

Ciberseguridad y Seguridad de la Información

**Breve descripción:**

El mundo digital es una realidad casi tangible en la vida actual. Cada día aumenta la cantidad de personas que está integrando el Internet a su estilo y condición de vida como productores, consumidores o espectadores, por eso el incremento en este tipo de prácticas supone una mayor exposición a riesgos de tipo informático que es necesario conocer y así evitar ser víctimas de algún tipo de fraude o delito de este tipo.

**Junio 2024**

Tabla de contenido

[Introducción 1](#_Toc169022937)

[1. Ciberseguridad 3](#_Toc169022938)

[1.1. Marcos de referencia 5](#_Toc169022939)

[1.2. Tríada de la Seguridad de la Información 14](#_Toc169022940)

[1.3. Amenazas 16](#_Toc169022941)

[1.4. Vulnerabilidades 18](#_Toc169022942)

[1.5. Activos de información 19](#_Toc169022943)

[2. Las redes sociales 25](#_Toc169022944)

[2.1. Tipos de redes sociales 25](#_Toc169022945)

[2.2. Usos de las redes sociales 27](#_Toc169022946)

[2.3. Características de seguridad en las redes sociales 28](#_Toc169022947)

[Síntesis 29](#_Toc169022948)

[Material complementario 30](#_Toc169022949)

[Glosario 31](#_Toc169022950)

[Referencias bibliográficas 32](#_Toc169022951)

[Créditos 33](#_Toc169022952)

Introducción

¿Qué es la ciberseguridad?

¿Qué es la seguridad de la información?

Estas preguntas y muchas más serán respondidas a lo largo del componente formativo, pero para comenzar, lo invitamos a ver el siguiente video.

1. Ciberseguridad y Seguridad de la Información: introducción



**[Enlace de reproducción del video](https://www.youtube.com/watch?v=fMhs0mUih78)**

|  |
| --- |
| **Síntesis del video: Ciberseguridad y Seguridad de la Información: introducción** |
| El mundo digital es una realidad de vida que se evidencia en la actualidad y requiere de atención y cuidado debido a sus diferentes riesgos. En la actualidad los delitos son de diferentes índoles entre los que se encuentran los que atacan la seguridad digital en sus diferentes formas, por eso en este contenido de formación usted los aprenderá a descubrir, identificar y saber prevenirlos, inclusive, debe trabajarlos desde la óptica de un ciudadano ciber conocedor que orienta y ayuda a orientar a las personas en el campo de la realidad digital, es para eso, que en este contenido se relaciona de cerca con conceptos de ciberseguridad, integridad e información, entre otros, adicionalmente se trabaja en el conocimiento de las redes sociales como generador de ese impacto digital, debido a que la mayoría de las veces éstas redes son la puerta de entrada a la novedad virtual desconociendo por parte del visitante los buenos usos de la información y dejando expuestos los diferentes tipos de datos personales y empresariales.  Usted como ciudadano digital debe conocer estos elementos, porque lo previenen de ser víctima de ataques de ciberseguridad contando con buena seguridad de la información. Recuerde que en esta época el oro es la información. |

# Ciberseguridad

¿Qué es la ciberseguridad?

Cano, J (2011), nos dice que es:

“El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

Y también incluye activos, bienes, servicios y datos de los dispositivos y usuarios conectados a una red; adicionalmente Cano (2011) agrega, que se pueden contar los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno en búsqueda de mantener las propiedades de seguridad en todos estos elementos de cualquier organización o persona sin importar cuál sea la red que frecuenta, su edad, su entorno y su uso”.

¿Sabía que en los últimos años el concepto de ciberseguridad se ha convertido en un estándar y en una necesidad en todas las organizaciones?

Esto se da porque cada vez más y con mayor frecuencia se recurre al uso de las tecnologías de la información y las comunicaciones para apalancar los procesos operativos junto con las propuestas de valor de los negocios.

El desarrollo y evolución de la tecnología nos lleva a hacer uso de servicios como Internet, la interconexión entre sedes y con mayor frecuencia la utilización de tecnologías de computación en la nube.

Las redes sociales y en general el Internet, hacen totalmente necesario proteger toda la información que se gestiona al ingresar en cualquiera de estos recursos digitales, solo de esa forma se pueden mantener monitoreadas las amenazas de las cuales se puede ser víctima.

Protegerse de los peligros de la actual coyuntura tecnológica, conlleva a diseñar y adoptar una serie de procesos que posibiliten la protección de los activos, recursos e información personal y empresarial de todos los seres digitales y para ello se recomienda la aplicación de las siguientes fases como paso inicial:

1. **Prevención**

Esta es la primera fase que ayudará de manera significativa en la disminución de los riesgos, actuar de manera temprana implica conocer los activos o recursos tecnológicos más usados y realizar un análisis de las posibles amenazas junto con la forma en que se previenen o contrarrestan, esta fase es de gran importancia para generar conciencia, preparar y capacitar a los usuarios y de esta forma disminuir el número de errores que ocurren por desconocimiento, recuerde siempre que una buena prevención es la mejor defensa.

1. **Localización**

Luego de prevenir los esfuerzos, se continúa con la adquisición e implementación de una serie de herramientas tecnológicas que generen una alerta en algún tipo de incidente, para localizar su fuente y afectación, con el fin de tomar las acciones correctivas a que dieran lugar.

Esto se logra cuando las medidas y herramientas empleadas están haciendo un constante monitoreo y gestión sobre los recursos tecnológicos. Normalmente, cuando se detectan los incidentes, estos ya han ocurrido muchos días antes, esto es debido a que los delincuentes cada vez utilizan más herramientas y estrategias que dificultan su detección, de ahí la importancia de una constante monitorización sobre los recursos y servicios tecnológicos.

