

Controles de seguridad

**Breve descripción:**

Para establecer salvaguardas que permitan garantizar la seguridad de la información en las organizaciones, es necesario adoptar controles que permitan reducir el riesgo que afecten negativamente la organización; estos controles pueden ser de diversos tipos y alcance, dado que el ámbito de la ciberseguridad no se concentra únicamente en el entorno digital.

**Junio 2023**

Tabla de contenido

[Introducción 1](#_Toc138793867)

[1. Gestión de acceso 3](#_Toc138793868)

[1.1. Tipos 4](#_Toc138793869)

[1.2. Características 5](#_Toc138793870)

[2. “Firewall” 7](#_Toc138793871)

[2.1. Funcionalidades 9](#_Toc138793872)

[2.2. Tipos 9](#_Toc138793873)

[3. IDS/IPS, Sistemas de detección y prevención de intrusos 12](#_Toc138793874)

[3.1. Definiciones 12](#_Toc138793875)

[IDS e IPS 12](#_Toc138793876)

[3.2. Características 15](#_Toc138793877)

[4. UTM/XTM 17](#_Toc138793878)

[4.1. Tipos 18](#_Toc138793879)

[4.2. Características 19](#_Toc138793880)

[5. “Antimalware” 20](#_Toc138793881)

[5.1. Tipos 22](#_Toc138793882)

[5.2. Características 23](#_Toc138793883)

[5.3. Detección y respuesta para “endpoints” (EDR) 24](#_Toc138793884)

[Características 25](#_Toc138793885)

[6. Cifrado 27](#_Toc138793886)

[6.1. Tipos 27](#_Toc138793887)

[6.2. Comunicaciones cifradas 28](#_Toc138793888)

[HTTPS 29](#_Toc138793889)

[FTPS 30](#_Toc138793890)

[SSH 31](#_Toc138793891)

[LDAPS 32](#_Toc138793892)

[6.3. Fuga de información 33](#_Toc138793893)

[Tipos 34](#_Toc138793894)

[Prevención 34](#_Toc138793895)

[7. Dispositivos móviles 37](#_Toc138793896)

[7.1. Tipos 37](#_Toc138793897)

[7.2. Características 39](#_Toc138793898)

[7.3. “Telework and Bring Your Own Device” (BYOD) “Security” (NIST-SP800-114) 39](#_Toc138793899)

[Aspectos importantes de la guía 39](#_Toc138793900)

[Seguridad en el teletrabajo 40](#_Toc138793901)

[8. Infraestructuras críticas 42](#_Toc138793902)

[Tipos 42](#_Toc138793903)

[8.1. Características 43](#_Toc138793904)

[8.2. Marco para mejorar la ciberseguridad de la infraestructura crítica 44](#_Toc138793905)

[Estructura del marco NIST 44](#_Toc138793906)

[Implementación 48](#_Toc138793907)

[9. Sistemas de correlacionamiento de “logs” y monitoreo 51](#_Toc138793908)

[9.1. Conceptos 51](#_Toc138793909)

[9.2. Tipos 52](#_Toc138793910)

[9.3. Características 53](#_Toc138793911)

[10. Parcheado y/o actualización 56](#_Toc138793912)

[10.1. Tipos 56](#_Toc138793913)

[10.2. Características 57](#_Toc138793914)

[11. Plan de capacitación y concienciación 59](#_Toc138793915)

[11.1. Ruta de actualización 59](#_Toc138793916)

[11.2. Estrategia de transferencia del conocimiento 61](#_Toc138793917)

[Síntesis 63](#_Toc138793918)

[Material complementario 64](#_Toc138793919)

[Glosario 65](#_Toc138793920)

[Referencias bibliográficas 66](#_Toc138793921)

[Créditos 69](#_Toc138793922)

Introducción

La gestión de la ciberseguridad en las organizaciones está cobrando cada vez mayor importancia dadas las últimas amenazas que se presentan de manera global, donde Colombia no ha sido ajeno, algunas organizaciones se vieron afectadas por incidentes de robo de información, cifrado, acceso abusivo y daños que repercuten en la calidad del servicio y, en algunos casos, en la imagen de confiabilidad que estas tienen y deben generar frente a sus interesados.

A continuación, vamos a revisar algunos de los controles para acceder a los activos de información de la empresa sugeridos y que se consideran de los más importantes.

1. Controles de seguridad



[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=R_0yRa7YXYo)

|  |
| --- |
| **Síntesis del video: Controles de seguridad** |
| La gestión de la ciberseguridad en las organizaciones es la respuesta a las constantes amenazas que se presentan de manera global, la información es un activo fundamental y cumple un rol vital en una empresa y los controles deben implementarse a partir de marcos de referencia, como el “firewall”, el cual examina la información que viene a través de la conexión a Internet.  Por otra parte, tenemos los IPS (Sistema de Prevención de Intrusiones), que funcionan como un sistema de prevención, monitoreo y detección.  Otra herramienta importante es el “anti-malware”, que puede evitar la aparición de una infección viral y eliminar los archivos infectados.  Además, es importante proteger los datos con métodos de cifrado, convirtiéndolos en texto sin formato; para acceder a los datos, se deben descodificar.  De esta manera, evitamos la fuga de información, la cual se debe delimitar con todas las acciones requeridas.  Finalmente, en el componente, se hablará de las actualizaciones y su implementación. |

# Gestión de acceso

La gestión de acceso cobra un gran valor, ya que permite establecer los controles y condiciones bajo los cuales un usuario puede hacer uso de los activos de información de la empresa.

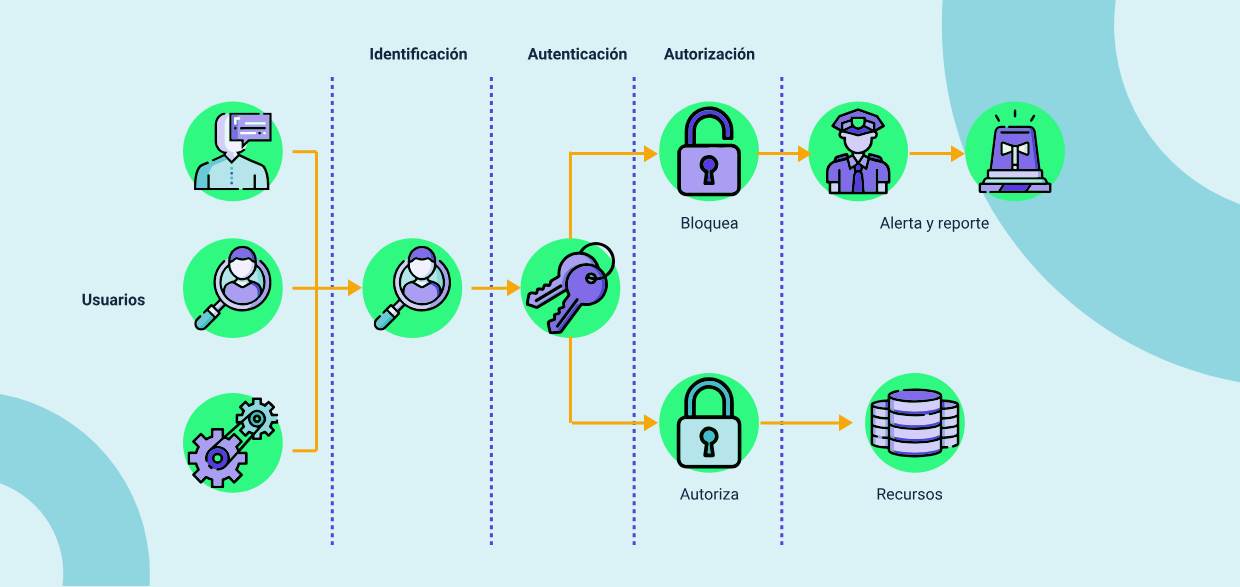
De acuerdo con el Instituto Nacional de Ciberseguridad de España, el objetivo de este control es “Establecer quién, cómo y cuándo puede acceder a los activos de información de la empresa y registrar convenientemente dichos accesos” (INCIBE, 2017). Esto conlleva establecer controles que permitan una adecuada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

A continuación, es posible ver los pasos técnicos que se deben valorar para gestionar una adecuada autorización y acceso a los recursos requeridos, y estos son:

* **Identificación.** Permite identificar particularmente un usuario o un sistema con un identificador único y diferenciarlo de otros.
* **Autenticación.** Permite validar que el usuario o sistema que intenta acceder a un recurso es quien dice ser, mediante la validación de un mecanismo como, por ejemplo: contraseña, pin, token o cualquier otro mecanismo asociado.
* **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.

A continuación, en la siguiente figura, es posible apreciar un esquema que ilustra los pasos de un control para la gestión de accesos:

1. Pasos de un control de gestión de acceso



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

## Tipos

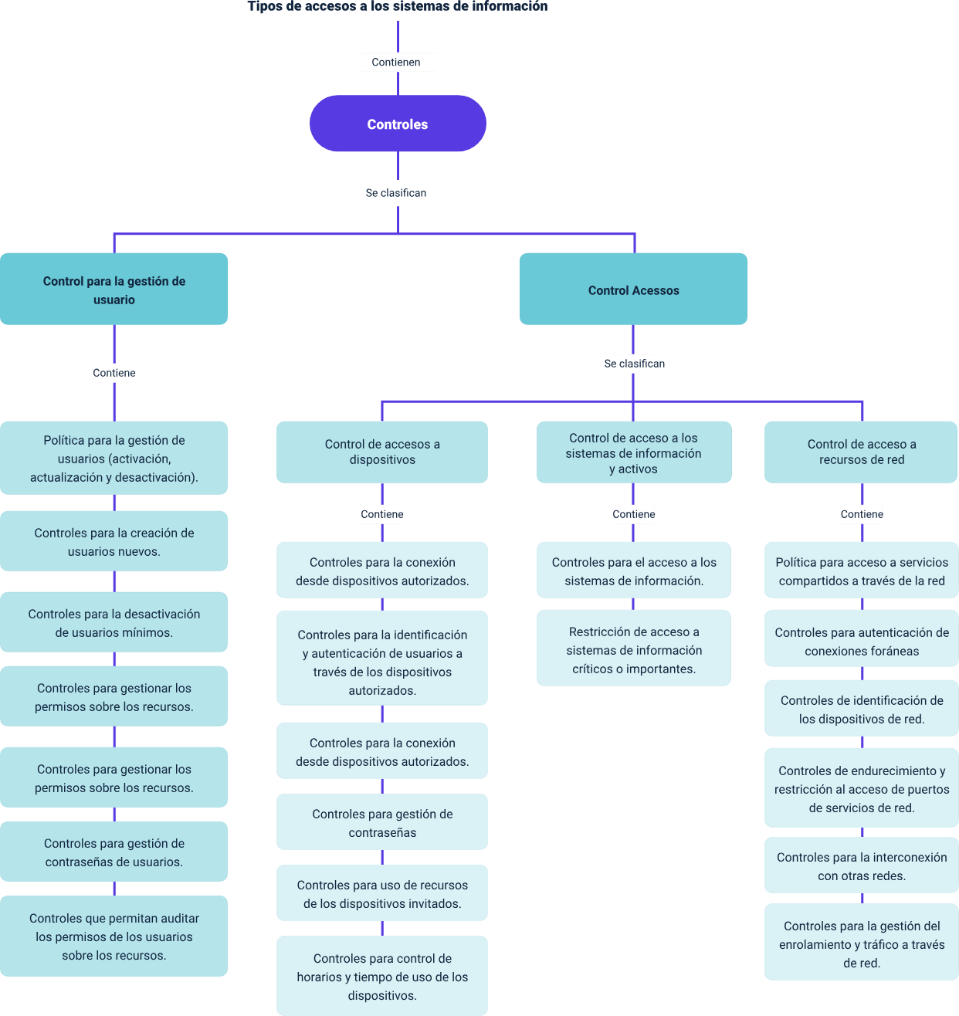
El control para la gestión de accesos se puede abordar desde diferentes frentes, tanto de gestión como técnicos. A continuación, se van a identificar algunos de los más comunes:

De acuerdo con la complejidad del control, estos pueden ser:

* **Básicos**. Su implementación no requiere de mayor esfuerzo ni ajustes en los sistemas de información y pueden abordarse con capacitaciones y controles básicos.
* **Avanzados.** Estos controles requieren de herramientas avanzadas y establecimiento de políticas y controles, como, por ejemplo, la implementación de servicios de directorio activo y la implementación de políticas de grupo.

