

# Activos de información y normatividad de la seguridad informática

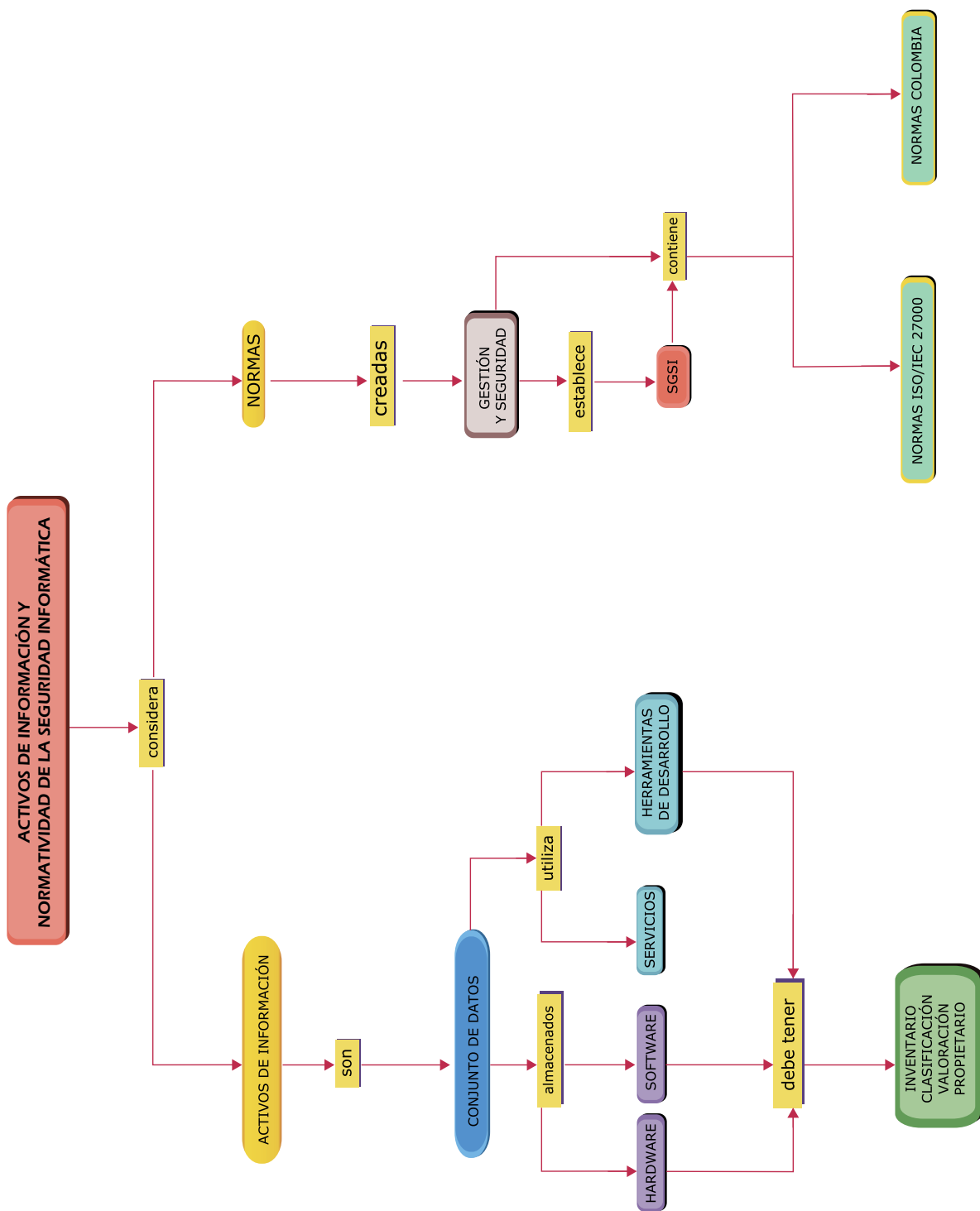
**Duración estimada de estudio (horas): 10 horas**