1. **Reacción**

Una vez se detecte una posible amenaza se debe realizar una reacción inmediata que permita su mitigación, para esto se recomienda seguir los siguientes pasos:

* Desconectar los activos de la red que están siendo afectados.
* Actualizar los sistemas de protección implementados, como antivirus, antimalware, antispyware, entre otras estrategias implementadas en la organización.
* Realizar un análisis exhaustivo sobre los sistemas o servicios afectados a fin de detectar el origen y afectación.
* Cambiar todas las contraseñas.
* Realizar una limpieza profunda de los recursos tecnológicos con las herramientas con que se cuente.

## Marcos de referencia

Los ataques cibernéticos son cada vez más comunes y frecuentes, como se mencionó anteriormente, debido a la inmersión de la tecnología en todos los procesos, tanto personales como empresariales; es clara la necesidad de protección en recursos, información y activos, sin embargo, el inicio puede ser lejano y para eso se hace el siguiente planteamiento:

Es ahí donde cobran importancia los marcos de referencia que se han venido desarrollando, porque con la adopción de estos marcos se tendrá clara y en orden, toda la información de valor y útil en el diseño de las estrategias de control y mitigación de riesgos de ciberseguridad.

Si bien se debe elegir un marco y trabajar con él, son solo una referencia y no una solución definitiva porque también es importante el enfoque del análisis de riesgos del cual se dará información más adelante. Son varios marcos, cada marco propone una serie de controles diferentes. Se debe elegir por su parte el marco indicado aplicable a su entorno y si se llegase a requerir algún ajuste se puede importar de alguno de los otros marcos y generar su propio marco de seguridad, es así como funciona esta información que con su prudente apropiación logra protección alta.

A continuación, se mencionan los marcos de referencia más utilizados y de mayor desarrollo, incluyendo algunos propósitos particulares para su adopción.

1. **El primer marco es el dispuesto desde Norteamérica como CSF (Cybersecurity Framework)**

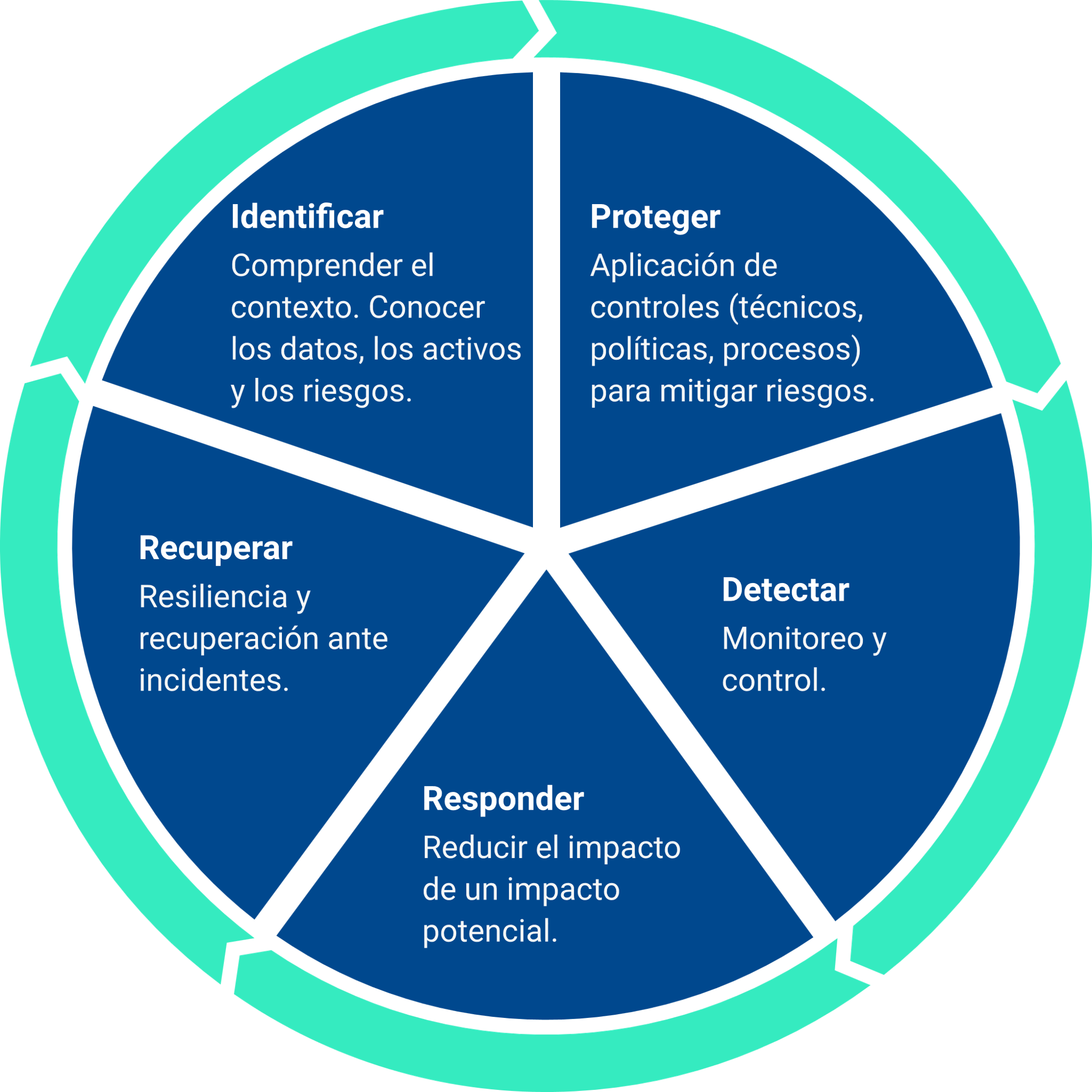
NIST CSF (National Institute of Standards and Technology - Cybersecurity Framework) - Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología.

Este marco establece una guía en la que cualquier empresa pueda recibir, comprender, administrar y reducir los riesgos cibernéticos junto con sus redes y datos. Este marco permite la comprensión del lenguaje común y enfoca buenas prácticas en ciberseguridad.