Dentro de los tipos de accesos a los sistemas de información, es necesario considerar los siguientes controles:

1. Tipos de accesos a los sistemas de información - Controles



## Características

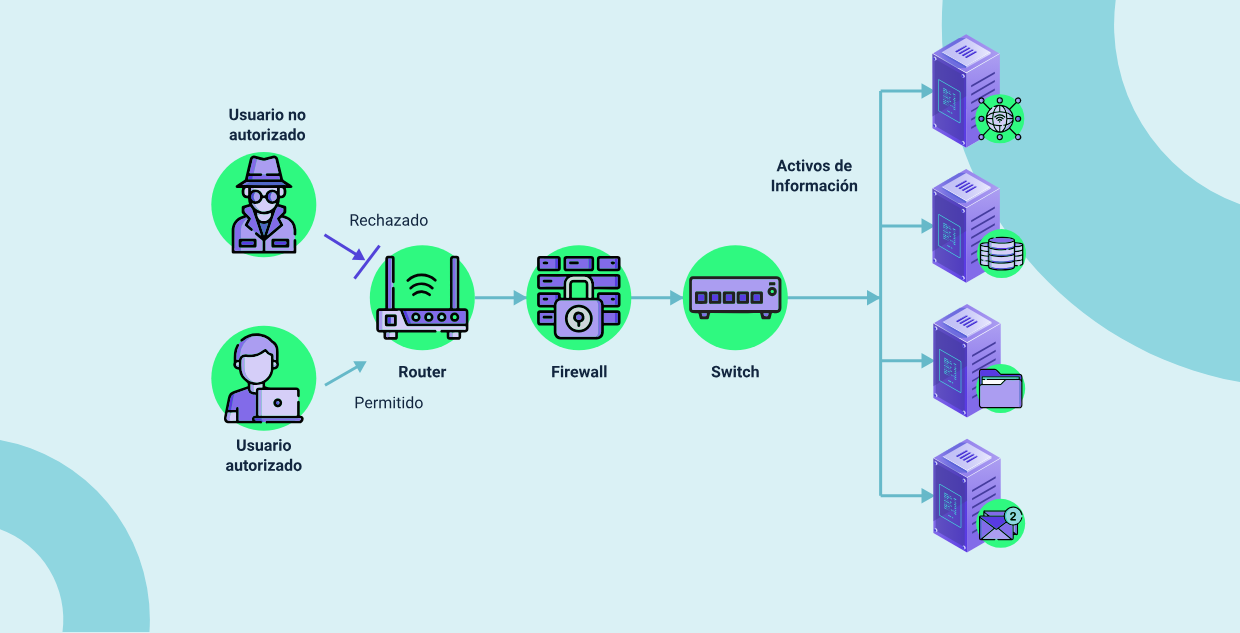
La implementación de los controles para gestión del acceso debe contemplar ciertas condiciones que eleven la complejidad y dificulten el acceso no autorizado a los activos de información de la organización, como, por ejemplo:

* **Privilegio mínimo.** Cualquier autorización de acceso debe darse de acuerdo con las necesidades de cada rol y necesidad, por ejemplo, no hacer uso de credenciales de DBA en un usuario de conexión a través de una página web.
* **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.
* **Actualización de credenciales**. Establecer los controles que requieran la actualización de contraseñas periódicamente.
* **Uso de credenciales complejas.** Promover, a través de controles, el uso de contraseñas seguras.
* **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, bajo algún mecanismo de cifrado de base de datos.

# “Firewall”

Los “firewalls”, 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 garantizar el acceso a partir de la aplicación de políticas, tal como se muestra en la siguiente figura. Teniendo presente el tráfico, por defecto, debe partir de la siguiente lógica:

* **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.

1. Gestión de tráfico entrante por “Firewall”

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

Los “firewalls” cuentan con políticas para la gestión de tráfico por defecto, pero cada administrador de red puede crear o modificarlas de acuerdo con sus necesidades.

Para la operación de un firewall, es necesario tener presentes ciertos conceptos y definiciones que son muy comunes y que su conocimiento permite realizar una adecuada gestión, de la siguiente manera:

* **“Host”.** Se refiere a 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 la red.
* **Paquete.** Un paquete se considera como los bloques que componen la información que viaja a través de la red.
* **Política**. Las políticas son condiciones bajo las cuales es posible autorizar o denegar el tráfico entre un origen y un destino en la red.
* **Puerto.** Un puerto se considera una entrada lógica hacia un servicio específico, por ejemplo, puerto 80 http, 443 https, 21 ftp, etc. Es posible encontrar un listado completo de los puertos TCP en el siguiente <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.>
* **Rango de IP.** Se conoce como rango de IP a un grupo de direcciones IP agrupadas para una función o política específica, por ejemplo: 192.168.1.10-192.168.1.20.
* **Servicio**. Un servicio es ofrecido por aplicaciones o sistemas para compartir información entre dos o más sistemas, a partir de la aplicación de protocolos, por ejemplo: el 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.
* Restringir el tráfico saliente hacia los destinos autorizados.
* Evitar ataques de presentación hacia la red interna, por ejemplo, deteniendo ataques de denegación de servicios o de suplantación IP “Address Spoofing”, entre otros.
* Brindar los informes necesarios para auditoría.

## Tipos

Existe actualmente gran variedad de soluciones “Firewall”, entre las cuales es importante identificar las relacionadas en el siguiente video:

1. Tipos de soluciones “Firewall”



[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=V-8J5rlLBb4)

|  |
| --- |
| **Síntesis del video: Tipos de soluciones “Firewall”** |
| Un “firewall” tiene como función principal la gestión del tráfico entre redes que se genera a partir de la implementación de políticas o reglas. A continuación, se describen estos:  **“Firewalls” basados en “hardware”**  En su mayoría, se implementan en dispositivos físicos que se administran a través de interfaces o administración remota, los cuales se integran a la red principal.  **“Firewalls” basados en “software”**  Se implementan bajo ciertos sistemas operativos, como Linux o Windows, y de licencia comercial, “Open Source”, líneas de pruebas, beta o simplemente de incursión.  **“Firewalls” de filtrado de paquetes**  Este “firewall” realiza la gestión de tráfico a partir de reglas aplicadas a direcciones de red junto con protocolos y puertos; dentro de este tipo de “firewalls”, se encuentran los WAF (“Web Application Firewall”).  **“Firewalls proxy”**  Este es de los más seguros a nivel de control de tráfico entre redes y su función es evitar un acceso directo desde el exterior.  **“Firewalls” de inspección con estado**  Este “firewall” además permite realizar un monitoreo al estado de cada conexión.  **“Firewalls” de próxima generación (NGFW)**  Permiten un filtrado de paquetes basados en proxy, desde las capas 3 y 4 del modelo OSI, con capacidades de llegar a extender su protección hasta la capa 7, sugeridos para la administración de redes de gran tamaño. |

# IDS/IPS, Sistemas de detección y prevención de intrusos

A continuación, se encuentra otro tipo de soluciones que complementan la seguridad perimetral de nuestra organización a partir del análisis del tráfico que pasa por la red, identificando accesos no autorizados hacia algún recurso del perímetro.

## Definiciones

Observe las siguientes definiciones de los diferentes conceptos y sus características:

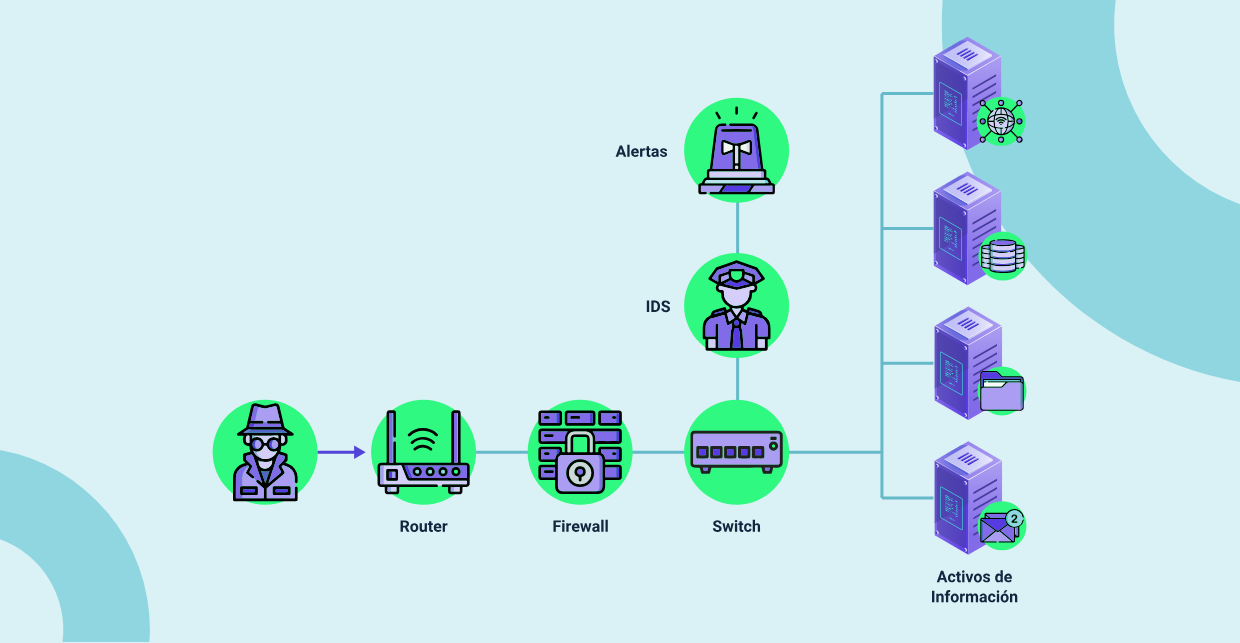
### IDS e IPS

* Se consolidan como herramientas para la detección y la prevención de intrusiones en redes de datos.
* Operan analizando el tráfico que circula desde redes externas y comparándolo con patrones basados en firmas.
* Permiten identificar comportamientos sospechosos.
* Establecen el comportamiento de los dispositivos frente al tráfico.

Las siguientes son las características de cada uno de ellos y la forma como se integran a las infraestructuras de red:

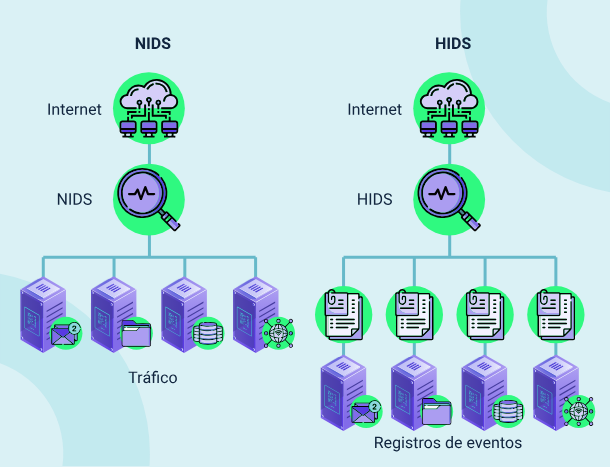
**IDS (“Intrusion Detection System”)**

* Soluciones para el monitoreo de la seguridad perimetral.
* Son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas.
* Se encargan de generar los mensajes de advertencia para que el administrador de la red tome las acciones correspondientes.
* 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.

1. Esquema de implementación de un IDS

De acuerdo con su funcionalidad, es posible encontrar dos tipos de IDS:

1. Diferencias entre NIDS y HIDS



Nota. Adaptado de Comparitech.com.

**HIDS “Host-based Intrusion Detection System”**: sistema de detección de intrusiones basado en “host”, analiza el comportamiento de un dispositivo a partir de los eventos registrados. Los HIDS analizan las anomalías registradas en los eventos de cualquier dispositivo de la red.

