**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Seguridad en aplicaciones web |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501111 - Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | RESULTADOS DE APRENDIZAJE | 22050111-03 - Tratar brechas de seguridad digital en aplicaciones web de acuerdo con resultado del monitoreo, estándares y normativa. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 007 |
| NOMBRE DEL COMPONENTE FORMATIVO | Incidentes y vulnerabilidades en seguridad orientada a aplicaciones web |
| BREVE DESCRIPCIÓN | Día a día las estadísticas por incidentes informáticos en el mundo aumentan, las diferentes técnicas de los ciberdelincuentes mejoran perfeccionando los ataques y cumpliendo con los objetivos que se proponen. |
| PALABRAS CLAVE | Ciberseguridad, *hacking*, HASH, informática forense |

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

1. **TABLA DE CONTENIDOS:**

**Introducción**

* + - 1. **Incidentes informáticos**
      2. **Auditoría forense**

2.1 Informática forense

2.2 Tableros de control

* + - 1. **Recolección de evidencia digital**
      2. **Informes incidentes de seguridad en aplicaciones**

1. **INTRODUCCIÓN**

Le damos la bienvenida al componente formativo denominado “**Incidentes y vulnerabilidades en seguridad orientada a aplicaciones web**”, el cual hace parte del programa de formación técnico en Seguridad en aplicaciones web, para lo cual se invita a observar el siguiente video:



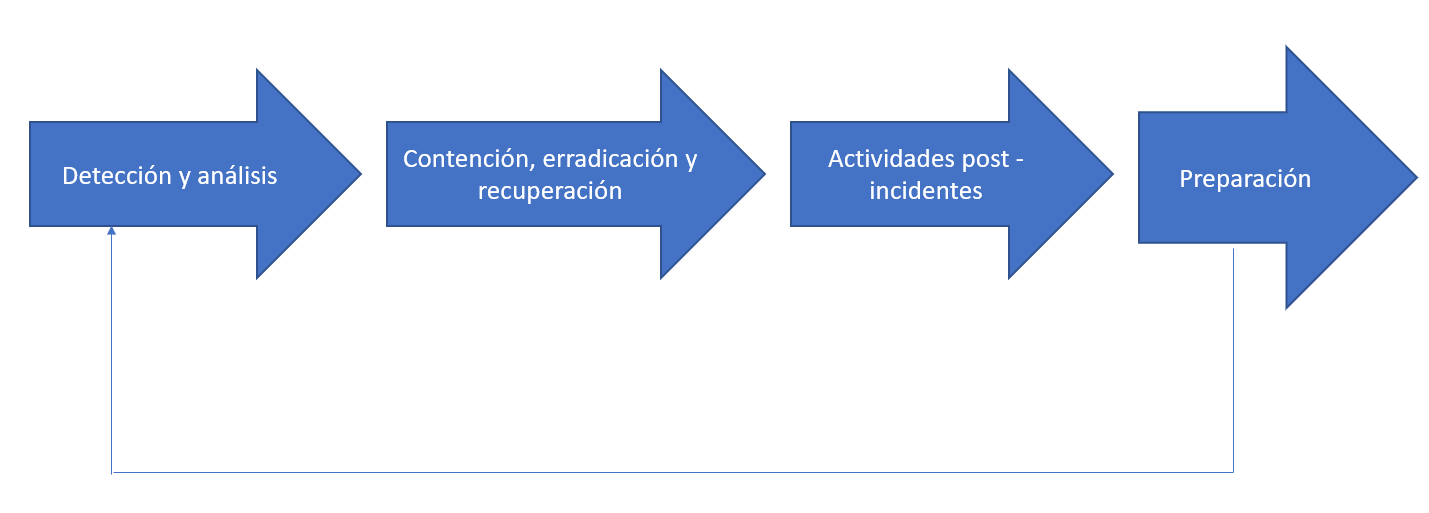
1. **DESARROLLO DE CONTENIDOS:** 
   * + 1. **Incidentes informáticos**

Dentro del tratamiento de incidentes de seguridad digital en las aplicaciones web, parte de la normatividad la establece el Ministerio de Tecnologías de Información y las Comunicaciones de Colombia mediante la Resolución 500 del año 2021 Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital”; por ello se debe recordar que al existir incidentes informáticos el Código Penal establece sanciones legales mediante la Ley 1273 de 2009.

