**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Técnico en tratamiento de riesgos de ciberseguridad en la micro, pequeña y mediana empresa (*mipyme*) |
| --- | --- |

| COMPETENCIA | 220501108 - Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica | RESULTADOS DE APRENDIZAJE | 220501108-01 - Aplicar métodos de análisis y valoración de riesgos de ciberseguridad en *mipymes*, de acuerdo con estándares internacionales y normatividad nacional. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF01 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | 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. |
| PALABRAS CLAVE | Metodología, redes, ciberseguridad, activo de información, estándar, riesgo. |

| ÁREA OCUPACIONAL | 2 - Ciencias Naturales, aplicadas y relacionadas |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS**

**1. Conceptos y fundamentos asociados a la gestión de la ciberseguridad**

1.1. Tipos de redes

1.2. Modelo OSI

1.3. Protocolo TCP/IP

1.4. IPv4 e IPv6

1.5. Enrutamiento IP

1.6. Arquitecturas Cloud y On-premises

1.7. Vulnerabilidad, amenaza y riesgo

**2.** **Normatividad y estándares de seguridad de la información**

2.1. ISO 27001

2.2. ISO 27002

2.3. ISO 27032

**3.** **Metodologías para la gestión del riesgo**

3.1. Magerit

3.2. ISO 31000

**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. **DESARROLLO DE CONTENIDOS**

**1. 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 cada día son más demandados con 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:



**1.1. 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.



Las organizaciones cuentan con uno o varios tipos de red, combinando 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.