## Estructura de contenidos

Introducción .....	3
1. Activos de información .....	4
1.1. Definición.....	4
1.2. Inventario de activos .....	4
1.3. Propiedad de los activos.....	5
1.4. Clasificación de activos .....	7
1.4.1. Activos puros .....	7
1.4.2. Activos físicos.....	8
1.4.3. Activos humanos .....	8
1.5. Valoración de activos .....	9
1.5.1. Disponibilidad.....	9
1.5.2. Integridad.....	9
1.5.3. Confidencialidad. ....	9
2. Normatividad de la seguridad informática.....	10
2.1. Contexto.....	10
2.2. Normas ISO/IEC 27000 .....	11
2.3. Normatividad en colombia .....	14
Recursos bibliográficos .....	16
Glosario .....	17



## Mapa Conceptual



## Introducción



Las organizaciones requieren identificar, valorar y clasificar los activos de información más importantes del negocio.

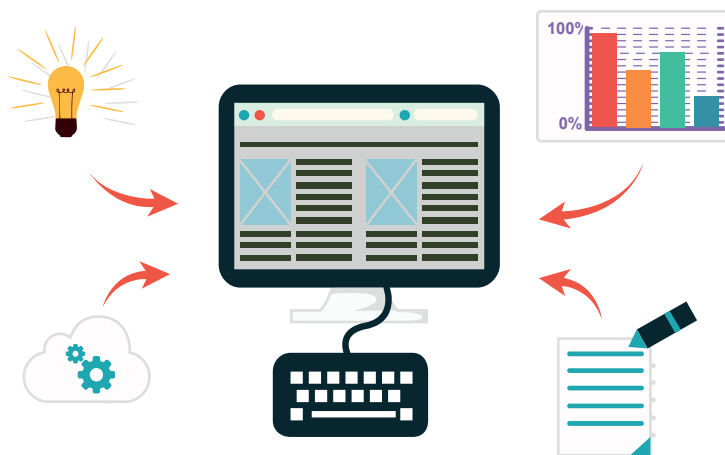
Los activos de información son considerados un factor esencial para el logro y mantenimiento de las actividades competitivas de una organización, se hace de vital importancia establecer un nivel de seguridad para proteger la información y evitar consecuencias producidas por daños o pérdidas.

Las organizaciones deben comprender y dimensionar los esfuerzos que se deben llevar a cabo para gestionar la seguridad de la información de manera sistemática más allá de la aplicación normativa y en común aplicación de estándares nacionales e internacionales.

# 1. ACTIVOS DE INFORMACIÓN

## 1.1. DEFINICIÓN

Los activos de información, son datos o información propiedad de una organización. Esta se almacena en cualquier tipo de medio físico o lógico y es considerada por la misma como indispensable para el cumplimiento de los objetivos de la organización. Un activo de información en el contexto de un SGSI y con base en la norma ISO/IEC 27001:2005 es: “algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger” (Cárdenas, F. s.f.).