**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. Los NIDS: analizan las sumas de comprobación de paquetes, comparándolos con firmas en bases de datos.

Además, los IDS, de acuerdo con los métodos de detección, se pueden clasificar como:

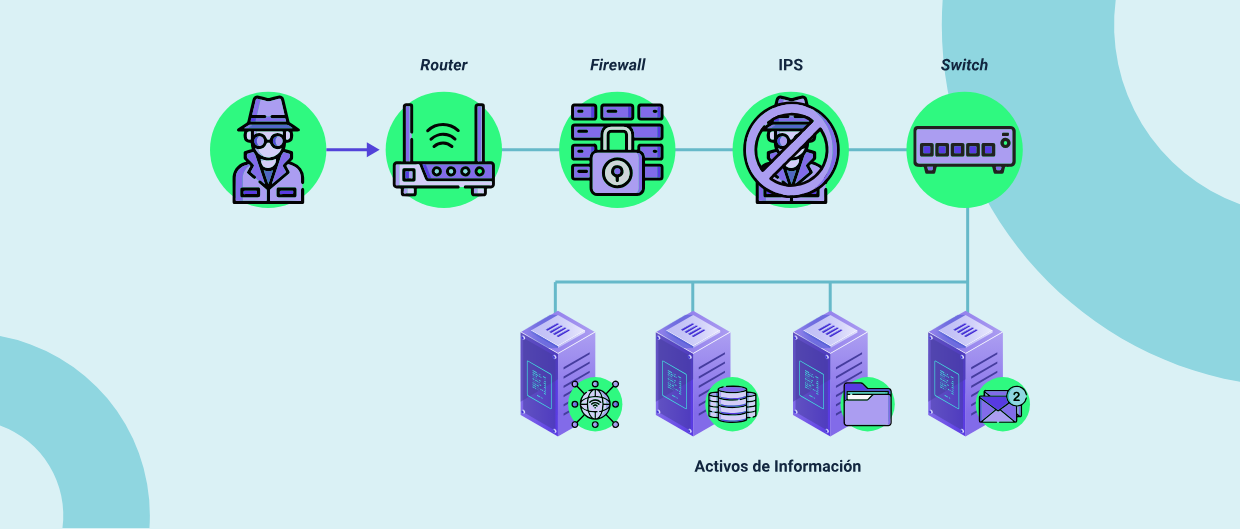
* **IDS basado en firmas:** este tipo de IDS está presente en NIDS y HIDS.
* **IDS basado en anomalías:** este tipo de IDS busca patrones de acuerdo con las actividades identificadas en el tráfico de paquetes. Para el caso de los HIDS, este analiza los eventos como los inicios de sesión no exitosos y reiterativos; para el caso de los NIDS, realiza comparaciones a partir de un comportamiento base.

Entre los IDS más conocidos, están

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

**IPS (“Intrusion Prevention System”)**

* Son soluciones que permiten asegurar de manera preventiva los recursos de la red de ataques e intrusiones.
* Realizan un análisis en tiempo real de las conexiones, con el fin de cotejar con patrones o comportamientos conocidos.
* Tienen el control para denegar paquetes, así como cerrar conexiones que consideren sospechosas.
* Operan desde la red interna, por lo general, después del “firewall” de seguridad perimetral.

1. Esquema de implementación de un IPS

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 la red.

## Características

Dentro de las características más relevantes de estos 2 sistemas, están:

1. IDS (“Intrusion Detection System”)

* Realiza análisis del tráfico a partir de verificación y comparación de patrones contra bases de datos con firmas conocidas de ataques maliciosos.
* Realiza monitoreo permanente del tráfico que pasa por la red.
* Cuenta con la 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 de actualización permanente de bases de datos con firmas

1. IPS (“Intrusion Prevention System”)

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

# UTM/XTM

Integra soluciones (como “firewall”, ids, ips) en un solo dispositivo conocido como UTM (“Unified Threat Management”) o Gestión Unificada de Amenazas y los XTM (Extensible UTM) o UTM Extendido, los cuales cubren las necesidades básicas y más comunes requeridas por las organizaciones en una única solución. A continuación, puede reconocer en qué se diferencia cada uno de ellos:

* **UTM (“Unified Threat Management”):** UTM, o Gestión Unificada de Amenazas, es una solución novedosa y que integra las soluciones que requieren las organizaciones hoy en día; de acuerdo con Fortinet, “consolida múltiples funciones de seguridad y redes con un “appliance” unificado que protege a las empresas y simplifica la infraestructura” (FORTINET, 2021), permitiendo encontrar en una sola solución herramientas como: “firewall”, IDS/IPS, antivirus, “antimalware”, filtrado antispam, filtrado web, acceso remoto seguro como VPN y una amplia variedad de reportes que simplifican la administración de este tipo de arquitecturas.
* **XTM (“Extensible UTM”):** XTM o UTM Extendido, como su nombre lo indica, permite ampliar las 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.

Este tipo de soluciones ha ganado campo de aplicación por sus capacidades de ajustarse a casi cualquier tipo de organización, facilitando su implementación y administración.

## Tipos

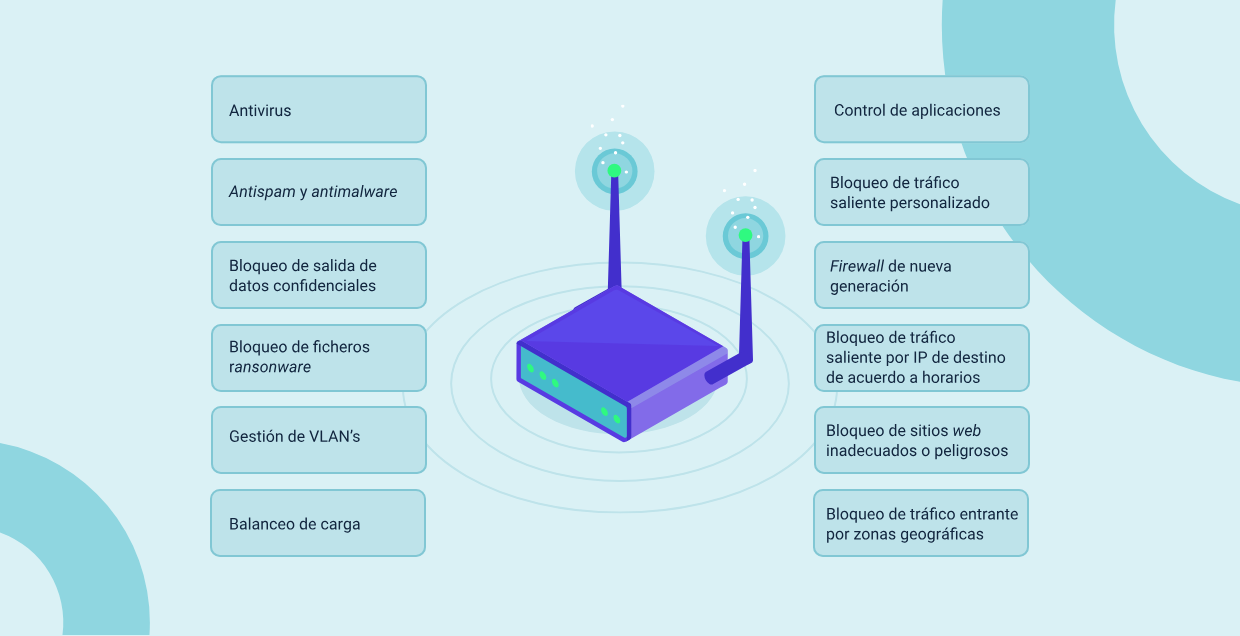
Las diferencias entre este tipo de dispositivos no son tan significativas a simple vista, se requiere de un análisis de las operaciones de análisis que puede realizar para identificar cuál es la más indicada para cada organización:

* **UTM/XTM**: este tipo de soluciones, como se mencionó anteriormente, además de sus funciones de “firewall”, cuenta 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 se puede encontrar tanto en presentación de “hardware” como “software”; este modelo es muy recomendado para pequeñas organizaciones.
* **NGFW:** este tipo de “firewall” de nueva generación incorpora herramientas para el análisis de amenazas recientes, así como “malware” que frecuentemente aparece en nuevas versiones y modalidades de ataques; este tipo de soluciones se recomienda en grandes organizaciones o aquellas que presentan gran cantidad de solicitudes y acceso a través de red.

Una de las principales diferencias entre estas soluciones es que el NGFW puede realizar una inspección avanzada de paquetes y permite establecer políticas para gestionar el acceso seguro a los recursos.

## Características

Este tipo de dispositivos UTM/XTM cuenta con las capacidades para realizar la gestión de la seguridad, mediante la administración tráfico, análisis de “malware”, control de aplicaciones, gestión de vlan, como lo demuestra la siguiente figura:

1. Características y funcionalidades de los UTM/XTM

Nota. Adaptado de <http://fibraoptica.blog.tartanga.eus/files/2018/01/Equipos-UTM-2-2.jpg>

# “Antimalware”

El “malware”, de acuerdo con MalwareBytes, “es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas” (MalwareBytes, 2021), es capaz de invadir nuestros sistemas de información de manera intrusiva para causar daños, generando pérdidas de información en caso de no estar preparados.

Existen varios tipos de “malware” y tienen su impacto diferente dependiendo de su funcionamiento; en el siguiente video, es posible identificar aquellos tipos de “malware” más conocidos y que han generado estragos en los últimos años:

1. Ataques de seguridad en la red



[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=x56FT_OVARQ)

|  |
| --- |
| **Síntesis del video: Ataques de seguridad en la red** |
| El video presenta los tipos de “malware”:  “Ransomware”: le chantajea.  “Spyware”: roba sus datos.  “Adware”: le muestra publicidad sin parar.  Gusanos: se propagan entre equipos.  Troyanos: introducen “malware” en su PC.  Redes de robots: convierten su PC en zombi. |

El “malware”, una vez logra afectar un dispositivo, puede presentar los siguientes síntomas, que llevan a identificar que se encuentra afectado por este tipo de programas:

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

Como mecanismos de protección y para no verse afectado por este tipo de programas, se recomienda el uso de tecnologías “antimalware”, las cuales vienen hoy en día integradas a las soluciones de antivirus como Norton 360, Avast, Mcafee, Kaspersky, o también podemos encontrar soluciones independientes, como Malwarebytes.

## Tipos

En la actualidad, se encuentran tecnologías “antimalware” que permiten mantener la seguridad de los dispositivos de la organización, como son:

* **“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 es muy común para recuperación de sistemas que ya han sido afectados.
* **Paquetes de “software” de seguridad.** Este tipo de solución, 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.** Este tipo de solución se integra a servicios que se encuentran en la nube y es común encontrarlo en servicios de correo electrónico o de alojamiento de archivos; generalmente, cuenta con 2 componentes, el cliente que se instala en los dispositivos administrados y el otro componente es el servicio web, el cual se encarga de validar la información reportada por el cliente.

El portal “Safety Detectives” comparte su post titulado “Las 7 mejores aplicaciones y protecciones “antimalware” (2022): Mejores herramientas”, entre las cuales sobresalen Norton 360, Bitdefender McAfee, TotalAV, Avira, así como la solución de MalwareBytes como herramienta autónoma sobresaliente para la gestión de “malware” para sistemas operativos Windows.

## Características

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

* **Protección frente a “malware”.** Debe presentar soporte para asegurar y recuperar recursos afectados por “malware” de manera permanente y actualizada.
* **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.
* **Velocidad de verificación.** Debe ser rápido en el proceso de revisión, análisis y detección de “malware”.
* **Actualización permanente.** Debe proveer actualizaciones tanto de la aplicación como de las bases de datos, de manera permanente y oportuna.
* **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.
* **Herramientas adicionales para la gestión de “malware”.** Debe proveer a los usuarios con las herramientas necesarias para el aseguramiento de sus dispositivos e información.
* **Compatibilidad con diferentes sistemas.** Debe soportar cualquier sistema operativo y ser compatible con la mayoría de las aplicaciones informáticas, con el objetivo de reconocer una aplicación afectada de una original.
* **Soporte.** Debe proveer soporte técnico especializado a los usuarios que cuentan con suscripciones activas.