**1.2.** **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*

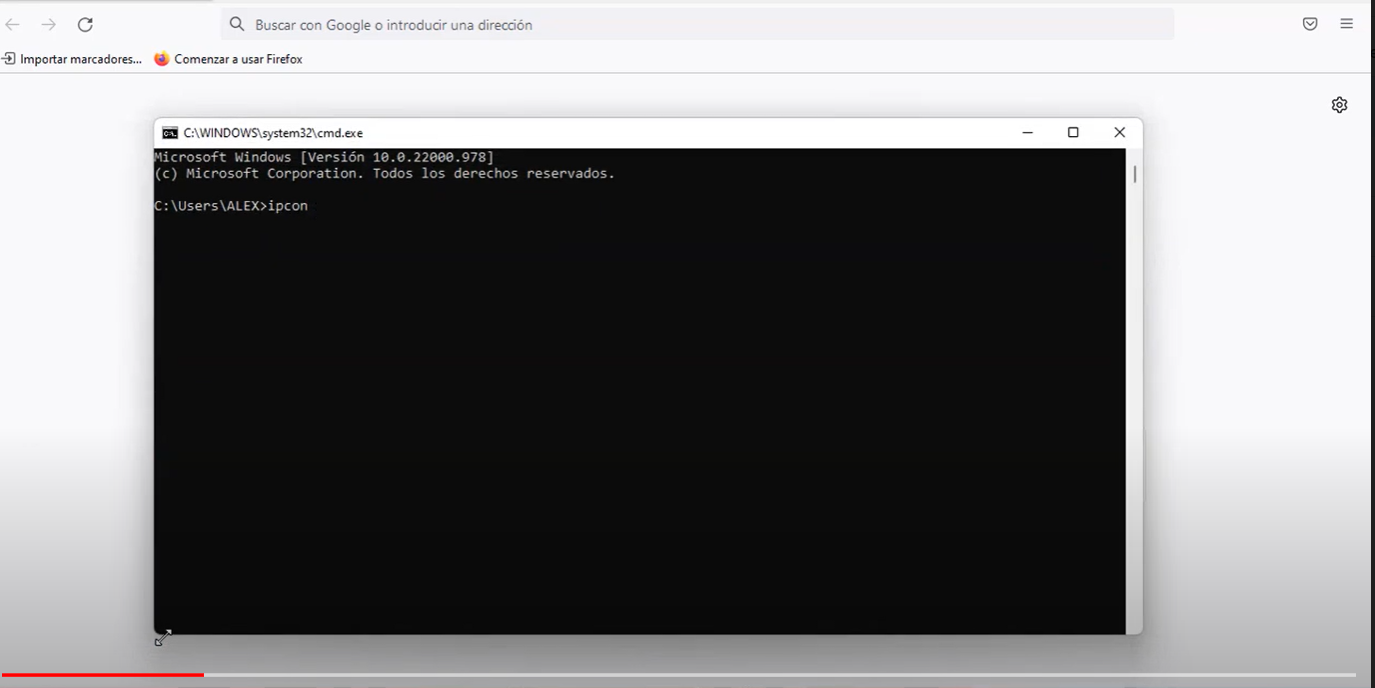


Profundice en las características de las capas del modelo y el trabajo que realiza cada una de estas a través de la revisión del siguiente recurso.





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



**1.3.** **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.

**Tabla 1**

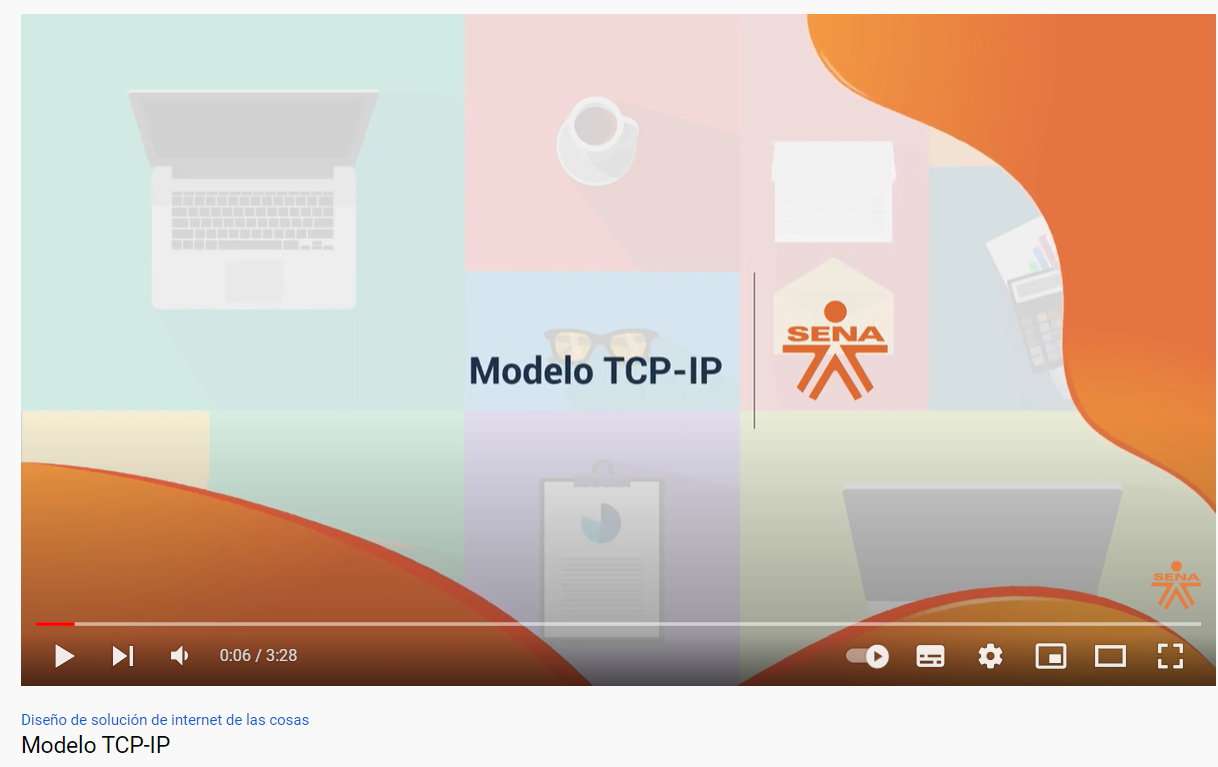
*Modelo TCP/IP con equivalencia al modelo OSI*

| 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.