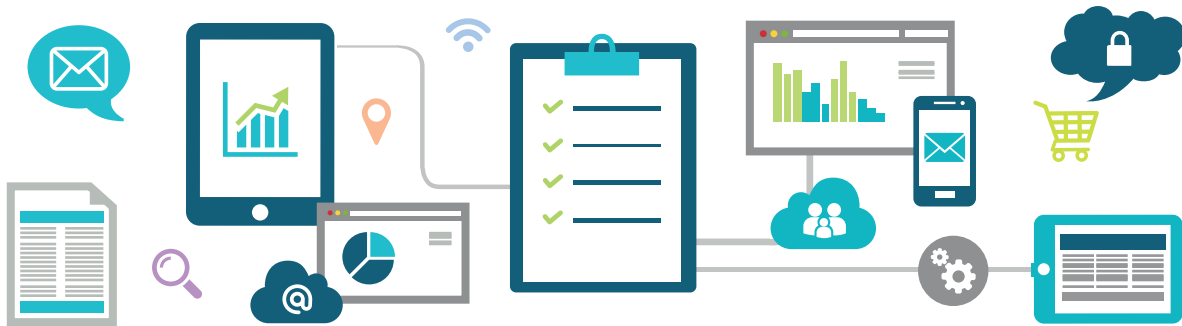


“Se debe considerar como un activo de información principalmente a cualquier conjunto de datos creado o utilizado por un proceso de la organización, así como el hardware y el software utilizado para su procesamiento o almacenamiento, los servicios utilizados para su transmisión o recepción y las herramientas y/o utilidades para el desarrollo y soporte de sistemas de información. En casos particulares, se puede considerar como un activo de información a personas que manejen datos, transacciones, o un conocimiento específico muy importante para la organización (Por ejemplo: secretos industriales, manejo de claves importantes, know how, cualquier cosa que tiene valor para la organización)”. (Cárdenas, F. s.f.).

## 1.2. INVENTARIO DE ACTIVOS








“Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos de información importantes de la organización”. (ISO/IEC 27002). Este inventario debería incluir toda

la información necesaria requerida para recuperarse de cualquier tipo de evento perjudicial a la organización.



Debe estar actualizado, de acuerdo con los cambios que surjan en los activos de la información. “Este inventario debe tener la valoración de cada activo, indicando bajo una escala definida por la organización, por ejemplo, si es de alto, medio, o bajo valor. Adicionalmente es importante que se indique cuáles son las propiedades más importantes de proteger para cada activo en términos de su CID (confidencialidad, Integridad, Disponibilidad), valorando cada propiedad. Se debe indicar cuál es la ubicación del activo de información y cuáles son los procesos que lo utilizan” (Cárdenas, F. s.f.).

Puede incluir:

-  Tipo de activo
-  Clase de activo
-  Nombre de activo
-  Ubicación
-  Propietario
-  Valoración
-  Información sobre licencias.

### 1.3. PROPIEDAD DE LOS ACTIVOS

Toda la información y los activos asociados con los servicios de procesamiento de información deberían ser “propietario” (propietario: identifica a un individuo o a una entidad que tiene responsabilidad aprobada



de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término “propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.), de una parte designada de la organización (ISO/IEC 27002).

Se puede determinar algunos entes que interactúan con los activos de información como lo son:

✳️**Propietario de la Información:** El cual es una parte designada de la organización, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso, que pueden hacer con la información, y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y al mismo tiempo, de definir que se hace con la información una vez ya no sea requerida, así como los tiempos de retención asociados a la misma.

El propietario del activo debería ser responsable de:

- Garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifiquen adecuadamente.
- Definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

✳️**Custodio técnico:** Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (copias de seguridad, asignar privilegios de: acceso, modificaciones, borrado) que el propietario de la información haya definido, con base en los controles de seguridad y recursos disponibles en la organización



✱ **Usuario:** Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la organización en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la organización. Son las personas u otros sistemas que utilizan la información para propósitos propios de su labor, y que tendrán el derecho manifiesto de su uso dentro del inventario de información. Para cada usuario se debería definir los derechos y niveles de acceso al activo de información (lectura, escritura, borrado, etc.).



### 1.4. CLASIFICACIÓN DE ACTIVOS

La información debería clasificarse en términos de su valor, de los requisitos legales, de su sensibilidad y la importancia para la organización. Estas son algunas clasificaciones:

#### 1.4.1. Activos puros

✱ **Datos digitales:** Financieros , legales, de investigación y desarrollo, estratégicos y comerciales, correo electrónico, contestadores automáticos, bases de datos, unidades lógicas (particiones) privadas y com partidas, copias de seguridad (CD, DVD), claves de cifrado.