## Detección y respuesta para “endpoints” (EDR)

Otro tipo de soluciones que permite mejorar la seguridad de los dispositivos de nuestra red son los EDR, los cuales permiten monitorear permanentemente los cambios presentados en los dispositivos.

A continuación, podrá reconocer los conceptos básicos relacionados con los EDR, por medio del siguiente video:

1. Detección y Respuesta para “Endpoints” (EDR)



[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=XuDaYwxGMU0)

|  |
| --- |
| **Síntesis del video: Detección y Respuesta para “Endpoints” (EDR)** |
| Un “endpoint” puede ser cualquier dispositivo que se encuentra conectado a la red informática de la organización, teléfonos, servidores, tabletas, etc.  EDR (“Endpoint Detection and Response”): Detección y Respuesta de “Endpoints” son soluciones que permiten detectar y responder ante actividades sospechosas en un dispositivo, evitando su replicación en otros dispositivos de la organización.  XDR : Detección y Respuesta Extendidas es una solución integral para la respuesta a incidentes a partir de la recolección de información de los “endpoints”.  EPP: su objetivo es prevenir incidentes de seguridad en los dispositivos de la red por “malware” o cualquier otra vulnerabilidad.  SIEM: soluciones de un orden superior aportando información útil desde una óptica de seguridad global. |

### Características

Dentro de las características requeridas por una solución para la detección y respuesta de “endpoints”, es importante tener presente que debe abordar los niveles de seguridad para este tipo de dispositivos, como son:

* **Análisis de riesgos y endurecimiento.** Capacidad de realizar un inventario y su correspondiente análisis de riesgos, generar un esquema de actualizaciones, sugiriendo aplicación de cifrado a la información, estableciendo controles de seguridad tanto a las aplicaciones como al dispositivo en general.
* **Prevención.** Proveer de soluciones de seguridad activa que protejan 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 el dispositivo, aislamiento de este, 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 “endpoints” de la organización.

En la siguiente figura, se puede observar la arquitectura de seguridad sugerida para una solución de “endpoint”:

1. Arquitectura adaptativa por niveles de seguridad para soluciones EDR

Nota. Basado en Bitdefender (s.f.).

# 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 permiten proteger la privacidad de esta al evitar que esta sea interpretada por personas no autorizadas.

El cifrado es “el proceso mediante el cual se codifica algo de modo que no resulte fácil de entender para quienes no tienen acceso autorizado” (WeLiveSecurity, 2021). También es necesario conocer sobre los procesos de criptografía.

Estos procesos tienen como objetivos:

* Garantizar la privacidad y confidencialidad de tal manera que únicamente el destinatario interesado pueda leerla.
* Integridad, evitando que esta sea modificada sin autorización.
* Autenticación, garantizando que solo se pueda interpretar por los interesados.
* No repudio, para evitar que se niegue el acceso a alguno de los interesados.

Puede conocer más sobre el proceso de cifrado en el video titulado Cifrado de datos: qué es y cómo puede ayudarte a proteger tu información en Internet, en el enlace <https://www.youtube.com/watch?v=wcJBmoz6Vlk>

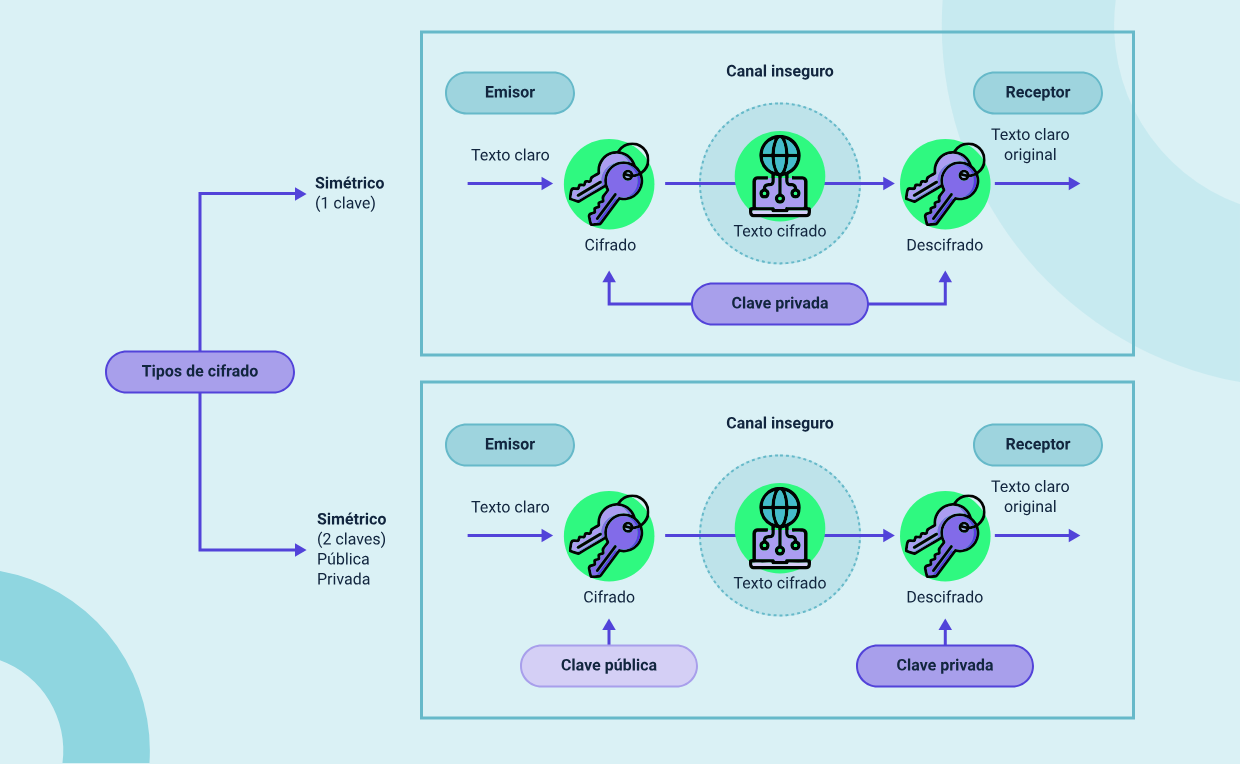
## Tipos

Se pueden identificar dos tipos de cifrado, como son:

1. Cifrado simétrico: este tipo de cifrado hace uso de una sola llave tanto para cifrar un mensaje como para recuperarlo.
2. Cifrado asimétrico: este tipo de cifrado hace uso de dos llaves:

* Llave pública: la cual se puede compartir.
* Llave privada: está únicamente debe ser conocida por el destinatario o interesado.

En la siguiente figura, puede observar el proceso para cifrar mensajes a partir de estos dos tipos de cifrado.

1. Tipos de cifrado

Nota. Adaptado de OSI (2019).

## Comunicaciones cifradas

Los controles de cifrado deben ser integrados en cualquier estrategia de seguridad como mecanismos vitales para salvaguardar la información confidencial y garantizar los pilares de la seguridad de la información.

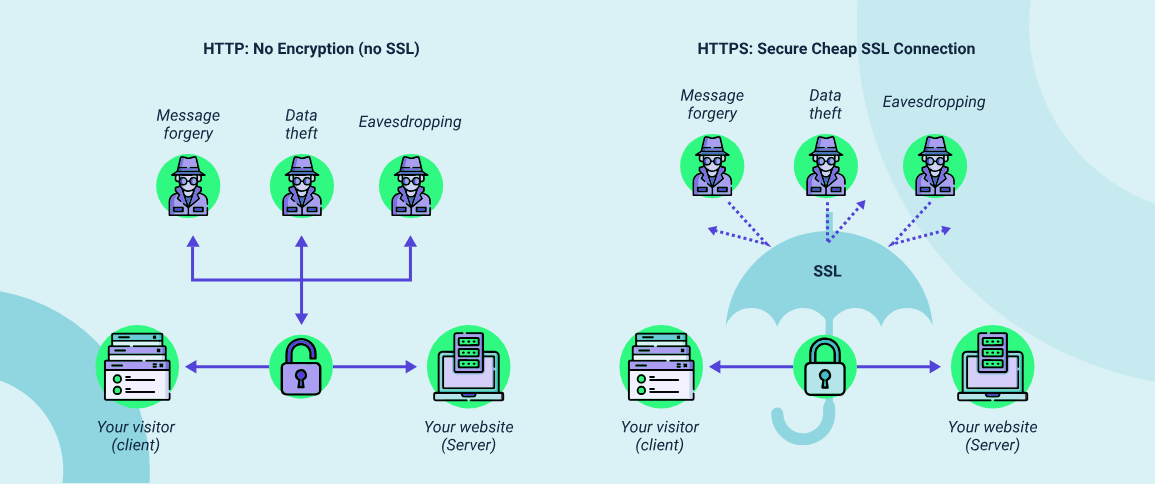
A continuación, se van a identificar algunas aplicaciones específicas en servicios de red:

### HTTPS

El protocolo de servicio web HTTP viaja de manera plana a través de los medios de comunicación, lo que lo hace vulnerable a cualquier interceptación, permitiendo recuperar información sensible, alterar y/o aplicar sentencias dañinas; para mejorar la seguridad de este protocolo, se realizan implementaciones como SSL, acrónimo de “Secure Sockets Layer”, la cual permite realizar un cifrado a la información transmitida entre dos puntos.

Asimismo, se cuenta con TLS, “Transport Layer Security”, la cual es una mejora al SSL agregando una capa de seguridad al transporte; los certificados web se distribuyen actualmente con tecnología TLS, aunque continúen llamándose SSL.

Estas implementaciones se realizan con la inclusión de un certificado digital en la operación del servidor web, como Apache, Ngnix o IIS, por nombrar algunos, habilitando el protocolo HTTPS. En la siguiente figura, puede observar cómo la implementación de cifrado SSL evita que el contenido que circula a través de la red pueda ser leído por terceros no autorizados:

1. Tráfico HTTP vs. HTTPS

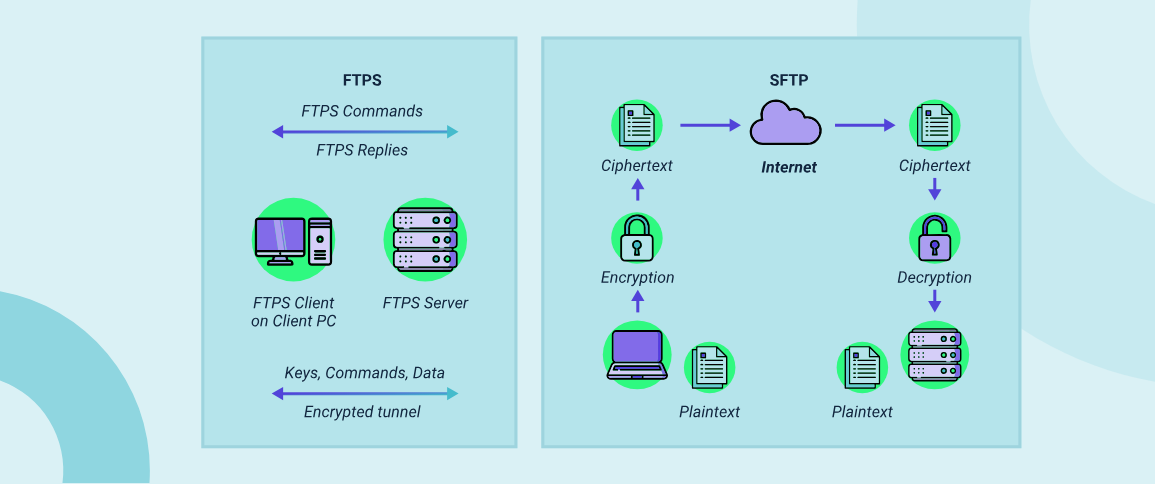
Nota. Basado en B, G (2002).

### FTPS

La transferencia de archivos aún sigue siendo un servicio que se consume en algunas organizaciones y es muy útil cuando se realiza transferencia de gran cantidad de archivos o estos son de gran tamaño, para ello se hace uso de protocolos como el FTP; lastimosamente, este servicio, en su implementación, es muy sensible y apetecido por ciberdelincuentes; para reducir estos inconvenientes, se puede realizar la implementación de FTPS (Protocolo de transferencia de archivos con soporte para Seguridad de la capa de transporte (SSL / TLS)).

