

Fundamentos para la gestión del riesgo de ciberseguridad

**Breve descripción:**

En este componente se aborda la fundamentación requerida para la implementación de métodos de análisis y valoración de los riesgos de ciberseguridad que se puedan presentar en una organización, utilizando una metodología y normativa adecuada.

**Junio 2023**

Tabla de contenido

[Introducción 1](#_Toc138780548)

[1. Conceptos y fundamentos asociados a la gestión de la ciberseguridad 3](#_Toc138780549)

[1.1. Tipos de redes 6](#_Toc138780550)

[1.2. Modelo OSI 9](#_Toc138780551)

[1.3. Protocolo TCP/IP 13](#_Toc138780552)

[1.4. IPv4 e IPv6 17](#_Toc138780553)

[1.5. Enrutamiento IP 23](#_Toc138780554)

[1.6. Arquitecturas “Cloud y On Premise” 26](#_Toc138780555)

[1.7. Vulnerabilidad, amenaza y riesgo 33](#_Toc138780556)

[2. Normatividad y estándares de seguridad de la información 40](#_Toc138780557)

[2.1. ISO 27001 41](#_Toc138780558)

[2.2. ISO 27002 7](#_Toc138780570)

[2.3. ISO 27032 13](#_Toc138780573)

[3. Metodologías para la gestión del riesgo 17](#_Toc138780574)

[3.1. Magerit 17](#_Toc138780575)

[3.2. ISO 31000 29](#_Toc138780583)

[Síntesis 33](#_Toc138780584)

[Material complementario 34](#_Toc138780585)

[Glosario 36](#_Toc138780586)

[Referencias bibliográficas 38](#_Toc138780587)

[Créditos 39](#_Toc138780588)

Introducción

Mediante la evaluación de la seguridad digital se puede determinar la situación de ciberseguridad al interior de una organización que permita implementar diversos estándares propios de la seguridad informática, aplicando el uso de metodologías para un acercamiento a los potenciales riesgos presentes en Internet. Por lo anterior, es muy importante elegir de acuerdo con los requerimientos específicos de cada organización los métodos y las metodologías indicados con base al modelo de seguridad que se quiera implementar. Revise el siguiente video de introducción al componente formativo.

1. Fundamentos para la gestión del riesgo de ciberseguridad



[**Enlace de reproducción del video**](https://youtu.be/rIInW1zOe_I)

|  |
| --- |
| **Síntesis del video: fundamentos para la gestión del riesgo de ciberseguridad** |
| En este componente formativo se definen algunos elementos básicos que conforman una red de comunicaciones, los riesgos que se presentan en ella y la importancia de implementar una metodología para determinar un análisis del riesgo y los correctivos necesarios para minimizarlo.  Será el espacio para conocer los diferentes tipos de redes existentes en las organizaciones, entender su funcionamiento, combinaciones y protocolos.  Y, a través del estudio de la normatividad propia de la seguridad de la información, reconocer una metodología que permita la implementación de la ciberseguridad acorde a cada situación organizacional en particular. |

# Conceptos y fundamentos asociados a la gestión de la ciberseguridad

Para entrar al mundo de la ciberseguridad, es clave conocer algunos conceptos asociados que permitan entender su funcionamiento, arquitectura, implementación y utilidad. Manejar estos conceptos permite tener un panorama claro al enfrentar diferentes escenarios, ya que cada organización cuenta con su propia implementación de las Tecnologías de la Información y la Comunicación.

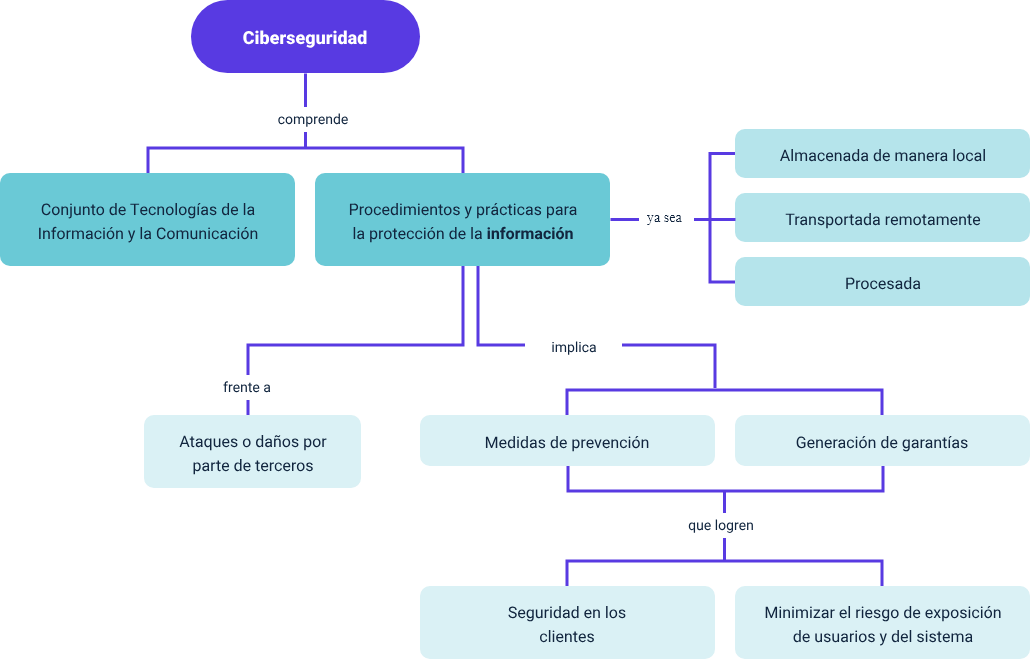
A medida que evoluciona la ciencia la dependencia o confianza en los sistemas informáticos sigue aumentando, la tecnología se incorpora cada vez más en todo tipo de organizaciones ya sean privadas o públicas. El uso de nuevas tecnologías y la necesidad de conexión con el mundo exterior trae consigo nuevos desafíos, que obligan a las empresas a pensar en la ciberseguridad como un tema de vital importancia, considerando que:

* La información que se maneja dentro de las empresas es el activo más importante.
* Las organizaciones están sometidas a la ley y esta las obliga a salvaguardar la información de sus usuarios.

De manera tal que, los expertos en temas de ciberseguridad son cada día más demandados y tienen mayores posibilidades laborales. Las empresas han entendido que la prevención es fundamental en la protección de sus activos informáticos, logrando así evitar vulnerabilidades que puedan desatar grandes daños en la organización, lo que hace que cada vez más se requiera tener profesionales con estas capacidades.

Observe la siguiente figura en un primer acercamiento a la definición de ciberseguridad:

**Figura 1.** Ciberseguridad



La ciberseguridad pretende proteger computadoras, dispositivos móviles, sistemas electrónicos, servidores de aplicaciones, base de datos, redes, entre otros, de la posibilidad de amenazas que se conviertan en ataques, afectando los activos informáticos. En ese sentido se hace relevante conocer las arquitecturas de red, los protocolos y cómo funciona el transporte de los datos para poder crear planes, procedimientos y políticas usando una metodología que ayude a mitigar el riesgo y darle garantías a los usuarios y a los sistemas.

Avance sobre los siguientes conceptos clave en el abordaje de la ciberseguridad:

* **Seguridad de red:** capacidad para proteger una red de dispositivos informáticos del ataque de intrusos, ya sea planeado intencionalmente o por parte de programas malignos que aprovechan vulnerabilidades.
* **Seguridad de aplicaciones:** garantía de que el “software” y dispositivos instalados en una organización se mantengan libres de amenazas. Las aplicaciones afectadas podrían generar agujeros de vulnerabilidad y dar acceso a datos importantes.
* **Seguridad de la información**: se debe garantizar la integridad y protección de los datos, ya sea que se haga de manera local, en el transporte o en la recepción.
* **Seguridad operacional:** procedimientos definidos para el manejo y protección de datos. Implica privilegios asignados a usuarios para el acceso a la red y los sistemas (cómo y cuándo pueden almacenar, modificar o compartir información).
* **Recuperación de desastres**: capacidad y procedimientos de una organización para responder a un incidente de ciberseguridad que pueda causar detenimiento de las operaciones diarias y/o pérdida de los datos.
* **Usuario final:** la principal preocupación de las organizaciones, ya que son las personas más difíciles de controlar, pudiendo incumplir con buenas prácticas de seguridad establecidas (ingreso accidental o intencional de virus al sistema).

## Tipos de redes

Las redes que se presentan a continuación están relacionadas con la interconexión física que se puede realizar entre computadoras, servidores, dispositivos móviles, impresoras, dispositivos electrónicos, entre otros. Estas redes se clasifican en diferentes tipos de acuerdo con su implementación, dependiendo del tamaño y la cobertura de la red de ordenadores o dispositivos electrónicos vinculados. Revise en el siguiente video los tipos de redes más importantes.

1. Tipos de redes



[**Enlace de reproducción del video**](https://youtu.be/sSQWQEna6ow)

|  |
| --- |
| **Síntesis del video: tipos de redes** |
| El video habla sobre los diferentes tipos de redes según su alcance y función. Estas redes incluyen:  “Personal Area Network” (PAN): Es utilizada para intercambiar información entre dispositivos inteligentes cercanos, como computadoras, smartphones y tabletas. Tiene una cobertura de corto alcance y se utiliza para compartir internet, archivos o jugar en red con dispositivos cercanos.  “Local Area Network” (LAN): Consiste en varios ordenadores conectados físicamente por cable o de forma inalámbrica. Utiliza el estándar Ethernet y requiere dispositivos adicionales como “routers, switches, firewalls” y puntos de acceso inalámbrico. Las LAN pueden cubrir múltiples oficinas en un edificio utilizando conexiones cableadas e inalámbricas.  “Metropolitan Area Network” (MAN): Permite la interconexión de múltiples redes LAN en un área geográfica cercana, como diferentes sedes de una empresa. Se utilizan conexiones de cableado de alta velocidad para lograr una mayor velocidad de transmisión de datos.  “Wide Area Network” (WAN): Son redes de área amplia que abarcan un alcance geográfico mayor, como entre países o continentes. Para implementar una WAN, se requiere contratar servicios de empresas de comunicaciones que se conectan a nivel mundial. La conexión se realiza a través de un servicio de datos público en una red global conocida como “Global Area Network” (GAN). La conexión de redes LAN a WAN puede presentar riesgos de seguridad y requiere controles para proteger la información.  “Virtual Private Network” (VPN): Permite la interconexión de redes LAN o equipos independientes utilizando un canal público, pero con medidas de protección adicionales. A diferencia de las WAN, que utilizan un canal físico, las VPN utilizan un canal virtual cifrado para proteger la información transmitida.  Cada tipo de red tiene sus características y propósitos específicos, y la elección depende de las necesidades de conectividad y seguridad de cada situación. |

Las organizaciones cuentan con uno o varios tipos de red, las cuales se pueden combinar para cumplir objetivos específicos. Una empresa puede iniciar con una oficina pequeña y una red LAN, pero con el tiempo abrir sedes en diferentes ciudades del país y contratar redes WAN para mayor seguridad, aunque con mayores costos, o utilizar el canal público creando canales virtuales de conexión con menor costo, pero que le implica apostar a esquemas de seguridad eficientes.

Conectarse a una red pública genera desafíos importantes para salvaguardar la información, por lo que se recomienda tomar medidas de protección como:

* Instalación de “firewall”, ya sean físicos o de “software” como los instalados en las computadoras.
* Utilización de “router” avanzados con capacidad de bloqueos de paquetes sospechosos.

## Modelo OSI

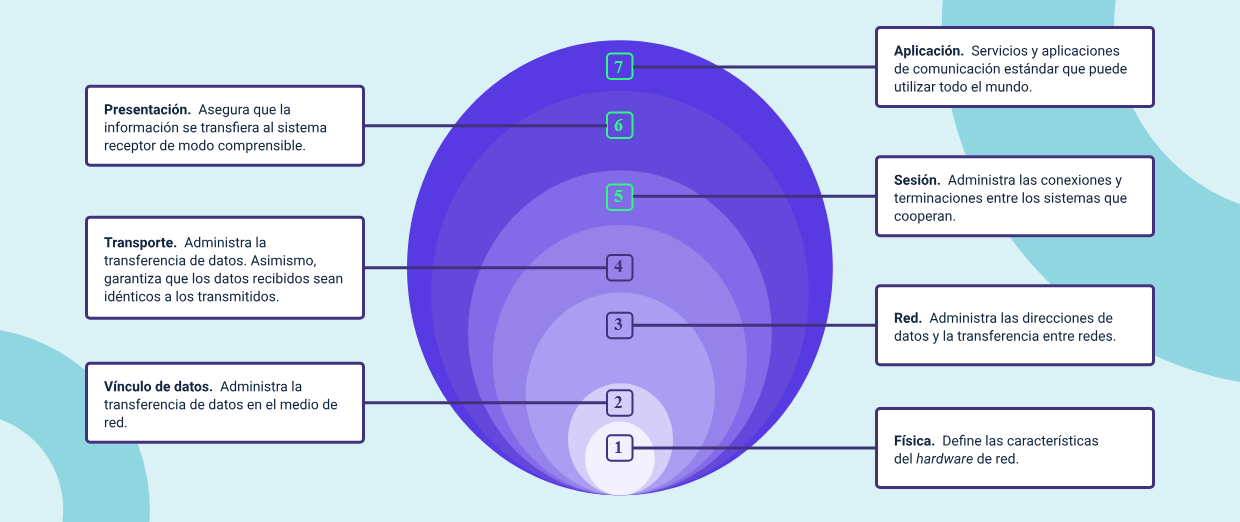
El modelo de interconexión de sistemas abiertos, creado por la Organización Internacional de Normalización (ISO) proporciona a los diversos sistemas de tecnología de la informática estándares para que se comuniquen entre sí.

