Seguridad en la red

Breve descripción:

Este componente formativo aborda aspectos generales y claves sobre la gestión de la seguridad de redes informáticas y la información que en ellas circula. Mediante el estudio responsable de todos los temas, el aprendiz se afianzará en seguridad, ataques, clasificación de “software”, políticas de seguridad y normativa.

Noviembre 2023

Tabla de contenido

Introducción

Tenga una cordial bienvenida al estudio de este componente denominado **Seguridad en la red**. Comience explorando el video que se propone enseguida, en el cual usted podrá tener una noción general de los temas que se desarrollarán.

¡**Adelante**!

Video 1. Seguridad en la red

Enlace de reproducción del video

Síntesis del video: Seguridad en la red
Junto con el monitoreo de la red, la seguridad se constituye en una premisa inquebrantable de cualquier organización que posea una infraestructura informática… Por dicha infraestructura, circula el activo más preciado de cualquier empresa y que representa los cimientos sobre los cuales se erige y, al mismo tiempo, representa su desarrollo funcional.

Hoy en día, el presupuesto asignado en las empresas para temas de seguridad en la red, es uno de los más altos, pues se reconoce que los datos son la materia prima necesaria para hacer crecer a la organización misma y reafirmar su razón de ser.

Conocer y apropiarse de todos los elementos que constituyen la gestión de la seguridad de las redes es clave y fundamental para, además, promover la cultura de la responsabilidad con la información, el uso adecuado de los datos, el respeto por la privacidad de personas y compañías, entre otras.

Ningún proceso de seguridad será efectivo si se desconocen las causas, las maneras y mecanismos en que se producen los riesgos, los ataques y las vulnerabilidades.

He ahí la importancia de asumir con carácter, seriedad, compromiso y profesionalismo, todos los saberes necesarios para la atención y prevención de problemáticas y eventos inseguros en las redes de información.

1. ¿Qué es la seguridad de la red?

La seguridad en la red es un campo especializado que contempla el uso de múltiples herramientas tecnológicas que van desde dispositivos de "hardware" y "software" que, en principio, evitan el ingreso y propagación de una gran variedad de amenazas y ataques.

Las organizaciones, entonces, deben:

- Promulgar políticas y controles de acceso a los recursos de la red.
- Permitir verificar e identificar accesos no autorizados.
- Hacer búsqueda permanente de vulnerabilidades que pueda tener la red de datos de la organización.

El siguiente video, explica en detalle las generalidades más destacadas de la seguridad en la red; preste suma atención:

Video 2. Generalidades de seguridad en la red

Enlace de reproducción del video

Síntesis del video: Generalidades de seguridad en la red
A la hora de hablar de seguridad en la red se debe tener en cuenta que estas son las actividades y medidas tomadas por la organización a fin de asegurar el correcto funcionamiento, la confiabilidad e integridad de una red y sus datos. Los objetivos principales de la seguridad en la red incluyen: confidencialidad, integridad y disponibilidad. La seguridad de la información comprende la protección de la información de acceso, uso, revelación, interrupción, modificación o destrucción no autorizado. La confidencialidad de los datos, está garantizada por la criptografía. La integridad de datos, es certeza de que los datos enviados no han sido alterados en tránsito. La autenticación de origen permite verificar la originalidad de la información recibida. La disponibilidad de datos es una forma de medición de la accesibilidad a los datos o recursos. Una red segura, promueve la efectiva gestión del acceso a la misma. Por tal motivo, las ubicaciones de la infraestructura como “racks” o gabinete de red y centros de datos, deben permanecer con acceso restringido, de forma segura. Al implementar herramientas de seguridad en la red, la organización debe hacer partícipes a todos los usuarios, generar y promover acciones para garantizar la correcta difusión y aplicación de las políticas de protección de los datos.

Incluyendo la prevención de ataques maliciosos, es clave la denegación del acceso a información sensible de la red.

El flujo de información en las redes de datos tiene su protocolo de encriptación que le permite ocultar dicha información.

El uso de la criptografía puede ser ampliamente usado en casi cualquier comunicación de datos.