Esta implementación también se realiza incorporando un certificado digital sobre el servicio FTP, como, por ejemplo, Vsftpd, Proftpd o Pure-FTPd.

No se debe confundir con SFTP (Protocolo de transferencia de archivos), el cual es un protocolo que permite transferir y manipular archivos a través de cualquier medio. Por lo general, se usa con el protocolo SSH-2. En la siguiente figura, puede observar algunas de las diferencias en operación de estos protocolos:

1. Diferencias entre FTPS Y SFTP

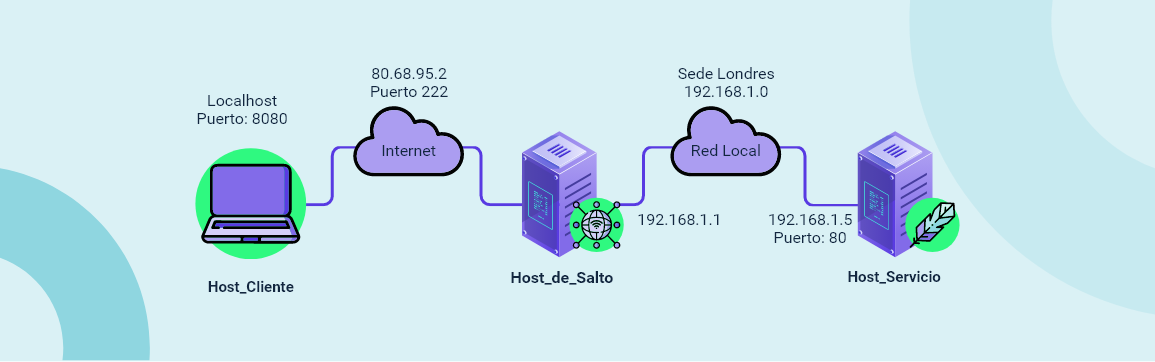
Nota. Basado en MSP (s.f.).

### SSH

Uno de los controles que no debe faltar en cualquier estrategia de seguridad es el que nos sugiere asegurar los accesos remotos y seguros, en especial, para la administración de dispositivos críticos, así como de consolas y “appliances” de seguridad; para abordar este control, se sugiere la implementación de acceso seguro a través de SSH (“Secure Shell”), el cual es un servicio que hace uso de protocolo de cifrado, como RSA y DSA, este establece las conexiones estableciendo canales seguros y cifrados entre los dos puntos de la conexión, resguardando la información que fluye por el medio.

En la siguiente figura, se puede identificar cómo, desde el exterior y haciendo uso de una conexión SSH, puede establecer conexión con un host al interior de la red, implementando un canal cifrado a través de la red pública; este servicio puede utilizarse a través de programas para la conexión remota, como Putty, y de transferencia de archivos segura, como WinSCP:

1. Funcionamiento de conexión SSH



Nota. Basado en Chasco (2015).

### LDAPS

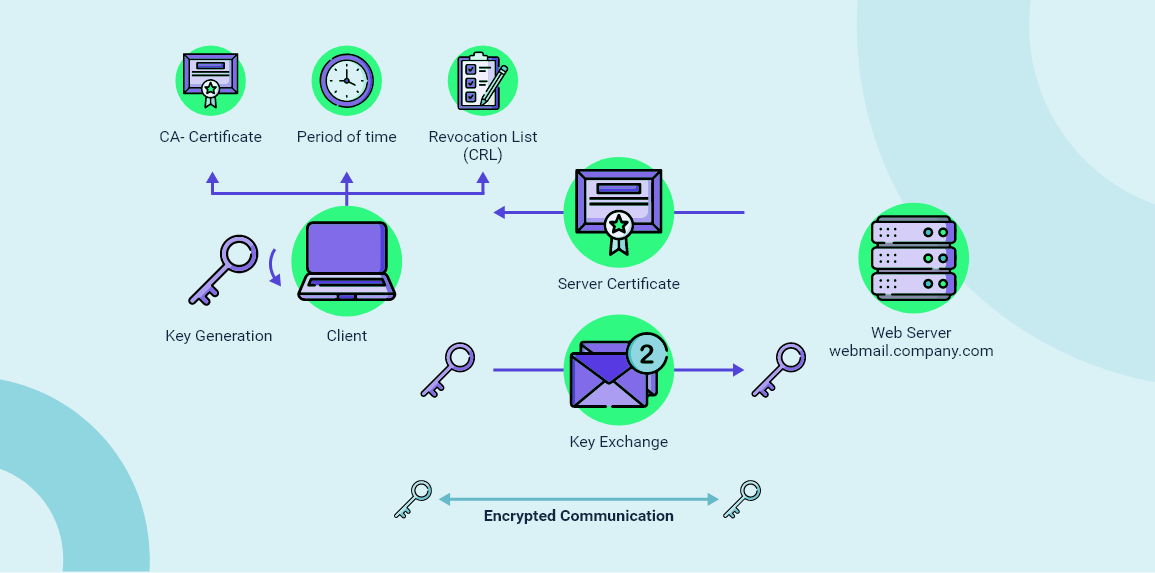
Uno de los controles sugeridos en las organizaciones son los relacionados con una adecuada gestión de usuarios y sobre su administración responsable, por lo cual es muy común encontrar soluciones de servicio de directorio basados en protocolo LDAP (“Lightweight Directory Access Protocol”), como OpenLDAP o Active de Directory de Microsoft.

Estos servicios basados en LDAP permiten implementar directorio de objetos (unidades organizacionales, grupos, usuarios, equipos, entre otros), están estructurados bajo el protocolo X.500 y contienen una estructura de manera jerárquica, esto permite su gestión centralizada, así como la asignación de privilegios a diferentes recursos de la red.

Este servicio se aprovecha a nivel de aplicación para que los usuarios se autentiquen y hagan uso de servicios, por ejemplo: inicio de sesión, escritorio remoto, carpetas compartidas, DNS, DHCP, autenticación desde otras aplicaciones, entre otros.

Al igual que los servicios anteriormente nombrados, para mejorar la seguridad en la transmisión de información, se recomienda la implementación de LDAPS (LDAP Seguro), esto se puede realizar con implementación de protocolos como SSL y TLS, los cuales requieren un certificado digital, como se puede observar en la siguiente figura:

1. Implementación de protocolo LDAPS



Nota. Basado en Kuenzler (2014).

## Fuga de información

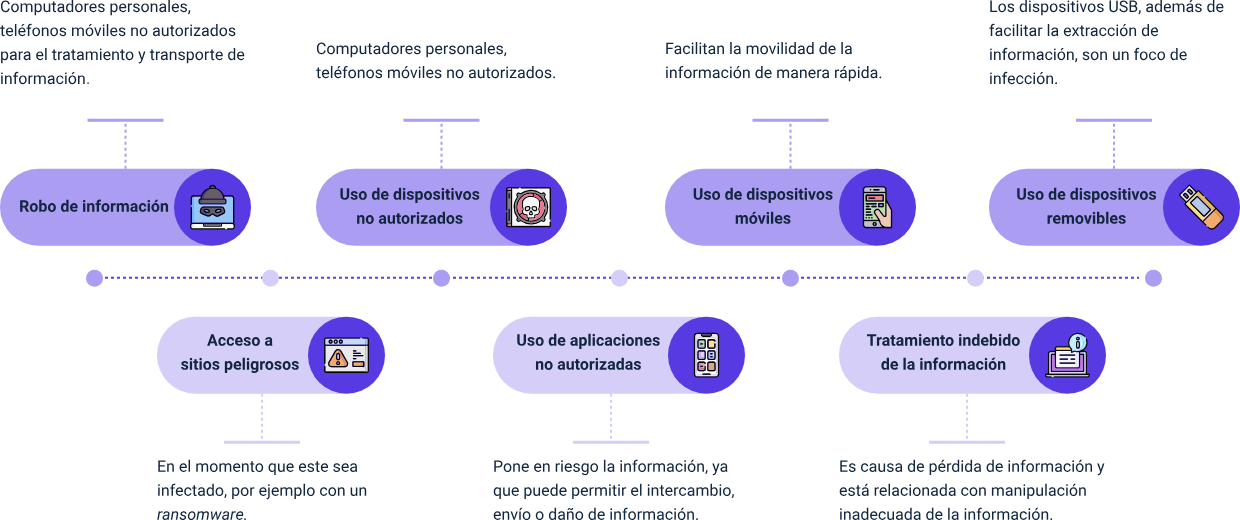
La pérdida de información en una organización puede presentarse por varios factores y se puede buscar reducir mediante la adopción de controles que reduzcan este tipo de riesgos.

De acuerdo con AUDEA, se denomina fuga de información “al incidente (tanto interno como externo, y a la vez 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” (AUDEA, 2020). La norma ISO 27001, en su Anexo A, establece controles que buscan mejorar las prácticas con el manejo de los activos de información.

### Tipos

Existen diversos tipos y causas por las cuales se desencadenan fugas o pérdida de información, entre los cuales se pueden encontrar:

1. Implementación de protocolo LDAPS



### Prevención

Conocer los activos de información se considera el primer paso para tomar decisiones y acciones que ayuden a prevenir incidentes relacionados con fuga o pérdida de información, así que, a continuación, se plantean las siguientes recomendaciones:

* Identificar los activos de información que gestiona.
* Clasificar los activos de 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 se pueden encontrar los siguientes tipos:

1. **Técnicas.** Implementación de soluciones de seguridad que permitan detectar y prevenir fuga de información, entre las cuales se consideran:

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

Para grandes organizaciones, se recomienda:

* Sistemas de prevención de pérdida de datos o DLP.
* Aplicación de controles orientados a la gestión del ciclo de vida de la información o ILM (“Information Lifecycle Management”).
* Adopción de herramientas que permitan controlar 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 que se cuente con políticas de seguridad apoyadas en acciones de concienciación a todo el personal.
2. **Jurídicas.** Todos los empleados y/o proveedores deben cumplir con las políticas de seguridad, las cuales 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 cuenta con controles que establecen los lineamientos para el uso de dispositivos móviles, lo anterior teniendo en cuenta las consideraciones de seguridad para su uso.

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

* **Terminal.** Se conoce a cualquier dispositivo móvil que permite registrar y consultar información.
* **“Smartphone”.** Teléfono inteligente que cuenta con funciones avanzadas para utilizar aplicaciones y gestionar información; estos dispositivos están compuestos por 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.

## Tipos

Los tipos de dispositivos móviles son utilizados para la comunicación y transmisión de información, entre los que se pueden identificar: teléfonos inteligentes, dispositivos “smart” entre los que se encuentran los relojes, dispositivos expansión de sonido, video o accesorios para interacción, como gafas 3D, que hacen parte de los dispositivos móviles y que cada uno, por el hecho de mantener una comunicación hacia la red y compartir datos sensibles, deben ser controlados y asegurados.

Entre algunas de las amenazas actuales a las que están expuestos este tipo de dispositivos móviles, se encuentran las siguientes:

* **Aplicaciones maliciosas.** Mediante las cuales se puede instalar apps maliciosas que pueden presentar algún tipo de filtración de datos o daño, tanto en los dispositivos como en la información.
* **Vulnerabilidades en los dispositivos.** Algunas marcas y/o modelos no cuentan con los componentes necesarios para un sistema seguro, lo que se considera una debilidad, y esta puede ser aprovechada por terceros para robar información.
* **“Phishing”.** Esta es una de las vulnerabilidades más comunes, con la cual buscan captar usuarios incautos para robar información, cuentas o acceder a información de sistemas bancarios o de redes sociales, para luego pedir algún rescate.
* **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 ella transita.
* **Ataques basados en la red.** Problemas de “malware” en dispositivos, que puede tomar el control y realizar acciones no requeridas, por ejemplo: envío masivo de mensajes a los contactos o publicación autónoma en las redes sociales.
* **Por pérdida o robo.** Información, contenido y si esta se encontraba cifrada o no.