Este modelo se divide en siete capas para realizar las actividades que la red necesita, asociando a cada capa una serie de protocolos, con el propósito de abordar la complejidad que conlleva la comunicación a través de problemas sencillos.

Se plantea una estructura jerarquizada en la que cada una de las capas realiza trabajos para la capa que está por encima de ella, devolviendo resultados y solicitando servicios a la capa ubicada en la parte inferior.

La siguiente imagen muestra las capas del modelo de interconexión de sistemas abiertos y su correspondiente descripción.

**Figura 2.** Modelo de referencia de interconexión de sistemas abiertos



A continuación, profundice en las características de las capas del modelo y el trabajo que realiza cada una de las etapas estudiadas en la anterior imagen.

* **Física:** en esta primera capa se encuentran los dispositivos físicos encargados de transportar los datos: los cables de red (de cobre para redes LAN o de fibra óptica para el transporte de información a grandes distancias), los “router” para el direccionamiento de paquetes, los “switch” que ayudan a la agrupación de varios equipos en una misma red, y en general todos los componentes que de alguna u otra manera se encargan de llevar información de un lado al otro.
* **Vínculo de los datos**: realiza la verificación de lo que entrega el medio físico en la búsqueda de errores para que, en caso de encontrarlos, se pueda corregir. También controla el flujo de datos que se transmiten. Presenta dos subcapas:
  + **MAC** (“Media Access Control”). Conecta varios equipos de cómputo a una red con una dirección física (dirección MAC) que identifica la ubicación del equipo para el envío y la recepción.
  + **LLC** (“Logical Link Control”). Maneja el control de flujo de los datos de la red.
* **Red:** garantiza que los datos lleguen a su destino aún sin que el emisor y receptor estén conectados de forma directa. Esta labor involucra dispositivos electrónicos enrutadores (“router”, en inglés). En esta capa se establece el direccionamiento IP tanto de origen como de destino, se priorizan paquetes y la toma de decisiones para dirigirlos por la ruta más eficiente.
* **Transporte:** nivel responsable de la confiabilidad del transporte, a través de dos protocolos:
  + **TCP:** establece una sesión entre dos ordenadores, garantizando fidelidad con la creación de una secuencia de datos para la entrega. Es un protocolo lento que verifica que la recepción de los paquetes esté completa y solicita el reenvío en caso de faltantes.
  + **UDP:** se ofrece sin conexión y sin establecer sesión entre ordenadores. Es mucho más rápido porque solo entrega información en el menor tiempo posible, sin verificar completitud.
* **Sesión:** en la capa de sesión la principal responsabilidad es inicializar y terminar la conexión entre dos ordenadores. Es esta capa la que inicia y sincroniza los equipos y realiza tareas como la de registro del “log” y algunas funciones de seguridad.
* **Presentación:** capa encargada de realizar el tratamiento de los datos: convertir códigos de caracteres, conversión y comprensión de la información. En caso de requerir el cifrado de los datos al realizar este tratamiento los datos ya estarían listos para ser entregados a la siguiente capa.
* **Aplicación:** finalmente, la capa 7, último nivel jerarquizado en el modelo OSI. Esta capa interactúa directamente con el usuario final, por ejemplo, la visualización de una página web cuando se hace una petición a una URL mediante el Protocolo HTTPS o el envío de un correo electrónico mediante el Protocolo SMTP. Son varios los protocolos que se activan, dependiendo la tarea que desee realizar el usuario final.

Para conocer la dirección física de un equipo siga el procedimiento que se detalla en el video:

1. Dirección Física



[**Enlace de reproducción del video**](https://youtu.be/C5BpaaNij8I)

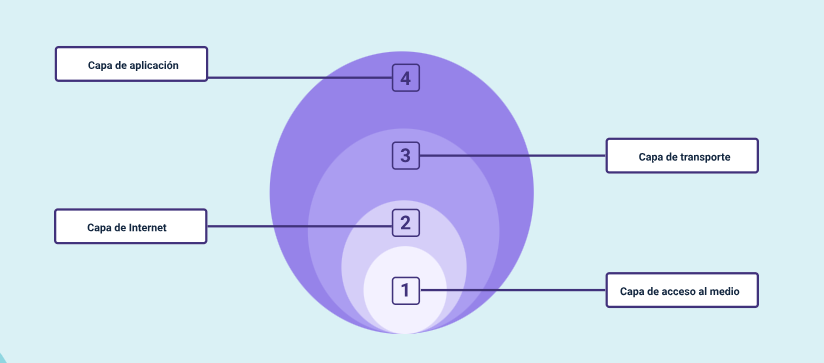
|  |
| --- |
| **Síntesis del video: dirección Física** |
| En este video se explora la dirección física, la cual es una identificación única asignada a la tarjeta de red de un dispositivo y se utiliza para identificar y comunicarse con dicho dispositivo en una red local. |

## Protocolo TCP/IP

Hace referencia a un grupo de protocolos de red que permiten que se realice la transferencia de los datos a través de los diferentes tipos de redes, dispositivos informáticos o de Internet. El protocolo de control de transmisión TCP es el que garantiza que se establezca la conectividad y el intercambio de información entre dos dispositivos y el transporte confiable de los datos. Mientras que el protocolo de Internet IP se encarga de llevar la información a otros equipos en la red, este utiliza identificadores de cuatro octetos separados por un punto decimal, por ejemplo, "192.168.0.1".

Al igual que en el modelo OSI, el modelo TCP/IP (ver figura 3) propone un conjunto de capas jerarquizadas, en la misma dinámica en la que la capa inferior entrega información a la capa superior y así progresivamente se hace el control de los paquetes en cada capa dependiendo de la función que le corresponda. Específicamente se revisarán los protocolos que se encargan de realizar estas tareas en cada uno de esos niveles.

**Figura 3.** Modelo TCP/IP



Para cada una de las capas del modelo TCP/IP se establece una serie de protocolos, cada uno con una función específica, que se presentan en la siguiente tabla con su respectiva equivalencia en el modelo OSI.

1. Modelo TCP/IP con equivalencia al modelo OSI

| Capa TCP/IP | Ejemplos de protocolos TCP/IP | Equivalente de capa OSI | Ref. OSI  Número de capa |
| --- | --- | --- | --- |
| Aplicación | NFS, NIS, DNS, LDAP, TELNET, FTP, RLOGIN, RSH, RCP, RIP, RDISC, SNMP Y OTROS. | Aplicación, sesión, presentación | 5, 6, 7 |
| Transporte | TCP, UDP, SCTP | Transporte | 4 |
| Internet | IPv4, IPv6, ARP, ICMP | Red | 3 |
| Red física | ETHERNET (IEEE 802.3), TOKEN RING, RS-232, FDDI Y OTROS.  PPP, IEEE 802.2 | Física | 1, 2 |

A continuación se definen algunos de los protocolos más importantes usados en el modelo TCP/IP.

* **Internet “Protocol”:** es el núcleo de todo el modelo. Se utiliza para especificar la dirección IP determinando así, la ruta que tiene que seguir el paquete.
* **Internet Control “Message Protocol”:** provee mensajes de diagnóstico y notificación de errores cuando fallan los datagramas IP.
* **“Address Resolution Protocol”:** ayuda al protocolo IP a guiar los datos, resolviendo la dirección de “hardware” o MAC.
* **“Reverse Address Resolution Protocol”:** lo mismo que el ARP, pero al revés, es decir, dada la MAC devuelve la IP.
* **“Network Address Translation”:** convierte la dirección IP privada a una pública.
* **“Routing” Information Protocol”:** utilizado por los “router” para intercambiar información de las distintas redes y encaminar con mayor eficiencia los paquetes.
* **Capa de transporte:** garantiza que los paquetes lleguen sin errores y en secuencia, uno después de otro.
* **“User Datagram Protocol”:** implementa una transmisión no fiable (no está exenta de errores), usada en aplicaciones de “streaming” y con actualizaciones en tiempo real.
* **“Transmission Control Protocol”:** establece una transmisión fiable de datos. Incluye detección de errores y formas de recuperar los datos perdidos.
* **Capa de aplicación:** proporciona servicios de red que conectan la interfaz con el sistema operativo para que el usuario interactúe con la máquina (enviar correos, descargar información, etc.).
* **“File Transfer Protocol”:** transferencia interactiva de archivos.
* **“Telnet”:** iniciación de la sesión de forma remota en máquinas de la red.
* **“Hypertext Transfer Protocol”:** transferir archivos que forman las páginas web de la **“World Wide Web”.**
* **“Simple Mail Transfer Protocol”:** transferencia de mensajes de correo electrónico y archivos adjuntos.
* **“Domain Name System”:** resolución del nombre de un “host” a la dirección IP.

Ahora, observe el siguiente video sobre el modelo TCP/IP, haciendo uso de un ejemplo:

1. Modelo TCP - IP



[**Enlace de reproducción del video**](https://youtu.be/HhgkV7YDhXY)

|  |
| --- |
| **Síntesis del video: modelo TCP - IP** |
| El video explica el modelo TCP/IP utilizando un ejemplo simple de envío de una página web desde un servidor a un cliente. El proceso comienza en la capa de aplicación, donde la página se formatea y codifica en binario. Luego, en la capa de transporte, se fragmentan los datos y se agrega información como los números de puerto. En la capa de red, se añaden direcciones IP y en la capa de enlace de datos se incluyen direcciones MAC. En la capa física, se codifican las señales para viajar a través del medio de comunicación. En el cliente, se decodifican las señales y se realiza el proceso inverso en cada capa. Los mensajes se llaman datos, segmentos, paquetes, tramas y bits en las diferentes capas. |

## IPv4 e IPv6

En la actualidad casi todo dispositivo que se conecta a la red lo realiza mediante el protocolo IP versión cuatro (IPv4). La estructura de este protocolo está formada por hasta 12 caracteres divididos por un punto en cuatro segmentos de hasta 3 caracteres, por ejemplo, la dirección IP de Google es 64.233.177.113, esta dirección es posible obtenerla gracias al sistema de nombres de dominios (DNS), que traduce un nombre de dominio a su respectiva dirección IP. Estas direcciones IP son asignadas públicamente y permiten el acceso desde cualquier lugar del mundo.

Para obtener la dirección pública de un sitio siga el procedimiento que se detalla en el video:

1. IP Pública



[**Enlace de reproducción del video**](https://youtu.be/eU9I0xE_5Yg)

|  |
| --- |
| **Síntesis del video: IP Pública** |
| El video presenta el procedimiento para obtener la dirección IP pública de un sitio web. La dirección IP pública es un identificador único asignado a un dispositivo en una red, en este caso, a un servidor web. Al obtener la dirección IP pública de un sitio, se puede acceder directamente a ese servidor utilizando la dirección IP en lugar de un nombre de dominio. |

Por otro lado, cada máquina privada debe tener una dirección IP propia que le permita identificarse de manera única dentro de una red local. Esto garantiza que cada ordenador sea reconocido y que los paquetes puedan llegar a él. De esta manera, no pueden existir direcciones IP con la misma numeración.

Para obtener la dirección IP privada de un sitio siga el procedimiento que se detalla en el video:

1. IP Privada



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

|  |
| --- |
| **Síntesis del video: IP Privada** |
| El video presenta cómo obtener la dirección IP privada de un sitio web, se centra en la obtención de la dirección IP privada de un sitio web, es importante destacar que la dirección IP privada es un identificador asignado a un dispositivo en una red local, como una red doméstica o empresarial. La dirección IP privada permite la comunicación interna dentro de esa red, pero no es accesible desde Internet público. |

Como se aprecia en el video esa dirección IP es asignada mediante adaptador físico inalámbrico “WiFi”. En caso de estar conectado por medio del cable, el adaptador físico sería el “ethernet”.

El direccionamiento IP de una organización es supremamente importante, toda vez que ayuda a identificar cuáles serán las áreas en las que se deben aplicar permisos o restricciones. Por ejemplo, el bloqueo o acceso controlado de las direcciones IP de los servidores de datos. También son útiles para realizar el monitoreo de la red e identificar posibles fallas de seguridad, entre otras funcionalidades.

En cuanto al protocolo de Internet versión seis (IPv6), una mejora de su antecesor, el protocolo IP versión cuatro, pretende mejorar la escasez de direcciones que se presentan con la versión anterior. En Colombia se promueve su implementación desde 2020 y su adopción es importante ya que contribuye con la transformación digital. Incrementar el número de direcciones IP aumentará la cantidad de dispositivos electrónicos conectados a la red, abriendo la posibilidad a nuevos servicios, aplicaciones y plataformas, también beneficiará el desarrollo de ciudades inteligentes, la implementación de Internet de las cosas, el uso de “blockchain” y redes de sensores, entre muchas más aplicaciones.

El gran número de direcciones que se pueden albergar radica en que se pasa de una estructura de 32 bits a una de 128 bits, cuatro veces superior a la versión número cuatro. El formato de texto de la dirección IPv6 es xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, donde cada x corresponde a un dígito hexadecimal que representa 4 bits, que si bien tiene una estructura más difícil de entender, generará múltiples beneficios.

