

Aplicación de estrategias de ciberseguridad

**Breve descripción:**

Con el estudio de este componente el aprendiz estará más y mejor capacitado en el reconocimiento y aplicación de las técnicas y herramientas especializadas de gestión de la seguridad. Podrá afianzar sus conocimientos y habilidades en la implementación de controles y estrategias que garantizan la estabilidad de los pilares de la información en las organizaciones.

**Noviembre 2023**

Tabla de contenido

[Introducción 4](#_Toc152856811)

[1. Gestión de acceso 4](#_Toc152856812)

[1.1. Pasos técnicos de la gestión de acceso 4](#_Toc152856813)

[1.2. Tipos de control para gestión de accesos 6](#_Toc152856814)

[1.3. Características 8](#_Toc152856815)

[2. “Firewalls” 9](#_Toc152856816)

[3. Sistemas de detección y prevención de intrusos IDS/IPS 12](#_Toc152856817)

[3.1. Características funcionales de los IDS 16](#_Toc152856818)

[3.2. Características de los IPS 17](#_Toc152856819)

[4. Gestión unificada de amenazas UTM/XTM 17](#_Toc152856820)

[5. “Antimalware” 21](#_Toc152856821)

[6. Detección y respuesta para “endpoints” (EDR) 24](#_Toc152856822)

[6.1. Aspectos clave de los EDR 24](#_Toc152856823)

[6.2. Tipos de soluciones de seguridad para “EndPoint” 25](#_Toc152856824)

[6.3. Características de las soluciones de seguridad 27](#_Toc152856825)

[7. Cifrado 28](#_Toc152856826)

[8. Fuga de información 29](#_Toc152856827)

[8.1. Prevención 31](#_Toc152856828)

[8.2. Recomendaciones para las organizaciones 31](#_Toc152856829)

[9. Dispositivos móviles 33](#_Toc152856830)

[9.1. Riesgos asociados 33](#_Toc152856831)

[9.2. Control 35](#_Toc152856832)

[10. GuíaNIST-SP800-114 35](#_Toc152856833)

[10.1. Aspectos importantes de la guía 35](#_Toc152856834)

[10.2. Seguridad en el teletrabajo 36](#_Toc152856835)

[11. Infraestructuras críticas 37](#_Toc152856836)

[12. Mejoras de ciberseguridad en infraestructuras 39](#_Toc152856837)

[13. Sistemas de correlacionamiento de “logs” y monitoreo 39](#_Toc152856838)

[14. Gestión de eventos e información de seguridad SIEM 41](#_Toc152856839)

[15. Parcheado y/o actualización 43](#_Toc152856840)

[Síntesis 47](#_Toc152856841)

[Glosario 48](#_Toc152856842)

[Material complementario 49](#_Toc152856843)

[Referencias bibliográficas 50](#_Toc152856844)

[Créditos 52](#_Toc152856845)

Introducción

En el ejercicio de implementación de las estrategias de seguridad se debe partir de los objetivos de seguridad propuestos, así como de la declaración de privacidad, lo cual indica los controles que habrían de ser adoptados en la organización y con ello, garantizar la seguridad de la información.

En este componente formativo podrá hacer un recorrido por algunas técnicas y herramientas, según el modelo y los estándares técnicos, que respondan de manera pertinente a la planificación en su organización, a la vez que profundiza en ellas.

# Gestión de acceso

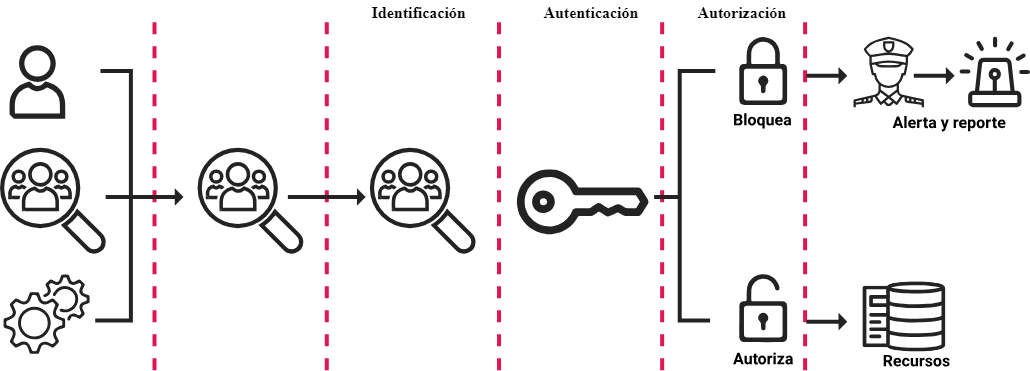
La información se considera uno de los activos más importantes para las organizaciones, debe contar con mecanismos que garanticen que, únicamente las personas autorizadas puedan acceder y realizar las acciones pertinentes y asociadas a sus funciones.

Es, en dichos mecanismos, en donde la gestión de acceso cobra un gran valor ya que permite controlar y fijar condiciones bajo los cuales un usuario pueda hacer uso de estos activos.

## Pasos técnicos de la gestión de acceso

De acuerdo con el Instituto Nacional de Ciberseguridad de España, un objetivo de este control es “establecer quién, cómo y cuándo puede acceder a los activos de información de la empresa y registrar convenientemente dichos accesos” (INCIBE, 2017); esto indica el establecimiento de controles que permitan una adecuada gestión de los permisos de los usuarios u otros sistemas de información para interactuar con los activos de una organización.

1. Pasos de un control de gestión de acceso



Nota. Adaptado de ICHI.PRO - Introducción a la gestión de identidades y accesos.

Durante el acceso a los sistemas de información se deben llevar a cabo una serie de **pasos técnicos,** los cuales debenvalorarse para gestionar una adecuada autorización y acceso a los recursos requeridos; estos son:

1. **Identificación**: permite identificar particularmente un usuario o un sistema con un identificador único y diferenciarlo de otros.
2. **Autenticación**: permite validar que el usuario o sistema que intenta acceder a un recurso es quien dice ser, mediante la validación de un mecanismo, por ejemplo, contraseña, pin, *token* o cualquier otro mecanismo asociado.
3. **Autorización**: consiste en el permiso específico sobre el recurso al cual desea acceder, por ejemplo, un rol en una tabla de una base de datos.
4. **Importante:** como factor fundamental de este control se debe considerar contar con mecanismos de auditoría que registren y/o alerten sobre accesos no permitidos, no autorizados o fallidos.

## Tipos de control para gestión de accesos

El control para la gestión de los accesos puede ser abordado desde diferentes frentes de gestión o con distintas técnicas de control. La aplicación de dichos controles de gestión de accesos es un factor de garantía de la seguridad de la información en la organización; pero no solo de esta, sino, además, de los activos de información, las personas, la infraestructura, entre otros.

Identifique, a continuación, algunos de las más comunes y funcionales controles:

1. **Por complejidad del control**

* Básicos: su implementación no requiere de mayor esfuerzo, ni ajustes en los sistemas de información; pueden abordarse con capacitaciones y controles básicos.
* Avanzados: requieren de herramientas avanzadas y establecimiento de políticas y controles.

1. **Controles según tipos de accesos**

En los tipos de accesos a sistemas de información se consideran estos controles:

* Control para la gestión de usuario.
* Control de accesos a dispositivos.
* Control de acceso a sistemas de información y activos.
* Control de acceso a recursos de red.

1. **Control para la gestión de usuario**

* Política para gestión de usuarios (activación, actualización y desactivación).
* Controles para creación de usuarios nuevos.
* Controles para la actualización de usuarios nuevos.
* Controles para la desactivación de usuarios nuevos.
* Controles para gestionar los permisos sobre los recursos.
* Controles para gestión de contraseñas de usuarios.
* Controles que permitan auditar los permisos de los usuarios sobre los recursos.

1. **Control de accesos a dispositivos**

Controles para conexión desde dispositivos autorizados, controles para identificación y autenticación de usuarios a través de dispositivos autorizados, controles para gestión de contraseñas, controles para uso de recursos de dispositivos invitados, controles para control de horarios y tiempo de uso de dispositivos.