Igualmente, hay que tener en cuenta los marcos de referencia ante un incidente de seguridad de la información guiándose con la ISO 27035 que es la norma de gestión de incidentes de seguridad de la información, el ciclo de vida de la gestión y contradicción de un incidente informático, así:

**Figura 1**

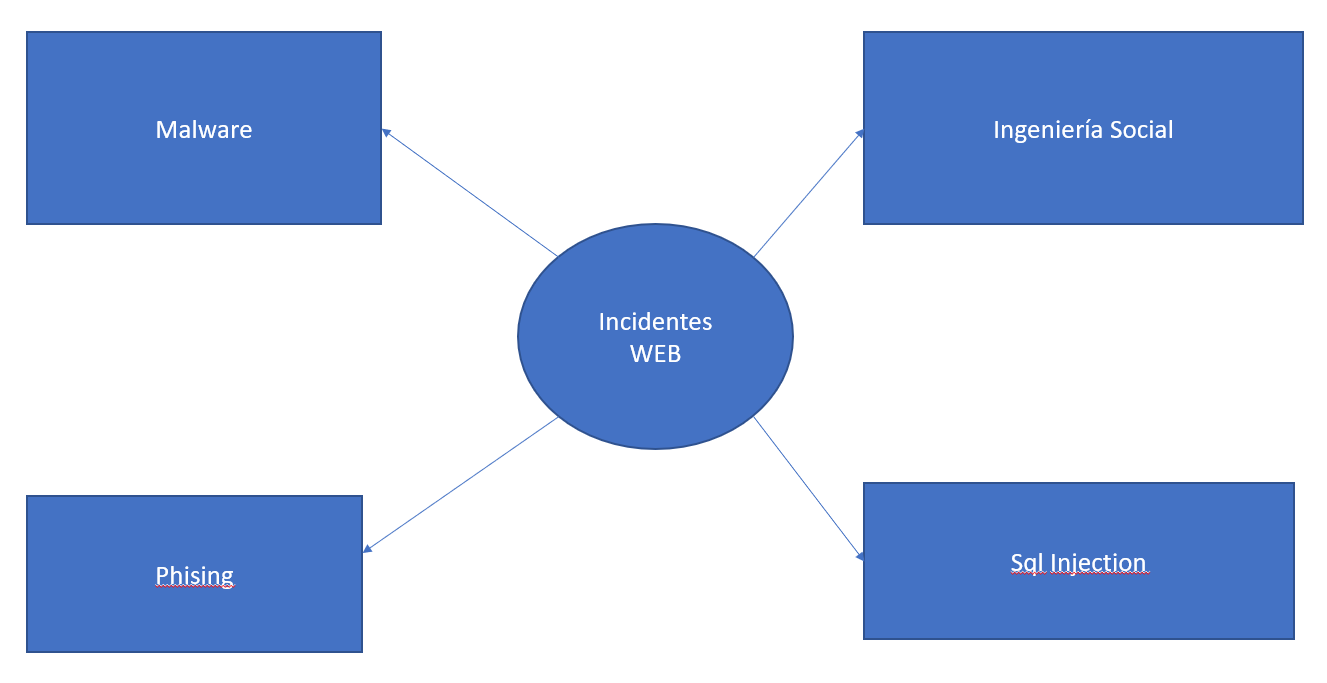
*Ciclos incidentes informáticos*



El ciclo siempre será repetitivo, el mismo puede controlarse o auditarse mediante políticas de seguridad de la información y que la organización tenga un departamento en atención frente a los diferentes incidentes de seguridad como un CSIRT como lo indica el Conpes 3701 de 2011; es necesario recordar que dentro los pilares de la información están:

* Confidencialidad.
* Integridad.
* Disponibilidad.

Los incidentes informáticos de seguridad en aplicaciones web pueden darse mediante técnicas de ingeniera social o *hacking* no autorizados, *malware* y *SQL injection,* como puede verse a continuación:



Se invita a conocer algunos conceptos importantes que identificará en el transcurso de este componente:



* + - 1. **Auditoría forense**

Las auditorías forenses se realizan cuando los incidentes informáticos pasan a ser denunciados penal o administrativamente y se requieren para las investigaciones legales pertinentes, también se pueden realizar auditorías forenses para detener los incidentes informáticos y fortalecimiento de acciones dentro de la organización. En Colombia la ley con que más se enfrentan los ataques cibernéticos es la Ley 1273 de 2009 por la que se crea el bien jurídico tutelado y el dato.

Se recomienda que las auditorías forenses sean realizadas por externos y que tengan conocimiento en procedimientos de informática forense y derecho informático, esto debido que al recaudar evidencias digitales en un futuro las sustentará ante un estrado judicial.