Para obtener la dirección IP privada de un sitio siga el procedimiento que se detalla en el video:

1. IPv6



[**Enlace de reproducción del video**](https://youtu.be/beKW7owSgdg)

|  |
| --- |
| **Síntesis del video: IPv6** |
| El video presenta cómo obtener la dirección IPv6 es el protocolo de Internet versión 6 (IP, Internet Protocol) que permite conectar diversos dispositivos a internet, identificándolos con una dirección única. |

La siguiente tabla diferencia los dos protocolos en algunas de sus características principales:

1. Diferencias entre el protocolo IPv4 e IPv6

|  |  |  |
| --- | --- | --- |
| Característica | IPv4 | IPv6 |
| Longitud de la dirección en *bits* | 32 *bits* | 128 *bits* |
| Representación de las direcciones | Decimal | Hexadecimal |
| Separador de octetos | Punto (.) | Dos puntos (:) |
| Límite de IP | 4.000 millones | 340 sextillones |
| Autoconfiguración | No. Solo configuración manual y a través de DHCP | Sí. Configuración automática y renumeración de direcciones |
| Cifrado | No compatible | Compatible a nivel protocolo |
| Ejemplo IP | 192.168.20.28 | 2800:484:2085:50b:5f9:60d:25aa:1369 |

La adopción de este protocolo tiene múltiples ventajas dentro de las que destacan:

* El número de direcciones IP será casi ilimitado.
* Mayor seguridad con el protocolo e IPsec.
* Mejores rendimientos en la configuración automática con respecto al DHCP utilizado en la anterior versión, está en la capacidad de dar soporte nativo para los dispositivos móviles.
* Mayor eficiencia al momento de simplificar el encabezado de los paquetes o al tener que hacer un enrutamiento más jerárquico.

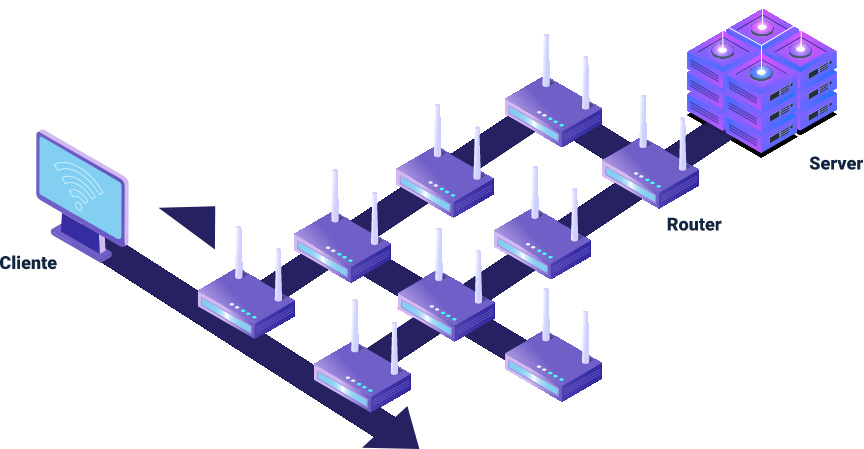
La adopción ha sido un poco lenta, pero ya se vienen preparando los diferentes dispositivos electrónicos para que se dé el cambio.

## Enrutamiento IP

El enrutamiento que realizan las redes de datos consiste en la selección óptima de una ruta o de una o múltiples redes. En general, los conceptos de enrutamiento son aplicables a cualquier tipo de red, que pueden ir desde redes telefónicas hasta la analogía con el transporte público. En cuanto a la red de Internet se realiza un enrutamiento teniendo en cuenta que los paquetes o datos del protocolo de Internet IP viajan desde su origen hasta su objetivo final, la selección de estas rutas es posible gracias a dispositivos de “hardware” que comúnmente conocemos como “router” o enrutadores.

Imagine tratando de llegar a su lugar de trabajo identificando posibles rutas. Es la ruta más corta en cuanto a recorrido, pero que normalmente presenta trancones y tráfico lento, y la ruta rápida en la que, aunque el recorrido es mucho mayor, avanza a mayor velocidad. Tal como se muestra en la figura 4 los “router” deben tomar ese tipo de decisiones, determinando cuál camino será el más eficiente para llegar al destino y realizando el monitoreo permanente de la red.

**Figura 4.** Enrutamiento IP



Los enrutadores deben guardar y actualizar periódicamente la tabla de enrutamiento, el servicio de enrutamiento de cada dispositivo se actualiza con las rutas que logre identificar. Estas tablas, leídas antes del reenvío de paquetes a la red del área local se encargan de realizar la identificación de la dirección IP de las redes conocidas por el sistema, que incluye la red del área local que está predeterminada. También enumeran las diferentes direcciones IP de un sistema de portal para las redes conocidas (los portales son sistemas que están preparados para recibir datos de salida y hacer el reenvío más allá de la red del área local).

El administrador de la red es el encargado de la configuración de rutas estáticas que se realizan manualmente dado que no pueden actualizarse automáticamente, como sí lo haría el protocolo de “routing” dinámico. En caso de cambiar la topología de la red se debe configurar nuevamente de forma manual.

El enrutamiento estático ofrece tanto ventajas como desventajas comparado con el “router” dinámico.

Dentro de sus principales ventajas es posible mencionar:

* Mejora la seguridad, ya que estas no se anuncian por toda la red.
* La ruta que utiliza un camino estático para compartir la información es conocida.
* El consumo del ancho de banda es mucho menor que los protocolos utilizados para el “routing” dinámico, ya que no es necesario utilizar ciclos de CPU para el cálculo y la comunicación de rutas.

En cuanto a sus desventajas se señala que:

* Demanda una configuración de inicio y un mantenimiento que ocupa mucho tiempo.
* Cuando se configuran redes de gran tamaño, las configuraciones son susceptibles de errores.
* Se necesita un administrador permanente que realice los cambios, cuando la información de la ruta cambie.
* Es necesario conocer toda la red para que la implementación se haga de manera correcta.

Los protocolos de “routing” dinámico están desarrollados para que el intercambio de información de “routing” entre los “router” sea más fácil. Estos protocolos conforman una serie de procesos, algoritmos y mensajes utilizados para permitir enviar y recibir información del “routing”, con el objetivo de llenar las tablas de enrutamiento seleccionando los caminos más eficientes.

Observe en la siguiente figura los principales objetivos y componentes de los protocolos de “routing”.

**Figura 5.** Protocolos de “routing”, objetivos y componentes

En la figura se presenta los objetivos  del routing estos son: Descubrimiento de redes remotas.
Actualización permanentemente de la información del routing.
Selección eficiente del mejor camino hacia redes destino.
En caso de fallas en la ruta establecida, descubrimiento de nuevos caminos.

Además, los componentes estos son: Estructura de datos. Utilizan para su almacenamiento y operación base de datos o tablas guardadas en la memoria RAM.
Mensajes del protocolo de routing. Para descubrir router vecinos utilizan una serie de mensajes para intercambiar información del routing y realizar tareas como descubrimiento de red y almacenamiento de información.
Algoritmos. Facilitan información en la tarea de encontrar los mejores caminos hacia una ruta destino.


Los protocolos de “routing” establecerán el mejor camino hacia la red destino, posteriormente esa ruta o camino se dispone en la tabla de “routing” y si no existe otra ruta con una distancia administrativa mucho menor, se instalará en la tabla de “routing”.

Las rutas estáticas son eficientes para redes pequeñas en las que solo se tiene una ruta a la red externa, ofrecen también un mayor nivel de seguridad en redes un poco más grandes para el tráfico específico o en caso de enlazarse con diferentes redes que necesiten más control.

La implementación de una técnica u otra dependerá de cada organización y puede utilizarse de manera independiente o de forma combinada.

## Arquitecturas “Cloud y On Premise”

Se inicia definiendo el término “On Premise” que hace referencia a la implementación de una infraestructura tecnológica que puede incluir servidores de aplicaciones, bases de datos, correo electrónico, instalación de “software”, entre otros. Este tipo de arquitecturas requieren una infraestructura compleja en la que se debe pensar en servidores de respaldo, energía de respaldo, copias de seguridad y un equipo especializado para el mantenimiento y la administración.

Las arquitecturas “On Premise” siguen siendo comunes en las empresas, ya que existen muchos “software” que fueron desarrollados pensando en este tipo de despliegues, en el que no era necesario tener una conexión a Internet para que el “software” funcionará correctamente.

El hecho de que las implementaciones estén pensadas solamente para funcionar dentro de la empresa genera inconvenientes como:

* Manipulación indebida y daños por parte de personal no calificado, y el contratarlo implica mayores costos para la organización.
* El acceso a la información que solo es posible directamente desde las oficinas.

En cuanto a las arquitecturas tipo “Cloud” y gracias a la evolución de Internet hoy se puede contar con implementaciones que inicialmente se pensaron para trabajar de manera local y migrar a arquitecturas de tipo nube, que combinan varios componentes tecnológicos que gracias a la tecnología denominada virtualización se agrupan y hacen posible compartirlos a través de la red.

Dentro de los componentes que incluye la arquitectura de la nube figuran los siguientes:

* **Plataforma “front-end”:** herramienta utilizada por el cliente o el dispositivo para acceder a la nube.
* **Plataforma “back-end”:** tiene que ver con el despliegue de servidores y el almacenamiento de información.
* **Modelo de implementación basado en la nube**: pueden ser implementaciones completamente en la nube, soluciones híbridas o de nube privada.
* **Red:** conexión a través de los diferentes tipos de red.

Al unir estas tecnologías en una arquitectura tecnológica informática tipo nube se pueden desplegar múltiples aplicaciones, brindando a sus usuarios todo el potencial y capacidad de aprovechamiento.

El siguiente video presenta las principales ventajas, posibilidades de la arquitectura y servicios en la nube, observe con atención:

1. Arquitectura y servicios en la nube



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

|  |
| --- |
| **Síntesis del video: arquitectura y servicios en la nube** |
| Arquitectura y servicios en la nube: las organizaciones recurren a la nube para optimizar el desarrollo de la informática operacional y, de esta forma, impactar en la producción, así como mejorar la infraestructura y la dinámica laboral. A la vez, se satisfacen las demandas actuales a un menor costo de tiempo, riesgo y producto.  En la última década, la nube ha evolucionado, pues cada tipo de servicio y método de implementación aporta distintos niveles de control, flexibilidad y administración. Esta solución informática basada en la internet, en la que recursos compartidos son entregados mediante redes, y la compatibilidad operativa de estos servicios en la nube, tradicionalmente se definen en tres tipos principales de servicio: IaaS, PaaS y SaaS. Estas ofrecen servicios que se establecen mediante capas, las cuales se distribuyen entre el usuario, el acceso al servicio y el recurso, para que todo lo anterior suceda efectiva y eficazmente.  Para lograr esto, los roles y sus responsabilidades de cada uno de los actores y de los escenarios que intervienen en el proceso, es decir, los usuarios, el administrador, los diferentes gerentes que tienen a cargo el direccionamiento y la gestión desde la operación hasta el seguimiento al cliente, los diferentes proveedores del servicio, hasta el gestor de riesgos y de seguridad en la prestación del servicio en la nube. Sin embargo, no existe una prestación de servicio perfecta, por lo que el plan de mejora debe ser una tarea permanente.  Esto es posible mediante la optimización de gastos, contar con un excelente equipo especializado y disponible 24/7 y, sobre todo, posibilitar auditorías permanentes que verifiquen e intervengan el proceso cuando se está prestando y no solamente a manera de apagar incendios. Esto es calidad. |

Ya sea que se enfrente a una arquitectura de implementación local, una arquitectura en la nube o un despliegue híbrido, siempre se deberá tener en cuenta una metodología para la implementación de políticas de ciberseguridad, entendiendo las características propias de cada una de las arquitecturas. Se puede tener la mejor infraestructura, pero sin procedimientos, permisos y restricciones claramente definidos a través de una buena metodología, se podrían enfrentar serios problemas en la integridad de la información.

Revise ahora algunos elementos clave a considerar en cuanto a costos y seguridad para la implementación de arquitecturas tecnológicas:

1. Implementación de arquitecturas tecnológicas



[**Enlace de reproducción del video**](https://youtu.be/0AO0cUe3CCg)

|  |
| --- |
| **Síntesis del video: implementación de arquitecturas tecnológicas** |
| Implementación de arquitecturas tecnológicas comparada con la arquitectura tipo “Cloud”: la arquitectura de implementación local requiere inversión de licenciamiento y desplegar toda una infraestructura basada en el “software”, haciendo necesario considerar gastos iniciales como compra de equipos, adecuación de área con condicionamiento climático, sistema de seguridad y vinculación de personal especializado.  Ahora bien, tras la instalación y puesta en marcha, los costos permanecen, ya que se necesita mantenimiento permanente a toda la infraestructura instalada para tener alta disponibilidad. Prácticamente, se debe duplicar todo lo implementado para que, al momento en que falle, por ejemplo, un servidor, se active el de respaldo. Cuando la implementación es una arquitectura que se realiza en la nube, se paga solamente por lo contratado. La empresa se desentiende de elementos de infraestructura que implican mantenimientos, copias de seguridad, sistemas de respaldo, alta disponibilidad, entre otros, que realizados de manera local implican mayores costos.  Otra importante ventaja es que, si el negocio crece vertiginosamente, se pueden aumentar las capacidades tecnológicas sin afectar la operación de la empresa. Se podría pensar que la infraestructura local ofrece mayores niveles de seguridad con protocolos propios, más seguros, que respalden la información. Pero también se está expuesto a una mala manipulación por parte de algún empleado no cualificado que puede incidir en la integridad de la información o la ocurrencia de un evento, como por ejemplo, un grave incendio, sin que sea posible salvaguardar los activos informáticos.  Actualmente, las grandes empresas que proveen servicios en la nube tienen múltiples centros de cómputo con tecnología de vanguardia en diferentes lugares del mundo. En caso de fallar alguno de estos Data Center, en cuestión de segundos se redirecciona a otros servidores sin perder información. Muchas empresas con infraestructuras locales utilizan la nube para labores de seguridad, como hacer los respaldos de copias de seguridad y manejo de archivos importantes.  Otro tema determinante en el montaje de la arquitectura tiene que ver con los ataques informáticos. Si se hace de manera local, se debe implementar equipos y “software” especializado, y contratar personal especializado en temas de seguridad. Si las implementaciones son en la nube, la empresa con la que se contrate el servicio garantizará la integridad de la información ante posibles ataques externos. En todo caso, sigue siendo responsabilidad de la empresa contratante la implementación de métodos y políticas para salvaguardar la integridad de la información desde su ámbito de acción. |

## Vulnerabilidad, amenaza y riesgo

Hoy en día, la seguridad de los activos informáticos es prioritaria para todas las empresas, ya que cuando los sistemas son atacados, pueden sufrir consecuencias lamentables: pérdida de información, suspensión del servicio, mala imagen ante los clientes e incluso el pago de sanciones económicas por no proteger correctamente la información.