1. **Control de acceso a los sistemas de información y activos**

* Controles para el acceso a los sistemas de información.
* Restricción de acceso a sistemas de información críticos o importantes.

1. **Control de acceso a recursos de red**

Política para acceso a servicios compartidos a través de la red, controles para autenticación de conexiones foráneas, controles de identificación de dispositivos de red, controles de endurecimiento y restricción al acceso de puertos de servicios de red, controles para la interconexión con otras redes, controles para la gestión enrutamiento y tráfico a través de red.

Como es evidente, hay una amplia variedad de controles que deben ser tenidos en cuenta, de acuerdo con las necesidades y recursos de cada organización y con los cuales se busca mantener una adecuada gestión de la gestión de usuarios.

## Características

La implementación de los controles para la **gestión del acceso** debe contemplar ciertas condiciones que eleven la complejidad y dificulten el acceso no autorizado a los activos de información de la organización.

Algunos ejemplos se presentan a continuación:

1. **Privilegio mínimo**

Toda autorización de acceso debe darse de acuerdo con las necesidades de cada rol, por ejemplo, no hacer uso de credenciales de DBA en un usuario de conexión a través de una página web.

1. **Usuarios por defecto**

Reducir el uso de usuarios que vienen por defecto en los sistemas operativos o aplicaciones, ya que estos son utilizados en ataques de fuerza bruta.

1. **Actualización de credenciales**

Establecer los controles que requieran la actualización de contraseñas periódicamente.

1. **Uso de credenciales complejas**

Promover a través de controles el uso de contraseñas seguras.

1. **Almacenamiento de credenciales seguro**

Toda la información relacionada con información de usuarios debe almacenarse de manera segura, haciendo uso de algoritmos de cifrado unidireccional y bajo, con algún mecanismo de cifrado de base de datos.

# “Firewalls”

Son “un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad” (CISCO, 2021).

Este tipo de dispositivos son de gran importancia y se han convertido en la primera línea de defensa para la gestión de la seguridad en las organizaciones, permitiendo controlar el tráfico entre redes internas y externas.

Explore el siguiente video, en el cual se presenta una amplia explicación sobre los “firewalls”, sus funcionalidades, tipos, características y otras generalidades que enriquecerán su conocimiento y formación.

¡**Adelante**!

1. “Firewall”



[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=VIN7MJvfs34)

|  |
| --- |
| **Síntesis del video:** “Firewall” |
| Los “firewall” o también conocidos como **cortafuegos** cumplen la función de proteger los activos de información de la organización, mediante la gestión del tráfico entrante y saliente entre redes, permitiendo bloquear o acceder.  Los “firewall” cuentan con políticas para la gestión de tráfico por defecto, pero cada administrador de red puede crearlas o modificarlas de acuerdo con sus necesidades.  **Tráfico entrante**: bloquea todo el tráfico entrante y autoriza lo necesario.  **Tráfico saliente**: permite todo el tráfico saliente y restringe los destinos no deseados o peligrosos.  Para la operación de un “firewall" es necesario tener presente ciertos conceptos y definiciones que son muy comunes y que su conocimiento permite realizar una adecuada gestión.  **“Host”**: cualquier dispositivo que se encuentra conectado a la red y que cuenta con una dirección IP y/o nombre asignado.  **NAT (“Network Address Translator”)**: traductor de direcciones de red que permite establecer la comunicación desde Internet hacia un dispositivo en el interior de nuestra red.  **Paquete**: uno de los bloques que componen la información que viaja a través de la red.  **Política**: condiciones bajo las cuales se permite autorizar o denegar el tráfico entre un origen o un destino en la red.  **Puerto**: entrada lógica hacia un servicio específico, por ejemplo, puerto 80 http, 443 https, 21 ftp, etc.  **Rango de IP**: grupo de direcciones IP, agrupadas para una función o política específica. (192.168.1.10-192.168.1.20. Este número de IP no se locuta pero sí se muestra en pantalla).  **Servicio**: ofrecido por aplicaciones o sistemas para compartir información entre 2 o más sistemas a partir de la aplicación de protocolos, por ejemplo, servicio web HTTP.  **Funcionalidades**  Entre las funciones que desempeña un “firewall”se encuentran:  **Proteger** los activos de información de la organización.  **Evitar accesos no permitidos** por usuarios no autorizados hacia nuestra red.  **Controlar** la cantidad de usuarios conectados a un servicio. |

# Sistemas de detección y prevención de intrusos IDS/IPS

Existe otro tipo de soluciones que complementan la seguridad perimetral de una organización, a partir del análisis del tráfico de la red e identificando accesos no autorizados hacia algún recurso del perímetro. Los **IDS** “**Intrusion Detection System”**, *en español* Sistemas de detección de intrusión, son otro tipo de soluciones para el monitoreo de la seguridad perimetral, usada para detectar accesos no autorizados a un equipo o red.

Se presentan algunos aspectos generales y de suma importancia relacionados con los sistemas de detección y prevención de intrusión IDS / IPS. Estúdielos con atención y lleve un registro en su libreta personal de apuntes.

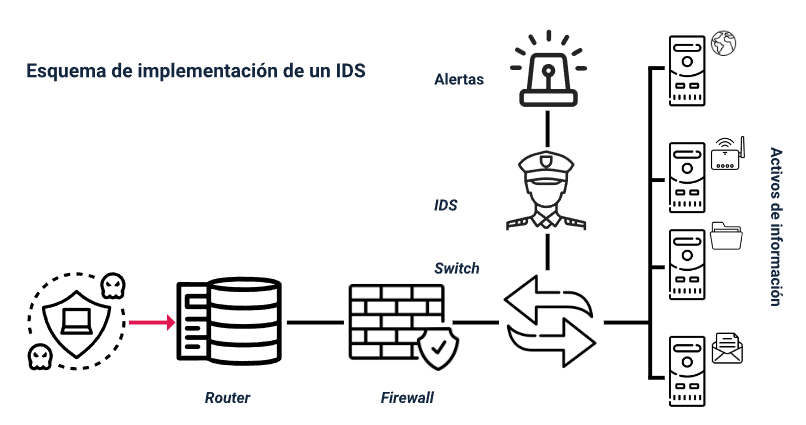
1. **Monitoreo**

Los IDS monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Este tipo de soluciones se encargan de generar los mensajes de advertencia para que el administrador de la red tome las acciones correspondientes (INCIBE, 2020).

1. **Enlace a la red interna**

Los IDS para realizar su función de monitoreo deben permanecer enlazados a la red interna, y desde su posición analizar el tráfico, confrontando comportamientos con bases de datos de diferentes fuentes para así poder emitir alertas.

**Esquema de implementación de un IDS**

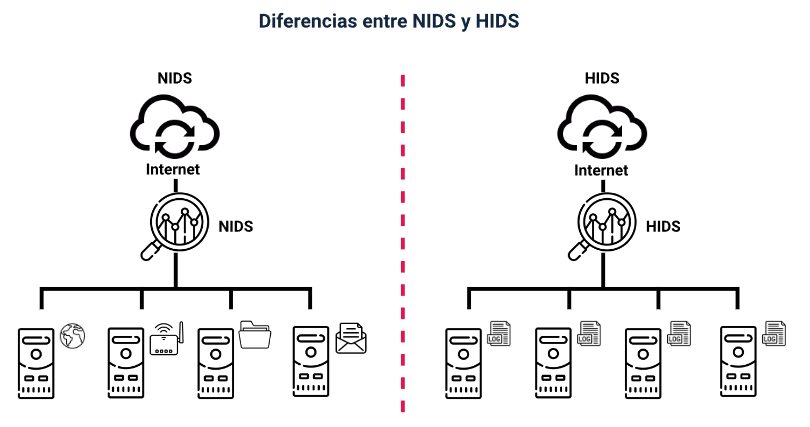


1. **Tipos de IDS de acuerdo a funcionalidad**

**HIDS “Host-based Intrusion Detection System”**: sistema de detección de intrusiones basado en *host,* analiza el comportamiento del dispositivo a partir de eventos registrados.