1.1. Causas de la inseguridad

Las organizaciones apuestan por el uso de sistemas de información que se componen de redes e infraestructuras tecnológicas; estas, a su vez, intercambian, de manera constante, datos valiosos, los cuales son vulnerables y pueden sufrir amenazas y ataques que afecten la confidencialidad, integridad y disponibilidad, tanto de datos como de recursos informáticos que preste la organización.

Las siguientes, son las principales vulnerabilidades presentes en un sistema informático:

Tabla 1. Familias de vulnerabilidades

Ámbitos físicos	Ámbitos organizativos	Ámbitos tecnológicos
Falta de redundancia y de recursos a nivel de equipo.	Falta de: • Recursos humanos y personal cualificado. • Comunicaciones.	Fallos en: • Los servicios y aplicaciones web y las bases de datos. • Recurrencia y falta de supervisión de incidentes.

Ámbitos físicos	Ámbitos organizativos	Ámbitos tecnológicos
Acceso a salas de informática no seguras.	Falta de: • Controles periódicos. • Documentos de procedimientos adaptados a la empresa. • Medios relativos a los riesgos.	Falta de: • Actualizaciones y parches de los sistemas operativos. • Control suficiente sobre los programas malintencionados.
Ausencia o mala estrategia de protección de datos.	Complejidad funcional.	Mala utilización del correo.

Nota: adaptada de Carpentier (2016).

La inseguridad en los sistemas informáticos incluye el estudio de los activos, las amenazas y los riegos. Para definir y demarcar el concepto de inseguridad informática, tenga en cuenta la especificación de los siguientes elementos:

a. **Activos**. Pueden estar representados por equipos, "hardware", programas informáticos, patentes, procesos y actividades de negocio.
b. **Amenazas**. Es alguien o algo que puede explotar una vulnerabilidad para obtener, modificar o impedir el acceso a un activo o comprometerlo. El conocimiento de los diferentes tipos de amenazas puede ayudar en la determinación de su peligrosidad y los controles apropiados para reducir su impacto potencial.
c. **Tipos de amenazas**. Entre las cuales están:

- Amenazas de “hardware”: daño físico a dispositivos de red o a su respectivo cableado y estaciones de trabajo.
- Amenazas ambientales: extremos de temperatura o extremos de humedad.
- Amenazas eléctricas: perturbaciones de voltaje, suministro de voltaje insuficiente, y caída total de la alimentación.
- Amenazas de mantenimiento: descarga electrostática, falta de repuestos críticos, cableado y etiquetado deficientes.

d. Riesgos. Es cada posibilidad de que un evento crítico aparezca. Su evaluación permite establecer las acciones para reducir y mantener la amenaza a un nivel razonable y aceptable. Estos mismos pueden clasificarse en externos e internos.

1.2. Clasificación de los ataques

La mayoría de las amenazas en la red se encargan de revelar las vulnerabilidades de la seguridad en la red de datos. Las agresiones a las redes de comunicaciones se pueden determinar como acciones deliberadas en aras de corromper o violar su seguridad.

El intruso emplea algún tipo de ataque informático a la hora de establecer un acceso no autorizado al sistema y estas agresiones se pueden clasificar en dos grupos, así:

a. Ataques pasivos. Este tipo de ataque consiste en monitorear los canales de comunicación sin alterar información alguna.

b. **Ataques activos**. Este tipo de ataque engloba alguna modificación del flujo de datos o la creación de datos falsos.

Los ataques pasivos están relacionados, principalmente, con el contenido del paquete y con el monitoreo del tráfico en red. El objetivo del ataque es capturar la información que está siendo transmitida, donde su principal objetivo es la vigilancia de la red a fin de descubrir vulnerabilidades a través del mapeo de la red y de los servicios prestados.

Este tipo de ataques también pueden ser llamados ataques de reconocimiento, los cuales suelen ser un requisito previo para que otros ataques obtengan acceso no autorizado a la red o interrumpan sus operaciones.