El Instituto Nacional de Normas y Tecnología (NIST), una agencia perteneciente al Departamento de Comercio de los Estados Unidos, desarrolló este marco, el cual utiliza un lenguaje cómodo que guía a las compañías en general, a gestionar algún impacto negativo de seguridad digital y así fortalecer la información.

Este marco no provee nuevas estructuras, más funciones de ciberseguridad, ni incrementa categorías, solo reúne las mejores prácticas conocidas al respecto como lo son ISO, ITU, CIS, NIST, entre otros; y las agrupa según afinidad. Se centra en el uso de lanzadores para guiar las actividades de seguridad digital de las empresas considerando los riesgos de la información como parte importante en la gestión de los riesgos.

1. Mejores prácticas conocidas



El Framework Core comprende un conjunto de actividades de ciberseguridad, resultados y referencias informativas que son comunes a través de los sectores de infraestructura crítica. Así, proporciona la orientación detallada para el desarrollo de perfiles individuales de la compañía. Mediante el uso de los perfiles, el marco ayudará a la organización a alinear sus actividades de ciberseguridad con sus requisitos de negocio, tolerancias de riesgo y recursos. Por su parte, los niveles de implementación del marco (tiers) proporcionan un mecanismo para que las empresas puedan ver y comprender las características de su enfoque para la gestión del riesgo de ciberseguridad.

**Las bases del marco CSF son:**

* Identificar estándares de seguridad y guías aplicables de forma trasversal a todos los sectores de infraestructuras críticas.
* Establecer un lenguaje común para gestionar riesgos de ciberseguridad.
* Proveer un enfoque priorizado, flexible, repetible, neutral, basado en desempeño y efectivo en términos de coste-beneficio basado en las necesidades del negocio.
* Ayudar a los responsables y operadores de infraestructuras críticas a identificar, inventariar y gestionar riesgos informáticos.
* Establecer criterios para la definición de métricas para el control del desempeño en la implementación.
* Establecer controles para proteger la propiedad intelectual, la privacidad de los individuos y las libertades civiles cuando se ejecuten actividades de ciberseguridad.
* Identificar áreas de mejora que permitan ser gestionadas a través de colaboraciones futuras con sectores particulares y organizaciones orientadas al desarrollo de estándares.
* No introducir nuevos estándares cuando existan iniciativas ya desarrolladas que cubran los objetivos de la orden ejecutiva.

De acuerdo con el NIST (s.f) “el marco de trabajo es una guía voluntaria, basada en estándares, directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen mejor y reduzcan el riesgo de ciberseguridad. Además, se diseñó para fomentar las comunicaciones de gestión del riesgo y la seguridad cibernética entre los interesados internos y externos de la organización“. Eso quiere decir que los objetivos del marco de trabajo en su implementación en una organización se podrían catalogar en los siguientes puntos:

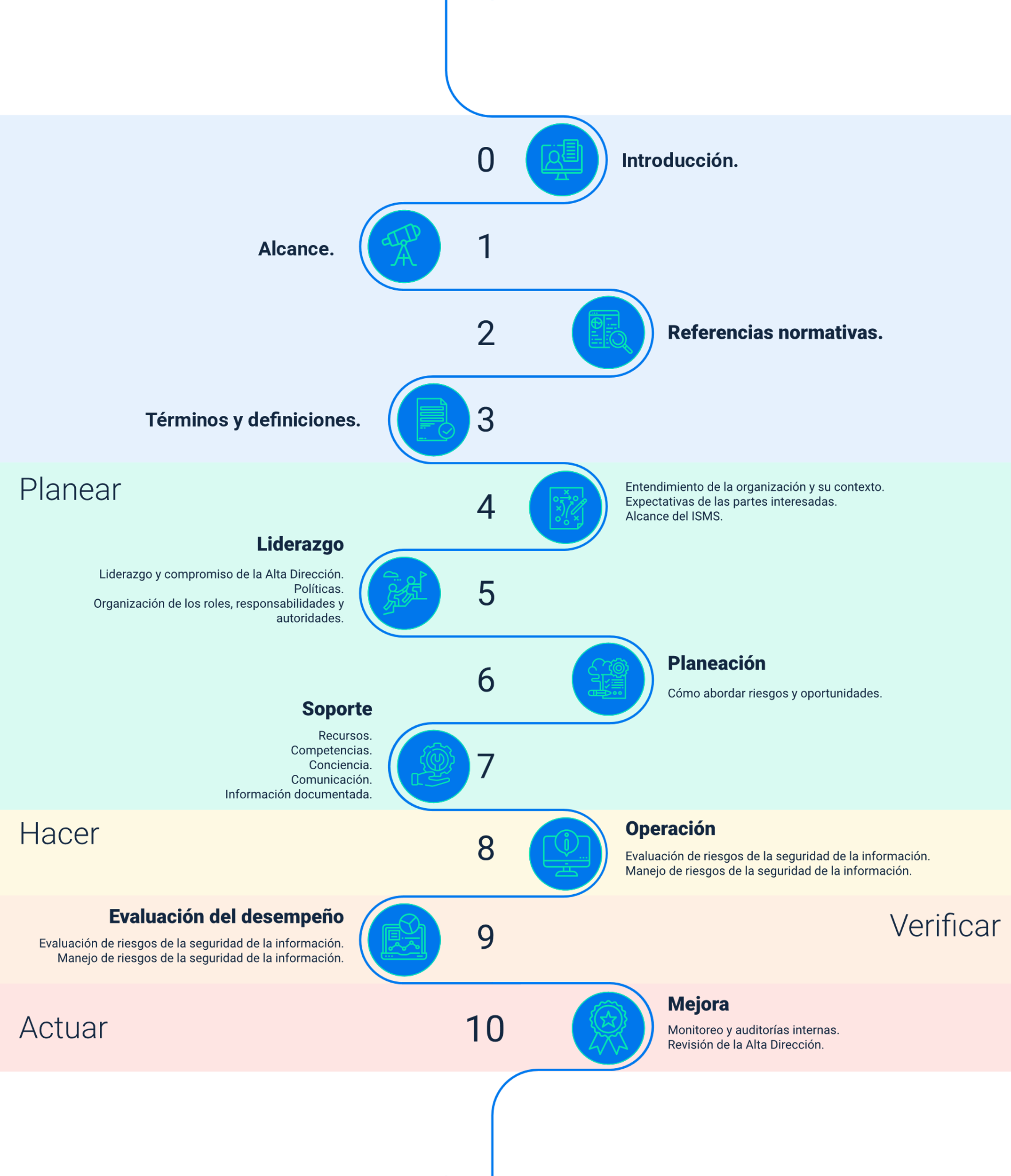
* Describir la postura actual de ciberseguridad.
* Describir el estado objetivo de ciberseguridad.
* Identificar y priorizar oportunidades de mejora en el contexto de un proceso continuo y repetible.
* Evaluar el progreso hacia el estado objetivo.
* Comunicación entre las partes interesadas internas y externas sobre el riesgo de ciberseguridad.