**NIDS “Network-based Intrusion Detection System”**: Sistema de detección de intrusiones basado en red, se encarga del análisis del tráfico que pasa por la red.

**Diferencias entre NIDS y HIDS**



1. **Clasificación de IDS, según métodos de detección**

IDS basado en firmas: presentes en NIDS y HIDS, los HIDS analizan las anomalías registradas en eventos de cualquier dispositivo de la red. También analizan sumas de comprobación de paquetes, comparándolos con firmas en bases de datos.

IDS basado en anomalías: buscan patrones de acuerdo con actividades identificadas en tráfico de paquetes. Los HIDS analizan eventos, como inicios de sesión no exitosos y reiterativos; los NIDS realizan comparaciones a partir de un comportamiento base.

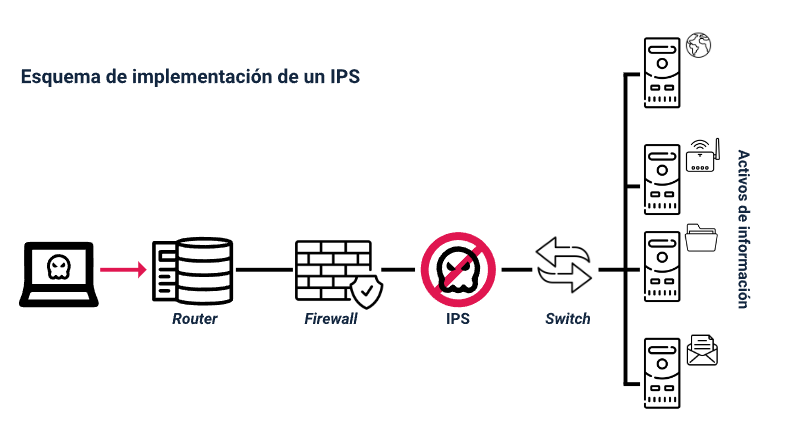
1. **IDS más reconocidos**

* Zeek: <https://zeek.org/>
* OSSEC: <https://www.ossec.net/>
* Snort: <https://www.snort.org/>
* Suricata: <https://suricata.io/>
* Security Onion: <https://securityonionsolutions.com/>
* Entre otros.

1. **IPS (Sistema de prevención de intrusiones)**

Son soluciones que permiten asegurar, de manera preventiva, los recursos de una red de ataques e intrusiones. Realizan análisis en tiempo real de conexiones, cotejan con patrones o comportamientos conocidos y tienen control para denegar paquetes, así como cerrar conexiones sospechosas.

**Esquema de implementación de un IPS**



1. **Operación desde la red interna**

Los IPS, por tener capacidad de denegar paquetes, en caso de corresponder a un comportamiento no autorizado, deben operar desde la red interna, por lo general después del “firewall” de seguridad perimetral.

En la actualidad existen muchas soluciones de tipo UTM, que incorporan estos 2 tipos de soluciones dentro de sus herramientas, permitiendo extender la cobertura y control del tráfico que circula en nuestra red.

## Características funcionales de los IDS

Tanto los IDS como los IPS cuentan con una serie de características que permiten no solo identificarlos, sino que, además, dan la opción de reconocer tareas y funcionalidades que cumplen.

Dentro de las características más relevantes de los IDS se pueden enunciar las siguientes:

* Realiza el análisis del tráfico a partir de la verificación y comparación de patrones contra bases de datos con firmas conocidas de ataques maliciosos.
* Realiza el monitoreo permanente del tráfico que pasa por la red.
* Cuenta con capacidad de monitorear el comportamiento de los sistemas de información para identificar la intención de algún ataque.
* Permite identificar cambios en las configuraciones de los dispositivos o servicios.
* Capacidad de emitir alertas en gran variedad de sistemas.
* Requiere la actualización permanente de bases de datos con firmas actualizadas.

## Características de los IPS

Tanto los IDS como los IPS trabajan de manera conjunta, conformando una **segunda línea** **de seguridad** perimetral, complementando así las acciones y funciones de un *“*firewall”.

Dentro de las características más relevantes de los OPS se presentan las siguientes:

* Complementa a los IDS, identificando y bloqueando conexiones con tráfico sospechoso.
* Permite descartar paquetes sospechosos.
* Permite bloquear direcciones sospechosas.

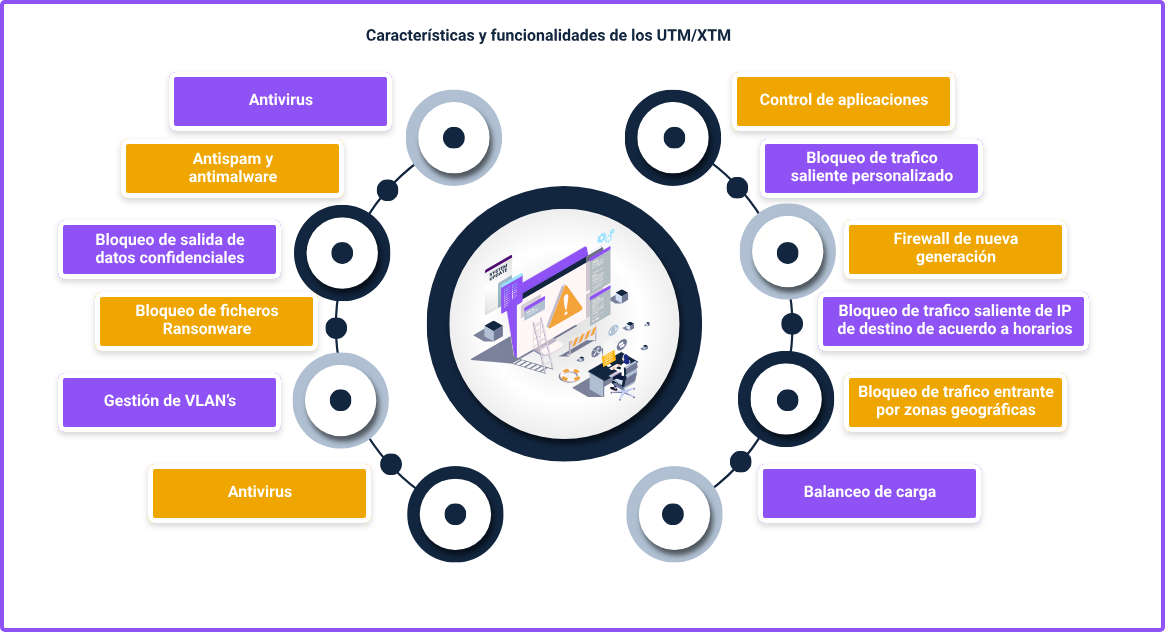
# Gestión unificada de amenazas UTM/XTM

En el reconocimiento de soluciones para la gestión de la seguridad en organizaciones hay que mencionar un tipo de producto que ha venido abarcando un amplio campo, por el hecho de integrar en un solo dispositivo soluciones como las vistas hasta ahora en este componente (“firewalls”, IDS, IPS).

Se trata del **UTM** (“Unified Threat Management”) o Gestión unificada de amenazas. Con ellos están los **XTM** (“Extensible UTM”) o UTM Extendido, los cuales cubren las necesidades básicas más comunes, requeridas por las organizaciones en una única solución.