## Características

Los dispositivos de comunicación actuales cuentan con mecanismos para la personalización y establecimiento de controles de seguridad directos de fábrica, como son bloqueos remotos, reporte de ubicación en tiempo real e, incluso, el enlace exclusivo con dispositivos específicos, con lo cual se pueden organizar estrategias para su aseguramiento.

La Oficina de Seguridad del Internauta OSI, brinda algunas recomendaciones básicas para contar con un nivel básico de seguridad en los dispositivos. [Enlace](https://www.incibe.es/ciudadania/blog/nuevas-guias-configura-tus-dispositivos-android-e-ios-para-que-esten).

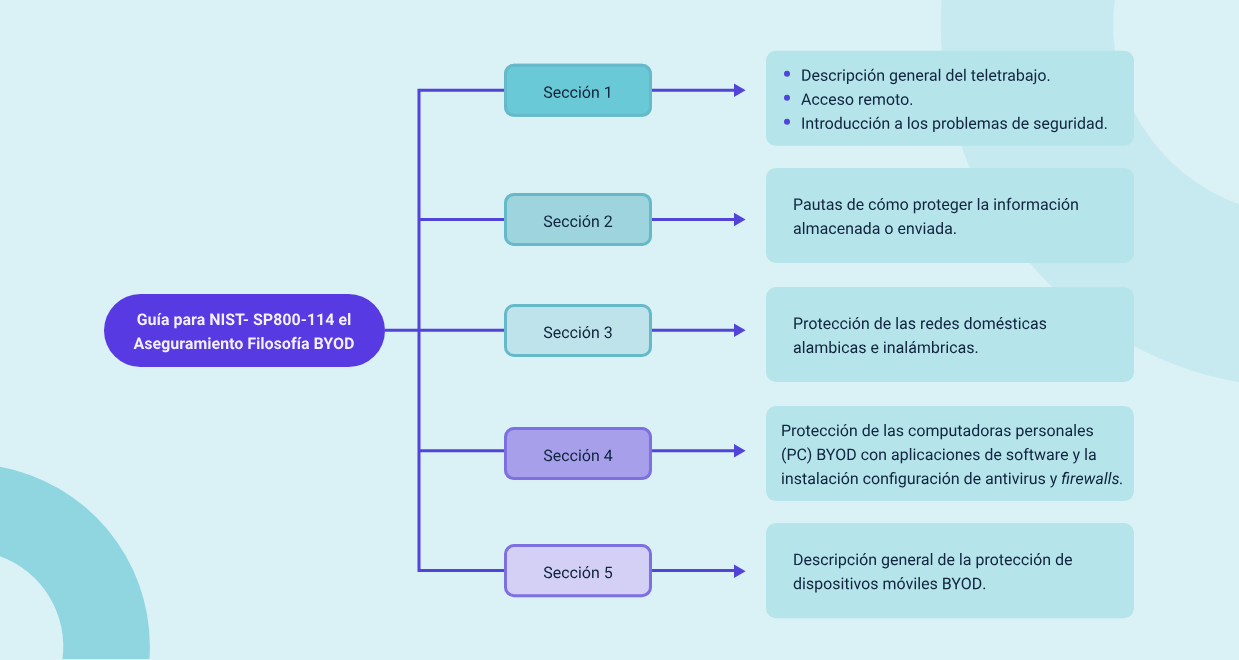
## “Telework and Bring Your Own Device” (BYOD) “Security” (NIST-SP800-114)

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 sus actividades contractuales. [Enlace](https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final).

### Aspectos importantes de la guía

La guía se encuentra estructurada por secciones que abordan los conceptos y las recomendaciones para la implantación de controles, de las cuales se resaltan seguidamente:

1. Guía para NIST-SP800-114



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

### Seguridad en el teletrabajo

Las organizaciones actualmente vienen habilitando las capacidades para poder desarrollar sus actividades sin que necesariamente sus empleados se encuentren en la sede física y, aprovechando la reglamentación y cumplimiento tanto legal como laboral, estas deben garantizar que los empleados cuenten con los recursos necesarios para el desarrollo de sus actividades; entre estos, se encuentran las condiciones de seguridad, por ello, 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 contra “malware” actualizadas.
* 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

A continuación, se van a abordar algunos conceptos importantes en el aseguramiento de infraestructuras críticas, las cuales son las industrias principales de un país.

Dentro de los conceptos relacionados con infraestructuras críticas, se encuentran los siguientes:

* **Infraestructura crítica**. LISA “Institute” define una infraestructura crítica como “las 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)
* **Servicio esencial.** LISA “Institute” lo define como “el 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)

### Tipos

Las infraestructuras críticas abordan sectores primordiales para el desarrollo de las regiones, entre los que se pueden encontrar:

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

## Características

Las infraestructuras críticas presentan algunas características especiales que las diferencian de una organización en particular, entre ellas, está definido que estas infraestructuras brindan servicios esenciales para la sociedad y que, si estas llegan a ser afectadas, podrían afectar negativamente la estabilidad de un país.

Su conformación y complejidad son de gran tamaño, dada la responsabilidad y los activos de información que deben gestionar, así como la obligación de mantener estos servicios casi que siempre disponibles.

Algo que hay que recalcar es que estas infraestructuras críticas, por lo general, están interconectadas con otras infraestructuras, por lo que su interrupción afectaría negativamente el desempeño de algunas otras.

## Marco para mejorar la ciberseguridad de la infraestructura crítica

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. [Enlace](https://www.nist.gov/cyberframework).

### Estructura del marco NIST

El “framework” de NIST se encuentra compuesto por 3 secciones, como se puede identificar a continuación (basado en Gómez, 2009):

1. **Marco básico (“Framework core”).** El “core” es un conjunto de actividades y resultados de ciberseguridad deseados, organizados en categorías y alineados con referencias informativas a estándares adoptados por la industria.

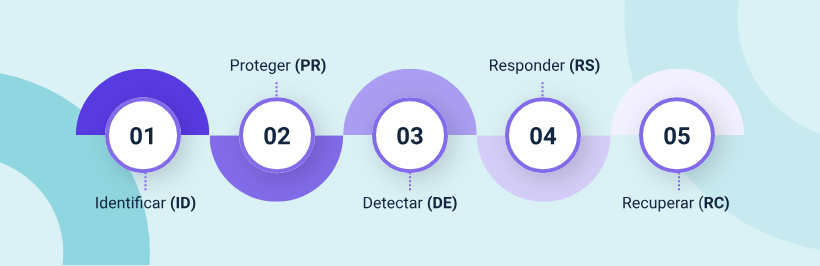
Está diseñado para ser intuitivo y actuar como una capa de traducción, para permitir la comunicación entre equipos multidisciplinarios mediante el uso del lenguaje simplista y no técnico.

El “core” consta de tres partes: funciones, categorías y subcategorías. Incluye cinco funciones de alto nivel: identificar, proteger, detectar, responder y recuperar.

1. **Niveles de implementación del marco (“Framework implementation Tiers”).** Los niveles de implementación le permiten a la organización catalogarse en un umbral predefinido en función de las prácticas actuales de gestión del riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y misión del negocio y las restricciones de la propia empresa.
2. **Perfiles del marco (“Framework profiles”).** Los perfiles se emplean para describir el estado actual (“current profile”) y el estado objetivo (“target profile”) de determinadas actividades de ciberseguridad. El análisis diferencial entre perfiles, permite la identificación de brechas que deberían ser gestionadas para cumplir con los objetivos de gestión de riesgos.

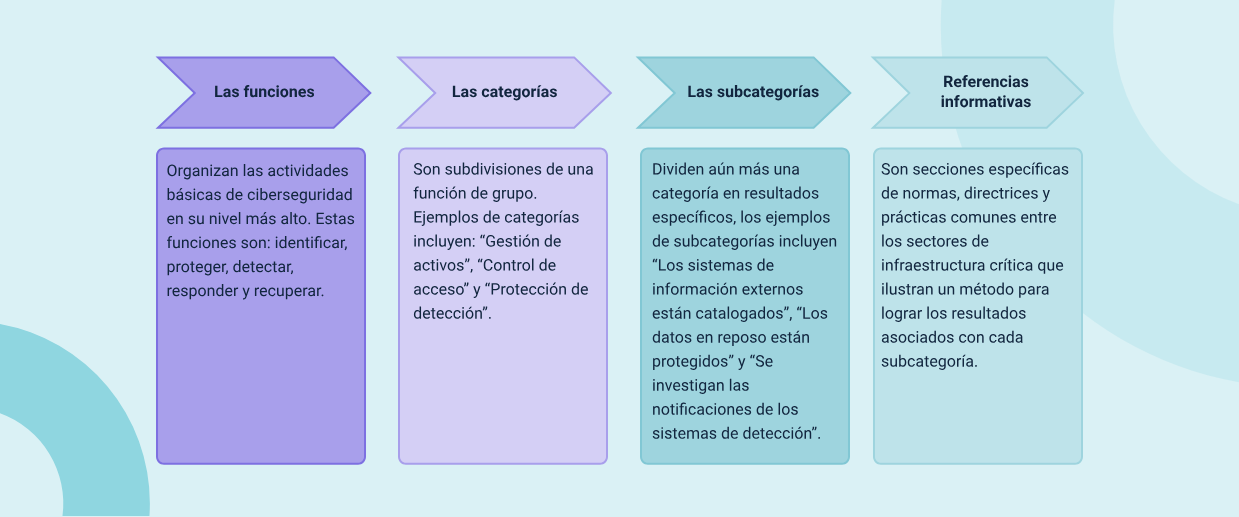
Así, el “core” del “Framework” plantea acciones de ciberseguridad para las infraestructuras críticas. Por otra parte, el núcleo del marco propone 5 funciones básicas secuenciales, como se muestra a continuación:

1. Funciones básicas del Framework de NIST



De igual manera, propone cuatro elementos que enmarcan las actividades y referentes para la aplicación del presente marco, como se puede observar a continuación:

1. Elementos que determinan las actividades a realizar



Nota. Basado en Gómez (2009).

Estas funciones y categorías se articulan para generar un modelo que permita gestionar la ciberseguridad en las organizaciones, como se presenta a continuación.

1. Distribución según tipo de dato

Para ver la tabla, lo invitamos a ver el PDF que se encuentra en la carpeta Anexos con el nombre Anexo Tabla 1.