Todo esto enmarcado en un enfoque orientado a la gestión del riesgo.

1. **El siguiente marco es el que presenta ISO denominado ISO / IEC 27001: 2013.**

Creado y publicado por la Organización Internacional de Normalización (ISO), es un marco general que funciona bien para empresas de diversos tamaños en una variedad de industrias. Es similar al NIST CSF. El marco es respetado y ampliamente conocido internacionalmente. El enfoque de ISO 27001 es la protección de la confidencialidad, integridad y disponibilidad de la información en una empresa. Su filosofía se basa en la gestión de riesgos: investigar dónde están y luego tratarlos de manera sistemática tal como se presenta en la siguiente gráfica:

1. ISO / IEC 27001: 2013

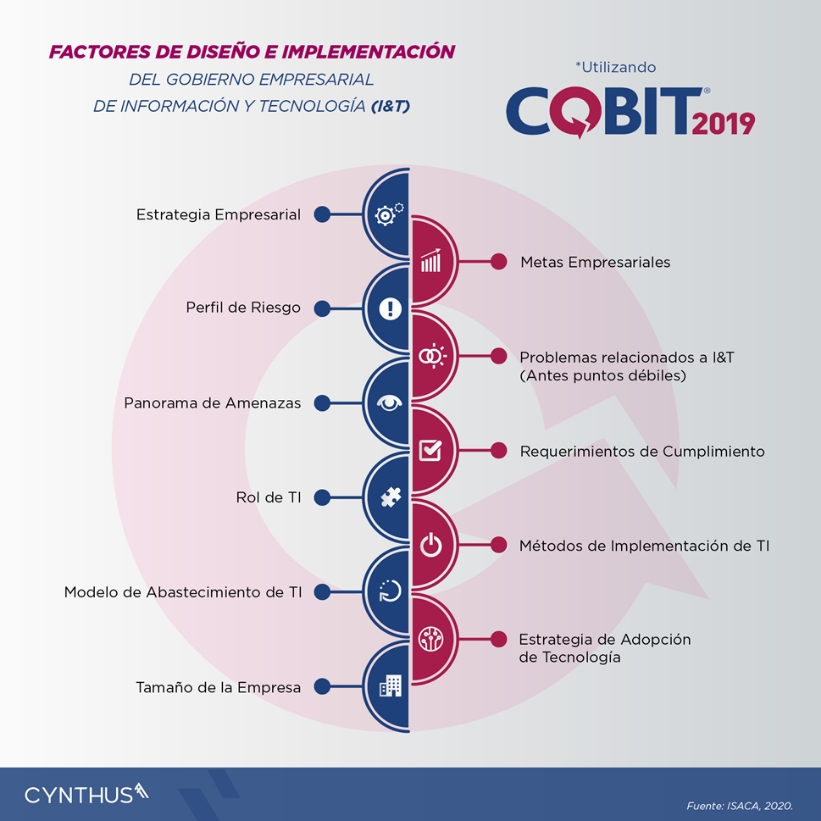


1. **En tercer lugar se ubica la famosa COBIT que traduce Objetivos de Control para Información y Tecnologías Relacionadas. Proveniente del inglés Control Objectives for Information and related Technology.**

COBIT fue desarrollado por ISACA, una organización global independiente sin fines de lucro, que se enfoca en el gobierno de TI (Tecnologías de la Información). Este marco es similar al marco de NIST e ISO, porque es un marco más general que la mayoría de las organizaciones pueden usar. También está enfocado en el negocio y orientado a procesos. COBIT a menudo es adoptado por auditores de empresas públicas y se utiliza como una herramienta de cumplimiento para Sarbanes-Oxley.

Es una guía de mejores prácticas, dirigida al control y supervisión de TI. Cuenta con una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo objetivos de control, mapas de auditoría, herramientas para su implementación y una guía de técnicas de gestión, como se puede ver en la siguiente figura:

1. Marco COBIT



Nota. Tomado de Cynthus (2020).

1. **El cuarto y último marco del contenido a revisar es el marco HITRUST CSF (Health Information Trust Alliance - Cybersecurity Framework)**.

HITRUST CSF fue desarrollado por Health Information Trust Alliance (HITRUST) y es el marco de seguridad más adoptado en la industria de la salud de los Estados Unidos. HITRUST originalmente desarrolló su CSF (Cybersecurity Framework – Marco de ciberseguridad) para enfocarse en elementos clave y riesgos inherentes a la industria de la salud, como las consideraciones de HIPAA (Ley de Responsabilidad y Portabilidad de Seguros de Salud) pero desde entonces han actualizado el marco con controles más amplios que se aplicarían a cualquier organización.

HITRUST CSF es un marco basado en el riesgo y el cumplimiento y se actualiza con bastante frecuencia. También se puede adaptar según una variedad de factores, que incluyen el tipo de organización, el tamaño y los sistemas, así como los requisitos reglamentarios.

## Tríada de la Seguridad de la Información

Seguridad de la información significa proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados. Soriano, M. (2014)

El siguiente video nos presenta, de forma más completa, este concepto.