Entre las herramientas de ataque de reconocimiento están las siguientes:

a. **Búsqueda de información en Internet**. Pueden revelar información sobre quién es el dueño de un dominio en particular y qué direcciones han sido asignadas a ese dominio.
b. **Barridos de "ping"**. Técnica de escaneo de redes básicas que determina qué rango de direcciones IP corresponde a los hosts activos.
c. **Escaneo de puertos**. Escaneo de un rango de números de puerto TCP o UDP en un "host" para detectar servicios abiertos.
d. **"Sniffers" de paquetes**. Aplicación de "software" que utiliza una tarjeta de red en modo promiscuo para capturar todos los paquetes de red que se transmitan a través de una red de área local (LAN).

Ataques de activos

En este tipo de ataque, principalmente, se busca la alteración de los recursos donde se intenta borrar, añadir o modificar los datos que se transmiten en la red; igualmente se afecta la prestación de los servicios de la organización. Un atacante activo amenaza los tres pilares de la seguridad (confidencialidad, integridad y disponibilidad).

Los tipos de ataques activos más comunes son:

a. **Denegación del servicio**. Estos envían un número excesivo de solicitudes en una red o en internet, lo que ocasiona que la calidad de funcionamiento del dispositivo de red que gestiona las solicitudes colapse, es así que los usuarios u organización se ven privados del acceso a las aplicaciones y procesos que normalmente se prestan.
b. **"Phishing"**. Es la capacidad de duplicar una página web a fin de usurpar la original de ahí el usuario que accede a dicha página se cree que es la auténtica.
c. **"Spam"**. Envío de correo electrónico que puede ser enviado en forma individual o masiva, estos mensajes pueden contener información variada que no fue solicitada por el destinatario de la información.
d. **"Spoofing"**. Es la suplantación de identidad, se aplica la falsificación en una transmisión de datos donde el atacante por medio de agentes maliciosos se hace pasar por una entidad o un usuario a fin de obtener información privada o el uso de credenciales falsas.

e. **“Main in the Middle”**. Se basa en la ubicación del atacante en medio de una comunicación entre dos entes, que busca leer o modificar la información transmitida entre las dos partes.

f. **Código malicioso**. Este puede ser representado en “hardware”, “software” o “firmware” el cual es alterado intencionalmente con código no autorizado a fin de incorporar virus, troyanos, gusanos, entre otros “malware” que permitan vulnerar los sistemas informáticos.

g. **“Hoax”**. Estos mensajes principalmente se envían vía correo electrónico que suele pertenecer a una cadena de información que busca ser difundida en la red, su principal finalidad es la obtención de direcciones de correo electrónico, o congestión de la red y de los servidores de correo.

Atacantes

Soriano (2014), define al atacante como el “Individuo que obtiene, o trata de obtener, permisos o acceso no autorizado al sistema de información”. Se debe resaltar que no solo existen atacantes externos o intrusos, sino también se deben considerar a los individuos internos a la organización.

Un atacante interno puede ser representado por cualquier usuario que pertenece a la organización y tiene acceso al sistema de información y a la infraestructura tecnológica de la red.

En relación con los atacantes, tenga en cuenta algunos aspectos destacados como:

a. **Espionaje**. Este tipo de atacante principalmente realiza una tarea de espionaje en búsqueda de vulnerabilidades que puedan usar para acceder a datos,

recursos y servicios al cual no tiene acceso autorizado poniendo en peligro a la información confidencial de la organización y así mismo, a los servicios que presta.

b. **Cuando son externos**. Por su parte, un atacante externo es generalmente un individuo o sistema de inteligencia artificial que no tiene ninguna relación directa con la empresa, sino que busca principalmente acceder al sistema informático y de la red, violando la seguridad aprovechando las vulnerabilidades que se presenten.

c. **"Hacking"**. Usualmente se usa el término "hackear" que según el MinTIC (2021) es "el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar", es así como al individuo que realiza dichas actividades usualmente se le denomina "hacker".

2. “Software” malicioso

Mantener la seguridad de la red y de la información que comparten los usuarios, requiere de vigilancia por parte de los profesionales responsables de la seguridad en redes, donde es de vital importancia estar atentos a los diferentes ataques y evolución de las amenazas.

El estudio de las diferentes vulnerabilidades de los dispositivos de red y sus correspondientes aplicaciones requieren una atención especial a fin de estar preparados de los posibles ataques que provengan desde el exterior, así como el interior de las organizaciones, captando errores y falencias en las conexiones en la red.