Se presentan los aspectos generales más importantes y definitorios de estos productos (**UTM/XTM**):

1. **UTM, Gestión unificada de amenazas:** integra otras soluciones que requieren las empresas; “consolida múltiples funciones de seguridad y redes con un “appliance” unificado, que protege a las empresas y simplifica la infraestructura”, permitiendo encontrar en una sola solución herramientas como: “firewall”, IDS/IPS, antivirus, antimalware, filtrado antispam, filtrado web, acceso remoto seguro y una amplia variedad de reportes, simplificando la administración de este tipo de arquitecturas (FORTINET, 2021).
2. **XTM, por la seguridad perimetral:** XTM o UTM extendido permite ampliar capacidades del UTM, agregando en una única solución herramientas de logging, protección de la reputación, correlación de eventos, herramientas para control de acceso a la red, capacidad de gestión de vulnerabilidades, así como capacidad de gestión del ancho de banda de red y control de tráfico, extendiendo así, las capacidades de administrar de una mejor manera la seguridad perimetral.
3. **Particularidades:** este tipo de soluciones han ganado un campo de aplicación por sus capacidades de ajustarse a casi cualquier tipo de organización, facilitando su implementación y administración. Las diferencias entre este tipo de dispositivos no son tan significativas a simple vista, se requiere de un análisis de las operaciones de análisis que puede realizar para identificar cuál es la más indicada para cada organización.
4. **Más sobre UTM/XTM:** además de sus funciones de “firewall”, cuentan con herramientas como sistemas de prevención de intrusiones, antivirus, filtros de URL, red privada virtual (VPN), balanceo de enlaces, informes de seguridad, entre otros; este tipo de soluciones pueden encontrarse en presentación de hardware como **“Software”**; este modelo es muy recomendado para pequeñas organizaciones.
5. **NGFW:** tipo de “firewall” que incorpora herramientas para el análisis de amenazas recientes, así como *malware* del que frecuentemente aparecen nuevas versiones y modalidades de ataques. Se recomienda para grandes organizaciones o aquellas que presentan gran cantidad de solicitudes y acceso a través de red. El **NGFW**, particularmente, puede realizar una inspección avanzada de paquetes y permite establecer políticas para gestionar el acceso seguro a los recursos.
6. **Características:** los dispositivos UTM/XTM pueden realizar la gestión de la seguridad mediante la administración de tráfico, análisis de *malware*, control de aplicaciones y gestión de *vlan’*



* Control de aplicaciones​
* Bloqueo de tráfico saliente personalizado​
* “Firewall” de nueva generación​
* Bloqueo de tráfico saliente por IP de destino de acuerdo con horarios​
* Bloqueo de sitios web inadecuado o peligrosos​
* Bloqueo de tráfico entrante por zonas geográficas​
* Balanceo de carga​
* Gestión de VLAN​
* Bloqueo de ficheros “Ransonware”​
* Bloqueo de salida de datos confidenciales​
* Antispam y antimalware​
* Antivirus

# “Antimalware”

En la actualidad es muy común escuchar del término “malware”, pero puede no haber una definición clara del mismo; así como tampoco hay claridades unificadas sobre cómo combatirlo y evitar pérdidas o daños en los activos de información.

**El “malware”** es un término amplio que describe cualquier programa o código malicioso, dañino para los sistemas. Puede invadir sistemas de información intrusivamente, causando daños, pérdidas de información, si no se está preparado.

Existen varios tipos de “malware” y tienen un impacto diferente, dependiendo de su funcionamiento:

* “Ransomware”.
* “Spyware.
* “Adware”.
* Gusanos.
* Troyanos.
* “Robots”.

Un dispositivo afectado por “malware” puede presentar síntomas que anuncian dicha situación de afección por programas maliciosos:

* Lentitud del dispositivo.
* Falta de espacio en el disco sin causa alguna.
* Ejecución automática de programas o mensajes emergentes.
* Consumo excesivo de recursos (CPU, memoria RAM, tráfico de red, entre otros) sin razón alguna.
* Otros comportamientos relacionados.

Como mecanismos de protección y para no sufrir afectaciones por este tipo de programas se recomienda el uso de tecnologías “antimalware”, que en la actualidad vienen integradas a las soluciones de antivirus como Norton 360, Avast, Mcafee, Kaspersky. También es posible encontrar soluciones independientes como “Malwarebytes”.

* **“Software” “antimalware” autónomo**

Este tipo de programa antimalware por lo general está enfocado en ciertos tipos de “malware” y se distribuye de manera independiente sin requerir de otros componentes para su funcionamiento; este tipo de soluciones son muy comunes para la recuperación de sistemas que ya han sido afectados.

* **Paquetes de “Software” de seguridad**

Por lo general viene integrado a otras herramientas como antivirus, soluciones corporativas o centralizadas que permiten gestionar la seguridad de los dispositivos de una organización en todo momento.

* **“Software” “antimalware” en la nube**

Se integra a servicios que se encuentran en la nube y es común encontrarla en servicios de correo electrónico o de alojamiento de archivos. Generalmente cuenta con 2 componentes:

1. El cliente, que se instala en los dispositivos administrados.
2. El servicio web, que se encarga de validar la información reportada por el cliente.

Las soluciones “antimalware” deben de incorporar características importantes como:

1. **Protección frente a “malware”:** debe presentar soporte para asegurar y recuperar recursos afectados por “malware”, de manera permanente y actualizada.
2. **Facilidad de uso**: debe proveer una interfaz de fácil uso, que permita al usuario realizar sus actividades de limpieza y recuperación, sin necesidad de contar con una persona especializada.
3. **Velocidad de verificación**: debe ser rápido en el proceso de revisión, análisis y detección de “malware”.
4. **Actualización permanente**: debe proveer actualizaciones tanto de la aplicación como de las bases de datos, de manera permanente y oportuna.
5. **Consumo de recursos:** debe presentar un consumo adecuado de los dispositivos controlados, de tal manera que no afecte el desarrollo de las actividades de los usuarios.
6. **Herramientas adicionales para la gestión de “malware”**: debe proveer a los usuarios de las herramientas necesarias para el aseguramiento de sus dispositivos e información.
7. **Compatibilidad con diferentes sistemas**: debe soportar cualquier sistema operativo y ser compatible con la mayoría de aplicaciones informáticas, con el objetivo de reconocer una aplicación afectada de una original.
8. **Soporte**: debe proveer soporte técnico especializado a los usuarios que cuentan con suscripciones activas.

# Detección y respuesta para “endpoints” (EDR)

En ciertas ocasiones las soluciones no son suficientes para garantizar la seguridad de los activos de información de la organización; a pesar de todos los controles centralizados implementados, aún existe un factor que puede ser el más vulnerable y es el factor humano.

Pero, ¿cuál o cuáles podrían ser las medidas apropiadas para superar la inseguridad digital causada por el personal de la organización? Aquí, una gran solución:

* **Personal vulnerable:** el talento humano puede, de cierto modo, ser la puerta de entrada de los diferentes incidentes que pueden presentarse en la organización.
* **Soluciones adicionales:** es justo allí donde se propone otro tipo de soluciones que permiten mejorar la seguridad de los dispositivos de una red.
* **Monitoreo de cambios en dispositivos:** Se trata de los EDR (“**Endpoint Detection and Response”**), en español Detección y Respuesta de “Endpoints”*,* los cuales permiten monitorear permanentemente los cambios presentados en los dispositivos.

## Aspectos clave de los EDR

Un “**Endpoint”** puede ser cualquier dispositivo que se encuentra conectado a la red informática de la organización, por ejemplo, computadores, portátiles, teléfonos, servidores,” Tablet”, etc. La detección y respuesta de “Endpoints” son aquellas soluciones que permiten detectar y responder ante actividades sospechosas en un dispositivo, de acuerdo con su comportamiento, evitando su reproducción o réplica en otros dispositivos de la organización.

Las **EPP** (“**Endpoint Protection Platform”**), aquellas plataformas de protección “Endpoint”, son las soluciones integradas de seguridad que, por lo general, están conformadas por antivirus y “antimalware”*,* entre otros, y que operan comparando archivos con bases, si su firma corresponde.

Los XDR (**Extended Detection and Response**), Detección y Respuesta Extendidas, son una solución integral para la respuesta a incidentes, a partir de la recolección de información de los “endpoint”.

## Tipos de soluciones de seguridad para “Endpoint”

Las soluciones de seguridad “Endpoin” permiten mantener bajo permanente monitoreo y control los dispositivos administrados; lo cual favorece realizar acciones a partir de políticas establecidas por el administrador de seguridad. Dependiendo del tipo de “Endpoint”, estos pueden presentar alertas, reportar a consolas centrales e incluso, aislar un dispositivo de la red cuando se presente una advertencia catalogada como crítica.

