

“Hardware” y “software” de seguridad en la red

**Breve descripción:**

El aprendiz debe apropiar los conocimientos y actividades que le permitan interpretar e implementar el plan de seguridad de las redes utilizadas y los datos que circulan a través de ellas, cumpliendo las normas establecidas vigentes.

**Octubre 2023**

Tabla de contenido

[Introducción 1](#_Toc149578717)

[1. Seguridad de información en la red 3](#_Toc149578718)

[1.1. Integridad 4](#_Toc149578719)

[1.2. Confidencialidad 4](#_Toc149578720)

[1.3. Disponibilidad 5](#_Toc149578721)

[1.4. Ataques a la seguridad de la red 5](#_Toc149578722)

[Ataques pasivos 8](#_Toc149578723)

[Ataques activos 9](#_Toc149578724)

[1.5. Herramientas de seguridad 9](#_Toc149578725)

[Autenticación 11](#_Toc149578726)

[Autorización 11](#_Toc149578727)

[Auditorías 12](#_Toc149578728)

[Cifrados 13](#_Toc149578729)

[Filtros de paquete 15](#_Toc149578730)

[“Firewalls” 15](#_Toc149578731)

[Detección de intrusos 16](#_Toc149578732)

[Funcionalidad 16](#_Toc149578733)

[Características 17](#_Toc149578734)

[1.6. Vulnerabilidades y amenazas 18](#_Toc149578735)

[Vulnerabilidad del día cero 20](#_Toc149578736)

[Vulnerabilidades conocidas 20](#_Toc149578737)

[1.7. Análisis de seguridad de la red 22](#_Toc149578738)

[1.8. Análisis de riesgos 22](#_Toc149578739)

[1.9. Matriz de control 24](#_Toc149578740)

[1.10. Estimación de la vulnerabilidad 28](#_Toc149578741)

[1.11. Requisitos de la seguridad 28](#_Toc149578742)

[1.12. Revisión y actualizaciones de la política de la seguridad 29](#_Toc149578743)

[2. Implementación 31](#_Toc149578744)

[2.1. Parámetros para establecer políticas de seguridad 31](#_Toc149578745)

[2.2. Plan de trabajo para establecer políticas de seguridad 32](#_Toc149578746)

[2.3. Recomendaciones para implementar políticas 33](#_Toc149578747)

[2.4. Normas y procedimientos 34](#_Toc149578748)

[2.5. Norma Técnica Colombiana NTC-ISO/IEC 27001 35](#_Toc149578749)

[Novedades 37](#_Toc149578750)

[Síntesis 39](#_Toc149578751)

[Material complementario 41](#_Toc149578752)

[Glosario 42](#_Toc149578753)

[Referencias bibliográficas 44](#_Toc149578754)

[Créditos 47](#_Toc149578755)

Introducción

Para comenzar con el estudio de la temática del componente formativo, lo invitamos a ver el siguiente video.

1. “Hardware” y “software” de seguridad en la red



[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=G11sauc5bws)

|  |
| --- |
| **Síntesis del video: “Hardware” y “software” de seguridad en la red** |
| La seguridad de la información, hoy por hoy, es uno de los temas más importantes en el mundo tecnológico, debido al incremento elevado de los ataques cibernéticos a los que los usuarios están expuestos.  Los “smartphones” pasaron de ser una moda a ser una herramienta de trabajo y/o también un estilo de vida.  Los ciber atacantes, día a día, se las ingenian para que los usuarios caigan en sus nuevas fechorías, sin que estos últimos lo sepan; es por esta razón que hay organizaciones que exigen tratar los datos haciendo uso de estándares los cuales disminuyen esa brecha de riesgo. |

# Seguridad de información en la red

Tradicionalmente, las redes cableadas o redes alámbricas se han considerado más seguras que las redes inalámbricas. El uso de internet y la evolución de las comunicaciones, han hecho que las instalaciones no sean únicas, sino que pueden situarse a miles de kilómetros. A su vez, una red privada virtual permite mediante el uso de internet, establecer esta conexión realizando una inversión moderada. Una VPN o red privada es, básicamente, una red virtual que se crea dentro de otra red, habitualmente internet. Para un cliente VPN se trata de una conexión que se establece entre su equipo y el servidor, esta conexión es transparente para él, simplemente los datos le son enviados de la misma manera que si llegaran a través de la LAN a la que se conecta.

Por lo que los IDS [“Intrusion Detection Systems” - Sistemas de Detección de Intrusiones] son un paso adelante en las funciones que implementan los cortafuegos (“firewalls”). Existen varias herramientas de detección de intrusos, pero su uso es bastante complejo, algunos ejemplos más representativos son “tripwire enterprise” (permite detectar las acciones en la red que no se ajustan a la política de seguridad de la empresa, e informar de aquellos que necesitan especial atención) y “snort” (es una aplicación de código abierto que permite tanto la detección de intrusión como su prevención) (B2B Consultores, 2020).

Este IDS escucha el tráfico de la red en tiempo real y lo relaciona con una serie de normas ya predefinidas, que pueden descargarse desde internet. Cuando encuentra alguna coincidencia alerta sobre ella, hace un log de dicho tráfico o lo ignora, según se ha indicado en la norma (B2B Consultores, 2020).

## Integridad

Es una característica que permite mantener los datos sin modificaciones no autorizadas, y que la información permanezca tal como fue generada, sin manipulación o alteraciones realizadas por personal no autorizado.

Hay violación de integridad cuando un empleado, proceso o programa, borra o modifica datos importantes que pertenecen a la información. Para conservar la integridad de un mensaje, se deben adjuntar los datos de comprobación de integridad, por ejemplo, la firma digital es uno de ellos.

## Confidencialidad

Según afirma Seguridad en redes (s.f.), es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.

De acuerdo con Seguridad en la red (s.f.): “… en una transacción por internet se requiere que el número de la tarjeta de crédito sea transmitida desde el comprador al comerciante y de este a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de estos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras tiene información confidencial en la pantalla, cuando se publica información privada, cuando una laptop con información sensible sobre una empresa es robada, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad (s.p.)”.

## Disponibilidad

Se define como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento, por ejemplo, el objetivo de la plataforma SENA Sofia Plus por el hecho de mantener disponible la información de los cursos disponibles. Constantemente está recibiendo consultas, acceso y peticiones, por lo que siempre deberá estar disponible para los usuarios. “La disponibilidad supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten” (www.pmg-ssi.com, 2018).

## Ataques a la seguridad de la red

Para conocer sobre este tema, lo invitamos a ver el siguiente video.