“Las principales vulnerabilidades de los dispositivos finales son los ataques de virus, gusanos y troyanos”. Ariganello (2020) (p. 291).

Tenga en cuenta:

- Estos programas maliciosos son solo una pequeña gota en el inmenso océano de amenazas a una red de información.
- Se hace necesario entonces la implementación de todo tipo de mecanismo de seguridad de acceso a la red.
- Los piratas informáticos solo requieren de un computador y “software” especializado para inmiscuirse en la red de información.
- No es necesario ningún contacto físico en ella.
- El “malware” o “software” malicioso se refiere a todos aquellos programas cuyo único propósito es realizar tareas dañinas afectando el “software” del sistema y averiando el correcto uso del “hardware”.

- El “malware” o “software” malicioso se instala en la máquina objetivo sin consentimiento del usuario.
- Cuando un “malware” se ejecuta puede alterar algunas prestaciones de la máquina infectada como lo puede ser la velocidad, las tareas que el usuario desea realizar y obtener información crítica del sistema.

2.1. Clasificación de “malware”

Para realizar una categorización del “malware” y de la proliferación de las amenazas presentes en la red, es necesario conocerlos, estos son:

a. **Código malicioso**. Son aplicaciones que pueden ejecutar dos funciones: primero, la posibilidad de replicarse o reproducirse y, segundo, la posibilidad de ataque mediante una carga nociva. Al código malicioso normalmente se le discrimina con el nombre de virus.
b. **Virus**. Bloque de código que se introduce en un huésped para propagarse, pero hay que ejecutarlo para que se active. Es diferente del gusano (“worm”), que se propaga por el correo electrónico o por fallos de la red. El gusano no contiene, necesariamente, una carga nociva.
c. **Troyanos**. Hay algunos programas furtivos dentro de los cuales se encuentran, principalmente, el troyano o “caballo de troya”. Se hacen pasar por archivos legítimos para engañar a víctimas para que, al clicarlos, se activen o instalen.
d. **“Spyware”**. Es una subcategoría del troyano; es un “software” que se instala sin que el usuario reciba una constancia de tal acción. Suele recopilar información y compartirla con terceros.

e. **“Rasnsomware”**. Tipo de “malware” que basa su funcionamiento en el robo o secuestro de información por la que se suele cobrar un rescate y, así, restaurar el acceso a los datos y evitar posibles daños posteriores.

2.2. Ciclo de vida de un virus

Con la proliferación de diversidad de virus informáticos, la seguridad del sistema se ha vuelto prioritaria. Los virus tienden a ser destructivos y se propagan a través de las redes haciendo copias de sí mismo; cuando llegan a un dispositivo, los virus normalmente empiezan a infectar y replicarse en el equipo destino del ataque o puede permanecer inactivo a la espera de que el usuario ejecute el programa infectado.

Estas son las fases por las que puede pasar un virus informático:

Figura 1. Fases del virus informático

Las fases de un virus informático, según la figura inmediatamente anterior, son:

- Fase durmiente, donde el virus no está activo.
- Fase de propagación, donde se replica y almacena copias en archivos.
- Fase de activación, en la cual inicia su estado activo.

- Fase de ejecución, en la que realiza tareas y código maliciosos, dañando el dispositivo.

Conozca otros aspectos clave sobre los virus informáticos, consultando el video que, a continuación, se propone:

Video 3. Ataques a la seguridad de la red

Enlace de reproducción del video

Síntesis del video: Ataques a la seguridad de la red
En este video se amplían y detallan conceptos clave ya trabajados en el componente formativo, tales como: ataques, seguridad, vulnerabilidad. Se describen, también, variados tipos de ciberataques entre los que destacan los ya tratados en este componente y otros como “keyloggers”, “adware”.

3. Servicios de seguridad y mecanismos de seguridad

Un servicio de seguridad, es una prestación que avala que todos los procesos que involucran la transferencia de datos e información, tendrán la seguridad apropiada. Esto se logra por medio de políticas establecidas en cuanto a seguridad de la información se refiere.