Entre las soluciones para la gestión de la seguridad de los “Endpoint” existen los siguientes tipos de solución:

1. **EPP**

Este tipo de soluciones tiene como objetivo prevenir incidentes de seguridad en los dispositivos de la red por “malware” o cualquier otra vulnerabilidad, estas soluciones realizan la identificación a partir de los siguientes métodos:

* Análisis de amenazas a partir de la comparación con firmas conocidas.
* Bloqueo o acceso desde puertos, servicios o aplicaciones a partir de listas de control de acceso.
* Brindar soluciones “sandbox” para la ejecución de aplicaciones sospechosas.
* Utilizar análisis de comportamiento y “machine learning” para el reporte de actividad sospechosa.

1. **Componentes de trabajo articulado**

Este tipo de solución cuenta con componentes que permiten trabajar de la mano con el centro de control disponible en la red o en la nube.

1. **EDR**

Permiten generar acciones a partir de la detección de un incidente que afecte el dispositivo. Este tipo de reacción se ejecuta a partir de acciones automatizadas como manuales.

* Brindan la información necesaria para el personal de seguridad, para el establecimiento de los indicadores de compromiso.
* Presentan alertas sobre incidentes que puedan afectar el dispositivo.
* Habilitan soluciones forenses que permiten recuperar información sobre incidentes y así identificar el origen.
* Aplican soluciones correctivas de manera autónoma para evitar la multiplicación de incidentes en los demás dispositivos de la organización.

1. **XDR**

Se presenta como una solución unificada, enfocada en la gestión de seguridad y respuesta a incidentes, con funciones de correlacionador de eventos, así como de los componentes que intervienen con el dispositivo y con capacidades de interactuar con soluciones de un orden superior como los SIEM, aportando información útil para el establecimiento de una óptica de seguridad global de la organización.

## Características de las soluciones de seguridad

Dentro de las características requeridas por una solución para la detección y respuesta de “Endpoints” es importante tener presente que deben abordarse los niveles de seguridad para este tipo de dispositivos.

Explore el recurso que se presenta a continuación y descubra los niveles de seguridad para estos dispositivos. Haga la asimilación de ellos y procure llevar registro en su libreta personal de apuntes.

* **Análisis de riesgos y endurecimiento:** capacidad para realizar un inventario y su correspondiente análisis de riesgos, generar un esquema de actualizaciones, sugiriendo la aplicación de cifrado de la información, estableciendo controles de seguridad en las aplicaciones como al dispositivo en general.
* **Prevención**: prever soluciones de seguridad activa, que proteja contra cualquier amenaza que pueda afectar los activos de información administrados, a partir del monitoreo permanente y aprendizaje de los comportamientos identificados, facilitando la defensa ante cualquier comportamiento anómalo presentado desde el “Endpoint”.
* **Detección y respuesta**: brindar un monitoreo permanente que permita identificar, de manera oportuna, amenazas que puedan afectar al dispositivo, aislamiento del mismo, y realizar las acciones necesarias para la limpieza y registro de las acciones adelantadas.
* **Informes e integración**

Debe brindar las capacidades de integrarse con soluciones y sistemas de monitoreo para una visualización general de los “Endpoint” de la organización.

* **Arquitectura para soluciones EDR**

Observe y analice la arquitectura de seguridad sugerida para una solución de “Endpoint”.

**Arquitectura adaptativa por niveles de seguridad para soluciones EDR**

Imagen que muestra la arquitectura adaptativa por niveles de seguridad para soluciones EDR en 4 fases:
1. Análisis de riesgos y endeudamiento
2. Prevención
3. Detección y respuesta
4. Informes e Integración

# Cifrado

Los controles de cifrado de información se han convertido en un elemento de gran importancia para la gestión de la seguridad de la información, ya que permite proteger la privacidad de la misma al evitar que esta sea interpretada por personas no autorizadas.

**Cifrado**. Ver documento en la carpeta de anexos, para profundizar en los aspectos conceptuales, operativos y funcionales del “cifrado”, correspondiente a este componente formativo, estudie atentamente el contenido.

# Fuga de información

La pérdida de información en una organización puede presentarse por varios factores. Esta pérdida y otros riesgos, sea en el nivel que sea, pueden ser mitigados y según la eficiencia en la aplicación de los controles y soluciones, podrían llegar a tener una mínima posibilidad de ocurrencia.

Preste mucha atención a las generalidades que, a continuación, se muestran sobre la **fuga de información en las organizaciones**:

1. **¿Qué es la fuga de información?** “Incidente, interno o externo, intencional o no, que pone en poder de una persona ajena a la organización información confidencial y que solo debería estar disponible para integrantes de la misma”. Cualquier vulnerabilidad que ponga en riesgo un activo de información de la organización debe ser abordado y controlado. La Norma ISO 27001 en su Anexo A, establece tales controles.
2. **¿Por qué ocurre la fuga de información?** Diversos aspectos pueden desencadenar en fuga o pérdida de información. El **robo de información** o extracción no autorizada de la misma, el **uso de dispositivos no autorizados** como computadores personales, teléfonos móviles no autorizados para el tratamiento y transporte de información; cuando estos son extraviados u olvidados la información queda a merced de terceros.
3. **Equipos móviles y removibles en la fuga:** los dispositivos móviles facilitan la movilidad de información de manera rápida, por ello se considera de vital importancia el control de estos para la gestión de la información de la organización. Por otra parte, el **uso de dispositivos removibles** facilita la extracción de información y son un foco de infección; esto puede acarrear la pérdida de información por infección con programas dañinos.
4. **Acceso a sitios peligrosos:** pone en riesgo la información gestionada desde el dispositivo en el momento que este sea infectado, por ejemplo, con un “ransomware”. También el uso de aplicaciones no autorizadas arriesga la información, ya que posibilita el intercambio, envío o daño de información, por ejemplo, aplicaciones de información compartida como en Internet como Dropbox, Google Drive, Onedrive, Wetransfer.
5. **Tratamiento indebido de información:** causa de pérdida de la información, y está relacionada con una manipulación inadecuada de la información y de los equipos, por ejemplo, un empleado es desprendido de sus labores y él, en señal de rechazo, puede borrarla, ocultarla, alterarla o extraerla para fines de beneficio propio.
6. **Eventos accidentales:** además de estas causas mencionadas y que pueden llevar a la pérdida o robo de información, puede haber otros eventos de riesgo, de tipo accidental, dados por un indebido manejo o tratamiento, o provocados por algún empleado en desacuerdo con la organización, por ejemplo.

## Prevención

Que la organización conozca sus activos de información se considera el primer paso para tomar decisiones y acciones que prevengan incidentes relacionados con la fuga o pérdida de información.

Para un proceso de conocimiento de activos pertinente se hacen las siguientes recomendaciones:

* Identificar los activos de la información que gestiona.
* Clasificar los activos de la información de acuerdo con su criticidad e importancia para la organización.
* Identificar el grado de seguridad actual, es decir, identificar los riesgos a los que está expuesto el activo de información.
* Implementar los controles que permitan mejorar la seguridad del activo de información.

A partir de este ejercicio, se pueden establecer los controles necesarios, entre los cuales destacan:

* Cifrado de información confidencial corporativa
* Instalación, configuración y actualización de “firewall”
* Actualización permanente de aplicaciones

## Recomendaciones para las organizaciones

A las organizaciones en el marco del tratamiento de los riesgos por fuga o pérdida de información, y con mayor razón si se trata de organizaciones grandes o con gran nivel de administración de información se les recomienda el manejo de sistemas de prevención de pérdida de datos o DLP, así como la aplicación de controles orientados a la gestión del ciclo de vida de la información o ILM (“Information Lifecycle Management”).

Estas son algunas recomendaciones adicionales para las organizaciones, referente al tratamiento y control de la fuga o robo de información:

1. **De dispositivos**

Desde luego, toda organización ha de adoptar herramientas de control de los dispositivos externos de almacenamiento, removibles y en línea, para evitar fugas de información.

1. **Organizativas**

Estos controles se relacionan con «la forma» en que se maneja o se trata la información. Por lo que se recomienda prevenir malas prácticas como compartir contraseñas o activos confidenciales, o hacer uso de contraseñas que son de conocimiento general. Esto conlleva a que se cuente con políticas de seguridad apoyadas en acciones de concienciación a todo el personal.

