**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| **PROGRAMA DE FORMACIÓN** | Implementación de auditoría técnica en seguridad de la información |
| --- | --- |

| **COMPETENCIA** | 220501110 - Implementar el sistema de seguridad de la información según modelo y estándares técnicos. | **RESULTADOS DE APRENDIZAJE** | 220501110-01. Seleccionar los principios, estándares y mejores prácticas de la seguridad de la información de acuerdo con la normatividad aplicable. |
| --- | --- | --- | --- |

| **NÚMERO DEL COMPONENTE FORMATIVO** | 1 |
| --- | --- |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Fundamentos y aplicaciones de políticas de SGSI |
| **BREVE DESCRIPCIÓN** | Las políticas de auditoría de seguridad de la información son indispensables en cualquier entidad o empresa. Uno de los activos más valiosos en la organización es la información, es importante tener claridad que día a día se ven diferentes ciberataques y vulnerabilidades a las empresas. |
| **PALABRAS CLAVE** | auditoría forense, ciberseguridad, *hacking*, informática forense, seguridad de la información, seguridad digital |

| **ÁREA OCUPACIONAL** | 6 - Ventas y servicios |
| --- | --- |
| **IDIOMA** | Español |

1. **Tabla de contenidos**

**Introducción**

**1. Conceptos Sistema de Gestión de Seguridad de la Información (SGSI)**

1.1. Conceptualización, identificación, conceptos de políticas de SGSI

1.2. Introducción conceptos de SGSI

**2. Herramientas para la valoración de riesgos**

2.1. Auditoría de activos

2.2. Identificación de riesgos

2.3. Áreas de impacto

2.4. Marco normativo

**3. Políticas SGSI**

**Síntesis**

1. **Desarrollo de contenidos**

**Introducción**

¿Qué es Seguridad de la Información? ¿Por qué se debe implementar? Son interrogantes que el siguiente video responde de forma general, como un abrebocas a la temática que se desarrollará en el componente formativo.



**1. Conceptos Sistema de Gestión de Seguridad de la Información (SGSI)**

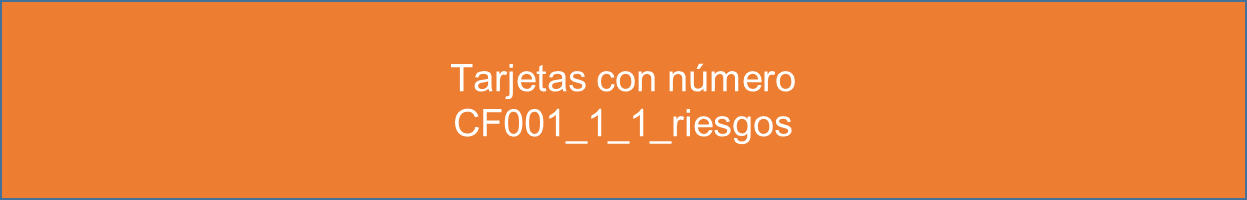
La seguridad de la información ha cobrado importancia en los últimos años; en el tema de calidad, se han estandarizado los procesos, y en la seguridad informática y de la información, se han implementado algunos controles y planes. Con el advenimiento de la norma ISO 27000, aparecen los conceptos de Gestión en Sistemas de Seguridad Informática y de la Información (SGSI), aprovechando las nuevas tecnologías y los sistemas de información, y junto a ellos, se alinean otros estándares que hasta el momento habían sido aplicados al análisis de riesgos informáticos y que posteriormente han sido usados para la gestión de riesgos de seguridad de la información.

**1.1. Conceptualización, identificación, conceptos de políticas de SGSI**

El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar los activos de información, el valor más importante en una organización, minimizando a la vez los riesgos de seguridad de la información:

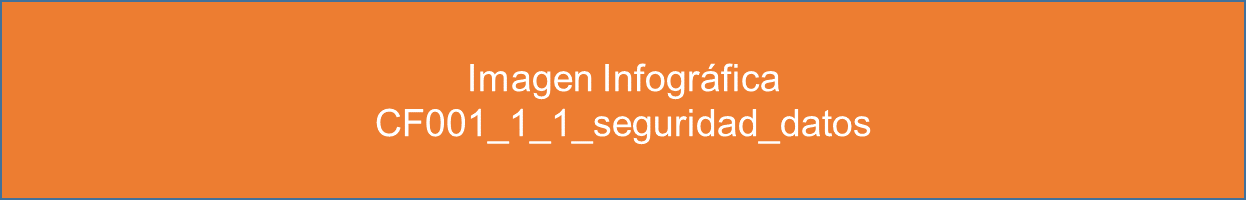
* Integridad.
* Confidencialidad.
* Disponibilidad.

