**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** | 220501110-02. Determinar el contexto de una organización respecto a aplicación, políticas y funciones orientadas a la ISO/IEC 27001. |
| --- | --- | --- | --- |

| **NÚMERO DEL COMPONENTE FORMATIVO** | 002 |
| --- | --- |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Etapas del riesgo en un SGSI |
| **BREVE DESCRIPCIÓN** | Actualmente, ante tantos ataques informáticos, las organizaciones deben contar con políticas de auditoría de seguridad de la información, debido a que estas son indispensables porque protegen uno de los activos más valiosos que es la información, por eso es importante blindarse ante cualquier riesgo digital o vulnerabilidad al que día a día están expuestas. |
| **PALABRAS CLAVE** | Informática forense, *malware*, *ransomware*, *spyware*, troyanos. |

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

1. **TABLA DE CONTENIDOS**

**Introducción**

**1. Ciclo PHVA**

**2. Etapas del proceso de gestión de riesgos de S.I.**

**3. Desarrollar y aplicar criterios de valoración de riesgos de seguridad en el contexto del negocio**

**4. Valoración de riesgo de seguridad en el contexto del negocio**

**5. Aplicar herramientas para la valoración de riesgo de S.I.**

**Introducción**

Bienvenido al componente formativo Etapas del riesgo en un SGSI. Se invita a consultar el siguiente video para conocer de manera general la temática a estudiar.



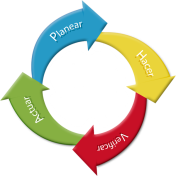
1. **DESARROLLO DE CONTENIDOS**
   * + 1. **Ciclo PHVA**

El ciclo PHVA por sus siglas en español o ciclo PDCA por sus siglas en Inglés, fue creado por el estadístico W. Edwards Deming, es el primer mecanismo de implementación del SGSI basado en la Norma ISO 27001; es un instrumento que se puede aplicar fácilmente en la gestión de procesos y proyectos de auditorías y, puede ser aprovechado en todos los métodos.

Para comenzar se deben conocer casos reales, la normatividad y las pautas de la entidad frente al riesgo de información; es por eso que las vulnerabilidades o ataques informáticos pueden constituirse como falta disciplinaria y/o sanción penal, para realizar un breve análisis y evaluación de riesgos se tiene en cuenta factores que miden el impacto, la estimación y la retención. Ver figura.

**Figura 1**

*Ciclo PHVA*



Mediante las fases del ciclo PHVA mostradas en la figura anterior se puede realizar un primer análisis de la siguiente forma, seleccionando un riesgo común de casi todas las empresas, en este caso el manejo adecuado de la información (esto sirve para la toma de decisiones que serán de forma inmediata y se mantendrán informados y actualizados en tiempo real), luego se describe cada paso del ciclo de la siguiente manera:



Se puede indicar que el ciclo PHVA se fundamenta en la primicia del auditor, por ello debe:

* Tener claro qué se va a hacer antes de hacerlo.
* Comparar los resultados con las acciones planificadas para tomar las acciones pertinentes en caso de que los resultados no sean los esperados.

Al analizar el manejo de los datos de la organización se obtienen los beneficios de la identificación oportuna de los posibles riesgos, la rápida valoración de un auditor permite detectar a tiempo los riesgos, identificando las consecuencias para la empresa y la probabilidad de la ocurrencia de estos, como se observa a continuación.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**2. Etapas del proceso de gestión de riesgos de S.I.**

Para realizar un buen manejo de la información utilizando parte de los requisitos de la seguridad de la información aplicables de la Norma ISO/IEC27001, se asumen, se obtienen derivaciones de valoración y tratamiento de riesgos y, se deben recolectar evidencias documentales de los procedimientos desarrollados, así como las exploraciones asociadas.

Para el SGSI los eventos auténticos son tan importantes como los sucesos negativos y cuando la afectación es auténtica ese riesgo se llamará oportunidad.