✱ **Activos tangibles:** Personales, financieros, legales, de investigación y desarrollo, estratégicos y comerciales, correo tradicional/electrónico, FAX, materiales de copia de seguridad/archivo, llaves de oficinas/ cajas fuertes y otros medios de almacenamiento, libros, revistas, periódicos.

✱ **Activos intangibles:** Conocimiento, relaciones y secretos comerciales, licencias, patentes, experiencia, conocimientos técnicos, imagen corporativa/marca/reputación comercial/confianza de los clientes, ventaja competitiva, ética, productividad.

✱ **Software de aplicación:** Propietario desarrollado por la organización, de cliente (compartido y aplicaciones de escritorio), planificación de recursos empresariales (ERP), de gestión de la información (MIS), utilidades y herramientas de bases de datos, aplicaciones de comercio electrónico, middleware.

✱ **Sistemas operativos:** Servidores, computadores de escritorio,

computadores portátiles, servidores centrales, dispositivos de red, dispositivos de mano e incrustados (incluyendo la BIOS y el firmware).

### 1.4.2. Activos físicos

- ✱ **Infraestructura:** Edificios, centros de datos, habitaciones de equipos y servidores, armarios (racks) de red o cableado, oficinas, escritorios, cajones, archivadores, salas de almacenamiento de medios físicos y cajas de seguridad, dispositivos de identificación y autenticación, control acceso del personal, circuito cerrado de televisión (CCTV).
- ✱ **Controles del entorno:** Equipos de alarma, supresión contra incendio, sistemas de alimentación ininterrumpida (SAI), alimentación de potencia y de red, acondicionadores, filtros, supresores de potencia, refrigeradores, alarmas de aire, alarmas de agua.
- ✱ **Hardware:** Dispositivos de almacenamiento y cómputo como computadoras de escritorio, estaciones de trabajo, portátiles, equipos de mano (tabletas), servidores, mainframes, módems, líneas de terminación de red, dispositivos de comunicaciones (nodos de la red), impresoras, fotocopadoras, fax.
- ✱ **Activos de servicios:** Servicios de autenticación de usuario y administración de procesos de usuario, enlaces, cortafuegos, servidores proxy, servicios de red, servicios inalámbricos, antispam, anti-virus, detección y/o prevención de intrusiones, teletrabajo, seguridad, FTP, correo electrónico, mensajería instantánea, servicios web, contratos de soporte y mantenimiento de software.

### 1.4.3. Activos humanos

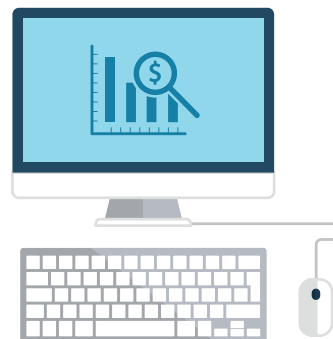
- ✱ **Empleados: personal,** directivos, directores ejecutivos, arquitectos de software y desarrolladores, probadores, administradores de sistemas, administradores de seguridad, operadores, abogados, auditores, usuarios con poder y expertos en general
- ✱ **Externos:** trabajadores temporales, consultores externos o asesores especialistas, contratistas especializados, proveedores y socios.



### 1.5. VALORACIÓN DE ACTIVOS

Al ser identificados los activos de la organización, deben tener un valor, ya que por medio de éste se identifica cuál es su importancia.

Lo primero que se debe considerar para la valoración de los activos de la organización, es determinar el daño que puede causar el activo, si éste, es deteriorado en disponibilidad, integridad y confidencialidad. Luego, se le asigna un valor donde se evalúa el daño del activo frente a:



- Violación de legislación aplicable.
- Reducción del rendimiento de la actividad.
- Efecto negativo en la reputación.
- Perdida económicas.
- Trastornos en el negocio.