En la actualidad, la mayor parte de la información reside en servidores, redes de información y almacenamientos como nube, discos extraíbles o *backups*, enmarcados dentro de lo que se conoce como sistemas de información. Estos sistemas de información están sujetos a vulnerabilidades, ataques informáticos, riesgos e inseguridades, tanto desde dentro de la propia organización como desde afuera. Los riesgos que se pueden presentar se dividen en:



En definitiva, con un SGSI, la empresa conoce los riesgos a los que está sometida su información y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

El Sistema de Seguridad de la Información está basado en tres principios básicos que se explican a continuación:

****

Un esquema que podría evaluar el nivel de impacto podría manejarse en la siguiente tabla:

**Tabla 1**

*Esquema para evaluar el nivel de impacto*

| **Activo X** | **Confidencialidad** | **Integridad** | **Disponibilidad** |
| --- | --- | --- | --- |
| Impacto | 0 – No aplica | 3 – Moderado | 1– Importante |

Es así como el auditor líder en las políticas de seguridad de la información tiene como funciones:

* Planear las auditorías y hacer uso adecuado de los recursos.
* Equilibrar fortalezas y debilidades del equipo auditor.
* Buena comunicación entre el cliente de la auditoría y el auditor. 
* Liderar con orden al equipo auditor seleccionado.
* Desarrollar una armoniosa relación de trabajo entre los miembros del equipo de auditoría.
* Orientar y transferir conocimiento al departamento TI auditor en formación.
* Liderar con el equipo las conclusiones de la auditoría.
* Establecer planes de mejora.
* Gestionar la perplejidad es el objetivo principal de la auditoría.
* Preparar y completar el informe de la auditoría.

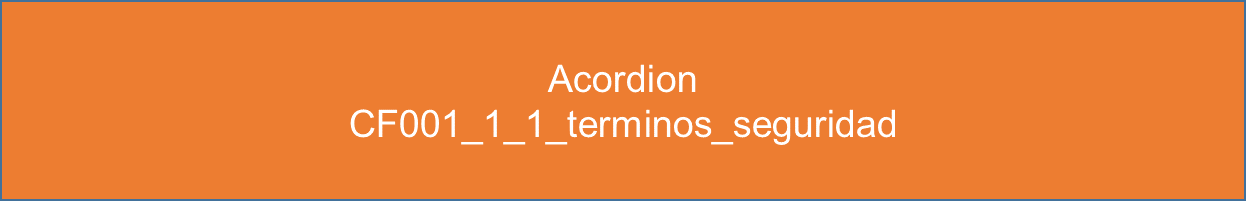
A continuación, se muestra un esquema donde se presentan las fases de una auditoría.

**Figura 1**

*Fases de una auditoría*



Teniendo clara la información anterior, es importante conocer los términos seguridad informática y seguridad de la información y la diferencia que existe entre ellos:



Recuerde que la seguridad informática y la seguridad de la información están encargadas de proteger los datos contra:

* Robo de información.
* Acceso no autorizado.
* Obstaculización al sistema informático.
* Manipulación y/o eliminación de datos.

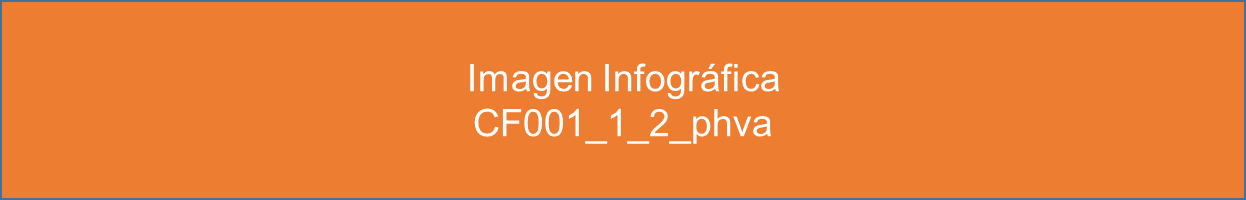
**1.2. Introducción conceptos de SGSI**

Cuando se habla de procesos empresariales impulsados en la transformación digital con tecnología de punta, se entiende que están expuestos a diferentes vulnerabilidades, amenazas y ataques informáticos dirigidos a la seguridad y la privacidad de la información.