Los sucesos de riesgo negativo se caracterizan por ser resultado de las amenazas que cumplen con sus objetivos y gracias a las vulnerabilidades de los sistemas los ciberdelincuentes alcanzan objetivos como:

Imagen de la pantalla de un celular de un mensaje en letras blancas

Descripción generada automáticamente con confianza baja

Tenga en cuenta que también existen amenazas externas que pueden causar pérdida de datos debido a fenómenos naturales.

Las organizaciones deben reconocer que el mayor activo de una empresa es la información y con ella vienen los datos personales de los empleados y de los clientes; una empresa puede correr el riesgo de perder credibilidad si sus datos se ven comprometidos, debido a que los clientes y el personal se verían expuestos y vulnerados. En Colombia la Ley 1581 de 2012 hace referencia a la protección de datos personales de la siguiente forma:

*Interfaz de usuario gráfica, Aplicación, PowerPoint

Descripción generada automáticamente*

Sobre la clasificación de los datos se puede decir que su seguridad se refiere a medidas de amparo de la reserva digital donde se emplean para impedir el acceso no autorizado a los sistemas de información, los cuales pueden encontrarse en:

* La nube.
* Computadores.
* Bases de datos.
* Sitios web.
* Redes sociales, etc.

La seguridad de datos también protege los datos de una posible corrupción.

Para ampliar la información se invita a consultar la **Norma ISO 27001**, que se encuentra en el material complementario.

**3. Desarrollar y aplicar criterios de valoración de riesgos de seguridad en el contexto del negocio**

La organización deberá seleccionar los roles pertinentes para la seguridad de la información, en este caso el rol principal es el del auditor del SGSI, seguido de su equipo de trabajo, igualmente, la empresa con base en la planeación estratégica debe tener liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información.

En la actualidad toda organización cuenta con parques computacionales que incorporan nuevas tecnologías a sus procesos, con el fin de optimizarlos, por ende, la seguridad de la información cobra más vigencia en los temas organizacionales y de calidad, haciendo parte de la transformación digital.

En lo contemplado en la Norma ISO/IEC 27001, un SGSI es un camino sistemático que permite que el activo más valioso (seguridad de la información de la organización) sea:

* Instaurado.
* Realizado.
* Operado.
* Monitoreado.
* Revisado.
* Mantenido.
* Mejorado.

También permite lograr todos los objetivos empresariales usando soluciones pertinentes para la organización de acuerdo con los niveles de riesgos detectados.

Contar con protocolos para salvaguardar la información de los posibles ataques cibernéticos es responsabilidad de las empresas, y respondiendo a la facilidad con la que hoy en día se realizan dichos ataques, no contar con estos protocolos llevaría a la empresa, entidad u organización a pérdidas millonarias y de credibilidad, de las cuales tardarían en recuperarse, además se haría necesario la implementación las políticas de seguridad de la información. En toda gestión del riesgo es fundamental identificar la mayor cantidad de riesgos posibles.

El proceso que se lleva a cabo para realizar dicha gestión es:

**Figura 2**

*Proceso de gestión del riesgo*

Captura de pantalla de un celular con letras

Descripción generada automáticamente con confianza media

En el establecimiento del contexto se encuentran los elementos que definen la identidad de la organización, los cuales son:

* Planeación estratégica.
* Políticas.
* Requisitos.
* Estructura.
* Procesos.
* Entorno.
* Restricciones.

Allí se definen los parámetros externos e internos a tener en cuenta al gestionar el riesgo, también los criterios para la gestión, donde finalmente se define la organización del proceso de gestión de riesgos. Para que el contexto pueda ser interno o externo hay que reconocer el impacto y la aceptación del tipo de riesgo. La eficacia del tratamiento del riesgo depende de los resultados de la evaluación de riesgos.