1. Ataques de seguridad en la red



[**Enlace de reproducción del video**](https://youtu.be/x56FT_OVARQ)

|  |
| --- |
| **Síntesis del video: Ataques de seguridad en la red** |
| El ataque de seguridad en la red se da cuando se saca provecho de una vulnerabilidad de un sistema de información para ocasionar daños por parte de terceros y con intenciones desconocidas para el administrador del sistema.  Existen numerosos tipos de ciberataques. A continuación, se describen los más reconocidos:   * “**Malware**”: se denomina también “software” malicioso, por la traducción del inglés “malicious software”. Al ingresar en un equipo tiene como función dañarlo de diferentes maneras. * **Virus**: tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo, propagarse de un equipo a otro e infectar las aplicaciones de este * “**Worms**” **(gusanos)**: programa de “software” malintencionado, el cual se propaga sin intervención del usuario, se activa de forma automática y sin ser visto, extendiéndose a otros sistemas informáticos por medio de las redes. * **Troyanos**: tienen la apariencia de un programa confiable, pero esconden otro tipo de “malware” que se instala automáticamente para asumir el control total del equipo. * “**Keyloggers**”: registran y captan todas las pulsaciones del teclado y esta información se emplea para conseguir contraseñas y datos de la víctima. * “**Spyware**”: el objetivo principal de este “malware” es el robo de información. * “**Adware**”: muestra publicidad al usuario a través de “banners”, “pop-ups”, nuevas ventanas en el explorador. En muchos casos, el objetivo secundario también es obtener información sobre la actividad del usuario en la red. * “**Ransomware**”: es el tipo de ataque más común en la actualidad. Se basa en el cifrado de los datos, restringiendo el acceso a los archivos del equipo para pedir un pago por el rescate de estos; en la mayoría de los casos en “bitcoins”. |

### Ataques pasivos

En lo referente a la Configuración de mecanismos de seguridad (ITCFA-Fepade, s.f.), se enuncia que: […] el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

* Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
* Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
* Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.
* Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información (s.p.).

### Ataques activos

Son aquellos que involucran modificaciones en la transmisión de datos, o creación de un flujo falso de datos, entre los cuales se pueden encontrar:

* **Degradación fraudulenta del servicio.** Este ataque frena el desarrollo y gestión de recursos informáticos y de comunicaciones, causando interrupciones del servicio de una red, eliminación de mensajes específicos, parálisis temporal de servidores FTP, web o de correo. La imagen da una idea de lo que puede suceder con este ataque.
* **Modificación de mensajes.** Se efectúa alteración, reordenación o retardo de los mensajes produciendo una situación no autorizada.
* **Repetición.** Se produce la captura y repetición de mensajes para producir un resultado no autorizado, un claro ejemplo es el de realizar consignaciones repetidas en una determinada cuenta.
* **Suplantación de identidad.** Aquí el intruso pretende ser otra entidad incluyendo otras formas activas de ataque y poder así capturar y repetir secuencias de autenticación, robar la contraseña de ingreso a una cuenta, permitiendo su acceso a los recursos especiales suplantando así al usuario que posee dichos privilegios.

## Herramientas de seguridad

Pueden utilizarse para revisar la seguridad de un sistema con buenas o con malas intenciones. Si no se revisa la seguridad del sistema, alguien lo hará. Por ejemplo, se encuentran los analizadores de red, que buscan equipos en la red, hacen barridos de puertos y descubrimiento de servicios, analizando los resultados para inferir información, como versión, tipo de sistema y/o servicios para exponer deficiencias de seguridad. Algunos de los más utilizados son nmap, SATAN y SAINT.

A continuación, le invitamos a consultar el PDF **Herramientas de seguridad,** el cual se encuentra en la carpeta Anexos, donde se amplía la información sobre las herramientas de seguridad más utilizadas.

Otro tipo de herramientas son los analizadores de seguridad para localizar todo tipo de posibles problemas que permiten detectar y exponer aplicaciones conocidas por su fragilidad, configuraciones particulares inseguras, uso de claves predefinidas y múltiples “bugs” y sus “exploits”. Uno de estos analizadores es Nessus:

“Una aplicación gratuita para uso no comercial (en origen era libre). Sus desarrolladores producen decenas de nuevos análisis de vulnerabilidades a la semana. Estos análisis (llamados “plugins”) se publican para uso gratuito una semana después de su puesta a disposición de los clientes de pago. OpenVAS (inicialmente Nessus) es un analizador libre que nació como una ramificación del último Nessus libre. Los análisis de vulnerabilidades son llamados NVT (“Network Vulnerability Tests”)” (Guimi.net, 2009).

Finalmente, los programas de descubrimiento de claves analizan listados de claves cifradas o resumidas (mediante algoritmos como MD4) para intentar descubrirlas. La herramienta más utilizada es John The Ripper (JTR), que es libre y autodetecta el tipo de resumen de la clave y ataca claves de multitud de algoritmos como DES, MD5, Blowfish, Kerberos o LM Hash (Windows) tanto en ficheros de texto como en repositorios sobre LDAP o MySQL, puede trabajar con ataques de diccionario y alteraciones o mediante fuerza bruta usando tablas de caracteres frecuentes para marcar el orden (Guimi.net, 2009).

### Autenticación

El procedimiento de autenticación se lleva a cabo por parte del administrador de servicios quien autoriza los servicios a ejecutar en el dominio y los usuarios permitidos para utilizar las herramientas del sistema informático; los tipos de autenticación que se pueden configurar, los puede ver en el PDF **Tipos de autenticación,** el cual se encuentra en la carpeta Anexos.

### Autorización

Es el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización. El mecanismo o el grado de autorización puede variar dependiendo de qué sea lo que se está protegiendo, pues no toda la información de la organización es igual de crítica (Mifsud, 2012).

Al respecto:

“Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización. Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente. En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o negando el acceso en lectura, modificación, creación o borrado de los datos. Por otra parte, solo se dará la autorización a acceder a un recurso a aquellos usuarios que lo requieran para la realización de su trabajo y si no se le negará”. (Mifsud, 2012)

### Auditorías

Es el estudio que comprende el análisis y gestión de sistemas llevados a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores. Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad (Cómo administrar tu propio negocio, 2014).

De acuerdo con lo que afirma USS Seguridad (2019), dependiendo de los fines de la auditoría, es posible contratar profesionales externos con un objetivo concreto en el análisis informático, y este puede ser:

* **Auditoría forense.** Es un servicio especializado para actuar ante un incidente de seguridad, con el fin de recopilar evidencias digitales que permitan reunir la mayor información posible sobre el ilícito y sus operaciones.
* **Auditorías de código.** Se refiere a pruebas de calidad del código fuente que permita identificar vulnerabilidades ante ataques informáticos y también ante el crecimiento de la demanda que la actividad realiza al “software”.
* **Auditoría web.** Este análisis está orientado a conocer las propiedades de las aplicaciones digitales y servicios web utilizados a diario en la estrategia de negocio, para adelantarse a posibles riesgos y optimizar así la seguridad.
* **Actualización de dispositivos.** Hace referencia a verificar la actualización del “software”, antivirus y comprobar el cumplimiento de las reglas de “firewalls”.
* **“Hacking” ético.** Se ponen a prueba las medidas de seguridad realizando un “test” de intrusión con técnicas de “hacking”, y tener así evidencia de la reacción.
* **Auditoría de redes.** Se provee un mapeo de todos los dispositivos conectados a la red interna, el estado de las conexiones y la actividad de los dispositivos gestionados.
* **Auditoría física.** Usado para proteger perimetralmente a la red a partir de controles físicos de entrada, alarmas contra incendios, sistemas de video vigilancia, el estado de las instalaciones de servicio de energía, agua y gas, entre otros.