Mediante la norma ISO 27001, la implementación del SGSI sigue el modelo Planificar – Hacer – Verificar -Actuar, para la mejora continua de los procesos del SGSI:

**Figura 2**

*PHVA - Icontec*





Cuando una empresa está interesada en realizar un sistema exhaustivo de Gestión de Seguridad de la Información, debe iniciar documentando procesos y conociendo cómo opera la misma, también debe revisar el manual de funciones de cada empleado; esto es fundamental al empezar a aplicar el ciclo PHVA, en la acción, para planear, es necesario conocer los procesos digitales críticos en la organización, luego, detalladamente, se deben analizar para implementar controles que puedan proteger los procesos utilizados ante amenazas cibernéticas.

Dentro del planear, se pueden detectar amenazas que no son externas, sino internas; las amenazas que están en Internet no son la causa de un ser humano con intenciones maliciosas, sino de los mismos empleados que, al no estar capacitados , descargan programas que vienen con troyanos o, sin intención maliciosa, pueden mover un directorio o archivo; también se deben revisar las políticas que tenga contempladas el departamento de TI de la organización.

**2. Herramientas para la valoración de riesgo**

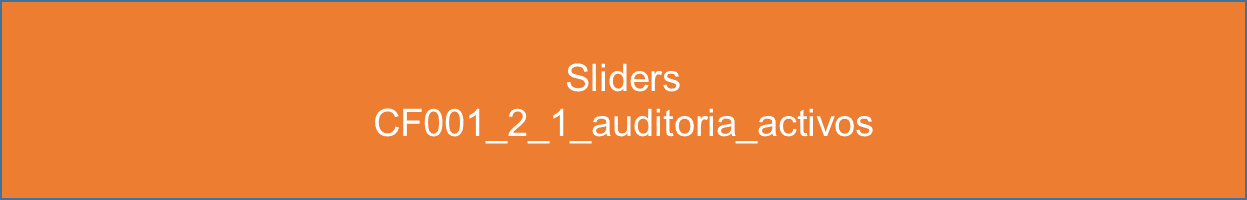
La valoración del riesgo asegura que el SGSI logre los efectos previstos, donde, con las mismas herramientas, se pueden prevenir o reducir efectos indeseados, logrando la mejora progresiva, integrando e implementando acciones en los procesos del sistema de gestión de la seguridad de la información.

Existen empresas en el mundo que ofrecen una gran cantidad de herramientas para la valoración del riesgo, como:

* spiraPlan de inflectra.
* Rastreados a 1.
* IsoMetriz.
* Entre otras.

**2.1. Auditoría de activos**

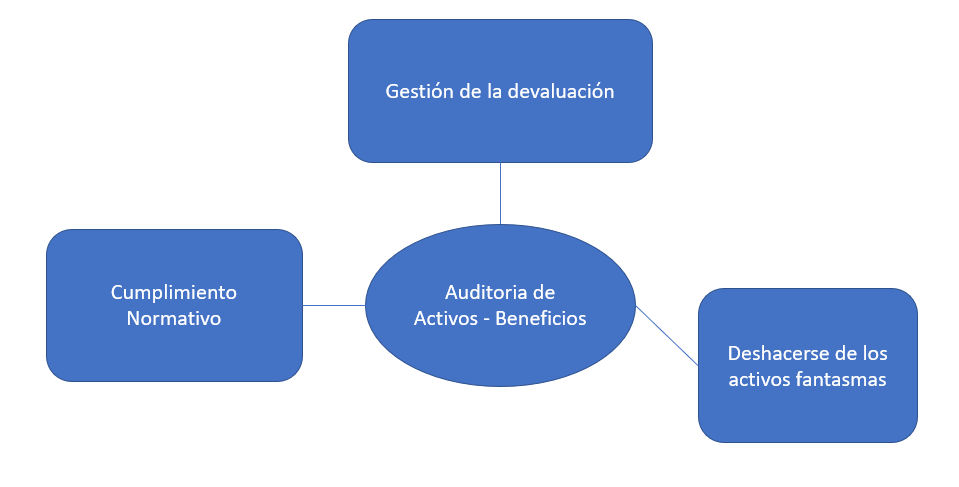
La auditoría de activos debe conocer cómo está conformada la infraestructura tecnológica, es decir, se deben saber los activos tecnológicos con los que cuenta la empresa al momento de iniciar, los cuales son:



Ahora, los beneficios de una auditoría de activos son:

**Figura 3**

*Beneficios de una auditoría de activos*



**2.2 Identificación de riesgos**

En la identificación de riesgos, se debe recordar que la inseguridad se enuncia en procesos de la composición de los resultados de un suceso y la probabilidad de ocurrencia asociada.

Las fuentes de riesgos pueden ser:

* Legales.
* Comportamiento humano (interno y externo).
* Comerciales.
* Economía y mercado.
* Circunstancias políticas.
* Tecnología.
* Eventos naturales.
* Organizacionales.

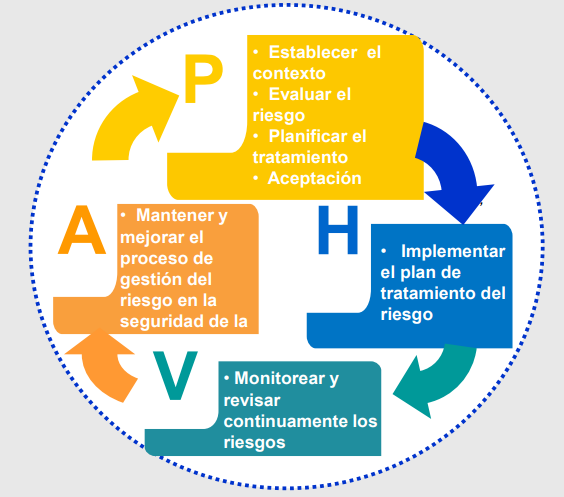
En la gestión del riesgo de Seguridad de la Información, se debe proteger la empresa ante posibles consecuencias, como:

* Pérdidas de confidencialidad.
* Integridad. 
* Disponibilidad.
* No-repudio.
* Autenticidad.
* Confiabilidad de los activos.
* Incumplimiento de la legislación.
* Pérdidas financieras.
* Impacto del orden público.
* Impacto del orden internacional.

Es así como se pueden relacionar el SGSI y la gestión del riesgo haciendo uso del diagrama PHVA, de la siguiente manera:

**Figura 4**

*El SGSI y la gestión del riesgo: Guía Icontec internacional educación*



Nota: Tomado de Guía de gestión de riesgos de seguridad de la información, 2021. <https://www.icontec.org>

**2.3. Áreas de impacto**

El impacto es la capacidad de saber el estado real de seguridad de un activo antes y después de materializar las amenazas. En un SGSI,al concretarse una amenaza, el activo cambia de estado, es decir, antes de producirse la amenaza, se tiene un valor del activo, y después que se efectúe la amenaza, se tiene la diferencia entre el estado anterior y el posterior a la amenaza.

Se clasifica, según el tipo de impacto, como:

* Extremo.
* Importante.
* Moderado.
* Menor.
* Incidental.

Cada clasificación se puede crear o dar dependiendo del tamaño de la organización y el valor podría darse en un rango de 0 a 5.

**2.4. Marco normativo**

Colombia es unos de los países de Latinoamérica que tiene mejor regulación en temas de protección de seguridad de la información; actualmente, hace parte del convenio de cibercriminalidad de Budapest y ha puesto en marcha y práctica con las instituciones del Estado el CONPES 3701 de 2011 sobre los lineamientos de ciberdefensa y ciberseguridad con el ColCERT.

Dentro del marco normativo, están leyes como:

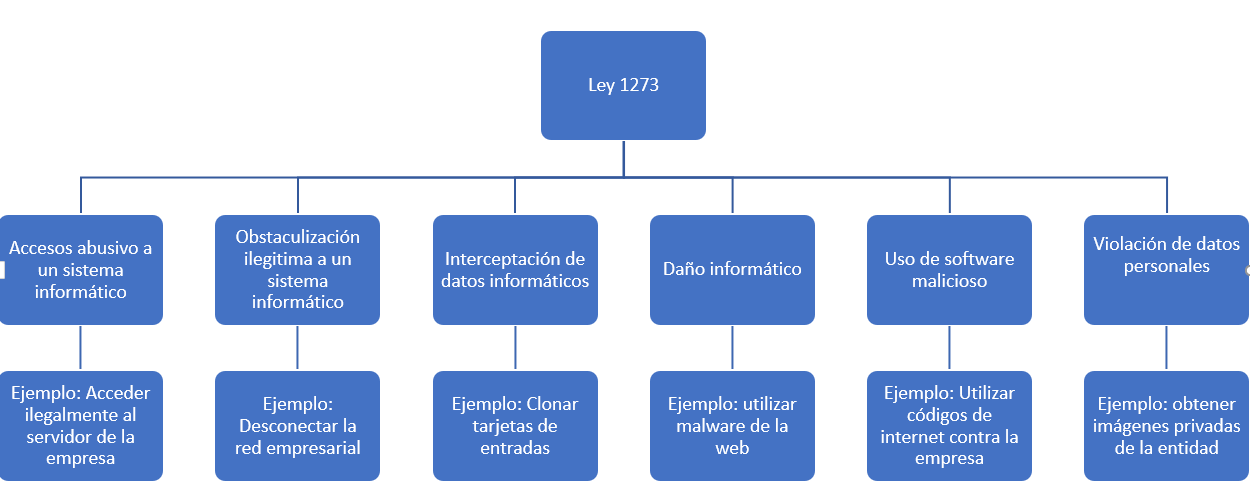


En la siguiente figura, se muestran los artículos de la ley 1273 con ejemplos básicos de posibles conductas punibles que se pueden cometer por su desconocimiento.

Es importante recordar que el desconocimiento de la ley o los delitos no es causal para el ordenamiento procesal colombiano e internacional. Colombia, al contar con una legislación y procedimientos de primera, hace parte del convenio de Budapest, donde se convierten en delitos transnacionales.

**Figura 5**

*Ley 1273 del ordenamiento procesal colombiano*



Nota. SIC (2009).

En la era de la 4º Revolución Industrial, las organizaciones migraron al teletrabajo y *home office*, nacieron conceptos como nómadas digitales, donde un trabajador, desde cualquier parte del mundo, puede cumplir con sus obligaciones y funciones contractuales, por lo que es fundamental que la organización se blinde ante la fuga de información y frente a posibles ataques cibernéticos.

En Colombia, también se cuenta con ley de teletrabajo y CONPES de transformación digital, el país está bien preparado en normatividad y afín a las nuevas tecnologías, se encuentra catalogado como el mejor respondiente a incidentes informáticos en Latinoamérica.

**3. Políticas SGSI**

Para establecer las políticas del SGSI, se debe:

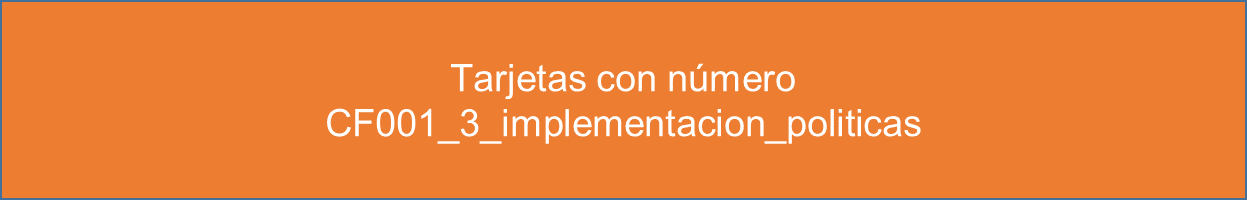


Dentro de las generalidades y aplicaciones, está la capacidad de identificar las maneras de tratamiento de riesgos, los tipos de control existentes y su integración dentro de las políticas y procedimientos para la estructuración del SGSI; esta es importante porque con ella se pueden establecer los controles existentes y planear, puede ser el punto de partida de las mejoras a implementar. Dentro de la ISO 27000, la estructura de alto nivel está contemplada en los requisitos del 4 al 10 y los controles técnicos van del 5 al 18, contemporáneos con el código de práctica de la ISO 27002.

**Tipos de técnicas de implementación de políticas SGSI**

Una política de seguridad es un lineamiento para la toma de una decisión sobre algún aspecto de la seguridad de la información; por ejemplo, se autoriza el acceso a la información a un científico de datos, pero no el análisis del *marketing* empresarial sobre la medición de ventas (toda vez que es para el cumplimiento de las funciones asignadas).

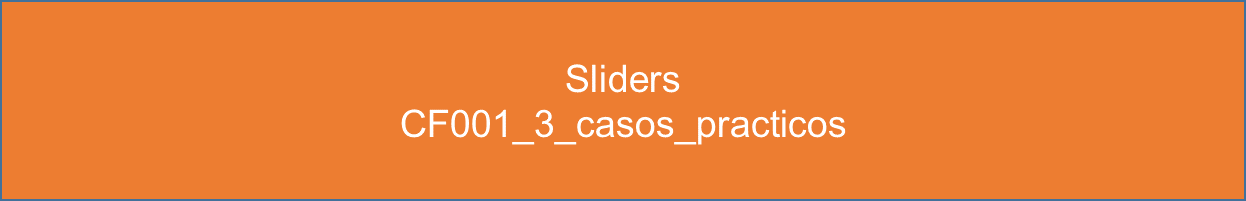
Otros tipos de controles podrían ser de tipo:



**Casos prácticos**

Para implementar políticas de seguridad de la información, se requiere de leyes y normas, requisitos de seguridad y tener claras las metas y objetivos de la seguridad. Con base en ello, se definen los requisitos para establecer las políticas de seguridad de la información, las mismas se documentan en la política institucional de seguridad, donde se especifican e implementan con procedimientos, estándares y controles.

Dentro de posibles casos, se pueden identificar los grupos de controles o requisitos de la norma ISO 27001. Por ejemplo:



**Síntesis**



1. **Actividades didácticas**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Conceptos generales |
| Objetivo de la actividad | Identifique dentro la actividad los conceptos de auditoría de políticas de seguridad de la información que van acordes con el concepto correspondiente. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexos\Anexo1\_CF01\_actividad\_didactica.docx |

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 Sistema de Gestión de Seguridad de la Información (SGSI) | Oficina de Seguridad para las Redes Informáticas. (s. f.). *Metodología para la gestión de la Seguridad Informática.* <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf> | Artículo | https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf |
| Herramientas para la valoración de riesgos | Erb, M. (2009). *Amenazas y Vulnerabilidades.* Gestión de Riesgo en la Seguridad Informática. <https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades> | Artículo | <https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades> |
| Marco normativo | Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2006). *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos* (NTC-ISO/IEC 27001). | Norma | https://www.icontec.org/ |
| Marco normativo | 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. Agosto 18 de 1999. DO. Nº. 43.673. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html> | PDF | Anexos/Anexo3\_CF001\_Ley\_527\_de\_1999 |
| Marco normativo | Ley 1273 de 2009. Por medio de la 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. Enero 5 de 2009. <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf> | PDF | Anexos/Anexo4\_CF001\_Ley\_1273\_2009.pdf |
| Marco normativo | Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf> | PDF | Anexos/Anexo5\_CF001\_Ley\_1581\_2012.pdf |
| Marco normativo | Departamento Nacional de Planeación [DNP]. (2011). *Lineamientos de Política para Ciberseguridad y Ciberdefensa* (Conpes 3701)*.* <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf> | PDF | Anexos/Anexo6\_CF001\_Conpes\_3701.pdf |
| Marco normativo | Departamento Nacional de Planeación [DNP]. (2016). *Política Nacional de Seguridad Digital* (Conpes 3854)*.* <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf> | PDF | Anexos/Anexo7\_CF001\_Conpes\_3854.pdf |
| Marco normativo | Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia*. <https://www.oas.org/juridico/english/cyb_pry_convenio.pdf> | PDF | Anexos/Anexo8\_CF001\_convenio\_budapest.pdf |

1. **Glosario**

| **TÉRMINO** | **SIGNIFICADO** |
| --- | --- |
| **Autenticación** | Es el acto de establecimiento o confirmación de algo como auténtico. La autenticación de un objeto puede significar la confirmación de su procedencia, mientras que la autenticación de una persona, a menudo, consiste en verificar su identidad. La autenticación depende de uno o varios factores.  Desde el punto digital existen varios tipos de autenticación, como las contraseñas, biométricos, token y otros. |
| **Base de datos** | De acuerdo con la empresa ORACLE, es una recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático. Normalmente, una base de datos está controlada por un sistema de gestión de base de datos (DBMS). En un conjunto, los datos y el DBMS, junto con las aplicaciones asociadas a ellos, reciben el nombre de sistema de base de datos, abreviado normalmente a simplemente base de datos. |
| **Evidencia digital** | Dentro de la guía de subproceso de policía judicial en Colombia, se encuentran definiciones de la unidad de delitos informáticos de la Fiscalía General de la Nación (FGN, 2009), también conocida como evidencia computacional única y conocida como: registros o archivos generados por computador u otro medio equivalente, registros o archivos no generados sino simplemente almacenados por o en computadores o medios equivalentes y registros o archivos híbridos que incluyen tanto registros generados por computador o medio equivalente como almacenados en los mismos. |
| **LOG** | Dentro de la guía de subproceso policía judicial en Colombia, se encuentran definiciones de la unidad de delitos informáticos de la Fiscalía General de la Nación (FGN, 2009), un *log* es un registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática, un *log* es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (*who, what, when, where* y *why, W5*) un evento ocurre para un dispositivo en particular o aplicación. La mayoría de los *logs* son almacenados o desplegados en el formato estándar, el cual es un conjunto de caracteres para dispositivos comunes y aplicaciones. De esta forma, cada *log* generado por un dispositivo en particular puede ser leído y desplegado en otro diferente. A su vez, la palabra *log* se relaciona con el término evidencia digital, un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales, lo que implica la lectura del *log* y deja al descubierto la actividad registrada en el mismo. |
| **Redes** | Dentro de la guía de subproceso policía judicial en Colombia, se encuentran definiciones de la unidad de delitos informáticos de la Fiscalía General de la Nación (FGN, 2009), una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos (computadoras y/o dispositivos) conectados, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a Internet, e-mail, chat, juegos), etc. |
| **Seguridad informática** | Gómez (2006) define la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o *software*. Por su parte, Kissel (2012) la define como la protección de información y sistemas de información de acceso no autorizado. |
| **Sistema de información** | Dentro de la guía de subproceso policía judicial en Colombia, se encuentran definiciones de la unidad de delitos informáticos de la Fiscalía General de la Nación (FGN, 2009), es el conjunto de procesos que, operando sobre una colección de datos estructurada de acuerdo con una empresa o entidad, recopila, elabora y distribuye (parte de) la información necesaria para el buen funcionamiento de ella. Además, apoya actividades de dirección y control correspondientes, apoyando al menos en parte, la toma de decisiones necesarias de acuerdo con su estrategia. |
| **Transmisión de datos** | Movimiento de información codificada de un punto a otro/s punto/s. Estos datos se transmitirán mediante señales eléctricas, ópticas, radio o electromagnéticas (FGN, 2009). |

1. **Referencias bibliográficas**

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia*. <https://www.oas.org/juridico/english/cyb_pry_convenio.pdf>

Departamento Nacional de Planeación [DNP]. (2011). *Lineamientos de Política para Ciberseguridad y Ciberdefensa* (Conpes 3701)*.* <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

Departamento Nacional de Planeación [DNP]. (2016). *Política Nacional de Seguridad Digital* (Conpes 3854)*.* <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Erb, M. (2005). *6. Amenazas y vulnerabilidades*. Gestión de riesgo en la seguridad informática*.* <https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/>

Fiscalía General de la Nación [FGN]. (2009). *Procedimientos Forenses de policía Judicial.*

Gomez, A. (2006). *Enciclopedia de la Seguridad Informática.* RA-Ma.

Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2006). *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos* (NTC-ISO/IEC 27001).

Kissel, R. (2012). *Glossary of Key Information Security Terms*. National Institute of Standards and Technology.

Mifsud, E. (2012). *Introducción a la seguridad informática.* Observatorio Tecnológico. <http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica>

Oficina de Seguridad para las Redes Informáticas. (s. f.). *Metodología para la gestión de la Seguridad Informática.* <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf>

ORACLE. (s. f.). *Base de datos definida.* <https://www.oracle.com/co/database/what-is-database/>

1. **Control del documento**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| --- | --- | --- | --- | --- |
| **Autor(es)** | Cesar Antonio Villamizar Núñez | Experto temático | Regional Norte de Santander - Centro de la industria, la empresa y los servicios. | Marzo 2022 |
| Gustavo Santis Mancipe | Diseñador instruccional | Regional Distrito Capital – Centro de Gestión Industrial. | Marzo 2022 |
| Ana Catalina Córdoba | Asesora Metodológica | Regional Distrito Capital – Centro de Diseño y Metrología. | Marzo 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura. | Marzo 2022 |
| Darío González | Corrección de estilo | Regional Distrito Capital – Centro de Diseño y Metrología | Marzo 2022 |

1. **Control de cambios**

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

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