Según Dordoigne (2020), dentro de los servicios de seguridad que se deben mantener están:

a. **Control de acceso al sistema**. Consiste, básicamente, en la protección física de los dispositivos de red, los sistemas operativos y otras aplicaciones. Estos deben protegerse mediante la configuración e instalación periódica de parches. Las redes pueden separarse entre sí y las comunicaciones deben filtrarse. El "software" antivirus debe instalarse y mantenerse en todas las estaciones de trabajo.
b. **Gestión de permisos**. Los "softwares", especialmente los sistemas operativos, utilizan su propio sistema de habilitación de accesos a los archivos o a los datos. Por ejemplo, Microsoft Windows utiliza los permisos NTFS, nombre tomado del sistema de archivos. Los sistemas Unix/Linux tienen una gestión basada en los accesos de lectura ("read"), de escritura ("write") y de ejecución ("execute").
c. **Integridad**. Verificar la integridad de la transferencia significa asegurarse de que no se realicen cambios entre el remitente y el destinatario.
d. **No denegación**. Este servicio lo proporciona la firma electrónica, que se puede utilizar en sitios web (validación de procedencia de los datos), en mensajes de correo electrónico, en el interior de un archivo, entre otros.

e. **Autenticación**. Si un equipo está en red, se requiere de un mecanismo de reconocimiento de identidad o "logueo" y uno de comprobación de dicha identidad.

f. **Confidencialidad**. Principalmente, se aplica el sistema de criptografía; para esto se realiza una transformación, llamada codificación de la información confidencial, el texto sin protección. El resultado es un texto cifrado o criptograma. El texto original se encuentra normalmente a través de una operación de descifrado.

4. Seguridad en servicios de red

La interconexión de redes presenta una amenaza que requiere de atención a la hora de establecer la seguridad en el ingreso y salida de información a la red interna privada.

Se pueden aplicar diferentes herramientas de protección, entre las que se encuentran:

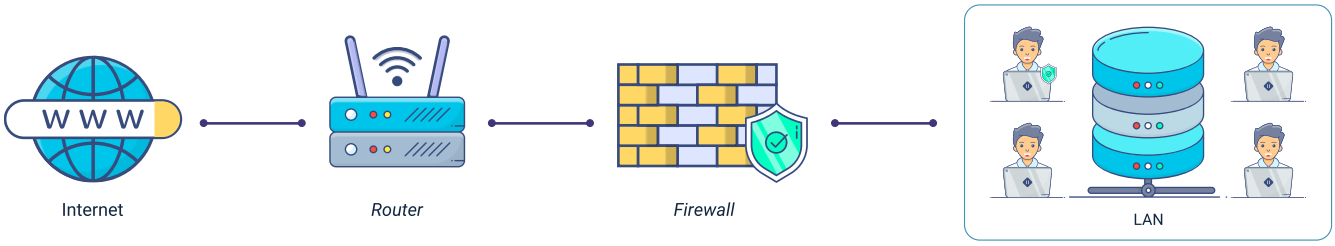
a. **"Router" de filtrado**. En los dispositivos de red se deben establecer mecanismos de filtrado que permitan llevar a cabo el bloqueo de direcciones IP y, a su vez, la prohibición de transmisión de protocolos de capa de red o de transporte utilizados (UDP, TCP o ICMP).
b. **Traducción de direcciones de red (NAT)**. Las grandes empresas pueden utilizar la misma dirección IP en las estaciones de trabajo, en varias redes conectadas. Para permitir la comunicación entre nodos en ambos lados, la referencia del remitente del paquete debe cambiarse para realizar una transmisión confiable sin conflictos.
c. **Protocolo TLS**. Es un protocolo estandarizado por la IETF ("Internet Engineering Task Force"); este proporciona seguridad de las comunicaciones a través de Internet. El objetivo principal de este protocolo es proporcionar confidencialidad e integridad de datos entre dos entidades que se comunican. Un uso importante de TLS es proteger el tráfico de la "World Wide Web" permitiendo transacciones seguras de comercio electrónico.
d. **Seguridad en el correo electrónico**. Al enviar información a través de correo electrónico es necesario la implementación de técnicas de cifrado para evitar la visualización y modificación del mensaje.