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

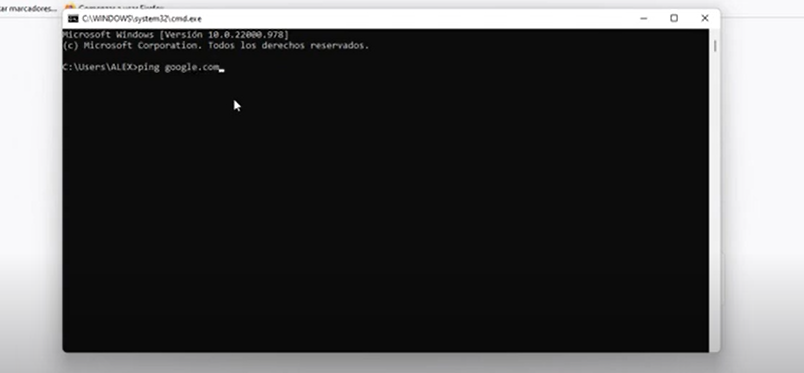


**1.4.** **IPv4 e IPv6**

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.



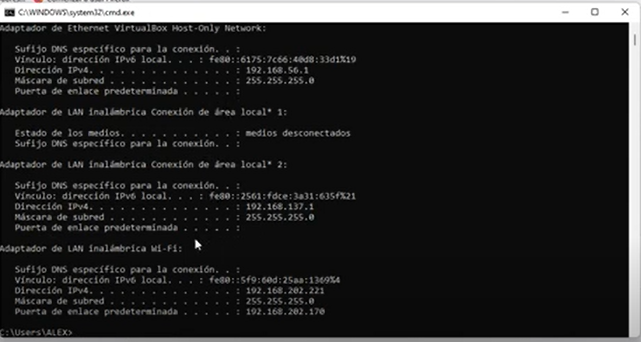
Para obtener la dirección IP pública de un sitio siga el procedimiento que se detalla en el video:



Por otro lado, cada máquina privada debe tener una dirección IP propia que le permita la identificación única dentro de una red local, identificando cada ordenador de modo que puedan llegar a este los paquetes, por lo que 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:



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 la 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.

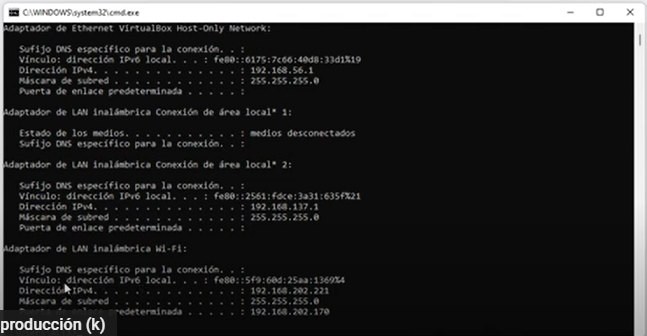
En cuanto al protocolo de Internet versión seis (IPv6), una mejora de su antecesor, el protocolo IP versión cuatro, pretende mejorar la escasez de direcciones que se presentan con la versión anterior. En Colombia se promueve su implementación desde 2020 y su adopción es importante ya que contribuye con 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:



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

**Tabla 2**

*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.

**1.5. Enrutamiento IP**

El enrutamiento que realizan las redes de datos consiste en la selección óptima de una ruta 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 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*



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.

**1.6. 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:



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:



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, puesto que 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:



**1.7. Vulnerabilidad, amenaza y riesgo**

Hoy en día es prioritaria la seguridad de los activos informáticos para todas las empresas, toda vez que cuando los sistemas son atacados pueden sufrir consecuencias lamentables: pérdida de información, suspensión del servicio, mala imagen ante los clientes, hasta 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*