1. Tríada de la seguridad de la Información



[**Enlace de reproducción del video**](https://www.youtube.com/watch?v=yax-5QX80T0)

|  |
| --- |
| **Síntesis del video: Tríada de la seguridad de la Información** |
| En esta oportunidad vamos a hablar sobre los conceptos básicos de ciberseguridad, es importante mencionar o es fundamental recordar que en las empresas protegen sus recursos, sus datos, su información, su patrimonio, puesto que todo esto es el resultado de un gran esfuerzo, de muchos años, de mucho trabajo, mucho sacrificio, luego es importante y fundamental protegerlos, en esta era de la información es supremamente importante promover la seguridad física y la seguridad en la red, no sólo desde el punto de vista empresarial sino desde el punto de vista personal, todos hoy en día somos usuarios de sistemas de información, de redes sociales, de estrategias tecnológicas, a través de las cuales estamos compartiendo nuestros recursos: personales, empresariales corporativos, a través de todas estas estrategias que hoy nos brinda la tecnología.  Para proteger estos recursos, la información y el patrimonio, es importante mencionar lo que conocemos como la tríada de la información, siendo este un conjunto que encierra tres conceptos fundamentales: la integridad, la confidencialidad y la disponibilidad, siendo la confidencialidad el hecho de garantizar que los recursos tecnológicos, la información y los datos que son generados de manera personal y empresarial, sean accesibles solamente por las personas adecuadas y dentro de sus niveles de autorización, si mencionamos la disponibilidad nos referimos a que los recursos tecnológicos, la información y nuestros datos siempre puedan estar disponibles para el momento en que sea necesario utilizarlos. La integridad se refiere a que los datos e información debe ser confiable, deben ser verídicos y sin modificaciones a su intencionalidad original. |

## Amenazas

Se refieren a la posibilidad que se presente algún tipo de evento, en cualquier instante de tiempo, y se produzca un daño material o inmaterial sobre los activos informáticos y los sistemas de información. Las amenazas son consideradas como los ataques cometidos por personas internas o externas, que pueden ocasionar daños a la infraestructura tecnológica, a los sistemas de información o a la misma información que circula en la organización.

Si bien cada vez son más y más especializadas, a continuación se mencionan algunas de las amenazas más comunes y que mayor afectación provocan en los recursos y medios digitales utilizados frecuentemente.

* **Spam**

Correo no deseado. Mucha gente se ve afectada cada año por correo no deseado que falsificó su información, engañando al usuario para que siga algunos de los enlaces que normalmente contiene y que los redirecciona a sitios previamente programados o en ocasiones, hace que se ejecuten algunos scripts o fragmento de código, que realizarán alguna actividad prohibida sobre los recursos tecnológicos.

* **Pharming**

Tiene por principal objetivo convencer al usuario de que visite un sitio web malicioso e ilegítimo redireccionando la URL legítima u original a una URL ilegítima, una vez dentro, el objetivo de los cibercriminales es conseguir que el usuario les dé su información personal.

* **Phishing**

Es una de las amenazas informáticas más fáciles de ejecutar. Consiste en enviar correos electrónicos falsos o mensajes que se parecen a los correos electrónicos enviados por compañías legítimas. Así, se hace pensar al usuario que es la compañía legítima y aumentan las probabilidades de que se comparta información personal y financiera, algunos ejemplos podemos encontrarlos en mensajes de banco o entidades financieras donde lo que se busca es robar las credenciales y contraseñas de acceso a sus cuentas.

* **Ransomware**

Este tipo de amenaza busca secuestrar o restringir el acceso a las computadoras e información de sus víctimas, para luego solicitar un pago a cambio de recuperar el control de sus datos.

* **Spyware**

Es un programa de computador malicioso que parece un software legítimo. Mientras está instalado en el ordenador del usuario, se ejecuta automáticamente y espía su sistema, capturando datos que permitan identificar el comportamiento del uso de los medios tecnológicos por parte del usuario o en algunas ocasiones, elimina sus archivos.

* **Malware**

Es un software malicioso. Este es el nombre común dado a varias amenazas de seguridad que se infiltran y dañan un recurso informático.

* **Virus**

Un virus informático es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo, siempre está oculto en un software o sitio web legítimo, infecta el ordenador y puede extenderse a todos los que se encuentran en su lista de contactos.

## Vulnerabilidades

Una vulnerabilidad informática es una debilidad en el software o en el hardware que permite a un posible atacante comprometer cualquiera de los elementos de la tríada de la seguridad, como es la integridad, disponibilidad o confidencialidad del sistema o de los datos que procesa.

Por errores en la configuración o parametrización de las herramientas que normalmente utilizamos por ejemplo al utilizar contraseñas no seguras, al no actualizar el sistema operativo o antivirus de nuestros dispositivos.

Para clasificarlos a continuación, se mencionan algunas de las vulnerabilidades más comunes:

* Errores en los sistemas de validación.
* Errores que permiten el acceso a directorios.
* Errores de configuración.
* Errores en la gestión y asignación de permisos.
* Errores en la gestión de recursos.

## Activos de información

Este término se relaciona con todos los elementos tecnológicos o relacionados con la tecnología que la organización utiliza, para el cumplimiento de sus metas o core del negocio. Según la norma ISO/IEC 27001, se entiende como activo todo aquello que es importante y que la organización valora, por lo tanto debe de protegerse.

Desde el punto de vista personal, activos informáticos serán todos aquellos elementos o herramientas tecnológicas tanto hardware (computadores, celulares, tabletas, PDA, entre otros) o elementos software como aplicaciones, correo electrónico, redes sociales, entre otras que son utilizadas dentro del contexto laboral o uso personal.

De acuerdo a la norma ISO/IEC 27001, es necesario clasificar e inventariar todos los activos de información de una empresa luego de ser identificados, esto se hace como cumplimiento al Modelo de Seguridad y Privacidad de la Información, el cual presenta la siguiente forma:

1. **Inventario de activos:**

Se deben identificar todos los activos de la compañía y a su vez crear un inventario de estos.