Ahora bien, a medida que las organizaciones realizan su implementación, se puede determinar su nivel de acuerdo con la siguiente clasificación propuesta:

1. Niveles de implementación

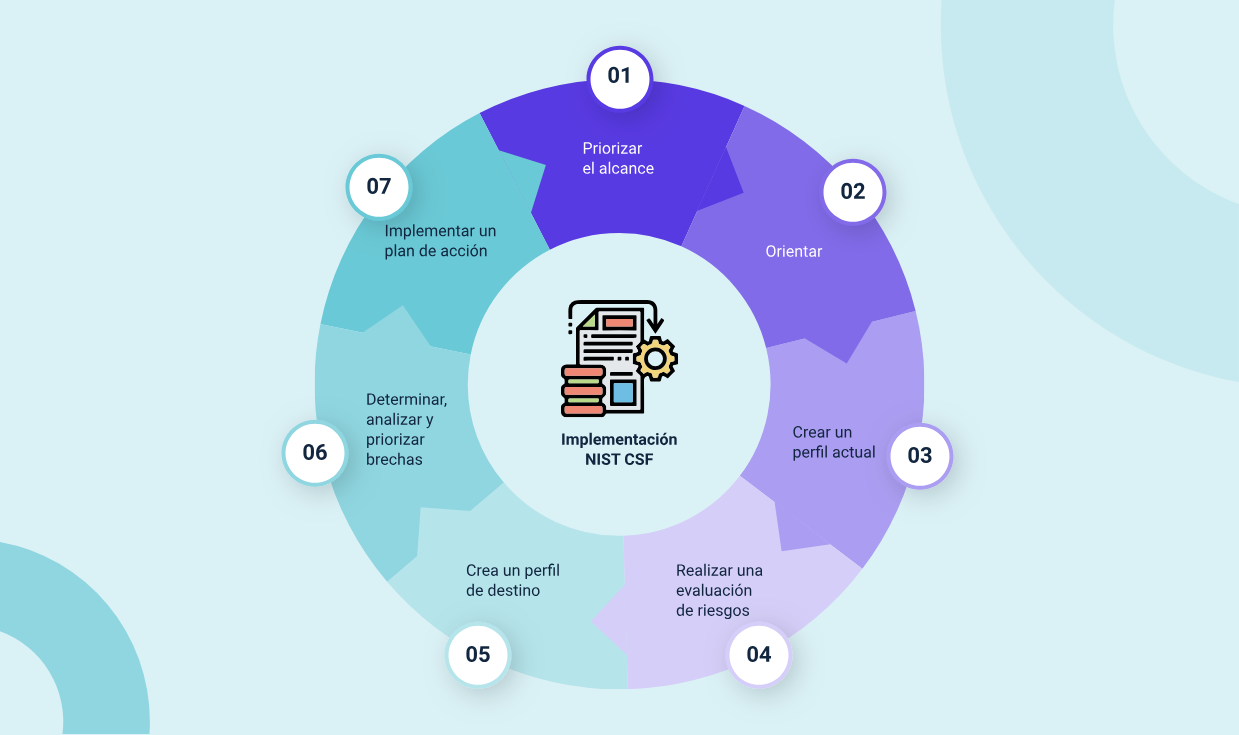
| Nivel | Tipo | Programa de gestión de procesos | Programa de gestión integrada de riesgos | Participación externa |
| --- | --- | --- | --- | --- |
| 1 | Parcial | No se formalizan las prácticas organizativas de gestión de riesgos de ciberseguridad y se gestiona el riesgo de manera ad hoc y a veces reactiva. | Se conoce muy poco el riesgo de ciberseguridad a nivel organizativo y no se ha establecido un enfoque de gestión del riesgo de ciberseguridad en toda la organización. | Puede no tener los procesos establecidos para participar en la coordinación o colaboración con otras entidades. |
| 2 | Riesgo informado | Las prácticas de gestión de riesgos son aprobadas por la administración por la administración, pero no pueden establecerse como políticas de toda la organización. | Se conoce el riesgo de ciberseguridad a nivel organizativo, pero no se ha establecido un enfoque a nivel de toda la organización. | La organización conoce su papel en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente. |
| 3 | Repetible | Las prácticas de gestión de riesgos de la organización son formalmente aprobadas y expresadas como políticas. | Existe un enfoque a nivel de toda la organización para gestionar el riesgo de ciberseguridad. | La organización entiende sus dependencias y socios y recibe información que permite la colaboración y las decisiones de gestión basadas en el riesgo. |
| 4 | Adaptable | La organización adapta sus prácticas de ciberseguridad basadas en las lecciones aprendidas y los indicadores predictivos. | Existe un enfoque a nivel de toda la organización para gestionar el riesgo de ciberseguridad que utiliza políticas, proceso y procedimientos. | La organización gestiona el riesgo y comparte activamente la información con los socios para garantizar que se distribuye información precisa para mejorar la ciberseguridad antes de que se produzca un evento. |

Nota. Basado en Gómez (2009).

### Implementación

El marco se puede implementar en cualquier organización. A continuación, se revisarán los pasos básicos para su adopción:

1. Pasos para la implementación de CSF en una organización



A continuación, se amplía cada uno de los pasos de acuerdo con su papel en la implementación NIST CSF:

* **Paso 1.** Priorizar el alcance: la organización debe identificar sus objetivos de negocio / misión y las prioridades organizacionales de alto nivel para tomar las decisiones estratégicas relacionadas con la implementación.
* **Paso 2.** Orientación: se identifican los sistemas, activos, requerimientos regulatorios, amenazas y vulnerabilidades vinculadas al entorno de aplicabilidad definido.
* **Paso 3.** Crear un perfil actual o literal: a través de las funciones del marco básico y empleando las categorías y subcategorías, se obtienen los resultados de implementación de controles en el entorno.
* **Paso 4.** Ejecutar un análisis de riesgos: se ejecuta un análisis de riesgos que permita determinar la probabilidad y el impacto de eventos de ciberseguridad en el entorno analizado.
* **Paso 5.** Crear un perfil objetivo: se establecen los objetivos que, en términos de ciberseguridad, la organización pretende cubrir.
* **Paso 6.** Determinar, analizar y priorizarlas brechas detectadas: mediante el análisis diferencial entre el perfil actual y el perfil objetivo, se define un plan de acción priorizado en términos de coste/beneficio, que permita la determinación de recursos y acciones de mejora.
* **Paso 7.** Implementar el plan de acción: se procede con la alineación de controles y despliegue de mejoras, de forma paulatina y monitorizada.

# Sistemas de correlacionamiento de “logs” y monitoreo

Los sistemas para el relacionamiento de “logs” y monitoreo de la actividad que pasa sobre nuestra red y dispositivos permiten visión actualizada del nivel de seguridad de los controles implementados.

Estos sistemas, como su nombre lo sugiere, permiten recoger e integrar las salidas de registros, también denominados logs, en una base de datos centralizada, permitiendo agrupar e identificar los comportamientos relacionados con el tráfico, tanto entrante como saliente, de nuestra red y, en especial, de los servidores, generando vistas gráficas de los aspectos más relevantes, como, por ejemplo, eventos de seguridad, dispositivos fuera de línea, ataques de denegación de servicio, entre otros, los cuales, a su vez, permiten notificar, a través de diferentes medios, a un destinatario en particular.

A continuación, podrá conocer algunos aspectos importantes de estos sistemas.

## Conceptos

Mantener una vista del estado de la seguridad de una red requiere de herramientas que permitan representar de manera fácil la información consolidada, esta información de monitoreo proviene de los activos de información y de los controles implementados, los cuales son los encargados de reportar las acciones realizadas. A continuación, se detalla cada uno de ellos:

* **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.
* **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. Estos sensores pueden ser IDS, IPS, sistemas de monitoreo, como, por ejemplo: Snort, Suricata, etc.
* **“Dashboard”.** También llamado 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 es necesario prestar atención. En la siguiente figura, es posible ver un ejemplo de un “dashboard” de un SIEM resaltando activamente las novedades a las que se debe prestar atención.
* **Registro “Log”.** Es un historial de registros de eventos, ordenados en orden cronológico, que almacenan la información de diferentes eventos, como, por ejemplo: sistema operativo, servicio, o registro de autenticación desde una aplicación.

## Tipos

Actualmente, existe una amplia gama de proveedores para soluciones SIEM y de correlación de eventos, entre los cuales es posible resaltar, de acuerdo con licenciamientos, modo de implementación, entre otros; por ejemplo:

Si se analizan las Soluciones SIEM, por tipo de licencia, se encontrará una amplia gama de productos dividida en dos categorías: las comerciales, que cuentan con servicios de actualización de reglas, soporte técnico, mecanismos de integración con más soluciones; y, por otra parte, las soluciones “Open Source”, que son proyectos, por lo general en desarrollo, y que por su naturaleza no ofrecen soporte técnico ni asesoría en la implementación, esto se debe adquirir por aparte.

En la siguiente figura, es posible observar un listado de los productos más representativos disponibles en el mercado:

1. Soluciones SIEM disponibles en el mercado



Nota. Basado en Marty (2013).

## Características

De acuerdo con INCIBE, 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).

Entre las funcionalidades más relevante de un SIEM, se pueden resaltar las siguientes:

* **Cumplimiento:** permite reconocer el nivel de cumplimiento frente a estándares y marcos de seguridad, por ejemplo: ISO 27001, NIST, CIS Controls, entre otras.
* **Analítica:** análisis de información proveniente de servicios o de generadores de datos, por ejemplo: ficheros log de servidores, bases de datos, etc.
* **Protección de dispositivos móviles**: vigilancia permanente de dispositivos móviles, dada la vulnerabilidad presentada por robo y su capacidad de perder información.
* **Protección ante amenazas:** búsqueda, reporte y bloqueo de nuevas amenazas.
* **Administración:** gestión centralizada de los dispositivos protegidos.
* **Protección de datos:** establecer las políticas para el comportamiento ante ciertas acciones.
* **Protección de dispositivos:** capacidad de gestionar dispositivos que presenten algún comportamiento extraño.
* **Protección de red:** capacidad de analizar el tráfico que fluye en la red y tomar acciones de acuerdo con patrones y políticas implementadas.

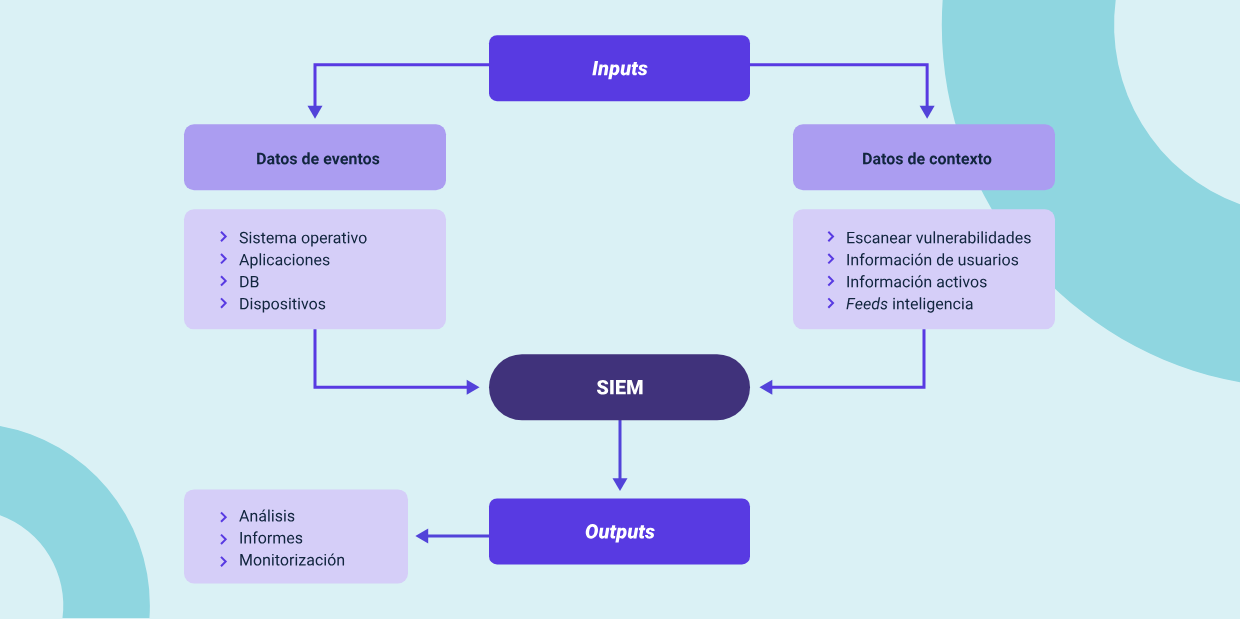
Como se puede observar en la siguiente figura, estas características deben incorporarse como mínimo en un SIEM en una organización para mantener un panorama completo de la seguridad:

1. Funcionalidades de un SIEM

La imagen presenta las funcionalidades de un SIEM, las cuales son:
Compliance
Analytics
Mobile Protection
Threat Protection
Management
Data Protection
Endpoint Protection
Network Protection

Asimismo, es importante resaltar el esquema lógico de un SIEM, que se puede apreciar en la siguiente figura, donde se presenta un esquema de 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, como se había visto en el “dashboard”:

1. Esquema lógico de un SIEM



# Parcheado y/o actualización

La gestión de las actualizaciones y parcheo de los sistemas de información o de los dispositivos de la organización se convierte en un factor fundamental para garantizar la seguridad de la información, ya que, a partir de esta gestión, es posible reducir amenazas por desactualización de sistemas y evitar que terceros puedan aprovecharla.

Desde los estándares de seguridad abordados, se presenta como una premisa que se deben mantener los sistemas de información, aplicaciones e incluso dispositivos de red actualizados en su última versión, lo que garantiza que cuenten con los últimos ajustes y solución a bugs que puedan ser aprovechados para abrir brechas a la seguridad de la información.

