad de la red: la implementación de medidas para proteger la red y los datos que se transmiten a través de ella de ataques y amenazas externas.
* Gestión de la red: la monitorización y administración continua de la red para garantizar su rendimiento óptimo.

Es importante destacar que, para garantizar el rendimiento en la administración de redes, es necesario un enfoque integral que abarque todos estos aspectos y tenga en cuenta las necesidades y requisitos de la organización. Una combinación de herramientas de software y hardware, así como un equipo altamente capacitado y experimentado, son esenciales para lograr un rendimiento óptimo en la administración de redes.

Hay otros puntos importantes a tener en cuenta en la administración de redes:

* Planificación a largo plazo: es importante planificar el crecimiento y la evolución de la red de manera proactiva para evitar problemas de rendimiento a largo plazo.
* Actualizaciones y mantenimiento: mantener los componentes de la red actualizados y en buen estado es esencial para garantizar su rendimiento y proteger la red contra posibles problemas.
* Monitoring y troubleshooting: una herramienta de monitorización y diagnóstico de problemas adecuada es esencial para identificar y solucionar problemas de rendimiento en la red de manera rápida y eficiente.
* Colaboración: trabajar de manera colaborativa con proveedores, equipos internos y usuarios finales es clave para garantizar un rendimiento óptimo en la administración de redes.
* Documentación y seguimiento: mantener una documentación completa y actualizada de la red y llevar un registro de los cambios y problemas puede ayudar a mejorar el rendimiento y la resolución de problemas a largo plazo.

En resumen, la administración de redes es un proceso continuo que requiere un enfoque integral y una combinación de habilidades técnicas y de gestión para garantizar un rendimiento óptimo.

## 1.4.1 Análisis de fallas

El análisis de fallas en redes es un proceso crucial para identificar y solucionar problemas de rendimiento en una red. Este proceso implica recopilar información sobre los problemas de rendimiento y analizar esta información para determinar la causa raíz de los problemas.

Hay varios pasos en el análisis de fallas en redes, incluyendo:

* Identificación del problema: recopilación de información sobre los problemas de rendimiento, incluyendo descripciones de los problemas y ubicación.
* Recopilación de datos: recopilación de información sobre los componentes de la red y su rendimiento, incluyendo registros de eventos, mediciones de rendimiento y registros de tráfico de red.
* Análisis de datos: análisis de la información recopilada para determinar la causa raíz de los problemas de rendimiento.
* Pruebas y verificación: realización de pruebas adicionales para confirmar la causa raíz del problema y verificar la solución propuesta.
* Solución y resolución: implementación de soluciones para resolver los problemas de rendimiento y verificación de que se han resuelto.

Es importante destacar que el análisis de fallas en redes debe llevarse a cabo de manera rápida y eficiente para minimizar el impacto en el rendimiento de la red y garantizar la continuidad del negocio. Una combinación de herramientas de software y habilidades técnicas esenciales para realizar un análisis de fallas efectivo en una red.

Cabe destacar que el análisis de fallas en redes también puede ayudar a mejorar la eficiencia y la optimización de la red, aumentar la seguridad de la red y prevenir futuros problemas de rendimiento.

Además de lo mencionado anteriormente, aquí hay algunos puntos adicionales a considerar sobre el análisis de fallas en redes:

* Herramientas: Hay muchas herramientas de software y hardware disponibles en el mercado para ayudar en el análisis de fallas en redes, incluyendo monitores de red, analizadores de paquetes y herramientas de diagnóstico de red.
* Documentación: Mantener una documentación detallada y actualizada de la topología de la red, la configuración de los dispositivos y los registros de eventos es esencial para el análisis de fallas en redes.
* Proactividad: Es importante llevar a cabo un monitoreo y análisis continuo de la red para detectar y resolver problemas de rendimiento antes de que causen interrupciones importantes.
* Colaboración: El análisis de fallas en redes puede ser un proceso colaborativo que involucre a varios departamentos, incluyendo TI, operaciones y soporte técnico.
* Capacitación: Es importante que los administradores de red tengan una formación sólida en técnicas y herramientas de análisis de fallas para poder llevar a cabo el análisis de manera efectiva.

Si se detecta una falla durante el análisis de fallas en redes, el siguiente paso sería solucionar el problema. Esto generalmente implica los siguientes pasos:

* Identificación del problema: Determinar la naturaleza exacta de la falla y su origen.
* Verificación de la solución: Verificar si existe una solución conocida para el problema identificado.
* Implementación de la solución: Aplicar la solución y verificar si ha resuelto el problema.
* Documentación: Documentar los detalles del problema y la solución implementada para referencia futura.
* Verificación de la resolución: Verificar si la solución implementada ha resuelto el problema y si hay algún impacto en el rendimiento de la red.

Es importante tener en cuenta que algunos problemas de red pueden ser complejos y requerir más tiempo y recursos para resolverlos. En estos casos, puede ser necesario escalar el problema a un equipo de soporte técnico con experiencia en solucionar problemas de red más avanzados.

En resumen, el análisis de fallas en redes es un proceso importante y complejo que requiere un enfoque sistemático y una combinación de herramientas, documentación, proactividad, colaboración y capacitación para garantizar un resultado efectivo.

## 1.4.2 Análisis de contabilidad

Es el proceso de recolección de información acerca de los recursos utilizados por los elementos de la red, desde equipos de interconexión hasta usuarios finales. Esto se realiza con el objetivo de realizar los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación, es muy común en los proveedores de servicio de Internet o ISP.

Su objetivo es controlar el grado de utilización de los recursos de red, controlar el acceso de usuarios y dispositivos a la red, obtener informes, establecer cuotas de uso, asignar privilegios de acceso a los recursos; medir los parámetros de utilización de la red de manera que el uso individual o de grupos pueda ser regulado adecuadamente. Esta regulación minimiza los problemas de la red ya que los recursos pueden repartirse según la capacidad disponible y además mejora la imparcialidad en el acceso de los usuarios a la red.

Finalmente se debe hacer un seguimiento del uso de recursos de la red por parte de un usuario o grupo de usuarios. Todo esto para regular apropiadamente las aplicaciones de un usuario o grupo y además permitir una buena planificación para el crecimiento de la red.

Los objetivos de la función de administración de contabilidad son:

* Vigilancia de abuso de privilegios de acceso.
* Evitar sobrecargas en la red y perjuicios a otros usuarios.
* Uso ineficiente de la red.
* Modificar la forma de trabajo para mejorar prestaciones.
* Planificación del crecimiento de la red.
* Saber si cada usuario o grupo tiene lo que necesita.
* El aumento o disminución de derechos de acceso a recursos.

Contabilidad tiene como misión la recolección de estadísticas que permitan generar informes de tarificación que reflejen la utilización de los recursos por parte de los usuarios.

Requiere la realización de las siguientes tareas:

* Cobro a los usuarios por la utilización de los recursos
* Establecimiento de cuotas.
* Recolección de datos sobre la utilización de los recursos

Este servicio provee datos concernientes al cargo por uso de la red. Entre los datos proporcionados están los siguientes:

* Tiempo de conexión y terminación.
* Número de mensajes transmitidos y recibidos.
* Nombre del punto de acceso al servicio.
* Razón por la que terminó la conexión.

Se encarga también de las mediciones, control de costes y facturación de los clientes.

La estadística de red es de gran importancia, ya que esta permite el manejo de la contabilidad, la resolución de problemas, la realización de pronósticos a largo plazo, la planificación de la capacidad entre otras.

Las herramientas de gestión generalmente tienen funcionalidades estadísticas.

## 1.4.3 Análisis de seguridad

El **análisis de seguridad** es un proceso sistemático que se utiliza para evaluar la seguridad de un sistema o aplicación informática. Este proceso identifica las debilidades y vulnerabilidades potenciales en el sistema, y luego recomienda medidas para corregirlas y fortalecer la seguridad.

El **análisis de seguridad** puede incluir diversas técnicas, como la revisión de código, la realización de pruebas de penetración, la revisión de registros de seguridad, entre otros. El objetivo es garantizar que el sistema sea resistente a ataques y cumpla con los estándares de seguridad adecuados.

Hay muchas técnicas que se utilizan en el análisis de seguridad, algunas de las más comunes incluyen:

* Revisión de código: examinando el código fuente de un sistema o aplicación para identificar posibles vulnerabilidades.
* Pruebas de penetración: simulando un ataque realista para identificar debilidades y vulnerabilidades en el sistema.
* Análisis de vulnerabilidades: buscando y evaluando las debilidades conocidas en el sistema o aplicación.
* Escaneo de puertos: identificando los puertos abiertos en un sistema o dispositivo para determinar posibles puntos de entrada para los atacantes.
* Evaluación de la configuración: revisando la configuración de seguridad de un sistema o aplicación para asegurarse de que esté configurada adecuadamente.
* Análisis de amenazas: identificando las amenazas potenciales que pueden afectar la seguridad del sistema, como virus, malware, ataques cibernéticos, entre otros.
* Análisis de registros de seguridad: examinando los registros de seguridad de un sistema o aplicación para identificar posibles incidentes de seguridad o patrones de comportamiento inusual.

El análisis de seguridad es un proceso clave para garantizar la seguridad de los sistemas y aplicaciones informáticas. A continuación, describo algunos de los aspectos más importantes:

1. Planificación: antes de realizar un análisis de seguridad, es necesario planificar cuidadosamente el proceso, incluyendo los objetivos, la metodología y los recursos necesarios.
2. Evaluación de riesgos: una parte importante del análisis de seguridad es la evaluación de los riesgos. Esto implica identificar las debilidades y vulnerabilidades potenciales en el sistema, así como las amenazas que pueden afectar la seguridad.
3. Implementación de controles de seguridad: una vez identificadas las debilidades y vulnerabilidades, el siguiente paso es implementar controles de seguridad adecuados para proteger el sistema. Esto puede incluir la instalación de software de seguridad, la configuración de firewalls, la implementación de políticas de seguridad, entre otros.
4. Pruebas y verificación: después de implementar los controles de seguridad, es necesario realizar pruebas y verificaciones para asegurarse de que el sistema esté protegido adecuadamente. Esto puede incluir la realización de pruebas de penetración, la revisión de registros de seguridad, entre otros.
5. Documentación y seguimiento: es importante documentar los resultados del análisis de seguridad, incluyendo las debilidades y vulnerabilidades identificadas, los controles de seguridad implementados y los resultados de las pruebas. Además, es necesario llevar un seguimiento regular del sistema para detectar cualquier cambio o incidente de seguridad.

Tipos de ataques en el análisis de seguridad

Hay muchos tipos diferentes de ataques que pueden ser considerados en el análisis de seguridad, aquí describo algunos de los más comunes:

* Ataques por fuerza bruta: consisten en probar todas las posibles combinaciones de contraseñas hasta encontrar la correcta.
* Ataques de phishing: intentan engañar a los usuarios para que revele información confidencial o realice una acción específica, como descargar software malicioso.
* Ataques de malware: incluyen virus, gusanos, troyanos, ransomware, entre otros, que buscan dañar o robar información.
* Ataques de denegación de servicio (DoS): intentan hacer que un sistema o aplicación quede inaccesible a los usuarios legítimos, generalmente mediante el envío de una gran cantidad de solicitudes al sistema.
* Ataques de inyección SQL: consisten en insertar código malicioso en una consulta SQL para obtener acceso no autorizado a la información almacenada en una base de datos.
* Ataques de elevación de privilegios: buscan obtener más privilegios en un sistema o aplicación de los que tienen actualmente.
* Ataques de interceptación de red: consisten en interceptar y leer información confidencial que se transmite a través de una red.

Estos son solo algunos de los tipos de ataques más comunes. La lista no es exhaustiva y hay muchos otros tipos de ataques que se deben tener en cuenta en el análisis de seguridad.

¿Es importante el análisis de seguridad?

Sí, el análisis de seguridad es extremadamente importante en la actualidad. Con la creciente dependencia de las tecnologías de la información y la explosión de la cantidad de información digital, la seguridad de la información se ha convertido en una preocupación crítica para organizaciones y personas de todo el mundo.

Hay varias razones por las que el análisis de seguridad es importante:

* Protección de la información confidencial: el análisis de seguridad ayuda a proteger la información confidencial y a garantizar que solo las personas autorizadas tienen acceso a ella.
* Prevención de daños: el análisis de seguridad ayuda a prevenir daños a los sistemas y a la información, lo que puede tener un impacto económico negativo.
* Cumplimiento normativo: muchas industrias y organizaciones están reguladas por leyes y normativas que requieren un nivel de seguridad de la información. El análisis de seguridad ayuda a garantizar que se cumplan estas regulaciones.
* Mejora de la reputación: un sistema o aplicación seguros mejoran la reputación de una organización y aumentan la confianza de los usuarios.

En resumen, el análisis de seguridad es un componente clave para garantizar la seguridad de la información y los sistemas en un entorno cada vez más digital.

Problemas que ocasionan si no se hace bien el análisis de seguridad

Hay muchos problemas que pueden surgir si el análisis de seguridad no se realiza adecuadamente. Algunos de los problemas más comunes incluyen:

* Ataques y violaciones de seguridad: si el análisis de seguridad no identifica y mitiga adecuadamente los riesgos de seguridad, es más probable que los sistemas y la información sean objeto de ataques y violaciones.
* Pérdida de información confidencial: sin un análisis de seguridad adecuado, es posible que la información confidencial se filtre o se pierda.
* Daños a los sistemas: si el análisis de seguridad no identifica y mitiga adecuadamente los riesgos, es posible que los sistemas sufran daños y sean inaccesibles.
* Costos elevados: los daños y la pérdida de información pueden tener un impacto económico negativo, y es posible que sea necesario realizar costosos reparaciones y mejoras.
* Desacreditación: un sistema o aplicación inseguros pueden dañar la reputación de una organización y disminuir la confianza de los usuarios.

# Bibliografía

*[1] SciELO - Scientific Electronic Library Online. (s. f.). http://scielo.sld.cu/scielo.php?pid=S1024-94352003000600012*

*[2] Hashing: Técnicas y Hash para la Protección de Datos. (s. f.). Recuperado 4 de febrero de 2023, de http://www.laccei.org/LACCEI2018-Lima/student\_Papers/SP96.pdf*

*[3] Admin, A. (2023). ¿Qué es el rendimiento de la red? - definición de techopedia. Icy Science.* [*https://es.theastrologypage.com/network-performance*](https://es.theastrologypage.com/network-performance)

*[4] Administración y seguridad de redes - Rendimiento. (s. f.).* [*https://sites.google.com/site/admoysegderedes/home/unidad-l/rendimiento*](https://sites.google.com/site/admoysegderedes/home/unidad-l/rendimiento)

*[5] ADMINISTRACIÓN DE LA SEGURIDAD DE RED. (2018, julio 26). Interpolados. https://interpolados.wordpress.com/2018/07/26/administracion-de-la-seguridad-de-red/*

*[6] Fundamentals of (IPS) intrusion prevention system. (2016, febrero 26).*

*[7] (S/f). Gestiopolis.com. Recuperado el 6 de febrero de 2023, de https://www.gestiopolis.com/administracion-de-redes-y-seguridad-informatica/*

*[8] Administración y seguridad de redes - Rendimiento. (s. f.). https://sites.google.com/site/admoysegderedes/home/unidad-l/rendimiento?pli=1*

*[9] CD-0006. (s. f.). bibdigital. https://bibdigital.epn.edu.ec/bitstream/15000/2353/1/CD-0006.pdf*

*[10] Moreno, M. J. (2012, 15 junio). 6.2 MONITOREO DE RENDIMIENTO,FALLAS Y CONTABILIDAD. Jhonny Moreno. https://morenojhonny.wordpress.com/2012/06/15/6-2-monitoreo-de-rendimientofallas-y-contabilidad/*

*[11] (2023, 6 febrero). 1.3 ADMINISTRACION DE CONTABILIDAD. http://adminredes-alejandrovivar.blogspot.com/2015/12/13-administracion-de-contabilidad.html*

*[12] Academy, B. (2023, 17 enero). ¿Qué es la criptografía simétrica? Bit2Me Academy. Recuperado 6 de febrero de 2023, de https://academy.bit2me.com/que-es-criptografia-simetrica/*

*[13] Hurtado, J. S. (2022, 8 agosto). Qué es la criptografía y para qué sirve. Thinking for Innovation. Recuperado 6 de febrero de 2023, de https://www.iebschool.com/blog/que-es-la-criptografia-y-para-que-sirve-finanzas/*

*[14] ¿Qué es la criptografía? - Explicación sobre la criptografía - AWS. (s. f.). Amazon Web Services, Inc. Recuperado 6 de febrero de 2023, de https://aws.amazon.com/es/what-is/cryptography/*