1. **Propiedad de activos:**

Cada activo identificado debe contar con un responsable o propietario.

1. **Clasificación de la información:**

Se debe realizar su respectiva clasificación dependiendo del requerimiento legal, valor, criticidad, divulgación y modificación.

1. **Manipulación de información:**

Se debe contar con procedimientos que permitan etiquetar la información y que funcione con el sistema de clasificación que definió la empresa.

La clasificación de un activo de información está dada por las propiedades de los datos, estas propiedades son:

* Confidencialidad.
* Integridad.
* Disponibilidad.

Observe que siempre realizamos énfasis en la tríada de la información como principio para el tratamiento de los datos; esta clasificación también revisa el impacto que tendrá cada uno de los principios en caso de ser vulnerado y el impacto en las personas o empresas en el suceso.

Debemos tener siempre presentes los riesgos informáticos, los cuales son todo tipo de vulnerabilidades, amenazas que pueden ocurrir sin previo aviso y producir numerosas pérdidas para las empresas o las personas. Los riesgos más perjudiciales son a las tecnologías de información y comunicaciones, como por ejemplo, la pérdida de datos debido a daño en los discos, virus informáticos, entre otros.

Cada amenaza es diferente y no todas tienen el mismo impacto en el sistema de seguridad de los sistemas informáticos, hay exigencias elevadas y exigencias que no son tan peligrosas, pero el sistema de información y riesgo se debe encargar de todas estas amenazas de manera consciente y firme, es por eso que las partes trabajan en integrar los tipos de riesgo en tres niveles, estableciendo de esa forma la exigencia o nivel en función de la seguridad.

* **Bajo**

Cuando una amenaza no representa un ataque importante en los procesos de una organización o institución.

* **Medio**

Se establece cuando la amenaza impacta de forma parcial a las actividades de la organización o institución.

* **Alto**

Se considera un riesgo alto cuando la amenaza representa gran impacto dentro de la institución u organización.

Recuerde: analizar el riesgo es el punto inicial de trabajo en la seguridad de información, puesto que ya con el riesgo identificado se decide si se elimina, se ignora, se transfiere o se logra mitigar sabiendo siempre su real impacto corporativo y personal, es decir, se hace la gestión del riesgo.

Anteriormente se estudió que existen diferentes riesgos informáticos, algunos de los más frecuentes son generados gracias al uso de dispositivos (informática) y se debe tener mucho cuidado porque algunos son de bajo riesgo, pero pueden subir de nivel con rapidez y facilidad:

* **Fraude a través de redes o medios computacionales**

Es algo muy común y que se debe tener en cuenta, ya que comprende la manipulación ilegal de la información de la empresa a través de la creación de datos falsos, la alteración de los datos originales, así como de los procesos informáticos de la compañía con el propósito de obtener algún beneficio o de perjudicar a la organización.

* **Utilizar ilegalmente los sistemas informáticos de otras personas**

Esto es algo que se ve mucho en las organizaciones y se trata de cuando los trabajadores, o personas ajenas a la organización, utilizan sin autorización los equipos y programas de un sistema informático ajeno, desde el plano personal es muy común cuando hacemos uso de los correos electrónicos, redes sociales y acceso a sistemas informáticos de nuestros familiares o amigos sin su consentimiento.

* **Riesgo de asociaciones con contrapartes**

Este tipo de riesgo se puede presentar al tomar la decisión de trabajar en un proyecto conjunto con un tercero. Los riesgos pueden surgir al momento de compartir información personal o empresarial.

* **Acceso**

Claves de seguridad débiles, predecibles o compartidas.

* **Utilidad**

Mal uso de la tecnología, utilizar los recursos o medios tecnológicos para propósitos distintos a los originalmente deseados.

* **Infraestructura**

Hurtos de activos como aparatos tecnológicos (computadoras, celulares, PDA, tabletas, entre otros dispositivos que contienen información personal y/o financiera).

En los protocolos de seguridad de la información ya determinamos los riesgos y las amenazas que pueden atacar tanto los recursos físicos como digitales, ahora nos preguntamos:

Para determinar cómo tratarlo y las acciones de mitigación a realizar, tenga en cuenta lo siguiente:

* Revisar las políticas de seguridad.
* Actualizar todos los filtros y antivirus.
* Ajustar y cambiar de contraseñas de manera periódica.
* Instalar firewalls.
* Reservar datos, no compartir contraseñas.
* No compartir cuentas y contraseñas de acceso a cuentas o recursos.

Con relación a las redes sociales se dispone el siguiente paso:

* No aceptar invitaciones de personas o perfiles que no reconozca.
* Revisar los contenidos antes de compartirlos para evitar problemas de seguridad.

Se deben tener los controles de manera preventiva antes de tener que actuar con los correctivos.

Una vez calculado el riesgo, se debe responder con mitigación inmediata por medio de estrategias activas. A continuación se hace mención de las cuatro estrategias principales que puede usar en el caso de requerir mitigar un riesgo:

1. Transferir el riesgo a un tercero. Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
2. Eliminar el riesgo. Por ejemplo, eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico que hemos expuesto, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.
3. Asumir el riesgo, se da cuando algún riesgo puede ser aceptados, ya que su impacto no es tan alto o porque mitigarlo puede resultar demasiado costoso.
4. Implantar medidas para mitigarlo. Por ejemplo, adquirir y actualizar periódicamente un sistema de protección antivirus.

# Las redes sociales

Sabía que las redes sociales son mega estructuras creadas en Internet por grupos de personas que contactan entre sí, para compartir intereses en común, para crear relaciones por gustos, pasiones, intereses o necesidades. Esta es la forma más rápida de relacionarse con una persona o empresa.

Las primeras redes sociales como tal, no surgieron hasta la popularización de Internet a principios del siglo XXI, en la web 2.0, cuya principal característica era dar la posibilidad a los usuarios de elaborar y publicar sus propios contenidos online.