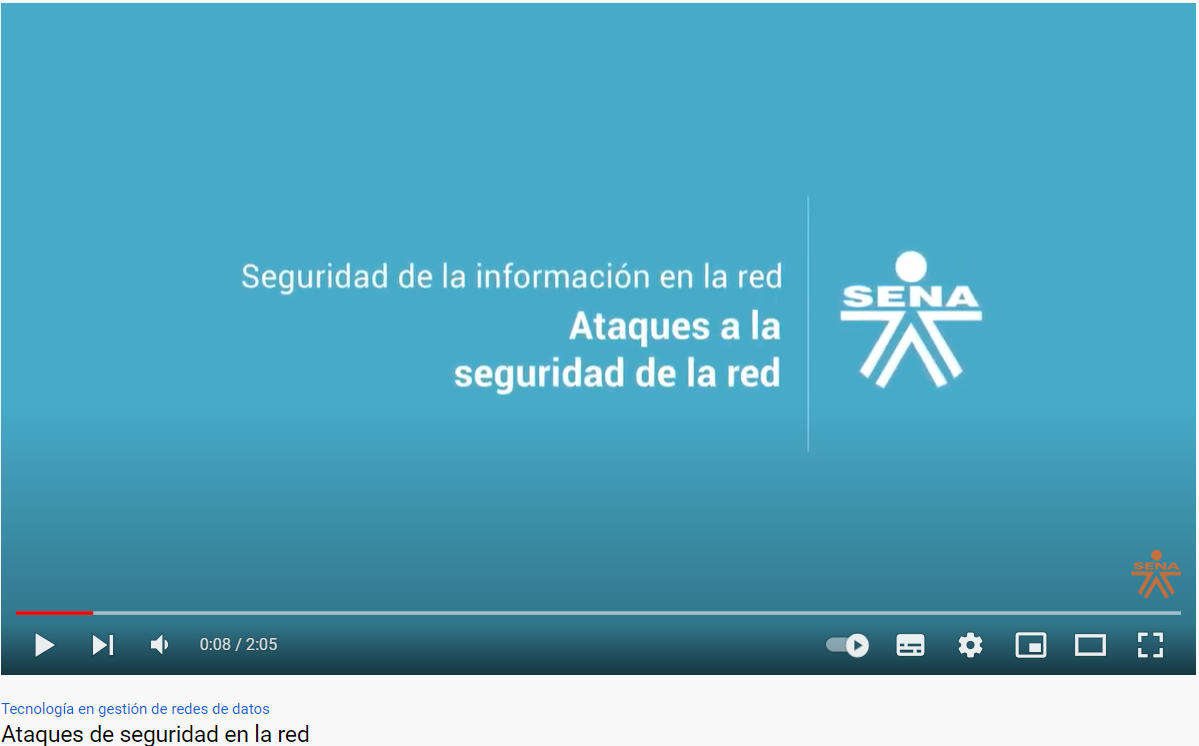


En sistemas informáticos, la **vulnerabilidad** se entiende como la incapacidad de un sistema para protegerse permitiendo ser atacado y recibiendo daño. Estas debilidades en los sistemas son ocasionadas normalmente por no contar con una eficiente protección ante amenazas externas, el no realizar actualizaciones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



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:



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.

**2. 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.

**2.1. 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*







* **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:



**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.

**Tabla 3**

*Relaciones de la familia de Normas ISO/IEC 27001*

| Estándar de vocabulario | ISO/IEC 27000  Sistemas de gestión de seguridad de la información: visión general y vocabulario | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Requerimientos  estándar | ISO/IEC 27001  Requisitos de los sistemas de gestión de la seguridad de la información | | ISO/IEC27006  Requisitos para organismos que brindan auditoría y certificación de los sistemas de gestión de seguridad de la información. | | | | ISO/IEC27009  Aplicación específica del sector de ISO/ EC 27001 Requisitos | | | |
| Normas de orientación | ISO /IEC 27002 Controles de seguridad de la información | ISO/IEC 27003 Guía de sistemas de gestión de seguridad de la información | ISO/IEC 27004 Gestión de la seguridad de la información - Seguimiento, medición, análisis y evaluación | ISO/IEC 27005 Gestión de riesgos de seguridad de la información | ISO/IEC 27007 Directrices para la auditoría de sistemas de gestión de seguridad de la información | Las directrices ISO/IEC 27008 forman la evaluación de los controles de seguridad de la información | ISO/IEC 27013 Directrices sobre la implementación integrada de ISO/IEC27001 e ISO/IEC20000-1 | ISO/IEC 27014 Gobernanza de la seguridad de la información | ISO/IEC 27016 Gestión de la seguridad de la información. Economía organizacional | ISO/IEC 27021 Requisitos de competencia para profesionales de sistemas de gestión de seguridad de la información |
| Normas de orientación específicas del sector | ISO/IEC 27010  Gestión de la seguridad de la información para comunicaciones intersectoriales e interorganizacionales | | ISO/IEC 27011  Código de prácticas para controles de seguridad de la información basado en ISO/EC 27002 para organizaciones de telecomunicaciones. | | ISO/IEC27017  Código de prácticas para controles de seguridad de la información basado en ISO7EC 27002 para servicios en la nube. | | ISO/IEC 27018  Código de prácticas para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII. | | ISO/IEC 27019  Controles de seguridad de la información para la industria de servicios públicos de energía. | ISO/IEC 27799  Informática de la salud: gestión de la seguridad de la información en salud utilizando ISO/IEC 27002 |
| Estándares de directrices específicos de controles | ISO/IEC 2705X | | | | ISO/IEC 2705X | | | | ISO/IEC 2705X | |