**La Norma ISO 27005 proporciona las directrices sobre la gestión de riesgos**.

1. **Valoración de riesgo de seguridad en el contexto del negocio**

Dentro de las fases de implementación de un sistema de gestión se debe realizar el análisis de los riesgos identificados y detectados mediante el ciclo PHVA, por ello es importante tener un cronograma de análisis de las entradas de riesgos detectadas y las acciones tomadas por el auditor con el equipo del departamento de TI de la organización. A continuación se definen estos elementos:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

El primer paso para tomar la decisión del riesgo es obtener un resultado del análisis de la evaluación satisfactorio, después dentro de las opciones se define el tratamiento del riesgo donde se establecen los planes de mejora junto con el valor de implementación y los beneficios o resultados de esta; como en todo plan de mejora quedarán algunos riesgos residuales donde se tomará una segunda decisión del riesgo y saldrá el proceso o tratamiento satisfactorio.

La siguiente figura establece un esquema sobre cómo realizar el tratamiento de los riesgos:

**Figura 3**

*Actividad tratamiento del riesgo*

Diagrama

Descripción generada automáticamente



Con el avance de la tecnología vienen de la mano nuevas amenazas, vulnerabilidades y ataques cibernéticos, donde pueden aumentar los riesgos evaluados previamente sobre todo los del nivel más bajo; cada riesgo debe ser tomado de forma separada.

El nivel de riesgo deseado puede ser:

* Alto.
* Medio.
* Bajo.

Algunas técnicas a tener en cuenta en la evaluación del riesgo son las metodologías que ayudan a la identificación de eventos o situaciones que se pueden convertir en fuentes de riesgos como se muestra a continuación:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Los incidentes informáticos son uno de los desafíos permanentes en la práctica de seguridad de la información. A continuación se establece un proceso común para reportar, conversar y actuar frente a los mismos:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Es importante mencionar que en todo proceso sistemático se deben identificar:

* Fuentes.
* Eventos.
* Causas.
* Consecuencias.

Cada proceso debe ser exhaustivo; cuando no se identifica un riesgo en la etapa inicial se hace más complejo encontrarlo más adelante.

Según las estadísticas de la Interpol y del Departamento cibernético en Colombia, siguen creciendo los ataques informáticos a las organizaciones.

Dentro de los riesgos se tienen incidentes no deseados que pueden ser una causa potencial en el daño a un sistema u organización como:

* Terremotos.
* Escasez de personal.
* Uso ilegal de *software*.

Por otra parte, las vulnerabilidades se dan en muchas empresas por factores básicos como:

Imagen de la pantalla de un celular de un mensaje en letras blancas

Descripción generada automáticamente con confianza baja

En tal sentido, para una amenaza pueden haber múltiples vulnerabilidades, por ello, siempre se deben detectar las comunes en el entorno personal, familiar y empresarial. Los riesgos a los que se ve expuesta una empresa están relacionadas con las vulnerabilidades y amenazas, como las que se ilustran en las siguientes figuras:

| **Figura 4**  *Tipos de amenazas*  Imagen que contiene Esquemático  Descripción generada automáticamente | **Figura 5**  *Vulnerabilidad*  Conjunto de iconos de hackers con diferentes tipos de hackers que roban información que rompe el sistema informático vector gratuito |
| --- | --- |

Ahora, en la siguiente tabla se describen algunas de las amenazas y vulnerabilidades más comunes:

**Tabla 1**

*Riesgos por amenazas y vulnerabilidades*

| **Amenazas** | **Vulnerabilidad** |
| --- | --- |
| Terremoto | Ubicación en área susceptible a terremotos.  No tienen planes o procedimientos de recuperación de información.  No dispone de copias de seguridad en la nube. |
| Ataques de negación de servicio | Gestión incongruente de la red.  Falta de actualización de parches. |
| Sabotaje | Seguridad física inadecuada.  Ausencia de control de cambios. |
| Ausencia o pérdida de personal | Procedimientos sin documentar.  Ausencia de un plan de transferencia de conocimiento. |

1. **Aplicar herramientas para la valoración de riesgo de S.I.**

El auditor puede aplicar herramientas como la matriz de riesgos, donde se establece imparcialmente cuáles son los riesgos notables de seguridad que existen en la organización. Para realizar una matriz de riesgos se debe:

* Priorizar los riesgos identificados.
* Evaluar la probabilidad y el impacto.
* Representar gráficamente los riesgos evaluados.