Pero, gracias a la popularización y cada vez más fácil el acceso a Internet y a elementos de comunicación móviles como los teléfonos inteligentes y las tabletas, las redes sociales han tomado una gran importancia y han incrementado el uso y acceso a este tipo de plataformas, donde el usuario busca la manera de conocerse y relacionarse e incluso busca la posibilidad de ofrecer y adquirir productos, hasta utilizarlas como estrategia para la búsqueda y consecución de empleo.

## Tipos de redes sociales

Se puede pensar equivocadamente que las redes sociales son todas iguales, pero no es así. De hecho, por lo general se dividen en diferentes tipos, de acuerdo con el objetivo de los usuarios al crear un perfil, de esa forma una misma red social puede ser útil de más de una manera.

Normalmente las redes sociales que más se usan tienen el mismo propósito, pero en realidad existen muchas otras alternativas dispuestas dependiendo del objetivo al momento del registro y crear una cuenta en ellas. La clasificación más común es:

* **Red social de relaciones**

El principal objetivo de esta red social es el de conectar personas, el caso más conocido es Facebook. Pero podemos citar innumerables otras redes, que también encajan en los otros tipos, como Instagram, LinkedIn, Twitter, etc.

* **Red social de entretenimiento**

Las redes sociales de entretenimiento son aquellas en las que el objetivo principal no es relacionarse con las personas, sino consumir contenido. El ejemplo más icónico es YouTube, la mayor plataforma de distribución de videos del mundo, en la que el objetivo es publicar y ver videos. Otro caso es el de Pinterest, en el que las personas publican y consumen imágenes.

* **Red social profesional**

Son redes donde el usuario tiene como objetivo crear relaciones profesionales con otros usuarios, divulgar proyectos y conquistas profesionales, presentar su currículum y habilidades, además de conseguir indicaciones, empleos, etc.

LinkedIn es la red social profesional más conocida y utilizada, pero hay otras que también vienen ganando un espacio y posicionándose, como Behance, Bebee, Bayt, Xing y Viadeo.

* **Red social de nicho**

Las redes sociales de nicho son aquellas dirigidas a un público específico, ya sea una categoría profesional o personas que tienen un interés específico en común.

Uno de los casos más emblemáticos es el de TripAdvisor, donde los usuarios atribuyen notas y comentarios a atracciones relacionadas con el sector gastronómico y turístico.

Si bien existen estas categorías de redes sociales, es importante mencionar que todas ellas fueron creadas con una visión o propósito inicial, pero que en la medida de su popularización y uso se han convertido en redes sociales que encajan perfectamente en varias de esta clasificación.

Es el caso de Facebook la cual originalmente fue creada como una red que conectara personas, en la actualidad viene siendo utilizada para ofertar productos y servicios, ofrecer entretenimiento y hasta ser un medio que facilita la publicación y contratación de oferta laboral.

## Usos de las redes sociales

Este uso está determinado por el tipo de red elegida para crear una cuenta entre muchas opciones. Los usos más comunes son:

* Mantener contacto con amigos y familiares.
* Mantenerse al día con noticias y eventos de actualidad.
* Llenar el tiempo libre.
* Encontrar contenido entretenido o divertido.
* Compartir su opinión sobre un determinado tema.
* Compartir fotos y videos con las demás personas.
* Generación de una red de contactos.
* Conocer personas.
* Compartir detalles de lo que se está haciendo en la vida diaria.
* Compartir perfil profesional y ofrecer buscar empleo.
* Promocionar productos y servicios.

## Características de seguridad en las redes sociales

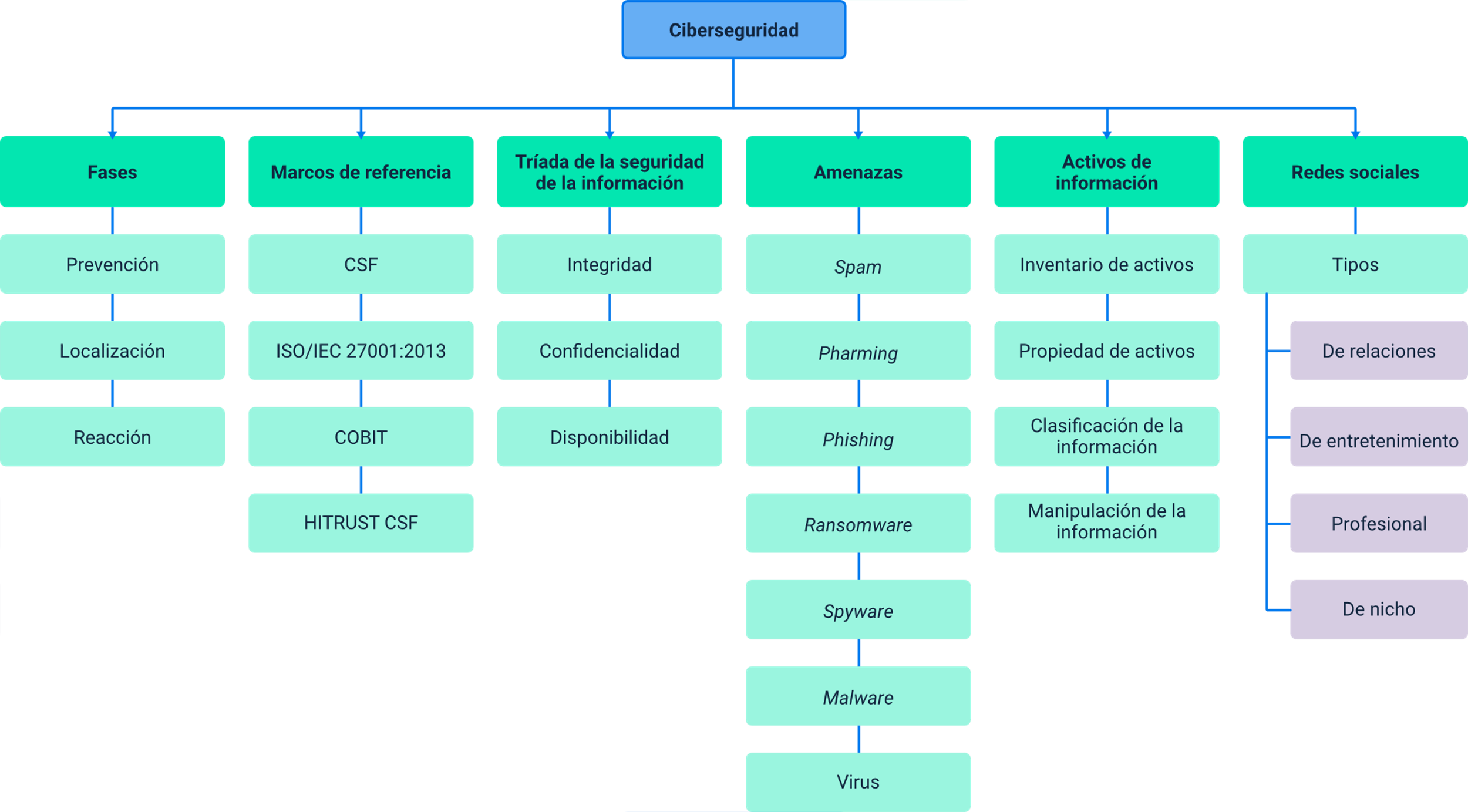
Dada la proliferación o aumento de uso de las redes sociales, a continuación se mencionan algunas características de seguridad a tener en cuenta al momento de utilizarlas.