La ciberseguridad, entonces, se convierte en una necesidad prioritaria para aquellas empresas que quieran obtener en el sector donde operan las garantías para blindar sus activos informáticos y por supuesto, la información.

En ciberseguridad se habla de tres conceptos importantes: amenazas, vulnerabilidades y riesgos, términos que para la mayoría de las personas no son del todo claros y suelen presentar confusiones.

Observe el pronunciamiento que al respecto hace la ley:

**Figura 6.** Riesgo, amenaza y vulnerabilidad

La figura presenta la Ley 1523 de 2012, que aborda los conceptos de Riesgo, Amenazas y Vulnerabilidad.

Riesgo se define como el daño o la pérdida potencial causada por eventos físicos peligrosos, ya sean de origen natural, socio-natural, tecnológico, biosanitario o humano. Este riesgo está determinado por la vulnerabilidad de los elementos expuestos. En otras palabras, el riesgo de desastres surge de la combinación de la amenaza y la vulnerabilidad.

Por su parte, las Amenazas se refieren al peligro latente de que ocurra un evento físico, ya sea de origen natural o causado accidentalmente por la acción humana. Estos eventos pueden ocasionar pérdida de vidas, impacto en la salud, daños en bienes, infraestructuras, medios de sustento, prestación de servicios y recursos ambientales.

La Vulnerabilidad se define como la predisposición a sufrir pérdidas o daños por parte de los seres humanos, sus medios de subsistencia y los sistemas físicos, sociales, económicos y de apoyo, después de haber sido afectados por eventos físicos peligrosos.

En sistemas informáticos, la vulnerabilidad se entiende como la incapacidad de un sistema para protegerse permitiendo ser atacado y recibiendo daño. Estas debilidades en los sistemas son ocasionadas normalmente por no contar con una eficiente protección ante amenazas externas, el no realizar actualizaciones periódicas, posibles fallos en la programación, entre otras causas.

A estas vulnerabilidades se les denomina agujeros de seguridad y aunque tienen la ventaja de que una vez descubierta la falla, se pueden solucionar, también dejan los datos y sistemas de una empresa en riesgo, comprometiendo la integridad, privacidad y disponibilidad de la información. Los huecos de seguridad exponen los sistemas a diversas amenazas que aumentan el riesgo de que se produzcan ataques en cualquier momento, enfrentando a las empresas a complejas situaciones.

Uno de los objetivos principales de la ciberseguridad consiste en lograr la identificación de las debilidades que puedan existir, aplicando los correctivos necesarios para que desaparezcan.

Las amenazas informáticas hacen referencia a eventos o situaciones de seguridad que pueden afectar un sistema en estado de vulnerabilidad y sufrir daños. Los sistemas informáticos regularmente están expuestos a amenazas que vienen de ataques externos como la denegación del servicio, inyecciones SQL, “malware , spyware”, crimen organizado, entre otros. Vea en qué consisten a través del siguiente video:

1. Ataques de seguridad en la red



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

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

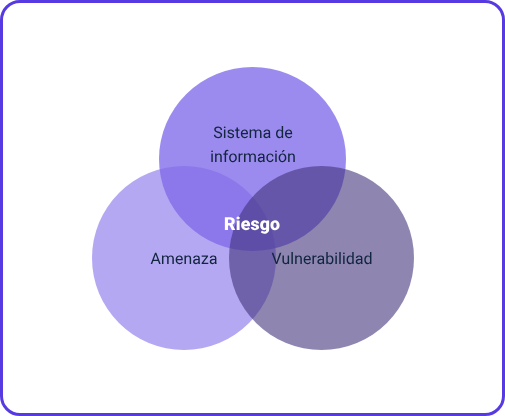
Las amenazas pueden provocar una vulnerabilidad, ya sea de manera intencional o accidentalmente y robar, dañar o eliminar un activo.

Las siguientes son consideradas las amenazas más comunes a las que se enfrenta la infraestructura IT:

* **Código malicioso**:ataques tipo “malware” cuyo objetivo es robar datos sensibles de dispositivos y servidores, como información bancaria. Los ataques “ransomware” constituyen una de las amenazas de mayor preocupación para los sistemas informáticos empresariales.
* **Amenazas persistentes avanzadas**: conocidas como APT, estos ataques se coordinan y dirigen hacia una empresa con el objetivo de robar su información, son muy difíciles de detectar ya que utilizan como estrategia la ingeniería social.
* **Denegación de servicio:** las amenazas DDoS vulneran los servidores enviando un gran volumen de peticiones de modo que estos no puedan responderlas y el servicio termine por colapsar.
* **Robo de identidad o “phishing”:** importante amenaza que consiste en engañar al usuario para que facilite involuntariamente sus datos de acceso a alguien desconocido, para posteriormente usarlos de forma fraudulenta.
* **Negligencia**:las equivocaciones humanas y el hacer caso omiso a las políticas y normativas de seguridad que la empresa establece, colocan en riesgo latente los sistemas e información de la compañía.

El término riesgo en ciberseguridad tiene que ver con las amenazas y las vulnerabilidades que pueden afectar parcial o totalmente los activos informáticos, dejando como consecuencia daños importantes en la información.

**Figura 7**. Representación del riesgo



El riesgo se determina, entonces, con la alineación de las amenazas, una vulnerabilidad y el dispositivo o sistema informático, por ejemplo, un ordenador que no cuente con protecciones mínimas como antivirus o un sistema operativo actualizado es un equipo que tiene vulnerabilidades, está expuesto a amenazas como “malware” que de llevarse a cabo podría instalar virus que encripten información y cobren luego por devolverla. Si además este equipo presenta la vulnerabilidad de no contar con usuario y contraseña para el ingreso, está amenazado por cualquier empleado de la organización que pueda extraer información importante como, por ejemplo, de tipo financiero.

Las amenazas siempre van a existir, y en cuanto a las vulnerabilidades lo que se debe hacer es minimizarlas al máximo. Llámese sistema de información, dispositivos de red o el usuario final, si se evita la alineación de estos elementos, la probabilidad del riesgo disminuye.

# Normatividad y estándares de seguridad de la información

La ciberseguridad toma cada día mayor fortaleza gracias al creciente número de incidentes que sufren las empresas a causa de los ataques asociados a los sistemas y a la información. Esto ha hecho que recurra a controles para garantizar la seguridad de los dispositivos informáticos, activos de información y redes de comunicaciones, entre otros. A partir de esta serie de nuevos requisitos se empieza a hablar del concepto de ciberseguridad.

Realizar un control eficaz a través de la implementación de un plan de ciberseguridad no es tarea sencilla, considerando el reto de enfrentarse a grandes cantidades de equipos, nuevas tecnologías, ciberdelincuencia en búsqueda permanente de nuevos ataques que allanen las vulnerabilidades de los sistemas. A pesar de esto, se puede pensar en la implementación de medidas para la protección de la información a través de procedimientos basados en estándares establecidos para temas de seguridad informática.

La Organización Internacional de Normalización (ISO) y la Comisión Electrónica Internacional (IEC) referentes en la normalización a nivel mundial, en conjunto construyen comités técnicos encargados de la elaboración de normativas internacionales que son redactadas con el objetivo de realizar la regulación de procesos específicos en todo lo que tiene que ver con la seguridad de la información. Hoy en día estos estándares y normas juegan un papel importante, instando a las organizaciones a adelantar su implementación, con altos niveles de cumplimiento, a través de lo cual adquieren prestigio y reconocimiento. El valor agregado que aporta este tipo de certificaciones es fundamental, haciendo que clientes y accionistas vean con buenos ojos a la organización y depositen en ella su confianza.

Las normas establecidas por la ISO están numeradas de manera incremental acorde con su objetivo, a su vez se dividen en familias que agrupan temáticas afines. El principal objetivo de estas normas y estándares yace en la identificación de nuevas y mejores técnicas, guías, capacitaciones, políticas, entre otras encaminadas a un propósito específico, por ejemplo, seguridad, calidad o escalabilidad.

## ISO 27001

Conocida como la “Norma Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos” ISO/IEC 27001 (en lo sucesivo, ISO/IEC 27001) especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). El SGSI presenta un enfoque sistemático para mantener segura la información confidencial y gestiona personas, procesos y sistemas de TI mediante la aplicación de procesos de gestión de riesgos. El SGSI de una organización certificado según la Norma ISO/IEC 27001 demuestra el compromiso de una organización con la seguridad de la información y brinda confianza a sus clientes, socios y partes interesadas.

ISO/IEC 27001 está diseñada para usarse junto con controles de apoyo, como los relacionados en el documento ISO/IEC 27002 (en lo sucesivo, ISO/IEC 27002) que detalla 114 controles de seguridad organizados en 14 secciones y 35 objetivos de control.

### Requisitos de certificación

Para cumplir con los requisitos de la certificación ISO/IEC 27001, el SGSI de una organización debe ser auditado por un organismo de certificación acreditado internacionalmente. Los requisitos de las secciones 4 a 10 de ISO/IEC 27001 son obligatorios y no se permiten exclusiones. Una vez superada la auditoría formal, el organismo de certificación otorga a la organización un certificado ISO/IEC 27001 por su SGSI válido por 3 años, luego de lo cual el SGSI debe volver a certificarse.

Durante el período de validez de 3 años, la organización debe realizar el mantenimiento del certificado para confirmar que el SGSI sigue cumpliendo, opera según lo especificado y mejora continuamente. Para mantener la certificación, el organismo de certificación visitará el sitio del SGSI al menos una vez al año para realizar una auditoría de vigilancia. Durante la auditoría de vigilancia solo se auditará una parte del SGSI. Hacia el final del período de 3 años el organismo de certificación audita todo el SGSI.

### Beneficios de la certificación

La certificación ISO/IEC 27001 traerá beneficios a la organización tanto en seguridad interna como en competitividad externa. Internamente al adoptar ISO/IEC 27001 una organización puede beneficiarse entre otros aspectos, de los relacionados en la siguiente figura.

**Figura 8.** Certificación ISO/IEC 27001 - Beneficios internos



Externamente, al dar a conocer el hecho de que ISO/IEC 27001 está certificada, la organización contaría dentro de sus beneficios con los elementos representados en la figura que aparece a continuación:

**Figura 9.** Certificación ISO/IEC 27001 – Beneficios externos

La figura representa los beneficios externos como: 
Proporcionar a los clientes y partes interesadas confianza en la gestión de riesgos y la seguridad de información confidencial. 

Salvaguardar y mejorar la reputación de la organización con procesos de seguridad validados por un organismo de certificación independiente.

Facilitar el cumplimiento de obligaciones legales como la ordenanza de la Privacidad de Datos Personales (PDP).

Recibir una ventaja competitiva, que ayuda a la organización a atraer más inversores y clientes.

Mejorar la consistencia en la entrega de servicios y productos, impactando la satisfacción y retención de los clientes.

Mejorar la protección de la organización, los activos, los accionistas y los directores.

Mejor preparación para enfrentar las expectativas de los clientes, cada vez más sensibles a los incidentes de seguridad de la información.

La certificación de un estándar internacional reconocido puede convertirse gradualmente en un requisito previo impuesto por muchos clientes.


### Organismos de certificación

El proceso de certificación ISO/IEC 27001 implica la acreditación por parte de organismos de certificación. Dicha acreditación se otorga a las organizaciones que han demostrado cumplir plenamente con los requisitos de las normas internacionales ISO/IEC 17021 “Evaluación de la conformidad: requisitos para los organismos que brindan auditoría y certificación de sistemas de gestión” e ISO/IEC 27006 “Requisitos para los organismos que brindan auditoría y certificación de sistemas de gestión de seguridad de la información”.

### Acreditación servicio por ISO/CEI 27001

La certificación fue lanzada oficialmente por el Servicio de Acreditación de Hong Kong (HKAS) el 15 de noviembre de 2011. Los organismos de certificación pueden comunicarse con HKAS y solicitar la acreditación de forma voluntaria.

### Costos de certificación

La certificación inicial incluye los costos tanto para implementar el SGSI como para certificar ISO/IEC 27001. El costo de implementación depende en gran medida de las brechas entre los controles de seguridad existentes y los controles requeridos dentro de la organización. En términos de costos de implementación hay costos y recursos para implementar controles de seguridad, redacción de documentación, capacitación del personal, etc. La certificación en sí, incluye el costo de los auditores externos (que cobran una tarifa determinada por día), tarifas de solicitud, tasas de certificados y tasas de mantenimiento.

### Nivel de adopción e implementación

Según ISO Survey (2020), había unos 44.500 certificados ISO/IEC 27001 válidos en 137 países y economías de todo el mundo al 31 de diciembre de 2020. Los tres principales países y economías por el número total de certificados válidos eran China (unos 12.00), Japón (unos 5.600) y el Reino Unido de Gran Bretaña e Irlanda del Norte (unos 3.300). Según la información de la misma encuesta, el número de certificados válidos en Hong Kong era de unos 186, número que incluía algunos departamentos gubernamentales certificados según ISO/IEC 27001 para áreas funcionales específicas.