A continuación se presentan varios ejemplos de matrices que el auditor podrá implementar como herramienta.

El punto de partida para la implantación de un SGSI en cualquier organización es realizar una matriz de riesgos de 3x3 (probabilidad del riesgo x impacto), se aplican herramientas y se analizan resultados de manera gráfica dándole valores a los riesgos.

Los resultados de aplicar la matriz de riesgos se muestran en la siguiente tabla:

* Si la probabilidad del riesgo es 1 (baja) y el impacto es 5 (bajo) se multiplica 1x5 y se obtiene como resultado 5.
* Se sigue aplicando la operación matemática a la tabla, multiplicando (valor de la probabilidad x valor del impacto), obteniendo valores de 5, 10, 15, 10, 20, 30, 20, 40 y 60.
* Los valores 30, 40 y 60 se encuentran en el sector rojo, mostrando así altos niveles de riesgos que podría tener la organización.

**Tabla 2**

*Matriz de riesgos 3x3*

| Probabilidad | 3 | Alta | 15 | 30 | 60 |
| --- | --- | --- | --- | --- | --- |
|
| 2 | Media | 10 | 20 | 40 |
|
| 1 | Baja | 5 | 10 | 20 |
|
|  |  |  | Bajo | Medio | Alto |
|  |  |  | 5 | 10 | 20 |
|  |  |  | Impacto | | |

A continuación se muestra una nueva valoración matemática donde se mide el riesgo de lo explicado en la tabla anterior (probabilidad x impacto). Para esto se establece una zona de riesgo:

* Aceptable.
* Tolerable.
* Moderado.
* Importante.
* Inaceptable.

Si bien el color muestra una lógica, se debe clasificar en qué zona de riesgo se encuentra la misma. Con base al valor del impacto se pueden tomar los correctivos adecuados en la implementación de las políticas de auditoría de seguridad de la información.

**Tabla 3**

*Valor del impacto y correctivos de implementación matriz de riesgos 3x3*

| Probabilidad | 3 | Alta | **15 zona moderada** prevenir riesgo | **30 zona de riesgo importante** prevenir riesgo mitigar el riesgo transferir el riesgo | **60 zona de riesgo inaceptable**  evitar el riesgo prevenir riesgo proteger o mitigar el riesgo compartir o transferir el riesgo |
| --- | --- | --- | --- | --- | --- |
|
| 2 | Media | **10 zona tolerable** se previene el riesgo | **20 zona moderado**  prevenir riesgo mitigar el riesgo transferir el riesgo | **40 zona de riesgo importante**  prevenir riesgo mitigar el riesgo transferir el riesgo |
|
| 1 | Baja | **5 zona aceptable** se asume el riesgo | **10 zona tolerable** se protege o mitiga el riesgo | **20 zona moderado**  mitigar el riesgo transferir el riesgo |
|
|  |  |  | Bajo | Medio | Alto |
|  |  |  | 5 | 10 | 20 |
|  |  |  | Impacto | | |

En las herramientas de matrices de riesgos existe otro ejemplo denominado matriz de control como mapa de riesgo inherente de corrupción de 3x5, en esta las probabilidades se llevan a dos extremos más para su mejor control y análisis como se observa en la siguiente tabla.

**Tabla 4**

*Matriz de riesgos 3x5*

| **Probabilidad** | Casi seguro |  |  |  |
| --- | --- | --- | --- | --- |
|
| Probable |  |  |  |
|
| Posible |  |  |  |
|
| Improbable |  |  |  |
|
| Rara vez |  |  |  |
|
|  |  | Moderado | Mayor | Catastrófico |
|  |  | **Impacto** | | |
|  |  |  | | |

Al ampliar la anterior herramienta a un mapa o matriz de riesgo inherente de 5x5 para un mayor control en una gran empresa u organización se tendrá control completo en los resultados, se tiene una probabilidad de:

* Rara vez.
* Improbable.
* Posible.
* Probable.
* Casi seguro

Y por el lado del impacto se tienen los ítems:

* Insignificante.
* Menor.
* Moderado.
* Mayor.
* Catastrófico.