5. Seguridad Perimetral

Como medida de seguridad perimetral por implementar, está el denominado cortafuegos o “firewall”, el cual se encarga de convertir las diversas redes a las que se conecta, en independientes. Al contrario que un “router”, no se conforma con transmitir la petición. Un cortafuegos segmenta los flujos asumiendo él mismo las peticiones. Para esto, establece dos conexiones y puede realizar una acción de autentificación.

El cortafuegos de infraestructura suele ir acompañado de un cortafuegos personal, instalado en los equipos de trabajo. Así, los equipos se protegen de ataques que podrían proceder, incluso, de dentro de la red local.

Figura 2. Conexión, en red, del “firewall”



Nota: adaptado de Dordoigne (2020)

Según lo muestra la figura, la protección de los equipos se da con la instalación del cortafuegos así:

- Internet
- “Router”
- “Firewall”
- LAN

La primera generación de estos equipos permitía distintos análisis en las cabeceras de los paquetes, de manera equivalente a los "routers" filtrantes. El cortafuegos de tabla de estado ("State full inspection"), más reciente, conserva en memoria una tabla de las conexiones establecidas. Así, las comunicaciones entre clientes, autorizadas después de la autentificación, pueden continuar sin problema.

La nueva generación de cortafuegos, llamada de aplicación, es capaz de analizar algunos cuerpos de paquetes, como los de los protocolos SMTP, HTTP. Este nivel de análisis permite atenuar las nuevas formas de ataque que se aprovechan de los fallos de las aplicaciones estándar.

Un complemento del cortafuegos es el servidor "proxy"; se utiliza particularmente en el ámbito del tráfico "Hyper Text Transfer Protocol" (HTTP) o, incluso, con "File Transfer Protocol" (FTP), en la red LAN e Internet. El servidor "proxy" intercepta una petición hacia el exterior, la redirecciona como si fuera suya y, seguidamente, almacena los datos recibidos. Por último, este los envía al solicitante inicial.

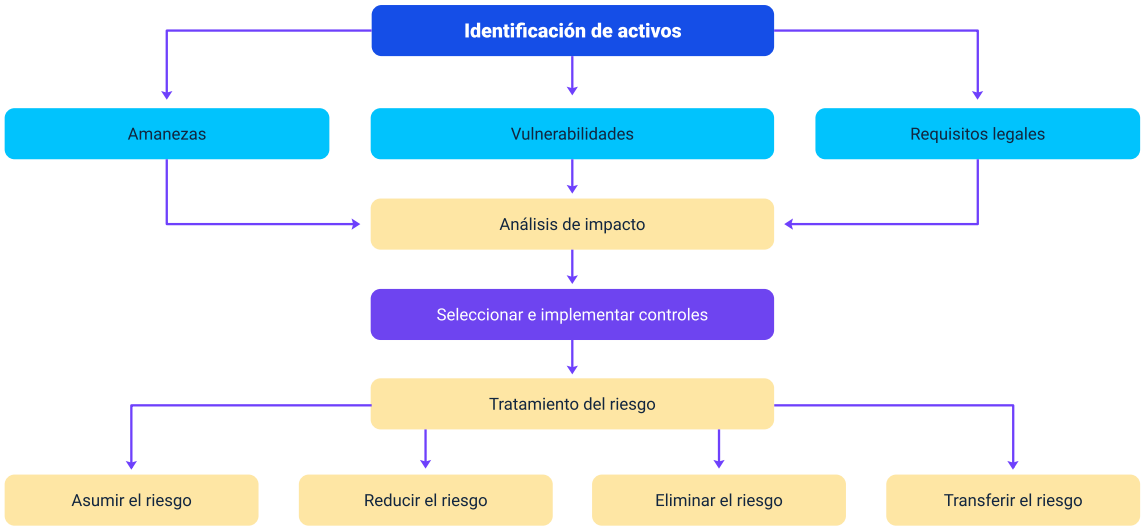
6. Políticas de seguridad

La organización debe integrar a sus mecanismos de seguridad, las políticas que rigen el correcto uso de los recursos de red, el uso de la información y el intercambio de la misma. Los usuarios de los equipos (estaciones de trabajo, servidores, centros de datos, entre otros) deben hacerse cargo y responsabilizarse de sus actividades en el marco de la utilización de herramientas informáticas.