### Descripción general del proceso de implementación y certificación de ISO/IEC 27001

Revise en el siguiente paso a paso el detalle del proceso de implementación y certificación para ISO/IEC 27001:

* **Paso 1.** **Definir la política de seguridad de la información.**

Tarea: identificar los objetivos comerciales y obtener el apoyo de la gerencia para implementar un programa de mejora de la seguridad.

* **Paso 2. Definir el alcance del SGSI.**

Tarea: comparar el sistema de gestión de seguridad de la información existente con los requisitos de ISO/ 2 IEC 27001 y seleccionar qué unidades de negocio, departamentos o sistemas cubrirá el SGSI.

* **Paso 3.** **Realizar una evaluación de riesgos.**

Tarea: definir un método de evaluación de riesgos, hacer un inventario de los activos de información para proteger y clasificar los activos, de acuerdo con la clasificación de los riesgos basada en la evaluación de los riesgos.

* **Paso 4.** **Gestionar el riesgo identificado.**

Tarea: crear un plan de tratamiento de los riesgos para identificar acciones de gestión, recursos, responsabilidades y prioridades apropiadas para gestionar los riesgos de seguridad de la información.

**Paso 5**. **Seleccionar los controles a implementar.**

Tarea: preparar una declaración de aplicabilidad (SoA) para documentar qué controles son aplicables al SGSI y la forma en que se implementarán.

* **Paso 6.** **Implementar controles**

Tarea: desarrollar programas para implementar los controles identificados.

* **Paso 7.** **Prepárese para la certificación.**

Tarea: operar el SGSI y realizar un ciclo completo de auditorías internas, revisiones de gestión y actividades.

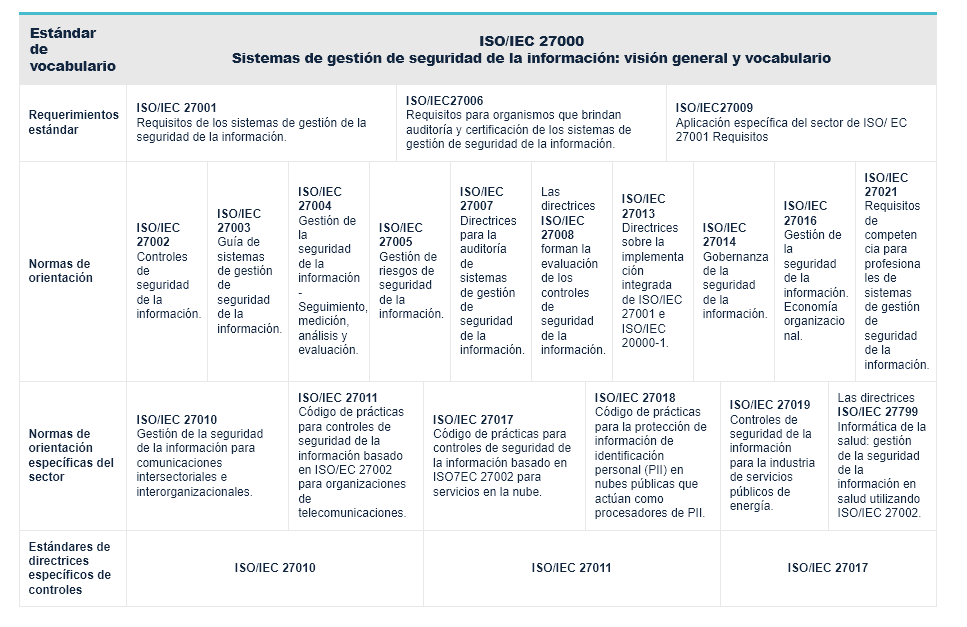
* **Paso 8.** **Solicitar la certificación.**

Tarea: continuar con la solicitud de la certificación que incluye etapas de revisión de los documentos y la auditoría de cumplimiento en el sitio.

### Familia de ISO/IEC 27000

Consta de normas y directrices interrelacionadas, ya publicadas o en desarrollo, y contiene una serie de componentes estructurales centrados en los estándares normativos que describen los requisitos del SGSI (ISO/IEC 27001), los requisitos de los organismos de certificación (ISO/IEC 27006) para aquellos que certifican la conformidad con ISO/IEC 27001, y marco de requisitos adicionales para las implementaciones específicas del sector del SGSI (ISO/IEC 27009). Otros estándares y pautas brindan orientación para varios aspectos de la implementación de un SGSI, abordando un proceso genérico, así como orientación específica del sector. Ver tabla 3.

1. Relaciones de la familia de Normas ISO/IEC 27001



Para consultar la tabla puede dirigirse a la carpeta Anexos y descargar el archivo **Relaciones de la familia de Normas ISO/IEC 27001.**

Además de las más mencionadas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27018, también es importante hacer referencia a otras normas de la familia ISO/IEC 27000 como las que se destacan a continuación:

* **ISO/IEC 27000:** **Sistemas de gestión de la seguridad de la información (descripción general y vocabulario).**

Proporciona una descripción general del SGSI y los términos y definiciones comúnmente utilizados en la familia de estándares del SGSI para garantizar coherencia; toda la familia de Normas 27000 se basa en los términos y definiciones proporcionados en

* **ISO/IEC 27003: Sistemas de gestión de la seguridad de la información – Orientación.**

Brinda orientación sobre los requisitos para un SGSI como se especifica en ISO/IEC 27001, así como las recomendaciones, posibilidades y permisos en relación con los requisitos.

* **ISO/IEC 27004: Gestión de la seguridad de la información - Monitoreo, medición, análisis y evaluación.**

Proporciona pautas para ayudar a las organizaciones a evaluar el desempeño de la seguridad de la información, la efectividad de un SGSI y cumplir con los requisitos de monitoreo, medición, análisis y evaluación como especifica la Norma ISO/IEC 27001.

* **ISO/IEC 27005: Gestión de riesgos de seguridad de la información.**

Ofrece directrices para la gestión de riesgos de seguridad de la información. Esta norma es compatible con los conceptos generales especificados en ISO/IEC 27001 y está diseñada para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

* **ISO/IEC 27017: Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube.**

Proporciona pautas que respaldan la implementación de controles de seguridad de la información para consumidores y proveedores de servicios en la nube. La selección de los controles apropiados y la aplicación de la guía de implementación se basa en la evaluación de riesgos y otros requisitos para el uso de servicios en la nube.

* **ISO/IEC 27031: Directrices para la preparación de la tecnología de la información y las comunicaciones para la continuidad del negocio.**

Describe los conceptos y principios de la preparación de las Tecnologías de la Información y la Comunicación (TIC) para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos para mejorar la preparación TIC de una organización y garantizar la continuidad del negocio.

* **ISO/IEC 27035-1: Gestión de incidentes de seguridad de la información - Parte 1: Principios de la gestión de incidentes.**

Proporciona conceptos básicos y fases de la gestión de incidentes de seguridad de la información, y combina estos conceptos con principios en un enfoque estructurado para detectar, informar, evaluar y responder a los incidentes y aplicar las lecciones aprendidas.

* **ISO/IEC 27035-2: Gestión de incidentes de seguridad de la información - Parte 2: Pautas para planificar y prepararse para la respuesta a incidentes.**

Proporciona pautas para planificar y prepararse para la respuesta a incidentes

* **ISO/IEC 27036-4: Seguridad de la información para las relaciones con los proveedores - Parte 4: Pautas para la seguridad de los servicios en la nube.**

Define las pautas que respaldan la implementación de SGSI para el uso de servicios en la nube.

* **ISO/IEC 27037: Pautas para la identificación, recopilación, adquisición y conservación de evidencia digital.**

Proporciona pautas para actividades específicas en el manejo de evidencia digital: identificación, recopilación, adquisición y preservación de evidencia digital potencial que puede tener valor probatorio.

* **ISO/IEC 27039: Selección, implementación y operaciones de sistemas de prevención y detección de intrusos (IDPS)**

Brinda pautas para ayudar a las organizaciones a prepararse para implementar IDPS, en particular, aborda la selección, el despliegue y las operaciones de IDPS.

* **ISO/IEC 27043: Principios y procesos de investigación de incidentes.**

Ofrece pautas basadas en modelos idealizados para procesos comunes de investigación de incidentes en varios escenarios que involucran evidencia digital. Incluye procesos que van desde la preparación previa al incidente hasta el cierre de la investigación, así como consejos generales y advertencias sobre dichos procesos.

* **ISO/IEC TS 27110: Pautas de desarrollo del marco de ciberseguridad.**

Especifica las pautas para desarrollar un marco de ciberseguridad, independientemente del tipo, tamaño o naturaleza de las organizaciones.

* **ISO/IEC TS 27570: Directrices de privacidad para ciudades inteligentes.**

Brinda orientación sobre la protección de la privacidad del ecosistema de ciudades inteligentes: cómo se pueden utilizar las normas a nivel mundial y a nivel organizativo en beneficio de los ciudadanos y procesos para la protección de la privacidad del ecosistema de la ciudad inteligente.

### Información de identificación personal (PII) en “Cloud Computing”

La computación en la nube está evolucionando como nunca antes con tendencia al crecimiento y al desarrollo en los próximos años. Es bien sabido que la computación en la nube tiene ventajas potenciales como método más rentable para usar, mantener y actualizar. El método de copia de seguridad y recuperación en la computación en la nube es relativamente más fácil que los métodos tradicionales de almacenamiento de datos. Además, ofrece la ventaja de una implementación rápida y un fácil acceso a la información.

Desde la perspectiva de las organizaciones, la seguridad de la computación en la nube es motivo de gran preocupación, especialmente en cuestiones de seguridad de datos y protección de la privacidad, lo que constituye el principal inhibidor para la adopción de este tipo de servicio.

El estándar ISO/IEC 27018:2019 (en adelante, ISO/IEC 27018) conocido como "Código de prácticas para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII”, es el primer estándar internacional centrado en la protección de datos personales en la nube pública. ISO/ IEC 27018 establece principalmente objetivos de control, controles y pautas comúnmente aceptados en relación con la protección de PII que procesan los proveedores de servicios de la nube pública, es decir, procesadores de PII.

ISO/IEC 27018 ha sido diseñado para todo tipo y tamaño de organización en el sector público y privado que brinde servicios de procesamiento de información a través de la nube como procesadores de PII.

### Controles de protección de PII de ISO/IEC 27018

ISO/IEC 27018 se desarrolló teniendo en cuenta los requisitos ya incluidos en ISO/IEC 27002. Aumenta ISO/ IEC 27002 en dos enfoques: en primer lugar, complementa la guía de implementación para los controles prescritos por ISO/IEC 27002 y en segundo lugar, proporciona controles adicionales y orientación asociada que se adapta para abordar los requisitos de protección de PII de la nube pública que no están cubiertos por el conjunto de controles ISO/IEC 27002. Para el primer enfoque, ISO/IEC 27018 proporciona una guía de implementación adicional sobre los siguientes 11 controles de ISO/IEC 27002:

* Políticas de seguridad de la información.
* Organización de la seguridad de la información.
* Seguridad de los recursos humanos.
* Control de acceso.
* Criptografía.
* Seguridad física y ambiental.
* Seguridad de las operaciones.
* Seguridad de las comunicaciones.
* Gestión de incidentes de seguridad de la información.
* Aspectos de seguridad de la información de la gestión de la continuidad del negocio.
* Cumplimiento.

Para el segundo enfoque, el Anexo A de ISO/IEC 27018 enumera 11 controles extendidos de ISO/IEC 27002 para cumplir con los requisitos de protección de PII que se aplican a los proveedores de servicios de la nube pública que actúan como procesadores de PII. Estos controles ampliados se clasifican según los 11 principios de privacidad de la Norma ISO/IEC 29100:2011 (en lo sucesivo, ISO/IEC 29100), conocida como "Tecnología de la información - Técnicas de seguridad - Marco de privacidad".

### Beneficios de ISO/IEC 27018

ISO/IEC 27018 se aplica al procesamiento de PII obtenida de un cliente para los fines determinados por el cliente en virtud de su contrato con el proveedor de servicios en la nube.

Al adoptar ISO/IEC 27018 una organización puede:

* Establecer una guía para facilitar el cumplimiento de los requisitos de protección de datos relevantes.
* Ganar la confianza de los clientes para dejar sus datos en la nube y así ampliar su base de clientes.
* Ayudar al proveedor de servicios de nube pública, que opera en un mercado multinacional, a cumplir con varios estándares nacionales de protección de datos y realizar evaluaciones complejas en cada jurisdicción.

**ISO/IEC 27001** establece una especificación formal para ISMS, con mucho énfasis en el "sistema de gestión" en lugar de la "seguridad de la información". Un SGSI certificado proporciona una fuerte indicación de que una organización está utilizando un enfoque sistemático para la identificación, evaluación y gestión de los riesgos de seguridad de la información. Si hay un SGSI efectivo en funcionamiento, entonces, el SGSI garantizará que existan controles de seguridad adecuados. El certificado ISO/IEC 27001 tiene potencial de marketing y debe ayudar a mejorar la credibilidad y aumentar la confianza del cliente.

## ISO 27002

El estándar internacional ISO/IEC 27002 hace referencia a la seguridad de la información en las empresas y organizaciones, con el principal objetivo de reducir el riesgo al máximo, evitando alteraciones en la información ya sea por robo, destrucción o pérdida.

La reducción del riesgo es un tema relevante que involucra el desarrollo de procesos y el seguimiento de medidas adecuadas y eficientes para la empresa en consideración a los requerimientos y las restricciones estipuladas por la legislación nacional e internacional. También es necesario que la organización tenga claridad en cuanto a sus objetivos, el bienestar de sus usuarios, ya sean clientes o empleados y los costos necesarios para la implementación y operación, no sea que incurra en medidas extremadamente costosas que estén por encima o afecten la rentabilidad de la compañía.