1. **Jurídicas**

Todos los empleados y/o proveedores deben cumplir con las políticas de seguridad; las cuales, en el caso de proveedores, se deben comunicar y aceptar mediante la firma de acuerdos de confidencialidad y de nivel de servicio (SLA) para proveedores.

# Dispositivos móviles

Dentro de la Norma ISO 27001 - Anexo A, se establecen los lineamientos de controles para el uso de dispositivos móviles, en función de las consideraciones de seguridad. En este punto del componente formativo podrá ahondar en aspectos y elementos de suma importancia en lo referente a **seguridad de la información y los dispositivos móviles**.

Para contextualizar sobre la seguridad de dispositivos móviles es importante tener presente los siguientes términos:

* **Terminal:** se conoce a cualquier dispositivo móvil que permite registrar y consultar información.
* **“Smartphone”*:*** *t*eléfono inteligente que cuenta con funciones avanzadas para utilizar aplicaciones y gestionar información, estos dispositivos están compuestos por un sistema operativo, aplicaciones e información.
* **Byod (“Bring Your Own Device”):** es una tendencia por la cual optan algunas organizaciones, permitiendo que sus trabajadores utilicen sus dispositivos personales para el desarrollo de actividades laborales.
* **Política de seguridad:** son controles lógicos que se aplican a dispositivos, con el objetivo de controlar acciones o capacidades de un dispositivo móvil.

## Riesgos asociados

Son muchas las amenazas de seguridad de información que en la actualidad podrían afectar negativamente los activos de información en las organizaciones y a las cuales están expuestas, especialmente, por el uso de dispositivos móviles sin control. El uso generalizado de los mismos y la necesidad de conexión a distintas redes de información favorecen esta situación.

Entre los riesgos y amenazas más comunes y recurrentes se encuentran:

* **Aplicaciones maliciosas**: mediante las cuales se pueden instalar “app” maliciosas que pueden presentar algún tipo de filtración de dato o daño, tanto en los dispositivos como en la información.
* **Vulnerabilidades en los dispositivos:** algunas marcas o modelos no cuentan con los componentes necesarios para un sistema seguro, lo que se considera una debilidad que puede ser aprovechada por terceros para robar información.
* **“Phishing”:**esta es una de las vulnerabilidades más comunes, con la cual buscan capturar usuarios incautos para robar información, cuentas, entre otras o acceder a información de sistemas bancarios o de redes sociales, para luego pedir algún rescate.
* **Ataques basados en la red:** Problemas de malware en dispositivos, los cuales pueden tomar el control y realizar acciones no requeridas, por ejemplo, envío masivo de mensajes a los contactos o publicación autónoma en las redes sociales.
* **Ataques “**Man-in-the-Middle”***:*** teniendo presente la cantidad de información que circula en las redes hoy, este tipo de ataque permite intervenir el tráfico para capturar la información que por ellas transitan.

Adicional a estas amenazas se pueden sumar las causadas por pérdida o robo de dispositivos, lo que estaría enlazado a la cantidad de información y contenido, y si esta se encontraba cifrada o no.

## Control

De acuerdo con el control 6.2.1 de la Norma ISO 27001 Anexo A, se deben de establecer políticas que establezcan las medidas para la seguridad de la información gestionada a través de dispositivos móviles, y adoptar los controles necesarios para su administración.

Por ejemplo, se han de aplicar controles para configurar dispositivos móviles, procurando contar con un nivel básico de seguridad en los mismos.

# GuíaNIST-SP800-114

Los procesos de ciberseguridad y seguridad de la información cuentan con orientaciones de las políticas internas de las organizaciones, las leyes vigentes de cada país, diferentes a las normas técnicas internacionales y guías.

Por su parte, el Instituto NIST ofrece la guía NIST-SP800-114 para el aseguramiento de actividades realizadas bajo la modalidad de teletrabajo y la adopción de la filosofía **BYOD** para el desarrollo de las actividades contractuales.

## Aspectos importantes de la guía

La guía se encuentra estructurada por secciones que abordan los conceptos y las recomendaciones para la implantación de controles.

Las secciones destacadas de la guía y que ofrecen orientaciones fundamentales para los procesos de seguridad son:

* **La sección 2**: proporciona una descripción general del teletrabajo, el acceso remoto y una introducción a los problemas de seguridad relacionados con los dispositivos de teletrabajo.
* **La sección 3** proporciona pautas sobre cómo proteger la información almacenada o enviada desde o hacia dispositivos de teletrabajo.
* **La sección 4** presenta recomendaciones para proteger las redes domésticas alámbricas e inalámbricas que se utilizan para el teletrabajo.
* **La sección 5** trata sobre la protección de las computadoras personales (PC) BYOD, a través de métodos como la aplicación de actualizaciones de **“Software”**, la instalación y configuración de **“Software”** antivirus y *firewalls* personales.
* **La sección 6** ofrece una descripción general de la protección de dispositivos móviles BYOD.

Si la organización tiene implementado modalidad de teletrabajo, se recomienda tener presente esta guía.

## Seguridad en el teletrabajo

Las organizaciones actualmente vienen habilitando las posibilidades para que su personal pueda desarrollar sus actividades sin que necesariamente se encuentren en la sede física, atendiendo, además, la reglamentación legal y laboral, estas deben garantizar que los empleados cuenten con los recursos necesarios para el desarrollo de sus actividades, entre estas se encuentran las condiciones de seguridad.

Por lo anterior, se sugiere considerar las siguientes recomendaciones adicionales para el desarrollo de actividades bajo la modalidad de teletrabajo.

* Uso de equipos adecuados.
* Garantizar el acceso a la información, de acuerdo con las condiciones y controles de seguridad anteriormente nombrados.
* Contar con mecanismos de conexión segura, evitando hacer uso de canales abiertos y públicos.
* Proveer de herramientas actualizadas contra *malware*.
* Mantener un monitoreo permanente del tráfico de la red donde se encuentran los activos de información.
* Contar con políticas de seguridad implementadas e informadas a todo el personal.

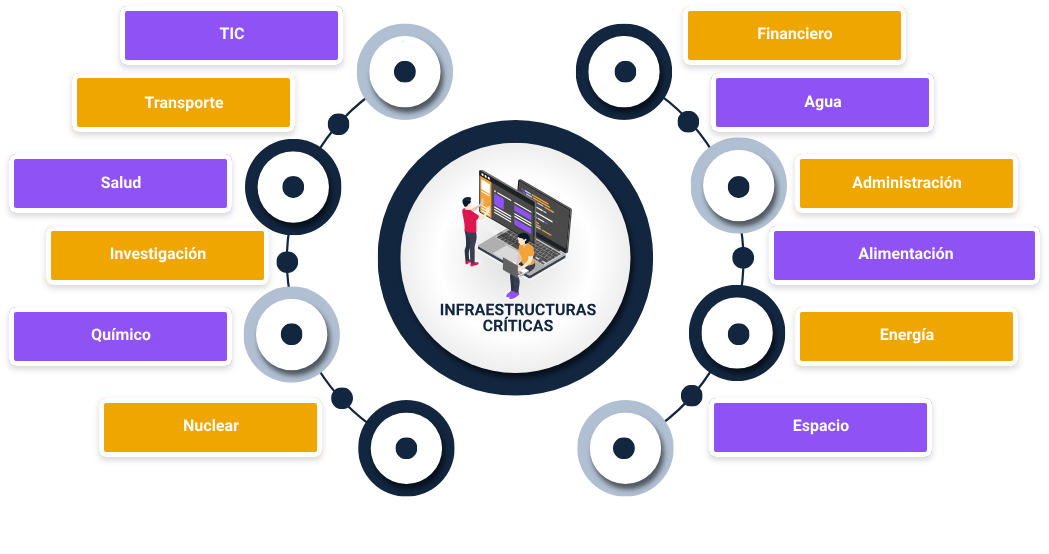
# Infraestructuras críticas

Es momento de abordar algunos conceptos importantes en el aseguramiento de infraestructuras críticas, aquellas que se han convertido en industrias de orden principal en el país. Se trata de aquellas “infraestructuras estratégicas que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales” (LISA Institute, 2020).

Un **Servicio esencial** es aquel “servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas”.