El establecimiento de las políticas de seguridad de la información se encuentra ampliamente contemplado en la norma ISO 27001 que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La misma, les permite a las organizaciones que adopten e implementen la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

Las fases de la metodología expuesta por el Sistema de Gestión de La Seguridad de la Información (SGSI) de la norma ISO 27001, se pueden resumir así:

Figura 3. Método de evaluación y tratamiento de riesgos



El método de evaluación y tratamiento de riesgos se estructura así, según la figura inmediatamente anterior:

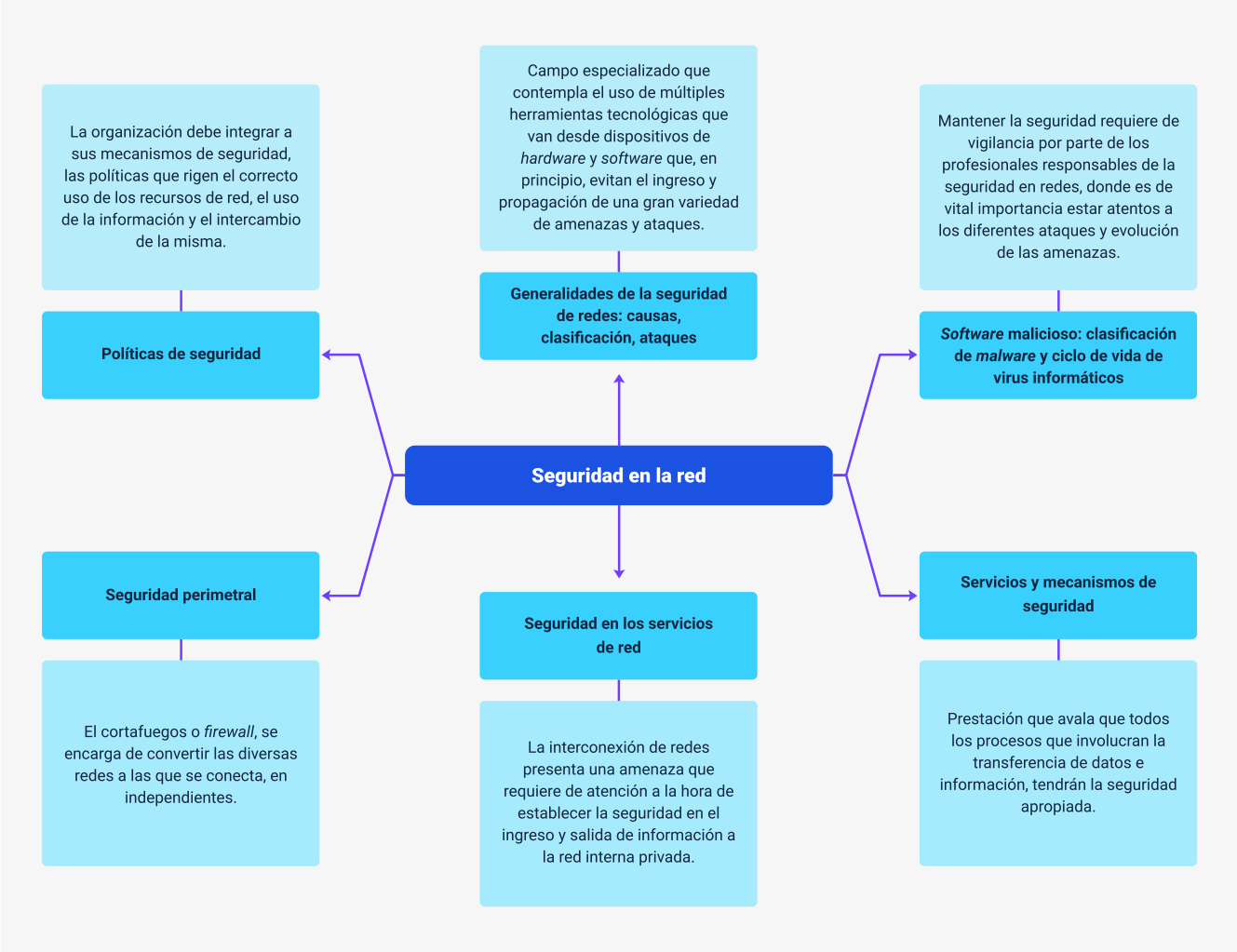
- Identificación de activos, que contempla amenazas, vulnerabilidades y requisitos legales.
- Análisis de impacto.
- Selección e implementación de controles.
- Tratamiento del riesgo, que vincula acciones como asumir el riesgo, reducirlo, eliminarlo, transferirlo.