Las etapas de la auditoría forense se conforman de la siguiente manera:



* Realización de auditoría forense.
* Definición de programas de auditoría forense.
* Ejecución de la auditoría forense.
* Elaboración del informe de auditoría forense.
* Entrega del informe al cliente.
  1. **Informática forense**



El cómputo forense ayuda a detectar y analizar todas las pistas sobre ataques informáticos, conversaciones, robos de información o evidencia digital al navegar por internet, accesos no autorizados a aplicaciones y correos electrónicos. La finalidad es la de identificar, preservar, extraer y documentar para que estas evidencias digitales pasen a ser pruebas en un estrado judicial.

En Colombia, existe la unidad de delitos informáticos de la Fiscalía General de la Nación y el CAI virtual de la DIJIN unidad de incidentes informáticos. Cuando una aplicación web es vulnerada se debe identificar por medio de la Informática forense de dónde provino el ataque, cuál fue la técnica utilizada y revisar las posibles vulnerabilidades de la herramienta para tomar los correctivos de esta.

* 1. **Tableros de control**

Los tableros de control se utilizan en las auditorías forenses para realizar chequeos y sacar conclusiones rápidamente, estos sirven para realizar tomas de información mediante los tableros de control; uno de ellos podría ser el siguiente:



En los dominios se puede colocar el tipo del ciclo del PHVA, el tipo de proceso sería el de evaluar y administración de riesgos informáticos y dentro de cada objetivo de control son los contextos, identificación, evolución, evaluación o respuestas de los riesgos.

Como auditores, en cada ítem se realizan preguntas y se ejecuta como:



Al empezar a aplicar el ciclo PHVA, en la acción planear se debe conocer los procesos digitales críticos en la organización, luego detalladamente se analizan, para implementar controles que protejan los procesos implementados ante amenazas cibernéticas.



Dentro de la lista de chequeo se pueden realizar preguntas y reformular las mismas conforme a la organización, frente al manejo y operación de las aplicaciones web donde se marca solo un ítem entre sí o no y una observación general en caso de justificar, la misma del ítem seleccionado; de igual forma, se pueden agregar más aspectos a evaluar dependido el análisis o tipo de auditoría o control que requiere realizar el profesional. A continuación se presenta dicho formato:



* + - 1. **Recolección de evidencia digital**

La IOCE (Organización Internacional de Evidencia Computacional) estableció en el año 1999 cinco principios internacionales para tener en cuenta para el adecuado manejo de la evidencia digital. Se invita a saber de qué tratan:



Además, toda evidencia digital es frágil y volátil, por lo que la misma se debe recolectar de manera adecuada para no ponerla en duda. A continuación, se relaciona el ciclo de la evidencia digital:





El análisis es aquel que se realiza en el laboratorio forense para realizar procedimientos en caso de borrado de navegación o al sistema de información, en la documentación debe ir explicado todo desde el inicio: características informáticas del *software,* método utilizado identificación del perito informático, tamaño de la información, nombre y versiones del *software* forense usado. La presentación es la terminación de ese informe junto con la evidencia digital recolectada cumpliendo los procedimientos forenses, y las conclusiones son con base en lo analizado y lo que no se pudo recuperar.

* + - 1. **Informes incidentes de seguridad en aplicaciones**

Antes de iniciar este tema, es importante observar el siguiente video explicativo:



Los informes se deben presentar claros, concisos y ordenados, los mismos deben ser exhaustivos respecto de las técnicas forenses utilizadas con conclusiones lógicas, bien argumentadas y en un lenguaje técnico, legal y explicativo para los demás

Lo anterior mediante el ASVS, que es un marco de referencia de requisitos de seguridad, controles funcionales y los no funcionales que se requieren al diseñar, desplegar y testear aplicaciones web. Así como con el OWASP top 10 que es el documento principal para tener en cuenta sobre los riesgos de seguridad más destacados en aplicaciones web, como se indica en la tabla a continuación:

**Tabla 3**

*Metodología de clasificación de riesgo*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Agente de amenaza | Explotabilidad | Prevalencia de vulnerabilidad | Detección de vulnerabilidad | Impacto Técnico | Impacto de Negocio |
| Específico de la aplicación. | 3 Fácil . | 3 Difundido. | 3 Fácil. | 3 Severo. | Específico del negocio. |
| 2 Promedio. | 2 Común. | 2 Promedio | 2 Moderado. |
| 1 Difícil. | 1 Poco común. | 1 Difícil | 1 Mínimo. |