No se pueden establecer controles para una seguridad total, pero sí se puede conseguir la reducción del riesgo al mínimo, que en caso de materializarse alguna amenaza, los daños sean menores y fáciles de restaurar.

Explore algunas categorías de seguridad incluidas en el estándar internacional ISO/IEC 27002:

* **Política de seguridad.** Cada organización debe crear su propio documento de políticas de seguridad de la información, que debe planificarse teniendo en cuenta tanto los requerimientos comerciales propios del negocio, como las leyes y las regulaciones que le apliquen.

El documento en primera instancia debe ser aprobado por la gerencia y luego socializado a todos los departamentos, jefes, empleados y externos importantes para la compañía.

* **Aspectos organizativos de la seguridad de la información.** Manejo de la seguridad de la información al interior de la organización y con respecto a terceros, identificando las actividades que involucren ingreso, modificación, manipulación e intercambio de información entre las partes.
* **Gestión de activos.** A cada activo dentro de la empresa se le debe asociar o asignar un responsable, también se precisa mantener el inventario permanentemente actualizado con todos los activos, su manejo correcto, clasificación y a quién pertenece.
* **Seguridad ligada a los recursos humanos.** Se debe garantizar que empleados, contratistas y grupos externos comprendan sus responsabilidades, valorando la idoneidad en las tareas delegadas, lo que contribuye a la reducción de riesgos como robo, fraude o mala manipulación de activos informáticos.
* **Seguridad física y ambiental.** Protección física en la que se tengan barreras o límites de protección (paredes, puertas de acceso con control inteligente o vigilancia privada) para salvaguardar las áreas en donde se almacena y procesa la información.

También se deben considerar amenazas externas o causadas ambientalmente (incendios, inundaciones, huracanes, terremotos, ataques terroristas) y en cuanto al ambiente (temperatura ideal, seguridad para el cableado, mantenimiento).

* **Gestión de comunicaciones y operaciones.** Orientada a garantizar la operación funcional y segura de los dispositivos encargados de procesar la información.
* **Control de acceso.** Estos controles se realizan a través del registro de usuario, validación de roles y privilegios, autenticación, denegación y activación de usuarios, entre otros.

En cuanto a los accesos desde dispositivos móviles, conexión a la red inalámbrica, acceso desde computadores portátiles o teletrabajo para personal que realice actividades desde casa se deben establecer unas políticas claras detallando cada uno de estos aspectos.

* **Adquisición, desarrollo y mantenimiento de los sistemas de información.**

Además de las consideraciones en calidad y valor, se debe estudiar la seguridad que proporcionan nuevos equipos y sistemas, con validaciones de entrada y salida de los datos, controles internos del procesamiento de las aplicaciones, y verificación de la integridad de los mensajes.

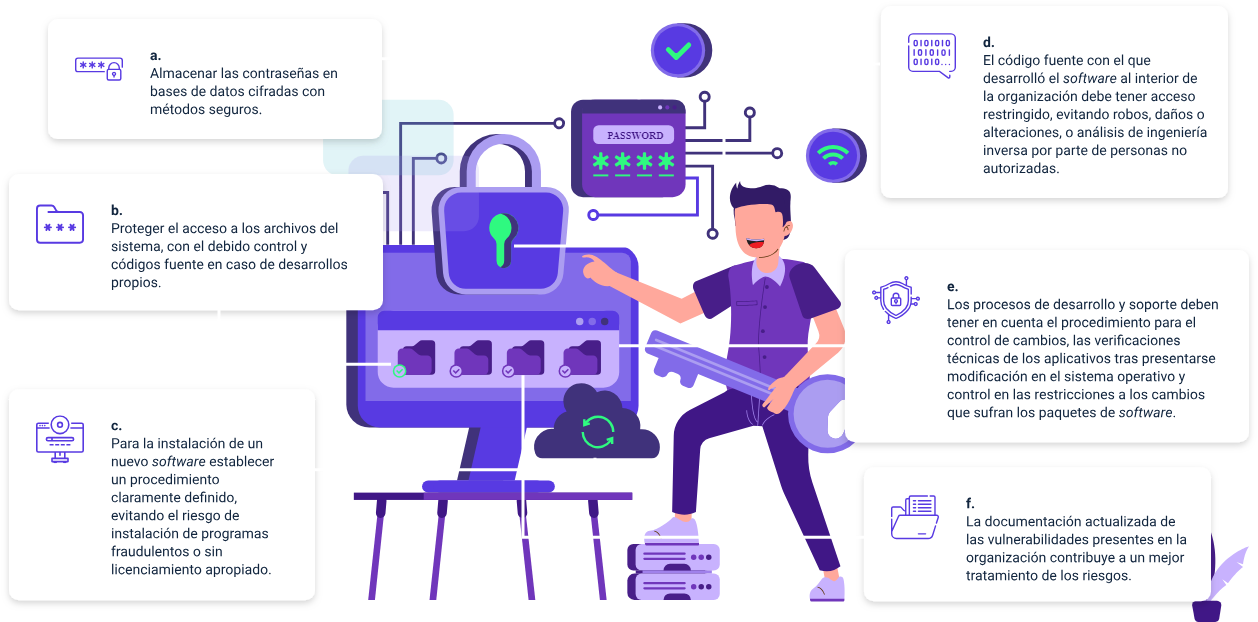
* **Gestión de incidentes en la seguridad de la información.** Los eventos y las debilidades que se presenten en la seguridad de los activos de información se deben documentar y crear informes que contribuyan a mantener una comunicación a tiempo, garantizando que las correcciones se apliquen oportunamente.
* **Gestión de la continuidad del negocio.** Los desastres que puedan provocar las fallas en la implementación de la seguridad, caídas o perdidas del servicio se deben validar con respecto al impacto en la operación comercial del negocio. En caso de desastres, contar con un plan de acción que indique la metodología con la que el negocio reanudará sus operaciones.
* **Cumplimiento.** Cumplir con los requerimientos legales debe ser una de las prioridades de toda organización, evitando incurrir en violaciones de la ley.

A manera de buenas prácticas se recomiendan las siguientes acciones para las categorías de seguridad:

1. Cada procedimiento en las operaciones debe estar debidamente documentado, no en la memoria de los administradores, así como el control de cambios realizado con previa autorización y posterior análisis de las mejoras alcanzadas. Nadie debe tener acceso a realizar modificaciones o a hacer uso de activos informáticos sin previa autorización.
2. Crear entornos separados: uno para ambiente de pruebas y operación, y otro para el entorno desarrollo, evitando posibles problemas operacionales.
3. Las empresas dedicadas a la venta de servicios deben realizar la implementación y conservar niveles adecuados de seguridad informática y asegurar que los servicios que se dispongan en línea cuenten con los acuerdos y compromisos correspondientes a este tipo de entrega a grupos externos.
4. Proteger contra los códigos maliciosos y los virus que se puedan descargar e instalar, implementando las medidas de detección, prevención y recuperación (implementación de antivirus con garantía de actualización).
5. Se debe mantener un plan de copias de seguridad eficiente, automatizado, con revisiones continuas a la integridad de la información, evitando grandes pérdidas de datos en la compañía y serios problemas en la operación.
6. Cuando se trate de redes, garantizar la protección de los datos transportados, además del aseguramiento de la infraestructura. Los servicios que se ofrecen en la red, igualmente deben ser seguros. Todos los activos informáticos y de red deben estar documentados, detallando cada elemento que la conforma.
7. El procedimiento para realizar los controles para intercambiar información a través de las herramientas y medios para la comunicación deben estar establecidos mediante políticas claras.
8. Para realizar un despliegue del comercio electrónico se debe garantizar la efectiva protección, blindándose de ataques fraudulentos, divulgación de información no autorizada, alteración de la información y demás problemas propios de exponer información en redes públicas.
9. Monitorear permanentemente los sistemas que permitan detectar las actividades que no están autorizadas, para ello también es importante contar con las auditorías necesarias.
10. De presentarse fallas deberán ser corregidas rápidamente y documentarse para posteriores análisis, que ayuden a la toma de medidas y acciones necesarias.

### Adquisición y mantenimiento de sistemas de información

En cuanto a los procesos de adquisición, desarrollo y mantenimiento de los sistemas de información es importante tener en cuenta los siguientes aspectos:



### Cumplimiento – ISO/IEC 27002

Y para la categoría de seguridad de cumplimiento, incluida en el estándar ISO/IEC 27002, se advierten las siguientes consideraciones.

* Tener claridad sobre las regulaciones de ley aplicables.
* Definir con precisión, realizar la documentación y mantener actualizado todo lo necesario para el cumplimiento legal de cada uno de los sistemas informáticos y en general de toda la empresa.
* Implementar procedimientos bien definidos que permitan garantizar el cumplimiento de cada requerimiento a nivel legislativo, regulaciones y acuerdos contractuales con relación a los derechos que existan en cuanto a propiedad intelectual o sobre el uso de “software” licenciado.
* Aplicar a la protección que se ofrece a los archivos dentro de la empresa, protección de datos y privacidad de datos personales y, garantizar la prevención de la utilización indebida sobre la aplicabilidad del tratamiento de los datos y las acciones realizadas al control mediante la criptografía.
* Cada sistema informático con el que cuente la organización debe estar permanentemente bajo supervisión y monitoreo, garantizando el cumplimiento de las normas, estándares y políticas propias de la ciberseguridad en la organización.
* Realizar permanentes auditorías y garantizar que se cumple con los procedimientos establecidos.
* Los controles que se piensen aplicar a la organización o a ciertas áreas deben estar cuidadosamente planificados, con el objetivo de causar el mínimo traumatismo en la operación diaria de la compañía.

## ISO 27032

La Norma ISO/IEC 27032 surge para el tratamiento de los desafíos asociados a la ciberseguridad, que tienen que ver con la seguridad en el ciberespacio, definiendo los estándares aplicados en este ámbito que cubren falencias que no fueron cubiertas por normas de seguridad creadas anteriormente, ampliando la cobertura en estos temas, toda vez que surgen nuevos y mejorados ataques y aumentan los riesgos que impactan peligrosamente a las compañías. Por otro lado, se gesta una alianza con los involucrados que administran actualmente el entorno, al que normalmente se conoce como el marco de seguridad o CSF (“Cybersecurity Framework”).

"El ciberespacio es un entorno complejo que consta de interacciones entre personas, “software” y servicios destinados a la distribución mundial de información y comunicación". Se trata de un contexto muy grande en el que "la colaboración es esencial para garantizar un entorno seguro", aseguró la ISO al momento de presentar este estándar.

Teniendo en cuenta los desafíos a los que actualmente se enfrentan las organizaciones en temas de ciberseguridad, se plantean cuatro temas importantes siguiendo el estándar de la norma: seguridad de la información, seguridad de las redes, seguridad en Internet y protección de infraestructuras críticas para la información.

A la vez que se establece un marco de ciberseguridad de cuatro principales áreas que darán un acercamiento a la gestión del riesgo:

* **Prevención**: consiste en la implementación de procedimientos y controles eficientes que detengan y minimicen los posibles daños que ocasionen situaciones de ciberseguridad.
* **Protección y detección:** se establecen un conjunto de controles previstos para gestionar la seguridad y el monitoreo de eventos de ciberseguridad, a fin de que se puedan detectar y aplicar medidas de prevención ante este tipo de circunstancias.
* **Respuesta y comunicación**: se debe preparar para reaccionar ante situaciones relacionadas con la ciberseguridad, realizando acciones que ayuden a minimizar su impacto.
* **Recuperación y aprendizaje:** es la capacidad para restaurar y recuperar los sistemas informáticos y la información ante eventuales incidentes de ciberseguridad. Con cada evento se debe mejorar para no incurrir nuevamente en ello.

Teniendo en cuenta los cuatro elementos mencionados, es posible implementar una serie de fases que contribuyan de manera organizada a implementar la estandarización, como se presenta a continuación.

* **Entender la organización**
* Conocer las diferentes áreas y su relación con el ciberespacio.
* Entender el flujo de información en los procesos de la organización.
* Revisar productos, servicios y el marco de la normatividad de la seguridad en uso.
* Recopilar el inventario de la documentación de seguridad.
* Establecer el inventario de los activos informáticos.
* Conocer los planes y las aplicaciones técnicas implementadas en ciberseguridad.
* **Analizar el riesgo.** Realizar una evaluación teniendo en cuenta puntos importantes como activos críticos, amenazas, vulnerabilidades, impacto, el riesgo y cuáles son las responsabilidades. Importante desarrollar esta tarea en línea con las normativas reconocidas internacionalmente, preparadas para realizar mantenimientos y gestionarse en el tiempo.
* **Plan de acción.** Establecer un plan que identifique las prioridades y las acciones a desarrollar con el objetivo de buscar la alineación con la norma, al tiempo que se ajuste con las necesidades propias del negocio. El plan puede incluir diferentes estrategias teniendo en cuenta los distintos niveles de la organización: políticos, identificación de roles, métodos de implementación como procesos afectados y controles tecnológicos.
* **Implementación.** Establecer los controles que consideren los niveles de seguridad alcanzados previamente, teniendo en cuenta las políticas y procedimientos de seguridad actuales.

Controles adicionales a nivel de aplicación (validación de datos, gestión de sesiones, autenticación, seguridad ante ataques), servidores (actualizaciones, control de parches, configuración segura, monitoreo), usuario final (antivirus, parametrización de seguridad, sistema operativo actualizado) e ingeniería social (planes de capacitación, pruebas periódicas, controles de seguridad, bloqueos).