Es potestad del equipo auditor implementar el que considere mejor para el análisis y obtención de resultados.

**Tabla 5**

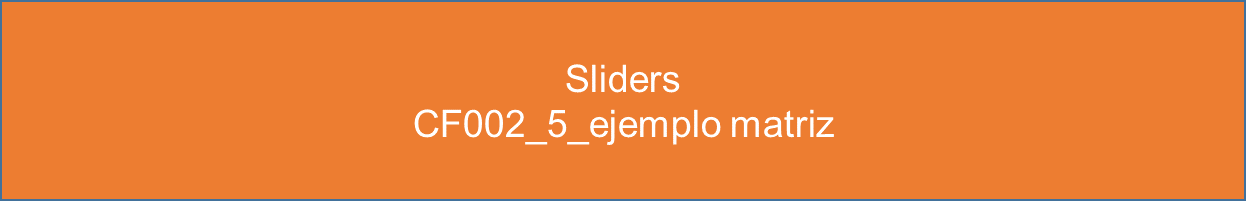
*Matriz de riesgos 5x5*

| **Probabilidad** | Casi seguro |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|
| Probable |  |  |  |  |  |
|
| Posible |  |  |  |  |  |
|
| Improbable |  |  |  |  |  |
|
| Rara vez |  |  |  |  |  |
|
|  |  | Insignificante | Menor | Moderado | Mayor | Catastrófico |
|  |  | **Impacto** | | | | |

Los mapas o matrices de riesgos se pueden ejecutar dependiendo del tamaño de la organización (pequeña, mediana o grande). Dentro de los riesgos web se toma el OWASP (Open Web Application Security) TOP 10: 2021, el cual representa los riesgos y amenazas más peligrosas para las organizaciones con el impacto en 5 por las diferentes probabilidades que se establezcan.

**Ejemplo práctico**

La siguiente herramienta matriz contiene un caso con valores de riesgos reales, con base en estos se puede decir:



La identificación y tipificación de los riesgos descritos previamente se muestran en las siguientes tablas:

**Tabla 6**

*Matriz de riesgos 5x5*

| **Probabilidad** | **Frecuente** |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ocasional** |  |  |  |  |  |
| **Remoto** |  | **4** |  |  |  |
| **Improbable** |  |  |  |  |  |
| **Muy bajo** |  | **2** |  |  | **5** |
|  |  | **BAJO** | **MENOR** | **MODERADO** | **MAYOR** | **CATASTRÓFICO** |

**Tabla 7**

*Valores matriz de riesgos*

| **Riesgos** | **Fallos de equipos computo** | **2** |
| --- | --- | --- |
| **Fallas eléctricas** | **4** |
| **Caída de Internet** |  |
| **Filtro de información** |  |
| **Virus/ataques cibernéticos** |  |
| **Terremotos** | **5** |

Después de realizar y analizar los valores de impactos se procede a realizar un plan de mejora que puede ser a:

* Largo.
* Mediano.
* Corto plazo.

Esto dependerá del tamaño de la empresa y del presupuesto que disponga para el parque computacional y transformación digital. En la siguiente tabla se muestra un posible escenario para dicho plan:

**Tabla 8**

*Plan de mejoras*

| **Fallos de equipos computo** | Implementar un programa de mantenimiento preestablecido. |
| --- | --- |
| **Fallas eléctricas** | Chequear cada instalación y/o tomacorriente antes de usar y establecer un plan de mantenimiento eléctrico. |
| **Caída de Internet** | Tener el contacto del proveedor y/o el de soporte técnico. |
| **Filtros de información** | Implementar cifrado de datos y socializar con los trabajadores, las consecuencias y precauciones que se debe tener para no filtrar la información. |
| **Virus/ataques cibernéticos** | Instalar *software* antivirus en todos los equipos de la empresa. |

Por otra parte, también es importante mencionar que para la valoración de riesgos existen plataformas pagas como:

* Isotools: [www.isotools.org](http://www.isotools.org)
* Enisa: <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory>

Finalmente, es importante indicar que es fundamental realizar el estudio del riesgo las veces que el auditor considere necesario, debido a que puede existir un gran número de preguntas frente a los diferentes ataques cibernéticos y vulnerabilidades informáticas identificadas en la empresa.