**Características de seguridad en las redes sociales**

Para iniciar debe tener en cuenta las redes sociales que usa y la cantidad de información que comparte al día junto con la veracidad de la misma, posterior a eso se deben tener en cuenta las siguientes condiciones de seguridad para el buen uso de las redes sociales. Lo invitamos a consultar el PDF "**Infografía Seguridad Redes**", el cual se encuentra en la carpeta Anexos.

Síntesis

A continuación, se presenta a manera de síntesis, un esquema que articula los elementos principales abordados en el desarrollo del componente formativo.



Material complementario

| Tema | Referencia | Tipo de material | Enlace del recurso |
| --- | --- | --- | --- |
| Ciberseguridad | Dimensión Tecnológica. (2023). Qué es la CIBERSEGURIDAD, Explicación y Ejemplos (video). YouTube | Video | <https://www.youtube.com/watch?v=dmrlfWp9bBc> |

Glosario

**Activo**: el término de activo de información se relaciona con todos esos elementos tecnológicos o relacionados con la tecnología que la organización utiliza para el cumplimiento de sus metas o core del negocio. Según la norma ISO/IEC 27001 se entiende como activo todo aquello que es importante y que la organización valora por lo tanto debe de protegerse.

**Amenaza**: cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas.

**ISO 27001**: estándar de organización de estándares internacionales relacionado con la seguridad de la información.

**Red social**: son estructuras formadas en Internet por personas u organizaciones que se conectan a partir de intereses o valores comunes.

**Riesgo**: es la posibilidad de que una amenaza se produzca, dando lugar a un ataque sobre un recurso o servicio tecnológico. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

**SGSI**: sistema de gestión de Seguridad de la Información.

**Vulnerabilidad**: es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

Referencias bibliográficas

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. Sistemas (Asociación Colombiana de Ingenieros de Sistemas), 119, 4-7.

Cynthus (2020). ¿Qué hay de nuevo en COBIT® 2019? <https://www.cynthus.com.mx/que-hay-de-nuevo-en-cobit-2019/>

NIST (s.f). Framework for Improving Critical Infrastructure Cybersecurity <https://www.businesswire.com/news/home/20180522005533/en/HITRUST%C2%AE-Provides-NIST-Cybersecurity-Framework-Certification>

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

Créditos

| Nombre | Cargo | Centro de Formación y Regional |
| --- | --- | --- |
| Milady Tatiana Villamil Castellanos | Responsable del Ecosistema | Dirección General |
| Olga Constanza Bermúdez Jaimes | Responsable de Línea de Producción | Centro de Servicios de Salud - Regional Antioquia |
| Henry Eduardo Bastidas Paruma | Instructor | Centro de Teleinformática y Producción Industrial - Regional Cauca |
| Luis Fernando Botero Mendoza | Diseñador Instruccional | Centro para la Industria de la Comunicación Gráfica - Regional Distrito Capital |
| Rafael Neftalí Lizcano Reyes | Asesor metodológico y pedagógico | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Ana Catalina Córdoba Sus | Evaluadora Instruccional | Centro de Servicios de Salud - Regional Antioquia |
| Juan Daniel Polanco Muñoz | Diseñador de Contenidos Digitales | Centro de Servicios de Salud - Regional Antioquia |
| Yuly Andrea Rey Quiñonez | Diseño web | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Luis Jesús Pérez Madariaga | Desarrollador Fullstack | Centro de Servicios de Salud - Regional Antioquia |
| Edgar Mauricio Cortés García | Actividad Didáctica | Centro de Servicios de Salud - Regional Antioquia |
| Camilo Andres Bolaño Rey | Desarrollo Front-end | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Andrés Mauricio Santaella Ochoa | Soporte Front-end | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Daniela Muñoz Bedoya | Animador y Productor Multimedia | Centro de Servicios de Salud - Regional Antioquia |
| Andrés Felipe Guevara Ariza | Locución | Centro de Servicios de Salud - Regional Antioquia |
| Luis Gabriel Urueta Álvarez | Validador de Recursos Educativos Digitales | Centro de Servicios de Salud - Regional Antioquia |
| Margarita Marcela Medrano Gómez | Evaluador para Contenidos Inclusivos y Accesibles | Centro de Servicios de Salud - Regional Antioquia |
| Daniel Ricardo Mutis Gómez | Evaluador para Contenidos Inclusivos y Accesibles | Centro de Servicios de Salud - Regional Antioquia |