# Metodologías para la gestión del riesgo

Suele ser de conocimiento general el proceso de gestión de riesgos en tanto la identificación, el análisis, la gestión, etc., documentado en las normas internacionales para la gestión de riesgos; sin embargo, el concepto de una metodología de gestión de riesgos parece bastante extraño para la mayoría.

Una metodología de riesgo define para una organización la visión general del proceso de gestión de riesgos. En lugar de identificar prácticamente los riesgos, establece cómo deben identificarse, los métodos que deben utilizarse, las personas que deben participar e incluso los documentos y plantillas apropiados.

No todas las organizaciones adoptan el mismo enfoque para la gestión de riesgos. Se evidencia que mientras algunas organizaciones abordan la gestión de riesgos con precisión militar, como una unidad organizada perfectamente orquestada para brindar resultados, otras utilizan un enfoque mucho más flexible, abriéndose camino a tientas en la oscuridad. La diferencia en estos enfoques puede considerarse como las diferencias en la implementación de la metodología de la gestión de riesgos.

Organizaciones de todo tipo y tamaño enfrentan factores e influencias internas y externas que hacen que sea incierto asegurar si lograrán sus objetivos y cuándo lo harán. El efecto que esta incertidumbre tiene sobre los objetivos de una organización es el riesgo. El riesgo está involucrado en cualquier actividad de una organización.

## Magerit

El Consejo Superior de Informática ha elaborado la Metodología de análisis y gestión de riesgos para los sistemas de información de las administraciones públicas (Magerit). El Consejo recomienda el uso de esta metodología como respuesta a la creciente dependencia de las administraciones públicas (y de la sociedad en su conjunto) a las tecnologías de la información. El propósito de Magerit está directamente relacionado con el uso extensivo y generalizado de las tecnologías de la información. Si bien las tecnologías de la información brindan beneficios evidentes a los ciudadanos, también generan ciertos riesgos que deben minimizarse a través de medidas de seguridad que garanticen la autenticidad y la confidencialidad.

### Objetivos

Dentro de los objetivos de la metodología Magerit destacan estudiar los riesgos que afectan a un sistema de información (SI) específico y su entorno relacionado, entendido el riesgo en su sentido más común, como la posible ocurrencia de un daño, y recomendar las medidas adecuadas que deben adoptarse para descubrir, prevenir, impedir, reducir o controlar los riesgos investigados.

Como objetivo a más largo plazo, Magerit está preparando mecanismos de evaluación y certificación de la seguridad de los sistemas de información.

Para programarlo, Magerit utiliza como referencia sistemática -Ll ITSEC (“Information Technologies Security Evaluation Criteria”), aprobado por el SOGIS (“Senior Officer Group of Information Systems”) de la Comisión de la UE y sujeto a la Recomendación de 7/4/1995 del Consejo de la UE; así como el Manual de evaluación de la seguridad de las tecnologías de la información (ITSEM) y, los conceptos y los términos acuñados por los criterios de evaluación para la seguridad de la tecnología de la información (ISO/IEC IS 15408).

Ambos criterios estipulan que los solicitantes de una evaluación o certificación de seguridad primero deben definir su “dominio” (“Target of Evaluation”, TOE) y sus amenazas ambientales junto con el “Target of Security” (TOS) solicitado. También establecen que esta definición previa debe hacerse con el apoyo de un método de análisis y gestión de riesgos como Magerit.

### Elementos

La estructura de Magerit se compone de dos tipos de elementos:

1. Un conjunto de manuales: introductorio, de procedimientos, de técnicas, un manual para desarrolladores de aplicaciones, para los responsables del dominio protegido y una guía de referencia de normas legales y técnicas.
2. Una serie de herramientas de apoyo con sus respectivos handbooks y con las especificaciones de la arquitectura de la información e interfaz para el intercambio de los datos.

La estructura Magerit permite realizar el análisis de los riesgos para identificar las amenazas a los diferentes componentes pertenecientes o relacionados con el sistema de información (conocidos como “activos”), evaluar la vulnerabilidad del sistema frente a dichas amenazas y estimar el impacto o el nivel de daño que una seguridad inadecuada puede tener sobre la organización, obteniendo así una cierta conciencia del riesgo en el que se incurre.

La gestión de riesgos se basa en los resultados obtenidos en el análisis anterior, y permite seleccionar e implementar las medidas de seguridad o “salvaguardas”, adecuadas para descubrir, prevenir, impedir, reducir o controlar los riesgos identificados, reduciendo así los posibles daños a un mínimo.

### Fases

A continuación se presentan las fases de recuperación de la seguridad propuestas por la metodología Magerit:

* + - * **Análisis y gestión de riesgos.** Fase central de “medición” y cálculo dentro del ciclo de gestión de la seguridad, punto de partida que requiere técnicas de proceso especiales (dentro del ámbito de la seguridad). La fase estará sujeta a un método Magerit especial, mientras el resto de fases a técnicas más genéricas y conocidas.
* **Objetivos, estrategia y política de seguridad de los sistemas de información.** En el ciclo inicial de gestión de la seguridad un análisis y gestión de riesgos integral ayuda a determinar los objetivos, la estrategia y la política, lo que a su vez afectará el análisis y la gestión de riesgos más detallado de ciclos posteriores.
* **Planificación de la seguridad de los sistemas de información.** Esta fase, consecuencia funcional más inmediata de la fase de análisis y gestión de riesgos, utiliza técnicas generales de planificación (resultados, progresión e hitos de decisión) adaptadas al ámbito de la seguridad.
* **Organización de la seguridad de los sistemas de información.** Consecuencia orgánica más inmediata de la fase de análisis y gestión de riesgos. Utiliza técnicas generales de organización (compromiso directivo, roles, responsabilidades, documentación reglamentaria) adaptadas al ámbito de la seguridad.
* **Implantación de salvaguardias y otras medidas de seguridad en los sistemas de información.** Resultante de las fases de planificación y organización, utiliza técnicas generales de gestión de proyectos y de la gestión de la configuración adaptadas al ámbito de la seguridad.
* **Concienciación sobre la seguridad en los sistemas de información.** Deriva de las fases de planificación y organización. Tiene en cuenta el papel fundamental de los recursos humanos internos en cualquier proyecto de seguridad y utiliza técnicas generales de la gestión de proyectos y de formación, comunicación y gestión de recursos humanos, adaptadas al entorno de seguridad.
* **Reacción a incidentes, atención y reporte de incidentes, y recuperación de estados aceptables de seguridad.** Fase fundamentalmente operativa que utiliza técnicas generales de gestión del día a día y servicios de emergencia, adaptadas al ámbito de la seguridad.
* **Seguimiento y gestión de la configuración y cambios en la seguridad de los sistemas de información.** Fase básicamente de mantenimiento, utiliza técnicas generales de seguimiento, gestión de la configuración y gestión del cambio, adaptadas al ámbito de la seguridad.

### Magerit en proyectos de mediana y alta complejidad

Los proyectos de mediana y alta complejidad en seguridad requieren más de un ciclo integral de gestión de seguridad. La aplicación del primer ciclo de gestión cubre todo el sistema en estudio. Se inicia con la fase de análisis y gestión de riesgos, con un enfoque amplio para obtener una primera separación o clasificación de los componentes del sistema en dos grandes bloques

* **Componentes de riesgos menores,** a los que se pueden aplicar medidas básicas de seguridad de “sentido común”, ampliamente aplicado.
* **Componentes que implican riesgos importantes**. Para cada uno de ellos será necesario aplicar un nuevo y más detallado análisis y gestión de riesgos. La primera aplicación ofrece una visión sintética inicial de la seguridad con la ayuda de las otras fases del ciclo de gestión de la seguridad, es decir, el establecimiento de objetivos, la estrategia y política integrales de seguridad, el establecimiento de la planificación inicial de seguridad, establecer una definición inicial de la organización necesaria para la seguridad, la implementación de salvaguardas generales en componentes de bajo riesgo, la conciencia de seguridad, la capacitación de personas para participar en la seguridad de componentes de bajo riesgo, y finalmente, capacitar a las personas para reaccionar ante cada evento, manejar y registrar incidentes y recuperar estados aceptables de seguridad relacionados con los componentes de bajo riesgo.

### Estructura de la fase de análisis y gestión de riesgos

El manual de procedimientos describe metódicamente la fase de análisis y gestión de riesgos, utilizando como referencia principal el método Magerit que comienza definiendo el nivel más general (para que pueda adaptarse a cualquier situación concreta). Magerit contempla una visión estratégica integral de la seguridad de los sistemas de información de las administraciones públicas, que comienza con un modelo de análisis y gestión de riesgos compuesto por tres submodelos. Ver figura 10.

**Figura 10.** Submodelos del análisis y gestión de riesgos



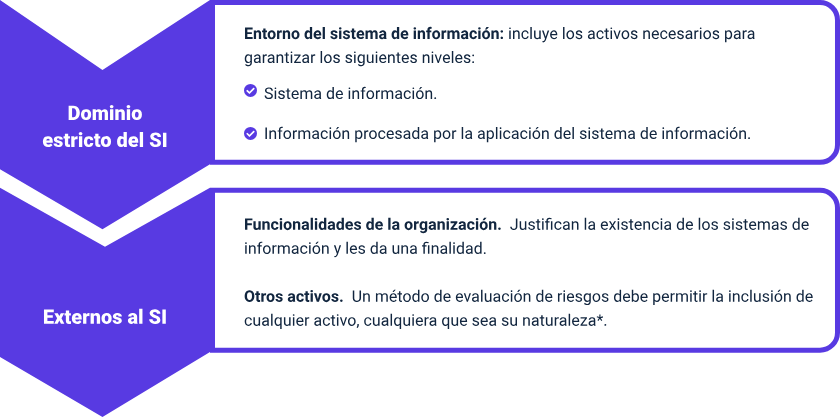
El submodelo de elementos proporciona los “componentes” que el submodelo de eventos interrelaciona entre sí y en el tiempo, mientras que el submodelo de procesos es la descripción funcional (“cuadro explicativo”) del proyecto de seguridad en construcción. Al construir un proyecto de seguridad específico, el submodelo de procesos ayuda, por un lado, a seguir el procedimiento general, por otro lado, a adaptarlo al problema concreto de que se trate, teniendo en cuenta la política de seguridad establecida por la dirección de la organización. Si esta adaptación es compleja o presenta elementos inciertos debe realizarse con la ayuda de un especialista en seguridad SI. El procedimiento adaptado a los requisitos de un proyecto de seguridad concreto determina las funciones y servicios de salvaguarda adecuados a los problemas detectados al aplicar el método, y señala los tipos de mecanismos de salvaguarda para solucionarlos.

Aunque no forma parte de Magerit, esta metodología prepara la planificación, la organización y las posteriores fases necesarias para la implementación y operación de dichos mecanismos, teniendo en cuenta la política de seguridad establecida por la dirección de la organización.

### Tipos de Magerit

El modelo considera cinco tipos o categorías principales de activos representados en la siguiente figura:

**Figura 11.** Clasificación de activos según Magerit



**Nota.** Este concepto amplio de activo (\*) sigue las directrices ISO/IEC para la gestión de la seguridad de TI, en las que se define cualquier cosa que una organización tiene o utiliza.

Para los objetivos específicos de algunos proyectos, Magerit puede desarrollar listas de activos diferentes o desgloses más detallados. También se suelen utilizar los siguientes grupos:

* **Grupos jerárquicos de activos**. Diferentes según el caso de estudio y el nivel de detalle adecuado a la “granularidad” prevista para la etapa de aplicación. Este desglose le permite identificar y definir directamente los activos y/o componentes específicos que se estudiarán, lo que facilita la colaboración entre los expertos en seguridad y los usuarios.
* **Grupos de activos según la amenaza**. Activos vulnerables a una amenaza común y grupos de activos según la salvaguardia, que permiten aplicar una salvaguardia común.
* **Activos no tipificados.** Magerit facilita la inclusión de cualquier activo, independientemente de su naturaleza. Esto permite un tratamiento muy flexible pero bien estructurado de las funcionalidades de la organización y de otros recursos no tangibles.

### Vulnerabilidad

Es la potencial o posible ocurrencia de la materialización de una amenaza, que caracteriza la relación entre un activo y una amenaza. La vulnerabilidad se ha vinculado a un activo más como una “no calidad” del activo, pero puede vincularse a la amenaza cuando se considera útil (en cualquier caso, la vulnerabilidad no es solo una “debilidad”, es decir, una “característica negativa” del elemento de activo). La vulnerabilidad es un concepto doble:

* Cumple una función de mediación (o predicado desde el punto de vista lingüístico) entre la amenaza como acción y el activo como objeto que modifica el estado de seguridad. Debido a este aspecto estático, la vulnerabilidad es parte del estado de seguridad del activo.
* En su aspecto dinámico es el mecanismo obligado que transforma una amenaza en una agresión materializada sobre un activo.

Así, a modo de ejemplo, la amenaza de inundación por el desbordamiento de un riachuelo junto con el activo “sitio de cómputo” ubicado en una zona fácilmente inundable se materializa en la vulnerabilidad de dicho activo ante esa amenaza. Esa vulnerabilidad depende del “ciclo de ocurrencia” (frecuencia) de inundaciones en esa área y la ubicación del sitio de la computadora (cercanía al cauce, ubicación del sótano, etc.). Un malentendido muy común es la asimilación de la vulnerabilidad como una probabilidad, utilizada como término científico y técnico relacionado con la teoría de las probabilidades. No se está hablando del cociente de un número de casos concretos (reales) frente a un número de casos totales (posibles), ya que el denominador no tendría ningún sentido. Magerit evita cuidadosamente los términos probable y probabilidad, utilizando los conceptos potencial y potencialidad en general como algo más cercano a la materialización de una amenaza en una agresión. La potencialidad se convierte en frecuencia en aquellos casos de cálculo definido, y posibilidad en aquellos casos de cálculo “borroso”.