A continuación, se van a revisar algunos detalles importantes relacionados con este ejercicio y así poder comprender su utilidad y necesidad de aplicarlos en la infraestructura tecnológica.

## Tipos

Los parches para las aplicaciones se pueden clasificar de acuerdo con cómo están estructurados y cómo se distribuyen, es así como es posible clasificarlos de acuerdo con el código:

* **Parches de archivos binarios:** cuando se realiza el reemplazo de un archivo ejecutable, compilado y que no puede ser alterado por el usuario final.
* **Parches de código fuente:** son las actualizaciones de fragmentos de aplicaciones o rutinas que se implementan en un sistema y este los puede interpretar a partir de un intérprete de comandos, o este tiene la potestad de compilar directamente sobre el sistema, muy comúnmente cuando se realiza parcheo de aplicaciones web.

Ahora bien, los parches también se pueden clasificar de acuerdo con el propósito para el cual fueron generados, es así como es posible clasificarlos de la siguiente manera:

* **Parche de reparación:** parche que corrige fallas o bugs en los sistemas.
* **Parche de seguridad:** parches que solucionan agujeros de seguridad o brechas en la seguridad de este, sin modificar la funcionalidad del sistema.
* **Parche de actualización**: este tipo de parches actualiza algunas rutinas, métodos, o agrega funcionalidades al sistema.
* **Parche de traducción:** este tipo de parches permite cambiar el lenguaje de un sistema.
* **Parche de piratería ilegal:** este parche, denominado también “crack”, permite liberar funcionalidades o alterar rutinas del sistema de manera ilegal.

No se recomienda la aplicación de este tipo de parches en organizaciones.

## Características

A continuación, se van a reconocer algunas características y recomendaciones para una adecuada gestión de parches y actualizaciones en sistemas de información y de arquitecturas tecnológicas en las organizaciones:

* Buscar información de actualizaciones y descargarlas de sitios oficiales.
* Validar las actualizaciones, tanto de manera previa como posterior, para verificación de funcionalidad de los sistemas.
* Preferiblemente, realizar la instalación en ambiente de pruebas, y posteriormente, en producción.
* Siempre mantener las actualizaciones de los sistemas al día, a excepción de las documentadas por requerimientos técnicos o compatibilidades.
* Mantener los sistemas operativos, sistemas de información y aplicaciones de uso diario actualizados.
* 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.

# Plan de capacitación y concienciación

La estrategia de formación a las personas interesadas, empleadas o que administran la información en las organizaciones hoy en día cobra gran importancia, dado que, aun a pesar de la gran capacidad de adquisición tecnológica, herramientas e implementación de controles, se necesitan fortalecer y formar en las siguientes habilidades:

* Formar conciencia en el manejo seguro de la información.
* Enfrentar amenazas de ingeniería social donde se aprovechan de estas debilidades de las personas que administran la información para socavarla, y, haciendo uso de engaños o campañas falsas, buscan acceder a los activos de la organización con fines delictivos.
* Fortalecer las habilidades para la gestión de entornos de trabajo seguros, donde sus empleados consigan organizar, en primer lugar. espacios limpios y que no dejen a disposición de terceros información sensible.
* Fortalecer las capacidades para gestionar la información haciendo uso de herramientas y buenas prácticas que eviten que terceros puedan interceptarla.

A continuación, vamos a establecer algunas recomendaciones para el establecimiento de planes de capacitación que se sugieren sean adoptados por las organizaciones.

## Ruta de actualización

Partiendo de la premisa que las organizaciones deben invertir en formar a su personal y establecer la forma en que estos deben gestionar y salvaguardar la información, estas deben de establecer los planes de formación y actualización que precisa su personal, estar al tanto de las últimas estrategias que utilizan los ciberdelincuentes para acceder a la información, así como reconocer algunos comportamientos anómalos que, si bien no conocen del tema por no ser de su competencia, deberán conocer una ruta para reportar a las áreas responsables de cada organización; para esto, se recomienda que las organizaciones consideren algunas de las siguientes rutas de información:

1. Técnicas más comunes utilizadas por los ciberdelincuentes:

* Ingeniería social.
* “Phishing”.
* “Spam”.
* “Pharming”.
* Accesos físicos.

1. Ataques más comunes de la actualidad:

* Cifrado (“Ransomware”).

1. Normatividad vigente:

* SGSI.
* Normatividad gubernamental (instituciones públicas).

1. Uso de herramientas seguras para la gestión de la información en la organización:

* Navegadores seguros.
* Herramientas criptográficas.

1. Buenas prácticas de seguridad:

* Campañas para mantener un escritorio y entorno limpios.

1. Ataques de ingeniería social:

* Reconocimiento.
* Actuación frente a un ataque.

1. Incidentes que afecten la seguridad de la información:

* Ruta para el reporte de incidentes.
* Acciones a realizar durante y después del incidente.

Los temas expuestos anteriormente son algunos de los que se recomienda sean abordados por el personal, lo cual permitirá reconocer y determinar el actuar frente a un incidente.

## Estrategia de transferencia del conocimiento

Las estrategias para la transferencia del conocimiento hacia el personal deben ser dinámicas y que no solo se queden en un momento de charla; se recomienda que se considere que los planes de capacitación cuenten con algunas de las siguientes estrategias que permitan reforzar la seguridad de la información:

* **Capacitaciones “in situ” periódicas.** Estas permitirán convocar a que las personas asistan a jornadas de capacitación sobre temas que permitan mejorar la seguridad de la información.
* **Canales de autoformación.** Establecer medios para que los empleados consulten y realicen ejercicios para mejorar sus capacidades de seguridad para la gestión de la información.
* **Ejercicios de demostración.** Conformar ejercicios para que los empleados se enfrenten a situaciones, como, por ejemplo, de ingeniería social, lo cual les permitirá reconocer patrones de comportamiento, así como identificar la ruta de actuación frente a una situación en particular.
* **Campañas de socialización**. Las campañas de socialización que se puedan desplegar a través de fondos de escritorios, volantes, correos, mensajería instantánea, donde se den tips y recomendaciones para la gestión de la seguridad.

Estas acciones se pueden articular de acuerdo con las características de cada una de las organizaciones y de los activos que administre, permitiendo fortalecer en sus empleados esas capacidades de identificar, enfrentar y evitar que se consoliden incidentes que afecten la seguridad de la información.

Síntesis

Como pudo darse cuenta con la presentación de las propuestas de controles que se pueden adoptar en una organización, es también importante tener presente que su análisis y viabilidad deben ser evaluados de acuerdo con sus características propias para determinar cuáles controles se consideran adecuados y cuáles deberían de obviarse para la gestión de la ciberseguridad. A continuación, se representa de forma visual lo visto en el componente:

La imagen nos presenta una síntesis de la temática estudiada en el componente formativo.
Comienza con los controles de seguridad, los cuales permiten recurrir a la probabilidad de materialización de una amenaza, a partir de la adopción de las normas técnicas (ISO 27001, ISO 27032 e ISO 31000), los marcos de trabajos basados en NIST, los marcos de buenas prácticas, basados en CIS Controls, y la normatividad vigente (MinTIC y Conpex).

Material complementario

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia | Tipo de material | Enlace del recurso |
| 1. Gestión de acceso | Arroyo, D., Gayoso, V. y Hernández, L. (2020). ¿Qué sabemos de? Ciberseguridad. Editorial CSIC. | Libro digital | <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/172144> |
| 1. Gestión de acceso | ISO. (2022). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. | Norma técnica | <https://www.iso.org/standard/54534.html> |
| 1. Gestión de acceso | NIST. (2021). Cybersecurity Framework. | Norma técnica | <https://www.nist.gov/cyberframework> |
| 2. Firewall | Server World. (2020a). Apache2: Configure SSL/TLS. | Artículo | <https://www.server-world.info/en/note?os=Ubuntu_20.04&p=httpd&f=3> |
| 2. Firewall | Server World. (2020b). FTP: Vsftpd Over SSL/TLS. | Artículo | <https://www.server-world.info/en/note?os=Ubuntu_20.04&p=ftp&f=6> |
| 2. Firewall | Server World. (2020c). OpenSSH: Password Authentication. | Artículo | <https://www.server-world.info/en/note?os=Ubuntu_20.04&p=ssh&f=1> |
| 7.1 Tipos | SeguriLatam. (2020). Seguridad en dispositivos móviles: ¿cuáles son las ciberamenazas más peligrosas? | Artículo | <https://www.segurilatam.com/actualidad/ciberseguridad-seguridad-en-dispositivos-moviles-cuales-son-las-ciberamenazas-mas-peligrosas_20201005.html> |

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.

Referencias bibliográficas

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

B, G. (2022). ¿Qué es SSL, TLS y HTTPS? Hostinger Tutoriales. <https://www.hostinger.es/tutoriales/ssl-tls-https>

Belcic, I. (2022). ¿Qué es el malware? Avast. <https://www.avast.com/es-es/c-malware>

Bitdefender. (s. f.). Unificación de la prevención, correlación entre endpoints, detección, respuesta y análisis de riesgos para cualquier organización. <https://www.bitdefender.es/business/products/gravityzone-enterprise-security.html>

C, K. (2018). SFTP vs. FTPS Comparison: Which One Is Better? MSP360. <https://www.msp360.com/resources/blog/sftp-vs-ftps/>

Chasco, I. (2015). SSH: Las cosas que no sabías. Irontec. <https://blog.irontec.com/ssh-las-cosas-que-no-sabias/>

Cisco Systems. (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. <https://www.fortinet.com/lat/products/smallbusiness/utm>

Gómez, G. (2019). ¿Qué es el Cybersecurity Framework de NIST de los Estados Unidos? Esan Business. <https://www.esan.edu.pe/conexion-esan/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos>

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

Instituto Nacional de Ciberseguridad [INCIBE]. (2020). ¿Qué son y para qué sirven los SIEM, IDS e IPS? <https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips>

ISO. (2022). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. <https://www.iso.org/standard/54534.html>

Kuenzler, J. (2014). LDAP over SSL – LDAPs with Windows Server 2008 R2 (Secure LDAP). Active Directory Faq. <https://activedirectoryfaq.com/2014/04/ldap-over-ssl-ldaps-server-2008-r2/>

LISA Institute. (2019). Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación. <https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas>

Malwarebytes. (2021). Malware. <https://es.malwarebytes.com/malware/#what-is-malware>

Marty, R. (2013). Log Management and SIEM Vendors. Raffael Marty – Blog. <https://raffy.ch/blog/2013/07/11/log-management-and-siem-vendors/>

Myers, L. (2016). Todo sobre cifrado: qué es y cuándo deberías usarlo. Welivesecurity. <https://www.welivesecurity.com/la-es/2016/02/09/todo-sobre-cifrado-cuando-usarlo/>

NIST. (2021). Cybersecurity Framework. <https://www.nist.gov/cyberframework>

Oficina de Seguridad del Internauta [OSI]. (2019). ¿Sabías que existen distintos tipos de cifrado para proteger la privacidad de nuestra información en Internet? <https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad>

Créditos

| Nombre | Cargo | Regional y Centro de Formación |
| --- | --- | --- |
| Claudia Patricia Aristizábal | Líder del Ecosistema | Dirección General |
| Rafael Neftalí Lizcano Reyes | Responsable de Línea de Producción | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Hernando José Peña Hidalgo | Experto Temático | Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander |
| Diego E. Acevedo Guevara | Diseñador Instruccional | Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Centro de Diseño y Metrología - Regional Distrito Capital |
| Darío González | Corrector de Estilo | Centro de Diseño y Metrología - Regional Distrito Capital |
| Francisco José Lizcano Reyes | Desarrollador Fullstack | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Juan Daniel Polanco Muñoz | Diseñador de Contenidos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Ángela María Maldonado Jaime | Ilustración | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Carlos Eduardo Garavito Parada | Animador y Productor Multimedia | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| María Carolina Tamayo López | Locución | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Emilsen Alfonso Bautista | Actividad Didáctica | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Zuleidy María Ruíz 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 | Evaluador para Contenidos Inclusivos y Accesibles | Centro Industrial del Diseño y la Manufactura - Regional Santander |