Para determinar si un activo es deteriorado frente a disponibilidad, integridad y confidencialidad, se debe determinar lo siguiente:

**1.5.1. Disponibilidad:** Se debe evaluar cuál es la importancia o el impacto para la organización si el activo o no estuviera disponible.

**1.5.2. Integridad:** Se debe evaluar si el activo de la organización, es alterado sin autorización y/o control.

**1.5.3. Confidencialidad:** Se debe evaluar cuál es el impacto para la organización, si se accede a los activos de forma no autorizada.

## 2. NORMATIVIDAD DE LA SEGURIDAD INFORMÁTICA

### 2.1. CONTEXTO

Las normas de seguridad de la información, son creadas para demostrar la gestión y seguridad competente y efectiva de los recursos y datos que se gestionan en una organización.

La herramienta utilizada para este proceso es SGSI (Sistema de Gestión de la Seguridad de la Información), el cual, por medio de procesos sistemáticos, documentados y conocidos por toda la organización, garantiza que la seguridad de la información es gestionada correctamente.



“El SGSI ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente” ([www.iso27000.es](http://www.iso27000.es)).

“El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente. Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se difunda de acuerdo con las necesidades de la organización” (NTC-ISO-IEC 27001).

## 2.2. NORMAS ISO/IEC 27000



Las normas ISO/IEC 27000, es un conjunto de estándares desarrollados (o en fase de desarrollo), por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

✳️ **ISO 27000:** Se describe la visión general y el vocabulario de sistemas de gestión de la seguridad de la información, y referencia la familia de normas de sistemas de gestión de la seguridad de la información con los términos y definiciones relacionadas.

✳️ **ISO 27001:** Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2013 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

La Norma ISO 27001, proporciona la metodología para la implementación de la seguridad de la información en cualquier tipo de organización, teniendo en cuenta los controles de seguridad, protección a los activos de información e identificación de riesgos.

**Fases:** La norma 27001 está formada por cuatro fases que se deben implementar constantemente para reducir los riesgos en confidencialidad, integridad, disponibilidad y auditabilidad de la información. Estas fases son:

**Fase de planificación (Plan):** Esta fase se enfoca en la planificación de políticas, procesos, procedimientos y objetivos de la seguridad de la información, con los cuales se identifican los controles pertinentes de seguridad. Esta es una fase para el establecimiento y gestión del SGSI, se debe tener en cuenta:

- Definir el alcance del sistema de gestión.
- Definir la política del SGSI.
- Definir la metodología para la valoración del riesgo.
- Identificar los riesgos.
- Elaborar un análisis y evaluación de dichos riesgos.
- Identificar los diferentes tratamientos de riesgo.
- Seleccionar los controles y objetivos de los mismos que posibilitarán dicho tratamiento.

**Fase de ejecución (Do):** En esta fase, se ejecutan los procesos planificados en la fase anterior. Es una fase para la implantación y puesta en marcha del SGSI, para ello, se debe tener en cuenta:

- Preparar un plan de tratamiento del riesgo.
- Implantar los controles que se hayan seleccionado.
- Medir la eficacia de dichos controles.
- Crear programas de formación y concienciación.

**Fase de seguimiento (Check):** En esta fase, se realiza monitoreo al SGSI, verificando el cumplimiento de los objetivos establecidos.

**Fase de mejora (Act):** Esta fase adopta acciones correctivas y preventivas basadas en auditorías y revisiones internas, o en otra información relevante a fin de alcanzar la mejora continua del

SGSI. En las fases de seguimiento (Check) y mejora (Act) para el control y evaluación del SGSI, se debe tener en cuenta:

Implantar una serie de procedimientos para el control y la revisión.

Puesta en marcha de una serie de revisiones regulares sobre la eficacia del SGSI, a partir de los resultados de las auditorias de seguridad y de las mediciones.

Tomar las medidas correctivas y preventivas.