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:



* **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.

**2.2. 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:



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







**2.3. 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, véalo:



**3. 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.

**3.1 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:

-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.

-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:



* **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.

**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 o las herramientas son muy accesibles. |
| 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.

**3.2 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:



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.



1. **ACTIVIDAD DIDÁCTICA**

| DESCRIPCIÓN DE LA ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Ciberseguridad |
| Objetivo de la actividad | Identificar los conceptos básicos de ciberseguridad que faciliten los procesos de gestión del riesgo en las organizaciones, atendiendo a los lineamientos y las normativas existentes. |
| Tipo de actividad sugerida | Cuestionario |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | DI\_CF01\_Actividad didáctica  (Carpeta formatos de diseño) |

1. **MATERIAL COMPLEMENTARIO**

| Tema | Referencia APA del material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del recurso o  archivo del documento o material |
| --- | --- | --- | --- |
| 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. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_elibroELB172144> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1j5choe/sena_elibroELB172144> |
| 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*. <https://revistacientificaesmic.com/index.php/esmic/article/view/866/836> | Artículo | <https://revistacientificaesmic.com/index.php/esmic/article/view/866/836> |
| Enrutamiento IP | Fernández, L. (2022). *Conoce qué es la tabla de enrutamiento en un router*. Redeszone. <https://www.redeszone.net/tutoriales/redes-cable/tabla-enrutamiento-router-que-es/> | 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. <https://www.avg.com/es/signal/ipv4-vs-ipv6> | Página web | <https://www.avg.com/es/signal/ipv4-vs-ipv6> |
| Protocolo TPC/IP | IBM. *Protocolos TCP/IP*. (s.f.). IBM. <https://www.ibm.com/docs/es/aix/7.2?topic=protocol-tcpip-protocols> | Página web | <https://www.ibm.com/docs/es/aix/7.2?topic=protocol-tcpip-protocols> |
| Tipos de redes | IBM*. Redes físicas*. (s.f.). IBM. <https://www.ibm.com/docs/es/aix/7.2?topic=concepts-physical-networks> | 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. <https://www.pc-history.org/17799.htm> | Línea de tiempo | <https://www.pc-history.org/17799.htm> |

1. **GLOSARIO**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| 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. |

1. **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>

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Ronald Alexander Vacca Ascanio | Experto temático | Regional Norte de Santander – Centro de la Industria, la Empresa y los Servicios | Septiembre de 2022 |
| Maribel Avellaneda Nieves | Diseñadora instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Octubre de 2022 |
| Silvia Milena Sequeda Cárdenas | Asesora pedagógica y metodológica | Regional Distrito Capital - Centro de diseño y Metrología | Octubre de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo desarrollo curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Octubre de 2022 |
| Julia Isabel Roberto | Correctora de estilo | Regional Distrito Capital - Centro de diseño y Metrología | Octubre de 2022 |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| --- | --- | --- | --- | --- | --- |
| Autor (es) |  |  |  |  |  |