**Ante el concepto de vulnerabilidad, Magerit considera dos significados principales:** la vulnerabilidad intrínseca del activo, en cuanto al tipo de amenaza que solo depende de estas dos entidades (activo y amenaza) y la vulnerabilidad efectiva del activo, que tiene en cuenta las salvaguardias aplicadas al activo en cada momento y también las formas en que un factor estima la efectividad global de las salvaguardias.

La vulnerabilidad intrínseca se puede desglosar, si es necesario, para realizar análisis detallados (sobre amenazas intencionales) de acuerdo con los siguientes grupos de atributos:

* Potencialidad autónoma, respecto del bien amenazado por la ocurrencia de una amenaza (por ejemplo, frecuencia de inundaciones en un lugar específico).
* Potencialidad derivada en la relación entre activo y amenaza (principalmente intencional).
* Factores subjetivos generadores de más o menos “fuerza” (motivación, disuasión).

Oportunidad de acceso al dominio con capacidad y recursos según los siguientes cuatro aspectos:

| Tipo de acceso | Escala |
| --- | --- |
| **Acceso físico**  Número de personas o entidades autorizadas que, en razón de sus funciones, tienen acceso al entorno del bien. | Una sola persona o entidad.  Pocas personas pertenecen a una entidad.  Muchas personas de algunas entidades diferentes.  Muchas personas de muchas entidades diferentes. |
| **Acceso físico cualificado**  Formación general y experiencia de los usuarios autorizados a tener acceso físico al entorno del bien. | Sin formación.  Bajo nivel de formación para el manejo de documentos técnicos.  Cierta experiencia en el manejo de documentos técnicos.  Alto nivel de formación y experiencia en el manejo de documentos técnicos. |
| **Acceso lógico competente**  Conocimiento técnico específico del activo atacable. | Sin conocimientos especiales.  Fácil de usar.  “Know-how” del desarrollador.  Experto calificado. |
| **Acceso lógico instrumental**  Disponibilidad de herramientas correspondientes a la tecnología del activo amenazado. | No se requieren herramientas especiales pero el acceso está restringido.  Se requieren herramientas especiales, aunque son accesibles con la tecnología estudiada.  Se requieren herramientas especiales y el acceso es muy difícil. |

Las métricas de vulnerabilidad se basan en la “distancia” entre la amenaza (potencial) y su materialización como agresión (real) sobre el activo. Magerit mide la vulnerabilidad cuando es factible, por su frecuencia histórica o por la posibilidad de materialización de la amenaza sobre ese activo. Se tienen datos cuantitativos específicos (confiabilidad de un componente de hardware, cantidad de fallas de software, etc.) para algunos activos y se usa la métrica [0.1], donde 0 significa que la amenaza no afecta el activo y 1 no es accesible como lo haría, lo que significa una agresión permanente.

Pero como esa medida no suele estar disponible, una primera aproximación cualitativa a la frecuencia o posibilidad de materialización de la amenaza lleva a utilizar la escala mostrada en amenazas potenciales (consideradas ahora como reales, es decir, agresiones).

La escala de niveles podría ser “objetiva” al comparar el tiempo medio entre ocurrencias en una unidad. En unos casos es recomendable que este plazo sea mayor (un año a efectos contables) y en otros menores (por ejemplo, un día, la ocurrencia diaria de una falla de un activo es un límite psicológico y material demasiado alto, inaceptable en condiciones normales de productividad, pero aceptable en la investigación de incidentes). Por lo tanto, las herramientas de soporte de Magerit pueden manejar fácilmente varias "escalas" objetivas.

## ISO 31000

La ISO 31000 es una norma internacional emitida en 2009 por la ISO (Organización Internacional de Normalización), que pretende servir como guía para el diseño, la implementación y el mantenimiento de la gestión de riesgos. La ISO 31000 describe un proceso sistemático y lógico, durante el cual las organizaciones gestionan el riesgo a través de su identificación y análisis para luego evaluar si el riesgo debe modificarse mediante un tratamiento para satisfacer sus criterios de riesgo. La gestión de riesgos puede aplicarse a toda una organización, en sus múltiples áreas y niveles, en cualquier momento, así como a funciones, proyectos y actividades específicas.

El estándar de gestión de riesgos ISO 31000 se basa en ocho principios de creación y protección de valor que se convierten en fundamento de la gestión de riesgos y deben tenerse en cuenta al establecer el marco y los procesos de gestión de riesgos de la organización, vea en qué consiste cada uno de estos:

* **La gestión de riesgos está integrada en los procesos de la organización**
* La gestión de riesgos no está separada de las principales actividades y procesos de la organización, es parte de la toma de decisiones en cada departamento.
* La gestión de riesgos está integrada en los procesos de la organización y forma parte de las responsabilidades de la dirección.
* **La gestión de riesgos es estructurada e integral**
* Aborda la gestión de riesgos de manera sistemática, contribuye a la eficiencia y a los resultados consistentes dentro de la organización, así como a la comprensión de todos los involucrados.
* La gestión de riesgos está estructurada con lineamientos y procedimientos a seguir para mantener la productividad y eficacia.
* **La gestión de riesgos se adapta a su organización**
* Los procesos de gestión de riesgos no son de talla única, deben adaptarse al contexto externo e interno de la organización para alcanzar los objetivos.
* Cuando el contexto se establece en entornos internos y externos, los objetivos se pueden capturar y la gestión de riesgos se puede personalizar para la organización.
* **La gestión de riesgos es inclusiva y transparente**
* La participación de los grupos de interés permite considerar sus conocimientos y puntos de vista, garantizando una gestión de riesgos pertinente y actualizada.
* La gestión de riesgos es transparente, fácil de entender y no incluye jerga confusa, lo que permite incluir a las partes interesadas en el marco.
* **La gestión de riesgos es dinámica, fluida y receptiva al cambio**
  + El contexto y el conocimiento dentro de una organización cambian constantemente y debe reconocerse cómo lo hacen.
  + La gestión de riesgos debe responder al cambio de manera continua y oportuna para mantener la eficiencia y los resultados.
  + Los riesgos surgen, cambian y desaparecen a medida que ocurren eventos internos y externos, por lo que la gestión de riesgos debe ser anticipatoria.
* **La gestión de riesgos toma en consideración la mejor información disponible**
  + Una organización nunca tendrá toda la información necesaria, pero se deben tomar medidas cuando una organización tiene los mejores datos disponibles.
  + Se debe tener en cuenta la información histórica y actual, así como sus limitaciones.
  + Toda la información conocida debe estar disponible para las partes interesadas.
* **La gestión de riesgos tiene en cuenta los factores humanos y la cultura de la empresa**
  + La gestión de riesgos está influenciada significativamente por el comportamiento y la cultura humana.
  + Las capacidades de la organización, así como las metas de las personas dentro y alrededor de ella deben ser reconocidas por la gestión de riesgos para lograr o inhibir las metas del negocio.
* **La gestión de riesgos fomenta e impulsa la mejora continua.**
  + Mejorar continuamente a través de la experiencia asegura la resiliencia de la organización.
  + La adecuada adaptación a los resultados en la gestión de riesgos permite a la organización crecer exponencialmente en todos los aspectos, y seguir haciéndolo.

Estos ocho principios son la base para la gestión del riesgo y se consideran al momento de crear procesos en todas las áreas de una organización con la Norma ISO 31000. Sin la base proporcionada por estos principios, el marco de la gestión de riesgos de ISO 31000 no sería sólido. La mejor gestión de riesgos utiliza estos principios para gestionar la incertidumbre de una organización, alcanzar sus objetivos y seguir logrando metas. Cuando una organización gestiona el riesgo mientras incorpora los ocho principios, verá resultados consistentes y confiables.

Síntesis

Revise el siguiente mapa conceptual que relaciona los principales contenidos abordados en el desarrollo del componente formativo.

En el mapa conceptual se explica la evaluación de la seguridad digital, la cual determina el nivel de ciberseguridad de las organizaciones. Esto implica considerar varios conceptos asociados a la ciberseguridad, a través de la vulnerabilidad, la amenaza, el riesgo, las redes, los protocolos, el enrutamiento IP y la arquitectura cloud y on-premise.

Además, es importante tener en cuenta la normatividad y los estándares en seguridad de la información. Para esto, se deben considerar diferentes leyes y normas, como la Ley 1523 de 2012 y las normas ISO 27001, 27002 y 27032. Estas normas son utilizadas para la implementación de la metodología para la gestión del riesgo basada en el modelo Magerit. Asimismo, la norma ISO 31000 proporciona la estructura de análisis y gestión de riesgos.

Material complementario

| Tema | Referencia | Tipo de material | Enlace del recurso |
| --- | --- | --- | --- |
| Conceptos y fundamentos asociados a la gestión de la ciberseguridad | Arroyo, D., Gayoso, V. y Hernández, L. (2020). Ciberseguridad. CSIC. Los Libros de la Catarata. | Libro | <https://sena-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=sena_elibroELB172144&vid=SENA&search_scope=sena_completo&tab=sena_completo&lang=es_ES&context=L> |
| Conceptos y fundamentos asociados a la gestión de la ciberseguridad | Cano, J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. Revista Científica General José María Córdova. | Artículo | <https://revistacientificaesmic.com/index.php/esmic/article/view/866> |
| Enrutamiento IP | Fernández, L. (2022). Conoce qué es la tabla de enrutamiento en un router. Redeszone. | Página web | <https://www.redeszone.net/tutoriales/redes-cable/tabla-enrutamiento-router-que-es/> |
| IPv4 e IPv6 | Freda, A. 2021. ¿Qué diferencia hay entre IPv4 e IPv6? AVG. | Página web | <https://www.avg.com/es/signal/ipv4-vs-ipv6> |
| Protocolo TPC/IP | IBM. Protocolos TCP/IP. (s.f.). IBM. | Página web | <https://www.ibm.com/docs/es/aix/7.2?topic=protocol-tcpip-protocols> |
| Tipos de redes | IBM. Redes físicas. (s.f.). IBM. | Página web | <https://www.ibm.com/docs/es/aix/7.2?topic=concepts-physical-networks> |
| Normatividad y estándares de seguridad de la información | The History of ISO 17799 and ISO 27001. (s.f.). Historial de PC. | Línea de tiempo | <https://www.pc-history.org/17799.htm> |

Glosario

**Amenaza:** las amenazas informáticas hacen referencia a eventos o situaciones de seguridad que pueden afectar un sistema en estado de vulnerabilidad y sufrir daños.

**Ataque:** conjunto de técnicas que se utilizan en búsqueda de una vulnerabilidad, con el objetivo de robar, alterar o dañar un sistema o información.

**Ciberseguridad:** conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

**Enrutamiento:** el enrutamiento de redes es el proceso de selección de una ruta a través de una o más redes.

**IPv4:** la estructura del protocolo ip versión cuatro (ipv4) está formada por 12 caracteres divididos por un punto en cuatro segmentos de hasta 3 caracteres.

**IPv6:** es una mejora a su antecesor, el protocolo ip versión cuatro, su implementación pretende mejorar la escasez de direcciones que se presentan con la versión cuatro.

**Metodología:** combinación de varios métodos enfocados en la gestión de riesgos con un enfoque de automatización durante las etapas de operación.

**Modelo OSI:**  modelo de interconexión de sistemas abiertos. proporciona a los diversos sistemas de tecnología informática estándares para que se comuniquen entre sí.

**Normatividad:** conjunto de leyes o reglamentos que rigen conductas y procedimientos según los criterios y los lineamientos de una institución u organización privada o estatal.

**Redes de informática**: conjunto de ordenadores y otros dispositivos conectados entre sí para intercambiar información (impresoras, archivos, etc.) y compartir recursos.

**Riesgo:** probabilidad de que se pueda presentar una amenaza, asociada a una vulnerabilidad.

**TCP/IP:** define cuidadosamente cómo se mueve la información desde el remitente hasta el destinatario.

**Vulnerabilidad:** incapacidad que tiene un sistema para protegerse, permitiendo ser atacado y recibiendo daño.

Referencias bibliográficas

IBM. (s.f.). *Protocolos* TCP/IP. IBM. <https://www.ibm.com/docs/es/aix/7.2?topic=protocol-tcpip-protocols>

ISO. (s.f.). *The ISO Survey*. ISO. <https://www.iso.org/the-iso-survey.html>

Ley 1523 de 2012. [Congreso de Colombia]. Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema nacional de gestión del riesgo de desastres y se dictan otras disposiciones. Abril 24 de 2012. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=47141>

Oracle Corporation. (2010). *Modelo de referencia OSI.* Oracle Corporation. <https://docs.oracle.com/cd/E19957-01/820-2981/ipov-8/index.html>

Créditos

| Nombre | Cargo | Regional y Centro de Formación |
| --- | --- | --- |
| Claudia Patricia Aristizábal | Líder del Ecosistema | Dirección General |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo desarrollo curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura |
| Ronald Alexander Vacca Ascanio | Experto Temático | Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander |
| Maribel Avellaneda Nieves | Diseñadora Instruccional | Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander |
| Silvia Milena Sequeda Cárdenas | Asesora Pedagógica y Metodológica | Centro de diseño y Metrología - Regional Distrito Capital |
| Julia Isabel Roberto | Correctora de Estilo | Centro de diseño y Metrología - Regional Distrito Capita |
| 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 |
| Wilson Andrés Arenales Cáceres | Storyboard e Ilustración | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Carmen Alicia Martínez Torres | Animador y Productor Multimedia | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Camilo Andrés Bolaño Rey | 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 Alvarez | 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 |