✳️**ISO 27002** : Es el nuevo nombre de ISO 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 35 objetivos de control y 114 controles, agrupados en 14 dominios (norma 27002:2013). Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2013.

✳️**ISO 27003**: Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación

✳️**ISO 27004**: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

✳️**ISO 27005**: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información.

- ✱ **ISO 27006:** Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSI) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSI.
- ✱ **ISO 27007:** Consiste en una guía de auditoría de un SGSI (auditorías internas).
- ✱ **ISO 27008:** Consiste en un estándar que suministra orientación acerca de la implementación y operación de los controles técnicos. Es aplicable a cualquier tipo y tamaño de empresa, tanto pública como privada que lleve a cabo revisiones relativas a la seguridad de la información y los controles de seguridad de la información.
- ✱ **ISO 27011:** Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).
- ✱ **ISO 27031:** Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y las comunicaciones.
- ✱ **ISO 27032:** Consiste en una guía relativa a la ciberseguridad.
- ✱ **ISO 27033:** Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPN y diseño e implementación de seguridad en redes.
- ✱ **ISO 27034:** Consiste en una guía de seguridad en aplicaciones.
- ✱ **ISO 27099:** Consiste en una guía para implantar la Norma ISO 27002 específica para entornos médicos.

### 2.3. NORMATIVIDAD EN COLOMBIA

Puede ser revisada la normatividad general expedida en nuestro país en la dirección <http://www.mintic.gov.co/portal/604/w3-propertyname-510.html>.



Estas son algunas normas representativas en nuestro país de los contenidos anteriormente vistos:



- ✳ **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- ✳ **Decreto 2364 de 2012:** Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- ✳ **Ley 1273 de 2009:** Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.
- ✳ **Ley 1581 de 2012:** Mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo.
- ✳ **Decreto 1377 del 27 de junio de 2013:** Tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información.
- ✳ **Ley 1341 de 2009:** Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC), se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

## RECURSOS BIBLIOGRÁFICOS

---

Alexander, A. (2013). Análisis y evaluación del riesgo de información: un caso en la Banca. Aplicación del ISO 27001:2005. Consultado el 12 de julio de 2015 en: [http://www.iso27000.es/download/Evaluacion\\_Riesgo\\_iso27001.pdf](http://www.iso27000.es/download/Evaluacion_Riesgo_iso27001.pdf)

Emaza. (2010). Los 10 tipos de activos en la Seguridad de la Información ¿Qué son y cómo valorarlos? Artículo web. Consultado el 12 de julio de 2015, en: <http://www.seguridadinformacion.net/los-10-tipos-de-activos-en-la-seguridad-de-la-informacion-que-son-y-como-valorarlos/>

Gómez, Á. (2007). Enciclopedia de la seguridad informática. Alfaomega grupo editor, México.

Icontec. (2013). Fundamentos sistema de gestión seguridad en la información. NTC/ISO 27001:2013.





## GLOSARIO


**ACTIVO:** Conjunto de todos los bienes y derechos con valor monetario que son propiedad de una organización, institución o individuo, y que se reflejan en su contabilidad.

**INFORMACIÓN:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.


**SEGURIDAD:** Ausencia de riesgo o también a la confianza en algo o alguien.



<b>OBJETO DE APRENDIZAJE</b>	<b>Activos de información y normatividad informática</b>
Desarrollador de contenido Experto temático	Jenny Marisol Henao García Yuly Paulín Sáenz Agudelo
Asesor Pedagógico	Claudia Milena Hernández Naranjo
Productor Multimedia	Luis Gabriel Urueta Alvarez
Productor de Audios	Victor hugo Tabares Carreño
Programadores	Heriberto Rojas Picon
Líder línea de producción	Santiago Lozada Garcés


**Atribución, no comercial, compartir igual**

Este material puede ser distribuido, copiado y exhibido por terceros si se muestra en los créditos. No se puede obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.


**Creative Commons**