Para definir una política robusta, eficiente y práctica, es necesario involucrar a todos aquellos usuarios que hacen uso de la red de datos, pues son ellos los que se enfrentarán a los posibles inconvenientes que puedan surgir.

Así mismo, estas políticas o indicaciones deben ser afines a las diligencias que realice la empresa y deben ser indicadas en un lenguaje que pueda ser interpretado o entendido por los usuarios de la malla.

Síntesis

Usted ha finalizado el estudio de los temas de este componente formativo. En este punto, haga un análisis del mapa conceptual que se muestra enseguida y realice su propia síntesis de los contenidos. ¡**Adelante**!



El anterior mapa de contenidos presenta el enfoque del componente formativo hacia los aspectos generales y claves de la gestión de seguridad de redes informáticas y de información. Los contenidos están orientados a la apropiación de lo relacionado con seguridad, ataques, clasificación de “software”, políticas de seguridad y normativa.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
6. Políticas de seguridad	ISOTools. (s.f.). La norma ISO 27001.	Informe - guía	https://www.isotools.us/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf
6. Políticas de seguridad	Procem Consultores. (2018, diciembre 3). ISO 27001 - Seguridad de la Información.	Vídeo	https://www.youtube.com/watch?v=BNdPQU32p2Y

Glosario

Agente: "software" programado para realizar una función específica.

"Cracking": acceso no autorizado y/o vandalismo contra los sistemas informáticos.

Dirección IP: representado por 32 "bits" que identifican a un equipo en una red. Se representa en notación decimal o binaria punteada.

Dispositivo: pieza de un equipo informático que realiza una función específica.

"Hardware": dispositivo, equipo, aparato. Parte física o tangible del ordenador.

"Host": dispositivo que participa directamente en la comunicación de la red.

SNMP: es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

Referencias bibliográficas

Ariganello, E. (2020). Redes cisco - Guía de estudio para la certificación CCNA 200-301. (1ª Ed.). RAMA.

Beekman, G. (2005). Introducción a la informática (traductor Díaz Martín, José Manuel). Pearson educación.

Carpentier, J. F. (2016). La seguridad informática en la PYME: Situación actual y mejores prácticas. Ediciones Eni.

Dordoigne, J. (2020). Redes informáticas: nociones fundamentales (protocolos, arquitecturas, redes inalámbricas, virtualización, seguridad, IPv6...). Cornellà De Llobregat, Ediciones Eni.

MinTIC. (2021). Hackear. https://www.mintic.gov.co/portal/inicio/5307:Hackear

Soriano, M. (2014). Seguridad en redes y seguridad de la información. https://www.academia.edu/40156122/Seguridad_en_redes_y_seguridad_de_la_informaci%C3%B3n

Valdivia, C. (2017). Informática Industrial 1.ª edición. Ediciones Paraninfo, S.A.

Créditos

Nombre	Cargo	Regional y Centro de Formación
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
Jorge Eliécer Loaiza Muñoz	Instructor	Centro de Servicios y Gestión Empresarial - Regional Antioquia
Carlos Mauricio Tovar Artunduaga	Instructor	Centro de Servicios y Gestión Empresarial - Regional Antioquia
Cinthia Rocío Trejos Chacón	Experta Temática	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Fabián Leonardo Correa Díaz	Fabián Leonardo Correa Díaz	Centro para la Industria de la Comunicación Gráfica - Centro de Diseño y Metrología
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
Wilson Andrés Arenales Cáceres	Storyboard e Ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carmen Alicia Martínez Torres	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniela Muñoz Bedoya	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Alfonso Bautista	Actividad Didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
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