LISA “Institute”. (2020).

Las infraestructuras críticas abordan sectores primordiales para el desarrollo de las regiones. En la siguiente herramienta visualice los diferentes ámbitos de las mismas y profundice en sus aspectos clave:



* **Sistema financiero y tributario**: entidades bancarias, información, valores e inversiones
* **Administración**: servicios básicos, instalaciones, redes de información, principales activos y monumentos del patrimonio nacional.
* **Agua**: embalses, almacenamiento, tratamiento y redes.
* **Alimentación**: producción, almacenamiento y distribución
* **Centrales y Redes de energía**: Producción y distribución.
* **Espacio:** Instalaciones relacionadas con el espacio exterior
* **Centrales nucleares**: producción, almacenamiento y transporte de mercancías peligrosas, materiales nucleares, radiológicos, etc.
* **Industria química**: producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, etc.
* **Investigación**: laboratorios que por su idiosincrasia dispongan o produzcan materiales, sustancias o elementos críticos o peligrosos.
* **Salud**: sector e infraestructura sanitaria.
* **Tecnologías de la Información y la Comunicación**: TIC, ya sean infraestructuras críticas en sí mismas como redes de telecomunicaciones, o den servicio de información y comunicaciones a otras infraestructuras críticas.
* **Transporte**: aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico.

# Mejoras de ciberseguridad en infraestructuras

Para la gestión de las infraestructuras críticas, dada su complejidad, es importante contar con un marco que le permita realizar una mejora continua a su nivel de seguridad. El NIST (“National Institute of Standards and Technology”) en el año 2018 publicó el “Framework for Improving Critical Infrastructure Cybersecurity”, con el cual busca promover una adecuada gestión de los riesgos de la ciberseguridad en las organizaciones, adoptando las mejores prácticas de ISO, ITU, CIS, NIST, entre otros.

**Mejoras de ciberseguridad en infraestructuras**. Ver documento en carpeta anexos. Estudie en detalle y profundice en los aspectos más importantes en el proceso de gestión de los riesgos de la ciberseguridad en las organizaciones.

# Sistemas de correlacionamiento de “logs” y monitoreo

Los sistemas para el correlacionamiento de “logs” y monitoreo de la actividad que pasa sobre las redes y dispositivos permiten una visión actualizada del nivel de seguridad de los controles implementados. Mantener una vista del estado de la seguridad de una red requiere de herramientas que permitan representar fácilmente la información consolidada.

Tal información de monitoreo proviene de los activos de información y de los controles implementados, los cuales son los encargados de reportar las acciones realizadas.

Estos son algunos conceptos y datos clave a tener en cuenta:

1. **Correlacionados de eventos / SIEM:** estas soluciones especializadas brindan la capacidad de crear centros de monitoreo a partir de las fuentes de información recolectadas como, por ejemplo, registro de un servidor web, registros de auditoría de un servicio LDAP, etc.
2. **Sensor:** mecanismos encargados de monitorear el comportamiento de un servicio o de un dispositivo, permitiendo recolectar la información sobre algún comportamiento irregular, por ejemplo, un sensor para monitoreo de servicio web.
3. **IDS / IPS:** estos sensores pueden ser IDS, IPS, sistemas de monitoreo, como, por ejemplo, “Snort”, Suricata, etc.
4. **“Dashboard”:** también llamados tablero de control, es una herramienta visual que representa mediante gráficas el estado actual de la red o puede presentar las alertas a las que se debe prestar atención.
5. **Registro “log”*:*** es un historial de registros de eventos ordenados en orden cronológico y almacenan la información de diferentes eventos como, por ejemplo, del sistema operativo, servicio o registro de autenticación desde una aplicación.

# Gestión de eventos e información de seguridad SIEM

Un **SIEM** es “una solución híbrida centralizada que engloba la gestión de información de seguridad (Security Information Management) y la gestión de eventos (Security Event Manager)” (INCIBE, 2020), como se muestra en la siguiente figura:

1. Funcionalidades de un SIEM

Imagen que muestra el diagrama de las funcionalidades de un SIEM, el cual consta de:
- Compliance
- Analytics
- Mobile protection
- Threat protection
- Management
- Data protection
- Endpoint protection
- Network protection

Descubra a continuación, los aspectos más importantes sobre la gestión de eventos de información de seguridad SIEM, sus esquemas lógicos, proveedores, entre otros.

**Esquema lógico de un SIEM**

La gráfica muestra cómo a partir de la ingesta o alimentación de fuentes de diferentes sistemas de información consigue realizar un procesamiento y correlación de patrones para generar una vista amigable.

Imagen que muestra un esquema lógico de un SIEM, el cual contiene:
1. Inputs - datos de eventos y datos contexto
2. Outputs - análisis, informes y monitorización

**Proveedores**

En la actualidad hay muchos proveedores para soluciones **SIEM** y de correlación de eventos. En la imagen conozca una serie de los productos más representativos. Tenga en cuenta que existen soluciones tanto comerciales como de licencia de **“Software”** libre.

**Soluciones SIEM disponibles en el mercado**



# Parcheado y/o actualización

La gestión de las actualizaciones y parcheo de los sistemas de información o de los dispositivos de la organización se convierten en un factor fundamental para garantizar la seguridad de la información, ya que a partir de esta gestión se puede reducir amenazas por desactualización de sistemas y evitar que terceros puedan aprovecharla, como se muestra en la siguiente figura:

1. Fases para la gestión de parches y/o actualizaciones

Imagen que relaciona las fases de la gestión de parches, las cuales son:
- Despliegue
- Identificación de activos y software base
- Disponibilidad
- Aplicabilidad
- Adquisición
- Validación

Los parches o actualizaciones son cambios que se aplican a los sistemas de información, sistemas operativos o incluso dispositivos *hardware* con los cuales se busca corregir errores, vulnerabilidades o implementar mejoras de los sistemas.

Para realizar una adecuada gestión de parches y/o actualizaciones se recomienda seguir metodologías apoyadas en soluciones que faciliten este trabajo. Tenga presentes las fases que se enuncian a continuación:

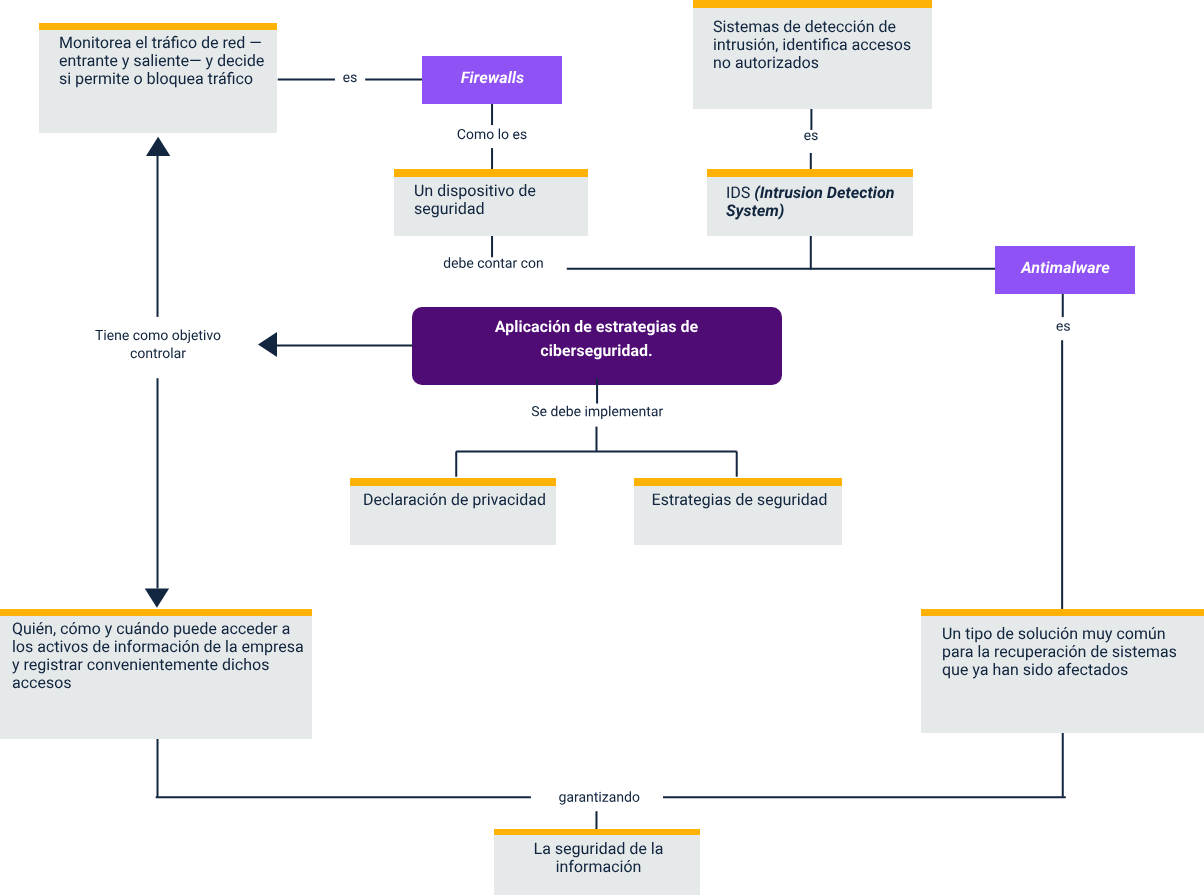
* **Identificación de activos y “Software” base**: mantener un inventario actualizado de los detalles de los activos de información, con el fin de determinar las actualizaciones correspondientes.
* **Disponibilidad**: identificar cuál parche específico, requerimientos y orden correspondiente debe aplicarse a cada uno de los sistemas y así evitar daños en sistemas por incompatibilidades.
* **Aplicabilidad**: verificar si la actualización es aplicable a cada sistema de información, ya que no siempre los parches son compatibles con todos los dispositivos.
* **Adquisición**: se recomienda que los archivos para la actualización o parcheo sean adquiridos a través de medios o fuentes confiables, preferiblemente de las casas productoras.
* **Validación**: se recomienda siempre realizar una validación previa y posterior a la actualización, con el fin de prevenir la pérdida de información o el no funcionamiento de dichos sistemas.
* **Despliegue**: realizar la programación de despliegue, incorporando los archivos necesarios y documentación sobre el proceso de implementación, así como la resolución de problemas más comunes.

**Recomendaciones para la adecuada gestión de parches y actualizaciones:**

* Buscar información de actualizaciones y descargarlas de sitios oficiales.
* Validar las actualizaciones de manera previa y posterior, para verificación de funcionalidad de los sistemas.
* Preferiblemente, realizar la instalación en ambiente de pruebas y posterior en producción.
* Siempre, mantener las actualizaciones al día de sus sistemas, a excepción de las documentadas por requerimientos técnicos o compatibilidades.
* Mantener los sistemas operativos, sistemas de información y aplicaciones de uso diario, actualizadas.
* Implemente soluciones para la automatización de actualizaciones generales como, por ejemplo, WSUS para sistemas Microsoft.
* Establezca horarios de actualizaciones automáticas que no afecten el desarrollo de las actividades laborales.

Síntesis

La aplicación de estrategias de ciberseguridad implica el uso de medidas y procedimientos para proteger sistemas, redes y datos contra amenazas cibernéticas, como ataques de hackers, malware y brechas de seguridad. Estas estrategias incluyen políticas, tecnologías y prácticas para prevenir, detectar y responder a amenazas cibernéticas, asegurando así la integridad, confidencialidad y disponibilidad de la información digital.



Glosario

**Auditoría:** proceso mediante el cual se busca verificar o validar que se esté cumpliendo una condición o la aplicación de un control.

**Control:** mecanismo de tipo lógico o técnico con el cual se busca regular o establecer restricciones de alguna acción.

**“Framework”:** es un marco de trabajo que provee los componentes y condiciones necesarias para su aplicación.

**Intrusión:** acceso no autorizado a un sistema o activo de información sin consentimiento del propietario.

**“Log”:** registro secuencial sobre eventos presentados en un sistema de información.

**“Malware”:** programa dañino que se instala en dispositivos y que puede generar daños o pérdida de información.

**Riesgo:** es la probabilidad de que una amenaza se materialice generando alguna consecuencia negativa.

Material complementario

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia | Tipo de material | Enlace del recurso |
| Dispositivos móviles | Organización Internacional de Normalización. (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad*. ISO 27001. | Norma técnica | <https://www.iso.org/standard/54534.html> |
| 1. Guía NIST-SP800-114 | NIST. (2021). *Cybersecurity framework*. NIST. | Página web | <https://www.nist.gov/cyberframework> |

Referencias bibliográficas

Audea. (2010). Fuga de información ¿Qué es y cómo se puede prevenir? Audea. <https://www.audea.com/fuga-de-informacion-que-es-y-como-se-puede-prevenir/>

Cisco. (2021). ¿Qué es un firewall? Cisco. <https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html>

FORTINET. (2021). Administración unificada de amenazas. FORTINET. <https://www.fortinet.com/lat/products/smallbusiness/utm>

Instituto Nacional de Ciberseguridad. (2017). Control de acceso. Políticas de seguridad para la pyme. Incibe. <https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf>

Instituto Nacional de Ciberseguridad. (2020). ¿Qué son y para qué sirven los SIEM, IDS e IPS? Incibe.

<https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips>

Organización Internacional de Normalización. (2013). Information technology — Security techniques — Information security management systems — Requirements. ISO 27001.

<https://www.iso.org/standard/54534.html>

LISA Institute. (2019). ¿Qué son las infraestructuras críticas? LISA Institute. <https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas>

Malwarebytes (2021). Todo acerca del malware. Malwarebytes. https://es.malwarebytes.com/malware/#what-is-malware

NIST. (2021). Marco de ciberseguridad. NIST. <https://www.nist.gov/cyberframework>

SeguriLatam. (2020). Seguridad en dispositivos móviles: ¿cuáles son las ciberamenazas más peligrosas? SeguriLatam. <https://www.segurilatam.com/actualidad/ciberseguridad-seguridad-en-dispositivos-moviles-cuales-son-las-ciberamenazas-mas-peligrosas_20201005.html>

Server World. (2020). Apache2: configure SSL/TLS. Server World. <https://www.server-world.info/en/note?os=Ubuntu_20.04&p=httpd&f=3>

Welivesecurity. (2021). Todo sobre cifrado: qué es y cuándo deberías usarlo. Welivesecurity.

<https://www.welivesecurity.com/la-es/2016/02/09/todo-sobre-cifrado-cuando-usarlo/>

Créditos

| Nombre | Cargo | Regional y Centro de Formación |
| --- | --- | --- |
| Claudia Patricia Aristizábal Gutiérrez | Líder del equipo | Dirección General |
| Liliana Victoria Morales Gualdrón | Responsable de línea de producción | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Hernando José Peña Hidalgo | Experto temático | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Fabián Leonardo Correa Díaz | Diseñador instruccional | Regional Tolima -Centro Agropecuario La Granja |
| Carolina Coca Salazar | Revisora metodológica y pedagógica | Regional Distrito Capital -Centro de Diseño y Metrología |
| Julia Isabel Roberto | Diseñadora y evaluadora instruccional | Regional Distrito Capital -Centro para la Industria de la Comunicación Gráfica |
| Nelly Parra Guarín | Adecuadora instruccional | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Alix Cecilia Chinchilla Rueda | Asesora metodológica | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Antonio Vecino Valero | Diseño web | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Jhon Jairo Urueta Alvarez | Desarrollo Fullstack | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Laura Gisselle Murcia Pardo | Animador y Productor Audiovisual | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Lady Adriana Ariza Luque | Validación de recursos educativos digitales | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Carolina Coca Salazar | Validación de recursos accesibles e inclusivos | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Leyson Fabián Castaño Pérez | Validación de recursos educativos digitales y vinculación LMS | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |
| Lina Marcela Pérez Manchego | Validación de recursos educativos digitales | Regional Distrito Capital -Centro de Gestión de Mercados, Logística y Tecnologías de la Información |