Para conocer los factores de riesgo que se asocian a la anterior tabla, se invita a dar clic en:



Según las tablas anteriores y los niveles de riesgos detectados por cada ítem de análisis en el informe, se debe especificar el tipo de amenaza según la aplicación, así:

**Tabla 5.**

*Impacto vs. valoración*

|  |  |  |
| --- | --- | --- |
| Impacto | Descripción | Valoración |
| Catastrófico. | Extremadamente dañino. | Alto. |
|
| Mayor. | Dañino. |
|
| Moderado. | Moderado. | Medio. |
|
| Menor. | Menor. | Baja. |
|
| Insignificante. | Ligeramente dañino. |
|

La descripción de la anterior tabla, se puede interpretar de la siguiente manera:



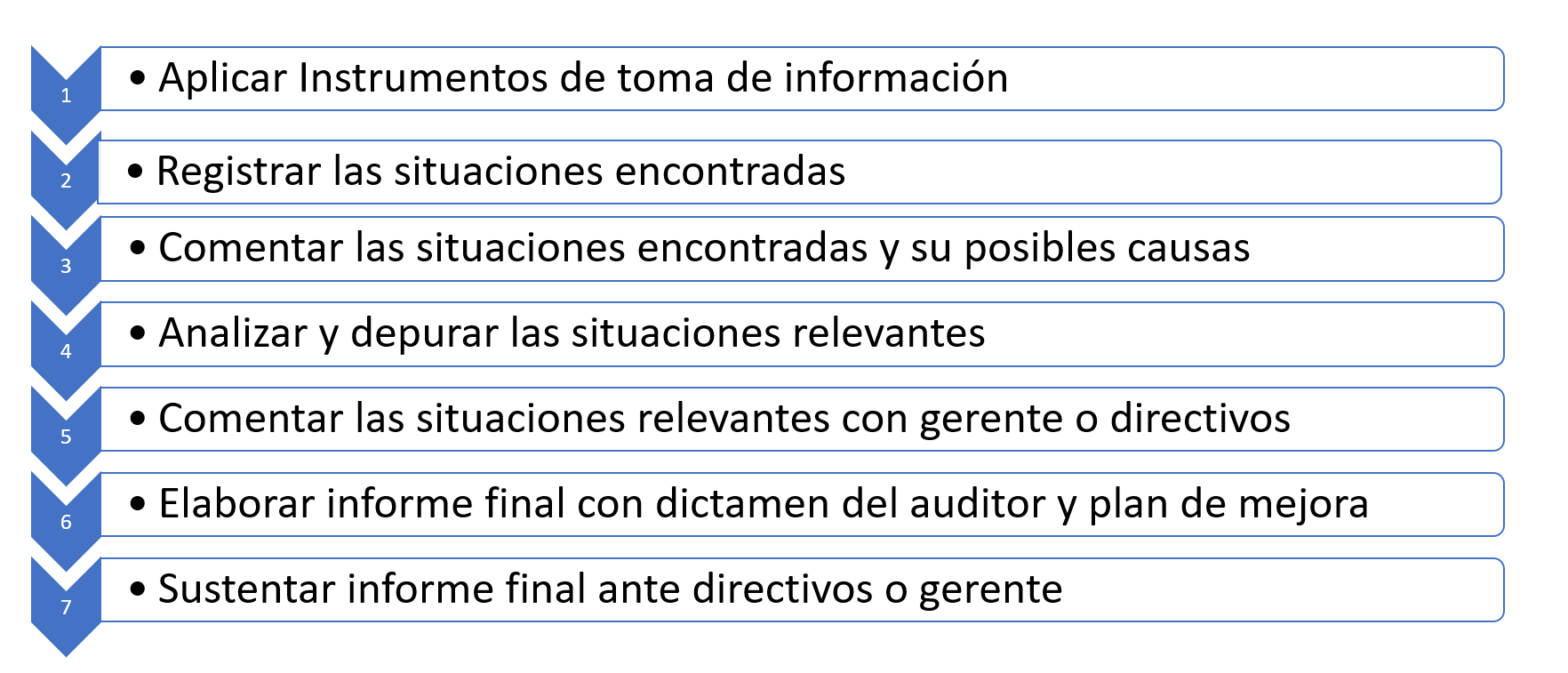
En la organización, y en este caso con las aplicaciones web, pueden ocurrir varios impactos y diferentes valoraciones que deben ser documentados y analizados en el informe, y de igual manera establecer un plan de mejora y control frente a incidentes informáticos.