### Cifrados

El cifrado de redes LAN inalámbricas se utiliza para añadir seguridad a una red inalámbrica mediante un protocolo de autenticación, que solicita una contraseña o clave de red cuando un usuario o dispositivo intenta conectarse. Si la red inalámbrica no está asegurada con algún tipo de cifrado, es posible que usuarios no autorizados accedan a ella y obtengan información personal, o que utilicen la conexión a Internet con fines maliciosos o ilegales. Además, también puede reducirse la velocidad o el rendimiento de la red si otras personas la utilizan sin conocimiento (Sony, 2021).

Entre los más conocidos se encuentran:

1. **Cifrado WEP.** Este cifrado es vulnerable y débil y se considera un cifrado “inseguro”. WEP ofrece una insuficiente protección, por tanto, no se recomienda usarlo.
2. **Cifrado WPA.** Surgió de la necesidad de solucionar los inconvenientes del cifrado WEP, este cifrado ofrece diferentes variantes según la finalidad que se le dé, y estas variantes son:

Las principales ventajas que conlleva la logística de automatización son:

* **WPA-Personal.** Requiere un sistema de contraseñas PSK o claves precompartidas donde el administrador especifica su propia contraseña y todos los usuarios acceden a la red con ella, para que sea fácil recordarla.
* **RADIUS.** Específico para empresas, se basa en un servidor donde los usuarios se autentican con un usuario y una contraseña diferente para cada uno y no con una contraseña global.
* **Cifrado WPA2.** Es la actualización de WPA, mejora tanto el rendimiento como la seguridad, cuenta con variantes de claves personales PSK y sistemas RADIUS para gestionar la red, el cifrado es superior al de WPA.

### Filtros de paquete

Se trata de una función presente en los “routers” que mejora la seguridad, es el filtrado MAC, el cual permite restringir el acceso a recursos de un dispositivo específico, por ejemplo, la red inalámbrica, acceso a Internet o servidor SAMBA.

### “Firewalls”

Sirven para proteger el equipo de conexiones salientes o entrantes a la red. Existen “Firewalls” de “software” y de “hardware”; entre sus principales beneficios se encuentran:

* Evitan los ataques de otros servidores a la red privada.
* Permiten al administrador de la red definir un embudo, manteniendo al margen los usuarios no autorizados.
* Permiten monitorear la seguridad, cuando aparece alguna actividad sospechosa, esto generará una alarma.
* Un “hacker” prefiere una computadora sin “Firewalls”.
* Concentran la seguridad, centralizan los accesos.
* Generan alarmas de seguridad. Traducen direcciones (NAT).
* Monitorean y registran el uso de servicios de WWW y FTP.
* Controlan el uso de internet. Permiten bloquear el material no adecuado (Seguridad en la red, s.f.).

### Detección de intrusos

Un Sistema de Detección de Intrusos (IDS: “Intrusion Detection System”), se implementa para detectar actividades inadecuadas, incorrectas o irregulares, ocurridas en el interior o exterior de los dispositivos e infraestructura de la red.

El IDS está basado en el patrón de comportamiento del intruso que es diferente al del usuario legítimo, por medio de análisis de estadísticas de uso. El IDS utiliza el uso de programas, archivos y dispositivos, a corto, mediano y largo plazo para crear los patrones de comportamiento de usuarios que permitan realizar la detección efectiva; también usa un sistema de reglas predefinidas llamadas firmas o rúbricas para representar las violaciones conocidas.

### Funcionalidad

Se enfoca en el análisis detallado del tráfico de red y el uso de los dispositivos. La evaluación se lleva a cabo comparando el suceso con comportamientos sospechosos o firmas de ataques conocidos. Las bases de datos de firmas de ataques conocidos de los IDS permiten distinguir entre el uso normal y el uso fraudulento de un terminal de red, y/o entre el tráfico normal de la red y el tráfico inusual debido a un ataque o intento del mismo.

Es importante para el IDS prestar atención si ocurre un escaneo de puertos, transmisión de paquetes de datos dañados, entre otros. El IDS generalmente se integra con el “firewall”, en la puerta de enlace de la red, uniendo así la inteligencia del IDS y el poder de bloqueo del “firewall”, en el lugar donde inevitablemente pasan los paquetes y se puedan bloquear antes de ingresar a la red.

### Características

Según B2B Consultores (2020):

Cualquier sistema de detección de intrusos, sea cual sea su tipo y base de funcionamiento, debería contar con las siguientes características:

* Funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en segundo plano como parte del dispositivo o la red que está siendo observada.
* Ser tolerante a fallos en el sentido que debe ser capaz de sobrevivir a una caída del sistema.
* Ser resistente a perturbaciones, en el sentido que puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado.
* Imponer mínima sobrecarga sobre el sistema. Un sistema que consume muchos recursos computacionales, no debe ser utilizado.
* Observar desviaciones sobre el comportamiento estándar.
* Fácilmente adaptable al sistema operativo ya instalado, pues cada uno tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones.
* Hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo.
* Que ayude a identificar de dónde provienen los ataques que se sufren, y recoger evidencias que pueden ser usadas para identificar intrusos.
* Difícil de vulnerar y suministrar a los especialistas de seguridad cierta tranquilidad.

Siguiendo este tema, Infotecs (2019) afirma que: "cada día se crean nuevas técnicas para exponer o vulnerar sistemas computacionales, y es un gran desafío para la seguridad de la información acompañar esta velocidad, e incluso estar al frente y no actuar de forma reactiva. La implementación de una buena política de IDS es fundamental en una arquitectura de seguridad, ya que este recurso, si se actualiza constantemente, es capaz de mantener la infraestructura distante de ataques oportunistas, ya sea desde una perspectiva de la red, o por la propia exposición de un dispositivo. Para poner en funcionamiento, un sistema de detección de intrusos se debe tener en cuenta que es posible optar por una solución de “hardware”, de “software”, o incluso una combinación de estos. La posibilidad de introducir un elemento “hardware” es debido al alto procesamiento de información en redes con mucho tráfico; a su vez, los registros de firmas y las bases de datos con los posibles ataques necesitan gran cantidad de almacenamiento. En la actualidad, además, el desarrollo de las estrategias de seguridades para los dispositivos y las redes de comunicación ha influido en el surgimiento de un nuevo tipo de defensa a tomar en consideración: los IPS o Sistemas de Prevención de Intrusiones, que en buena medida pueden interpretarse como una evolución de los IDS tradicionales".

## Vulnerabilidades y amenazas

De acuerdo con Mifsud (2012):

“La vulnerabilidad es la debilidad de cualquier tipo que compromete la seguridad del sistema informático. Se define como amenaza el escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático. Cuando a un sistema informático se le detecta una vulnerabilidad y existe una amenaza asociada a dicha vulnerabilidad, puede ocurrir que el suceso o evento se produzca y el sistema esté en riesgo. Si el evento se produce y el riesgo que era probable ahora es real, el sistema informático sufrirá daños que habrá que valorar cualitativa y cuantitativamente, y esto se llama 'impacto'. Es decir, un evento producido en el sistema informático que constituye una amenaza asociada a una vulnerabilidad del sistema produce un impacto sobre él. Si se quieren eliminar las vulnerabilidades del sistema informático o queremos disminuir el impacto que puedan producir sobre él, ha de proteger el sistema mediante una serie de medidas que se pueden llamar defensas o salvaguardas”.

Las vulnerabilidades se pueden agrupar en función de:

1. **Diseño**

* Debilidad en el diseño de protocolos utilizados en las redes.
* Políticas de seguridad deficiente e inexistente.

1. **Implementación**

* Errores de programación.
* Existencia de “puertas traseras” en los sistemas informáticos.
* Descuido de los fabricantes.

1. **Uso**

* Configuración inadecuada de los sistemas informáticos.
* Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
* Disponibilidad de herramientas que facilitan los ataques.
* Limitación gubernamental de tecnologías de seguridad.

### Vulnerabilidad del día cero

Aquellas vulnerabilidades para las cuales no existe una solución “conocida”, pero se sabe cómo explotarla. (Mifsud, 2012).

### Vulnerabilidades conocidas

Estas vulnerabilidades están en las bases de datos de ataques conocidos usadas para comparar y detectar los posibles intrusos que quieran acceder al sistema informático, entre ellas se tienen:

* **Desbordamiento de “buffer”.** Ocurre cuando un programa no controla la cantidad de datos que se copian en “buffer”, si esa cantidad es superior a la capacidad del “buffer” los “bytes” sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Se aprovecha para ejecutar código que permita privilegios de administrador.
* **Condición de carrera (“Race Condition”).** Sucede cuando varios procesos acceden al mismo tiempo a recursos compartidos.
* **Error de formato de cadena (“Format String Bugs”).** Aquí se acepta la entrada de datos proporcionada por el usuario sin validar. Es un error de programación para el lenguaje C/C++. Un ataque con esta vulnerabilidad permite ejecutar código arbitrario y revelar información confidencial.
* **“Cross Site Scripting” (XSS).** Incluye ataques que permiten ejecutar scripts como VBScript o JavaScript, en el ambiente de otro sitio web. Este error se presenta en aplicaciones que presentan la información en navegadores web. Esta vulnerabilidad realiza “phishing” constante con el fin de obtener contraseñas de usuarios atacados.
* **Inserción SQL.** Hay inserción de código SQL usurpador entre el código SQL programado, para alterar la marcha normal del programa y conseguir así que se ejecute la porción de código “invasor” introducido, en la base de datos.
* **Vulnerabilidades de denegación del servicio.** Se pierde el acceso a recursos y servicios por parte de los usuarios legítimos, hay pérdida de conectividad de la red por el consumo del ancho de banda de la red o sobrecarga de los recursos informáticos del sistema de la víctima.
* **Ventanas engañosas (“Window Spoofing”).** Estas ventanas ofrecen premios, rebajas, primicias mentirosas para capturar información y efectuar un ataque (Mifsud, 2012).

## Análisis de seguridad de la red

El análisis de la seguridad en la red se debe realizar para detectar irregularidades, comportamiento inusual de usuarios y demás amenazas. Para ello, se almacenan datos de la organización, se convierten en información accionable, de manera que los profesionales de tecnología de la información (TI) actúen con rapidez y se minimicen los riesgos.

Para ampliar la información, lo invitamos a ver el PDF **Análisis de seguridad de la red,** el cual se encuentra en la carpeta Anexos.

## Análisis de riesgos

La academia Cisco (2005), menciona que el análisis de riesgo tiene como objetivo determinar los componentes que requieren protección dentro del sistema, las amenazas que lo colocan en peligro y las vulnerabilidades que los debilitan con el fin de evaluar el grado de riesgo. En el campo de la seguridad informática, el método más usado para el análisis y valoración del riesgo está basado en la siguiente fórmula matemática:

Riesgo = Magnitud de Daño \* Probabilidad de Amenaza

Para presentar el resultado del análisis de riesgo se hace uso de una gráfica de dos dimensiones, donde, el eje **x** horizontal representa la magnitud de daño y el eje **y** vertical la probabilidad de amenaza. La probabilidad de amenaza y magnitud de daño pueden tomar condiciones entre insignificante (1) y muy alta (5). Aunque no es necesario dar valores numéricos a las condiciones de las variables, es útil porque, facilita el uso de hojas de cálculo en su representación. El análisis de riesgo permite ubicar los factores que influyen, positiva o negativamente.

Es importante reconocer que los riesgos son dinámicos, cambiantes, con diferentes caracteres de vulnerabilidad y con percepción distinta dependiendo del área que lo perciba, por tanto, deben participar los especialistas de todas las dependencias de la organización (gerencia, coordinación, administración financiera, técnicos, soporte técnico externo, etc.). Como conclusión de esta representación gráfica se puede observar que entre más alta la probabilidad de amenaza y magnitud de daño, más grande será el riesgo y el peligro al sistema, por lo cual se deben implementar medidas de protección. Esta representación se evidencia en la siguiente tabla:

1. Representación gráfica análisis

**Análisis de riesgo**

Riesgo = Probabilidad de amenaza \* Magnitud del daño

|  |  | Magnitud del daño 1 | Magnitud del daño 2 | Magnitud del daño 3 | Magnitud del daño 4 | Magnitud del daño 5 |
| --- | --- | --- | --- | --- | --- | --- |
| Probabilidad de amenaza - Frecuente | 5 | 5 | 10 | 15 | 20 | 25 |
| Probabilidad de amenaza – Probable | 4 | 4 | 8 | 12 | 16 | 20 |
| Probabilidad de amenaza – Mediana | 3 | 3 | 6 | 9 | 12 | 15 |
| Probabilidad de amenaza - Baja | 2 | 2 | 4 | 6 | 8 | 10 |
| Probabilidad de amenaza - Insignificante | 1 | 1 | 2 | 3 | 4 | 5 |

Riesgo muy alto (15 - 25)

Riesgo alto (10 - 14)

Riesgo medio (5 - 9)

Riesgo bajo (1 - 4)

## Matriz de control

Esta herramienta posibilita medir la efectividad de una gestión de riesgo adecuada, permite identificar las actividades de la organización, clasifica el tipo de riesgo según la intensidad y los diferentes factores que lo producen. A partir de la información documentada, se diagnostica la condición de riesgo de una entidad. El método debe incluir las diferentes áreas de negocio de la empresa con el fin de comparar los productos, proyectos y procesos.

Al respecto, Mejía (2006) afirma que:

“La ventaja principal de la matriz de control es la facilidad para identificar los riesgos, determinar los controles existentes y proponer nuevos. Su principal desventaja es la cantidad de información y cuadros que se deben desarrollar, pues pueden dificultar, complicar o demorar su aplicación. Esta desventaja se ha subsanado con el uso de herramientas computarizadas”.

La matriz de control también permite identificar los riesgos y plantear estrategias enfocadas al desarrollo del modelo de gestión pertinente.

El método utilizado para el diseño de la matriz, es el Delphi, donde se consulta a los especialistas o expertos temáticos acerca del medio y las actividades de la organización o del proyecto. En la matriz se establecen y plasman los componentes, los recursos y las posibles amenazas sobre el objeto de análisis, tal como se muestra en la siguiente tabla.

1. Componentes matriz de control

**Matriz de riesgos graficada**

| Matriz de control de riesgo | Matriz de control de riesgo | Matriz de control de riesgo | Probabilidad amenaza | Probabilidad amenaza | Probabilidad amenaza | Probabilidad amenaza | Probabilidad amenaza |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Elementos de información | Magnitud de daño | Criminalidad - Robo | Criminalidad - Virus | Sucesos físicos - Incencio | Sucesos físicos – Falta de corriente | Negligencia – Compartir contraseñas | Negligencia – No cifrar datos críticos |
| Datos e información |  | 3 | 4 | 2 | 3 | 5 | 3 |
| RR.HH. | 3 | 9 | 12 | 6 | 9 | 15 | 9 |
| Finanzas | 4 | 12 | 16 | 8 | 12 | 20 | 12 |

| Matriz de control de riesgo | Matriz de control de riesgo | Matriz de control de riesgo | Probabilidad amenaza | Probabilidad amenaza | Probabilidad amenaza | Probabilidad amenaza | Probabilidad amenaza |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Elementos de información | Magnitud de daño | Criminalidad - Robo | Criminalidad - Virus | Sucesos físicos - Incencio | Sucesos físicos – Falta de corriente | Negligencia – Compartir contraseñas | Negligencia – No cifrar datos críticos |
| Sistemas de información |  |  |  |  |  |  |  |
| Computadores | 2 | 6 | 8 | 4 | 6 | 10 | 6 |
| Portátiles | 3 | 9 | 12 | 6 | 9 | 15 | 9 |

| Matriz de control de riesgo | Matriz de control de riesgo | Matriz de control de riesgo | Probabilidad amenaza | Probabilidad amenaza | Probabilidad amenaza | Probabilidad amenaza | Probabilidad amenaza |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Elementos de información | Magnitud de daño | Criminalidad - Robo | Criminalidad - Virus | Sucesos físicos - Incencio | Sucesos físicos – Falta de corriente | Negligencia – Compartir contraseñas | Negligencia – No cifrar datos críticos |
| Personal |  |  |  |  |  |  |  |
| Coordinador | 4 | 12 | 16 | 8 | 12 | 20 | 12 |
| Personal técnico | 5 | 15 | 20 | 10 | 15 | 25 | 15 |

Color rojo: riesgo muy grave. Requieren mitigación: planes de actuación correctivas. Requiere medidas correctivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.

Color naranja: riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo durante el proyecto.

Color amarillo: riesgo apreciable. Necesitan investigación: planes de actuación preventivos. Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.

Color verde: riesgo marginal. Necesitan monitoreo: planes de actuación detectivos. Se vigilará, aunque no requiere medidas preventivas de partida.

La matriz se construye ubicando los recursos amenazados (componentes) encabezando las filas y las amenazas encabezando las columnas. Los componentes se refieren a los recursos que se quieren proteger y las amenazas a los eventos negativos que puedan generar pérdida o afectar los componentes. Cuando se han identificado los riesgos, se determina la probabilidad de ocurrencia y el valor de la misma, luego, se realizan los procesos de evaluación y estimación del riesgo.

## Estimación de la vulnerabilidad

Es la probabilidad que tiene un sistema de sufrir probables pérdidas, pueden ser físicas o de “software”, esto debido a diferentes causas de acuerdo con el tipo de ataque que se realice. El riesgo se mide de acuerdo con la vulnerabilidad. Se estima con base en el período de recurrencia de los hechos. Teniendo en cuenta los diferentes componentes se mencionan:

* **“Software”.** Vulnerabilidades por parte de las aplicaciones instaladas en los equipos de la red.
* **“Hardware”.** Están descritas de acuerdo con las configuraciones realizadas por parte del administrador.
* **Topología.** Dentro de este grupo se menciona el cableado estructurado, basado en el estándar.

## Requisitos de la seguridad

La seguridad debe contar con requisitos mínimos entre los cuales se pueden enunciar los siguientes:

* **Parche en sistema operativo.** Instalar las actualizaciones de “software”, preferiblemente de forma automática, que permitan solucionar las fallas de seguridad en los sistemas operativos.
* **Seguridad en los servicios de red.** Los servicios de red se deben limitar en necesidad, acceso, pertinencia y seguridad, haciendo uso del “firewall”.
* **Contraseñas robustas.** Crear y usar contraseñas que cumplan con los requerimientos de la organización.
* **Cifrado para autenticación.** La autenticación en el sistema informático, se debe proteger mediante el uso de cifrado.
* **Protección de “software”.** Ejecutar y actualizar automáticamente y de forma regular, los antivirus y “firewall”, para garantizar la seguridad del sistema.
* **Seguridad física.** Proteger físicamente el sistema, medios fijos y portátiles, de manipulación, acceso no autorizado o robo.

## Revisión y actualizaciones de la política de la seguridad

Es una de las etapas necesarias una vez que las políticas ya están funcionando dentro de una organización, no obstante, el tiempo que transcurre desde que éstas ya están implementadas dentro de la organización hasta su primera revisión es variable, ya que no existe un tiempo determinado. Este periodo de tiempo no está estipulado, sin embargo, varios ingenieros y analistas de sistemas de seguridad informática opinan que la revisión de las políticas de seguridad debe estar dentro de un lapso de entre seis (6) meses y un año, por ser tiempo suficiente para encontrar patrones que requieren algún tipo de ajuste.

El periodo de revisión de las políticas debe ser establecido por el comité de seguridad de manera empírica, dependiendo de diversos factores que afectan a la organización entre los que se encuentran la experiencia del personal de seguridad, las necesidades de seguridad que se tengan, cambios en la organización, el alza en número de incidentes, entre otros.

Para que cualquier metodología establecida funcione, todos los usuarios deben haber sido capacitados previamente en las PSI. Una vez capacitados, todos los usuarios pueden participar en la propuesta de modificaciones, ajustes o cambios para la mejora de las PSI. Las propuestas y observaciones deben pasar por un primer filtro, el cual consiste en la revisión de dicha propuesta por parte del administrador o responsable donde surgió la propuesta. Una vez que el personal responsable y administradores acuerdan que la propuesta es viable y que es en beneficio para la organización, acuerdan entregar el trabajo al personal de seguridad que revisa, evalúa, analiza y estudia las observaciones para elaborar una propuesta que será presentada al comité de seguridad para su aprobación.

# Implementación

El desarrollo de un plan de seguridad de red consiste en hacer las preguntas correctas y sus respuestas impulsarán la implementación. Al formular un plan de seguridad de red razonable, se pueden hacer preguntas importantes, tales como:

* ¿Qué necesito proteger?
* ¿Qué regulaciones gubernamentales debo seguir?
* ¿Cómo auditar mi plan de seguridad de red?
* ¿Qué herramientas pueden soportar mi plan de seguridad de red?

## Parámetros para establecer políticas de seguridad

Cuando se formulen las políticas de seguridad informática, es indispensable tener en cuenta, por lo menos, los aspectos siguientes:

* Realizar análisis de riesgo informático, valorar los activos y adecuar las políticas a la realidad de la organización.
* Programar reuniones con los departamentos dueños de los recursos, pues con su experiencia permiten establecer el alcance y definir las violaciones a la seguridad.
* Informar al personal involucrado sobre el desarrollo de las políticas, los beneficios, riesgos relacionados con los bienes, recursos y elementos de seguridad.
* Identificar en cada departamento el personal que toma las decisiones, pues son los encargados de salvaguardar los activos críticos del área.
* Monitorear periódicamente las operaciones y procedimientos de la empresa, para actualizar de forma oportuna las políticas ante los cambios ocurridos.
* Detallar correcta y explícitamente el alcance de las políticas y así evitar tensiones cuando se establezcan los mecanismos de seguridad conforme con las políticas trazadas (Coite y Romero, s.f.).

## Plan de trabajo para establecer políticas de seguridad

El plan de seguridad informática permite entender dónde pueden existir vulnerabilidades en los sistemas informáticos, para, una vez detectados, tomar las medidas necesarias que permitan prevenir dichos problemas. Este plan debe tener la capacidad de proteger los datos y los sistemas críticos del negocio, ajustándose a la Ley de Protección de Datos y a la legislación vigente; así mismo, el plan de seguridad contiene varios pasos que se deben dejar por escrito, a saber:

* **Identificación.** Se debe indagar por el conjunto de activos de la organización, incluido el “hardware”, “software”, personal, sistemas y datos, servidores, programas informáticos, y servicios externos como alojamiento web que conforman el sistema informático.
* **Evaluación de riesgos.** Establecer qué pone en peligro los activos anteriores. Por ejemplo, los virus informáticos, “hackers”, daños físicos o errores de los funcionarios.
* **Priorizar la protección IT.** Decidir cuáles son las amenazas más relevantes e interesantes que se deban proteger, estableciendo jerarquías de acuerdo con la importancia de cada dispositivo.
* **Tomar las precauciones adecuadas.** Una vez identificados los riesgos, decidir los pasos a seguir para asegurar que el negocio operará normalmente si ocurre una crisis. Por ejemplo, restringir el acceso a servidores o instalar un “firewall” de “hardware” (Noriega, 2016).

## Recomendaciones para implementar políticas

Es fundamental implementar internamente una política de seguridad informática que permita resguardar las áreas importantes de la organización para evitar robos de información, para ello se pueden adoptar las siguientes medidas:

* **Usar gestor de contraseñas.** El uso de contraseñas es el modelo de autenticación más utilizado para proteger las cuentas de plataformas, programas y servicios, aunque los usuarios vean la importancia de establecer una contraseña robusta con cambio periódico que impida el robo de la misma. La solución de los problemas anteriores la puede dar un gestor de contraseñas, que permite tener una contraseña maestra para dar acceso a las cuentas.
* **Valorar la encriptación de datos.** Para potenciar la seguridad informática de la empresa se puede usar la encriptación o cifrado que permite proteger los datos y archivos transportados a través de internet aplicando algoritmos de codificación para volver comprensible la información sensible.
* **Utilizar el escaneo de credenciales.** Permite detectar vulnerabilidades y evitar inconvenientes, rotando credenciales. Igualmente sirve para restringir, admitir o eliminar las credenciales compartidas para el acceso a otras áreas del sistema.
* **Administrar bien las cuentas privilegiadas.** Gestionar correctamente las cuentas es vital para evitar riesgos de seguridad informática. Es importante controlar los accesos a las cuentas privilegiadas de la organización y reducir al mínimo el número de cuentas, evitando así las brechas de seguridad (Gb-advisor, 2019).

## Normas y procedimientos

Se debe tener en cuenta que una norma de seguridad establece las condiciones de los elementos a proteger, así como los requisitos sustentados en la política y que regulan determinados aspectos de seguridad. Además, debe ser clara, concisa y no ser ambigua en su interpretación.

Estas normas se pueden agrupar con base en las diferentes áreas de la seguridad dentro de la organización: de seguridad física, de control de acceso a sistemas, de gestión de soportes, de clasificación de información, etc.

Al respecto:

“Un procedimiento de seguridad define las tareas o acciones a realizar en el desarrollo de un proceso relacionado con la seguridad y los grupos o personas responsables de su ejecución. Se especifican los pasos relacionados con la ejecución de un proceso o actividad que cumple con una norma o garantizar que en la ejecución de actividades cuenten con determinados aspectos de seguridad. Un procedimiento debe ser claro, sencillo de interpretar y sin ambigüedad en su ejecución” (Seguinfo, 2008).

## Norma Técnica Colombiana NTC-ISO/IEC 27001

La NTC ISO 27001 es una norma colombiana usada por las organizaciones con el fin de asegurar la confidencialidad e integridad de toda la información que poseen. La versión ISO 27001:2013 internacional es la que rige y está vigente, por lo cual debe ser el referente mundial en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

**Objetivo**

Implementar un SGSI con base en NTC ISO 27001, tiene como objetivo evaluar riesgos aplicando los controles existentes y, de ese modo, lograr su reducción o eliminación total. Las organizaciones que utilicen la ISO 27001 logran una ventaja competitiva y mejoran la imagen de marca.

**Estructura**

La NTC ISO 27001, posee una estructura de alto nivel, llamada también Anexo SL, en la cual se abarcan diferentes aspectos que se pueden visualizar en la siguiente tabla.

1. Estructura ISO-27001

| Aspecto | Contenido |
| --- | --- |
| Objeto y campo de aplicación. | Al inicio de la norma se establecen las orientaciones necesarias para el uso, finalidad y aplicación de la norma. |
| Referencias normativas. | Indica los documentos a consultar relacionados con la seguridad de la información. |
| Términos y definiciones. | Se describe la terminología que se utiliza a lo largo de la norma. |
| Contexto de la organización. | Permite a las organizaciones conocer el contexto en el que se desarrolla la actividad, tanto externa como interna, conocer qué necesitan los clientes y adoptar medidas para cubrir estas necesidades. |
| Liderazgo. | Permite que todo el personal involucrado en el SGSI participe activamente en la implementación de la norma ISO 27001. |
| Planificación. | Identificar los riesgos, objetivos y forma de lograrlos. |
| Soporte. | Tener los recursos suficientes, contar con las competencias, información y comunicación adecuada, que permitan al SGSI funcionar con éxito. |
| Operación. | Realizando la planificación, implementación y control de los procesos organizacionales, llevando a cabo una valoración de los riesgos permite el cumplimiento de los requisitos de un SGSI a cabalidad. |
| Evaluación de desempeño. | Es importante realizar el seguimiento, medición, análisis, evaluación, auditoría interna y revisión por la dirección del SGSI para que se asegure el funcionamiento según lo planificado. |
| Mejora. | Se establece la necesidad de las organizaciones a trabajar por la mejora continua, detectar no conformidades y adoptar medidas de solución, mejorando continuamente el SGSI. |

### Novedades

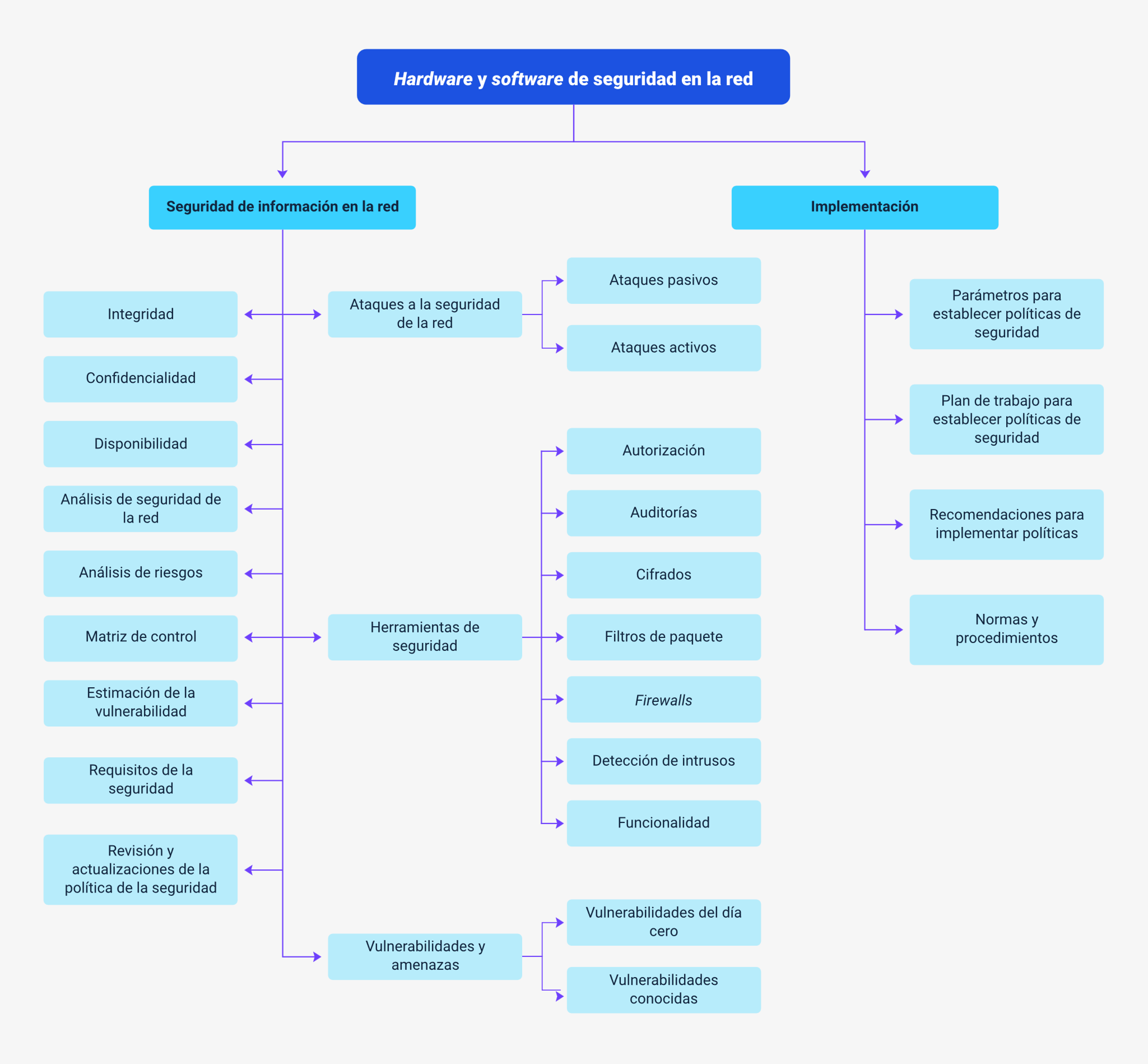
Al realizar la comparación con la edición anterior, en la última revisión se modificaron algunos requerimientos de la norma ISO 27001, por lo que las organizaciones deben realizar un proceso de transición que les permita adaptarse a los requisitos de la versión vigente y así el SGSI siga operando eficazmente. A continuación, se mencionan algunas novedades importantes:

* Desaparece el capítulo de enfoque a procesos, la ventaja actual permite mayor flexibilidad sin imponer la metodología PHVA.
* Se suprime el carácter obligatorio de ciertos documentos y solo es obligatoria la declaración de aplicabilidad.
* Hay cambios destacables en los requisitos y controles.
* Se opta por el enfoque del análisis del riesgo en la fase de planificación y operación del SGSI.

Las organizaciones deben cumplir con los requisitos establecidos por la NTC ISO 27001 y también con las buenas prácticas y controles definidos por la ISO 27002 (ISOTools Excellence, s.f.).

Síntesis

A continuación, se presenta una síntesis de la temática estudiada en el componente formativo.



El esquema presenta la síntesis de la temática estudiada en el componente formativo, comenzando por “hardware” y “software” de seguridad en la red, el cual está compuesto por:

* **Seguridad de información en la red:** incluye integridad, confidencialidad, disponibilidad, análisis de seguridad de la red, análisis de riesgos, matriz de control, estimación de la vulnerabilidad, requisitos de la seguridad, revisión y actualizaciones de la política de la seguridad, ataques a la seguridad de la red (ataques pasivos y ataques activos), herramientas de seguridad (autorización, auditorías, cifrados, filtros de paquete, “firewalls”, detección de intrusos, funcionalidad) y vulnerabilidades y amenazas (vulnerabilidades del día cero, vulnerabilidades conocidas).
* **Implementación:** incluye parámetros para establecer políticas de seguridad, plan de trabajo para establecer políticas de seguridad, recomendaciones para implementar políticas y normas y procedimientos.

Material complementario

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia | Tipo de material | Enlace del recurso |
| Seguridad de información en la red | Alonso, C. G., Gabriel, D., O., Ignacio, A., A., y Elio, S., R. (2014). Procesos y herramientas para la seguridad de redes. UNED. | Libro | <https://pdfcoffee.com/procesos-y-herramientas-para-la-daaz-orueta-gabrielcb-3-pdf-free.html> |

Glosario

**Amenaza:** circunstancia que tiene el potencial de causar daños o pérdidas, puede ser en forma de robo, destrucción, divulgación, modificación de datos o denegación de servicio (DOS).

**Auditoría:** proceso que se realiza para verificar que una organización cumple con normas, políticas o estándares.

**“Backup”:** copia de respaldo de la información existente para evitar pérdidas.

**Biométrico:** sistema que utiliza rasgos humanos únicos como medio de seguridad.

**“Bug”:** propiedad no deseada de un sistema.

**Capex:** gasto de capital, costo de desarrollo o el suministro de componentes no consumibles para el producto o sistema.

**Carga destructiva:** actividad maliciosa que realiza el “malware”. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el “malware”.

**Ciberdelincuente:** persona que se dedica a cometer delitos en internet.

**Ciberseguridad:** condición caracterizada por un mínimo de riesgos y amenazas a la infraestructura tecnológica, los componentes lógicos de la información y las interacciones en el ciberespacio.

**Cifrado:** proceso de codificación de información sensible para poder evitar que esta llegue a personas no autorizadas.

**Delito informático:** comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

**DevOps:** metodología de desarrollo de “software” que integra las capas de desarrollo, pruebas, implementación, calidad y gestión.

**Encriptación:** proceso para volver ilegible información considerada importante. La información una vez encriptada solo puede leerse aplicando una clave.

**Fuga de datos:** salida no controlada de información que hace que esta llegue a personas no autorizadas.

**“Hacker”:** persona experta en tecnología dedicada a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones.

**ISO:** International Organization for Standardization.

**Opex:** costo permanente para el funcionamiento de un producto, negocio o sistema.

**Programa malicioso:** también conocidos como “malware” que contienen virus, “spyware” y otros programas indeseados que se instalan sin consentimiento.

Referencias bibliográficas

B2B Consultores. (2020). Intrusion Detection System. <https://btob.com.mx/ciberseguridad/que-es-ids-intrusion-detection-system/>

Cisco. (2005). Política de seguridad de la red: informe oficial de mejores prácticas. <https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/13601-secpol.html>

Coite, A., y Romero, H. (s.f.). Auditoría de sistema y políticas de seguridad informática. <http://www.monografias.com/trabajos12/fichagr/fichagr.shtml#POLIT>

Cómo administrar tu propio negocio. (2014). Auditoría informática y seguridad informática. Cómo administrar tu propio negocio. <https://administratunegocioencasa.blogspot.com/p/cual-es-la-relacion-entre-la-auditoria.html>

Gb-advisor. (2019). 5 recomendaciones para potenciar la seguridad informática de tu empresa. <https://www.gb-advisors.com/es/5-recomendaciones-para-potenciar-la-seguridad-informatica-de-tu-empresa/>

Guimi.net. (2009). Herramientas de seguridad de redes. <https://guimi.net/monograficos/G-Redes_de_comunicaciones/G-RCnode64.html>

Informática. (2021). Autenticación y seguridad de infraestructura. <https://docs.informatica.com/es_es/data-engineering/shared-content-for-data-engineering/10-5/guia-de-seguridad/introduccion-a-la-seguridad-de-informatica/seguridad-de-infraestructura/autenticacion.html>

Infotecs. (2019). Sistema de detección de intrusos. <https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html>

ISOTools Excellence (s.f.). Plataforma tecnológica para la gestión de la excelencia. <https://www.isotools.com.co/normas/ntc-iso-27001>

ITCFA-Fepade. (s.f.). Configuración de mecanismos de seguridad U4.6 Ataques pasivos vs ataques activos. <https://virtual.itca.edu.sv/Mediadores/cms/u46_ataques_pasivos_vs_ataques_activos.html>

Mejía, R. (2006). Administración de riesgos: un enfoque empresarial. Universidad Eafit.

Mifsud, E. (2012). Introducción a la seguridad informática. <http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1>

Noriega, C. (2016). Sistemas operativos de software libre para servidores. <https://sites.google.com/site/isctallerdesistemasoperativos1/unidad-3---sistemas-operativos-de-software-libres-para-servidores>

Seguinfo. (2008). Políticas, normas, procedimientos de seguridad y otros documentos de un SGSI <https://seguinfo.wordpress.com/2008/07/31/politicas-normas-procedimientos-de-seguridad-y-otros-documentos-de-un-sgsi/>

Seguridad en la red. (s.f.). Seguridad en la red. <https://sites.google.com/site/seguridadenlaared/concepcion-de-la-seguridad-de-la-informacion/integridad>

Sony. (2021). ¿Qué es el cifrado de redes LAN inalámbricas y por qué se utiliza? <https://www.sony.es/electronics/support/articles/00009475>

USS Seguridad. (2019). ¿Qué tipos de auditorías de seguridad informática se realizan? <https://uss.com.ar/corporativo/auditoria-de-seguridad-informatica/>

Créditos

| Nombre | Cargo | Centro de Formación y Regional |
| --- | --- | --- |
| Claudia Patricia Aristizábal | Responsable del Ecosistema | Dirección General |
| Rafael Neftalí Lizcano Reyes | Responsable de Línea de Producción | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Carlos Mauricio Tovar Artunduaga | Experto temático | Centro de Servicios y Gestión Empresarial Regional Antioquia |
| Jorge Eliécer Loaiza Muñoz | Experto temático | Centro de Diseño e Innovación Tecnológica Industrial Regional Antioquia |
| Claudia López Arboleda | Experta temática | Centro de Teleinformática y Producción Industrial Regional Cauca |
| Ana Catalina Córdoba Sus | Metodólogo para formación virtual | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Yerson Fabian Zarate Saavedra | Diseñador de Contenidos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Edward Leonardo Pico Cabra | Desarrollador Fullstack | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Jesús Antonio Vecino Valero | Diseño web | Centro Industrial del Diseño y la Manufactura Regional Santander |
| John Andrés Ayala Angarita | Desarrollo front-End | Centro Industrial del Diseño y la Manufactura Regional Santander |
| Ángela María Maldonado Jaime | Producción audiovisual | Centro Industrial del Diseño y la Manufactura Regional Santander |
| Carlos Eduardo Garavito Parada | Producción audiovisual | Centro Industrial del Diseño y la Manufactura Regional Santander |
| Gilberto Junior Rodríguez Rodríguez | Producción audiovisual | Centro Industrial del Diseño y la Manufactura Regional Santander |
| Lina Marcela Pérez Manchego | Producción audiovisual | Centro Industrial del Diseño y la Manufactura Regional Santander |
| María Carolina Tamayo López | Producción audiovisual | Centro Industrial del Diseño y la Manufactura Regional Santander |
| Víctor Raúl Cárdenas Cáceres | Producción audiovisual | Centro Industrial del Diseño y la Manufactura Regional Santander |
| Wilson Andrés Arenales Cáceres | Producción audiovisual | Centro Industrial del Diseño y la Manufactura Regional Santander |
| Zuleidy María Ruiz Torres | Producción audiovisual | Centro Industrial del Diseño y la Manufactura Regional Santander |
| Jenny Paola Montillo Gélvez | Validación de diseño y contenido | Centro Industrial del Diseño y la Manufactura Regional Santander |
| Edward Leonardo Pico Cabra | Actividad Didáctica | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Zuleidy María Ruiz Torres | Validador de Recursos Educativos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Luis Gabriel Urueta Álvarez | Validador de Recursos Educativos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Daniel Ricardo Mutis Gómez | Evaluador para contenidos inclusivos y accesibles | Centro Industrial del Diseño y la Manufactura - Regional Santander |