**Síntesis**

*Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente*

1. **ACTIVIDADES DIDÁCTICAS (Se debe incorporar mínimo 1, máximo 2)**

| DESCRIPCIÓN DE LA ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Conceptos generales |
| Objetivo de la actividad | Identificar los conceptos sobre riesgo estudiados en el componente formativo. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad | Anexos\Anexo1\_CF02\_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** |
| --- | --- | --- | --- |
| Etapas del proceso de gestión de riesgos de S.I. | Normas ISO. (s.f.). *Norma ISO 27001.* <https://www.normas-iso.com/iso-27001/> | Página web | <https://www.normas-iso.com/iso-27001/> |
| Etapas del proceso de gestión de riesgos de S.I. | 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 21 de 1999. DO No. 43.673. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html> | Otro | <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html> |
| Desarrollar y aplicar criterios de valoración de riesgos de seguridad en el contexto del negocio | 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. DO No. 47.223. <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf> | Otro | <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf> |
| Desarrollar y aplicar criterios de valoración de riesgos de seguridad en el contexto del negocio | Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO No. <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf> | Otro | <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf> |
| Desarrollar y aplicar criterios de valoración de riesgos de seguridad en el contexto del negocio | Consejo Nacional de Política Económica y Social. (2011). *Lineamientos de política para ciberseguridad y ciberdefensa*. CONPES. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf> | PDF | <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf> |
| Valoración de riesgo de seguridad en el contexto del negocio | MinTIC. (s.f.). *Seguridad y privacidad de la información.* MinTIC. <https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf> | PDF | <https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.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 se tiene varios tipos de autenticación como las contraseñas, biométricos, *token* y otros. |
| **Base de datos** | 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.  De esta manera se tiene un significado frente al término de base de datos. |
| **Evidencia digital** | 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. |
| **ICONTEC** | Instituto Colombiano de Normas Técnicas y Certificación |
| **ISO** | Organización Internacional de Normalización. |
| ***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 *log* 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** | 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.) |
| **Riesgo** | En el ámbito informático la definición de riesgo son las amenazas digitales a las que se está expuesto día a día cuando se usa la tecnología. |
| **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. |
| **SGSI** | Sistema de Gestión de Seguridad de la Información. |
| **Sistema de información** | 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 Nacional de Política Económica y Social. (2016). Política nacional de seguridad digital. CONPES. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Consejo Nacional de Política Económica y Social. (2011). Lineamientos de política para ciberseguridad y ciberdefensa. CONPES. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

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

Gómez, A. (2006). *Enciclopedia de la seguridad informática.* RA-Ma.

Kissel, R. (2012). *Glossary of key information security terms.* National Institute of Standards and Technology.

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO No. <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf>

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. DO No. 47.223. <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

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 21 de 1999. DO No. 43.673. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html>

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

Oficina de Seguridad para las Redes Informáticas*.* (2002). *Metodología para la gestión de la seguridad informática*. <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf>

1. **CONTROL DEL DOCUMENTO**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| --- | --- | --- | --- | --- |
| **Autor (es)** | Cesar Antonio Villamizar Núñez | Experto temático | Región Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Marzo de 2022 |
| Gustavo Santis Mancipe | Diseñador instruccional | Regional Distrito Capital – Centro de Gestión Industrial | Abril de 2022 |
| Ana Catalina Córdoba Sus | Asesora metodológica | Regional Distrito Capital – Centro de Diseño y Metrología | Abril de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo desarrollo curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Abril de 2022 |
|  | Julia Isabel Roberto | Correctora de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Mayo de 2022 |

1. **CONTROL DE CAMBIOS**

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

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