En cuanto a la urgencia frente a incidentes informáticos en aplicaciones web, se tienen de la siguiente manera:



Estos tiempos de respuestas también deben de ser tenidos en cuenta en la realización del informe, tener en cuenta los tiempos mínimos y máximo según el incidente informático en la aplicación web. Es importante establecer políticas de control en las aplicaciones web; la ISO 27001 juega un papel fundamental en ese plan de mejora.

Un informe de auditoría debe contar con todas las evidencias recolectadas (*logs*, errores humanos detectados, irregularidades) y el procedimiento es el siguiente:



En los **informes de incidentes de seguridad en aplicaciones**, se incluyen los ajustes de controles que hacen referencia a los planes de mejora; así se detienen y previenen futuros incidentes informáticos, ya que los mismos buscan establecer mecanismos de prevención y control. Como política general de ajuste de control se debe contemplar las actualizaciones de *software* o parches de seguridad en la herramienta de aplicaciones web cada vez que se detecte una. A continuación, se conocerá los niveles de planes de mejora y tablero de control, básico, intermedio y avanzado:



Los planes de mejora son las conclusiones que toda auditoría deja por defecto tomando correctivos para que los riesgos y amenazas no vuelvan a la aplicación web, con este tipo de control y seguimiento se previenen riesgos y amenazas.

1. **Síntesis**

Ya se conoció en detalle las diferentes temáticas abordadas en este componente formativo, ahora es momento de verlas de manera resumida y puntual a través del siguiente esquema conceptual:



1. **ACTIVIDADES DIDÁCTICAS**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Conceptos generales |
| Objetivo de la actividad | Reconocer los conceptos de vulnerabilidades y auditorías que van acordes a incidentes y vulnerabilidades en seguridad orientadas a aplicaciones web. |
| Tipo de actividad sugerida | Completar los espacios |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexos / Anexo5\_ActividadDidactica\_CF07 |

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 |
| 1. Incidentes informáticos | Incibe. (s. f.). *Gestión de riegos.* <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf> | Documento | <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf> |
| 3. Recolección de evidencia digital | Oficina de Seguridad para las Redes Informáticas. (s. f.). *Metodología para la gestión de la seguridad informática (proyecto).* <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf> | Articulo | <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf> |
| 3. Recolección de evidencia digital | Congreso de Colombia. (1999). 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. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html> | Ley | <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html> |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Autenticación | 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 tenemos varios tipos de autenticación como las contraseñas, biométricos, token y otros. (educalingo, s.f.). |
| Base de datos | 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 (Oracle, 2022) |
| 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 (FGN, 2009). |
| *Log* | 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 (FGN, 2009). |
| 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. (FGN, 2009) |
| Seguridad informática | 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* (Gómez, 2006). Por su parte, Kissel (2012) la define como la protección de información y sistemas de información de acceso no autorizado. |
| Sistema de información | 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 (FGN, 2009). |
| 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:**

Congreso de Colombia. (2009). 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. <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

Congreso de Colombia. (2012). Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf>

DNP. (2011). Documento Conpes 3701. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

DNP. (2016). Documento Conpes 3854.<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Educalingo. (s.f.). *Autenticación*. <https://educalingo.com/es/dic-es/autenticacion>

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

FGN. (2009). *Procedimientos forenses de policía judicial.* FGN.

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

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

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

Oracle. (2022). *Base de datos definida.* <https://www.oracle.com/co/database/what-is-database/>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Cesar Antonio Villamizar Núñez | Experto Temático | Región Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Mayo de 2022 |
| Hernando José Peña Hidalgo | Experto Temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Mayo de 2022 |
| Carlos Hernán Muñoz | Experto Temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Mayo de 2022 |
| Danny Alejandro Solano | Experto Temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Mayo de 2022 |
| David Eduardo Lozada | Experto Temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Mayo de 2022 |
| Paula Andrea Taborda Ortiz | Diseñadora Instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y Los Servicios | Junio de 2022 |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital - Centro de Diseño y Metrología | Junio de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura. | Junio de 2022 |
|  | José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital - Centro de Diseño y Metrología. | Julio del 2022. |

1. **CONTROL DE CAMBIOS**

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

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

**Nota:**Para la propuesta instruccional se deben tener en cuenta las métricas desarrolladas en el equipo: