**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** | 220501110-04 Definir indicadores, métricas y controles de una organización respecto de los objetivos de seguridad de la información. |
| --- | --- | --- | --- |

| **NÚMERO DEL COMPONENTE FORMATIVO** | 4 |
| --- | --- |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Evaluación de métricas y controles |
| **BREVE DESCRIPCIÓN** | En el presente componente el estudiante estará en la capacidad de implementar un programa de auditoría interna con base a la norma ISO 27001, manteniendo la competencia como auditor y aplicando los diferentes conceptos y técnicas de auditoría, así como los requisitos y controles de un sistema integrado de seguridad de la información. |
| **PALABRAS CLAVE** | *Botnet*, informática forense, *malware, ransomware, spyware*, troyanos. |

| **ÁREA OCUPACIONAL** | 6 - VENTAS Y SERVICIOS |
| --- | --- |
| **IDIOMA** | Español |

1. **TABLA DE CONTENIDO:**

**Introducción**

**1. Diseñar, implementar y evaluar un programa de auditoría interna de un SGSI**

**2. Desarrollar y mantener la competencia de los auditores**

**3. Conocer y aplicar conceptos y técnicas de auditoría a los requisitos y controles de un SGSI**

**INTRODUCCIÓN**

La implementación, evaluación y análisis de métricas y controles es la fase del SGSI donde se prepara, aprueba y realiza la distribución del informe final de la auditoría.



1. **DESARROLLO DE CONTENIDOS:**

**1. Diseñar, implementar y evaluar un programa de auditoría interna de un SGSI**

Como primera instancia, es importante recalcar que los auditores deben determinar las necesidades de monitoreo y medición, por lo tanto, deben ser profesionales con:

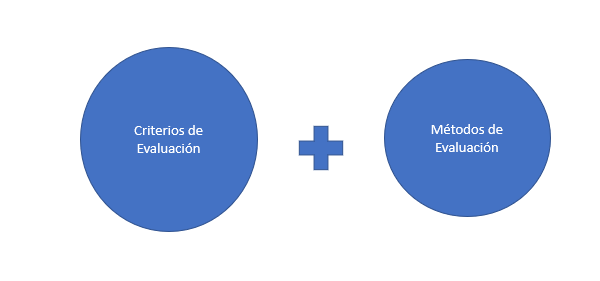
* Habilidades
* Conocimientos
* Conductas ejemplares
* Experiencia laboral

en auditorías, auditorías informáticas o forenses.

En tal sentido, para un proceso de auditoría se deben tener en cuenta:

**Figura 1**

*Proceso de auditoría*



Por otra parte, dentro de los monitoreos y controles de evaluación, los métodos a implementar establecidos por el auditor (con formación en el área, experiencia laboral, experiencia como auditor adiciona) deben tener en cuenta:

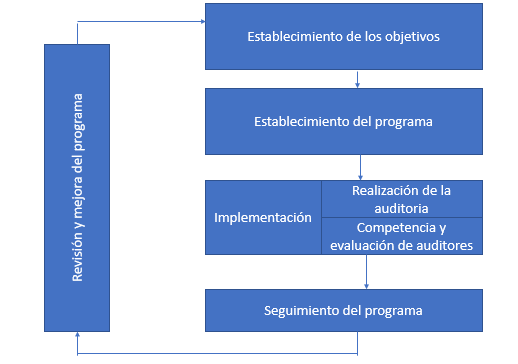
* Revisión de registros.
* Retroalimentación en cada proceso.
* Examen final.
* Revisión posterior.

Dicho lo anterior, se debe tener presente que una buena planeación es el éxito de una auditoría, porque las organizaciones quieren resultados y medidas para proteger su activo más valioso: la información.

Para lograrlo, el trabajo en equipo y la sinergia son las principales directrices que debe enmarcar el auditor líder, porque equilibra fortalezas y debilidades en el equipo y organización, los informes, reuniones y comunicaciones entre el cliente de la auditoría y el auditado deben estar enmarcadas en un buen clima laboral, esta es una responsabilidad del auditor líder, para tener los mejores resultados en pro de la organización la armonía y prevenir los conflictos. La siguiente figura representa los elementos que conforman un programa de auditoría:

**Figura 2**

*Programa de auditoría*

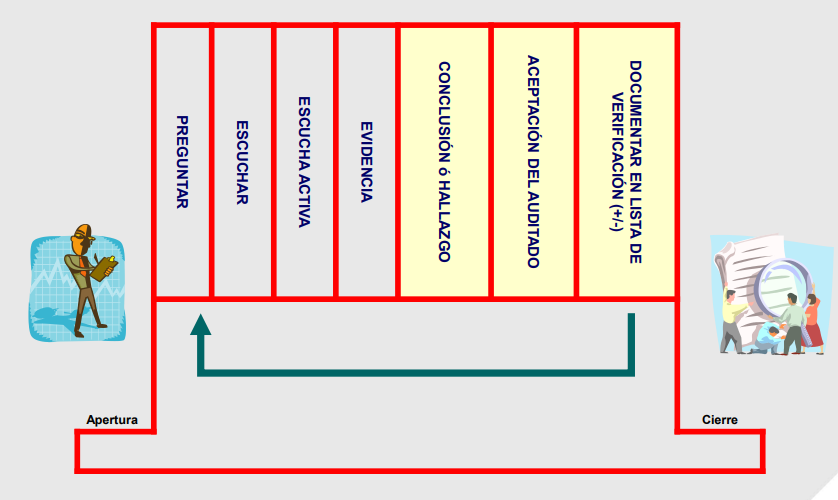


En relación con métodos de medición y seguimiento, uno de los más utilizados es la entrevista, en esta se debe elogiar lo positivo, realizar críticas colaboradoras, tener tacto y paciencia, dejar hablar, mantener contacto visual y concentración.

Los siguientes son algunos de los elementos involucrados en la entrevista:

**Figura 3**

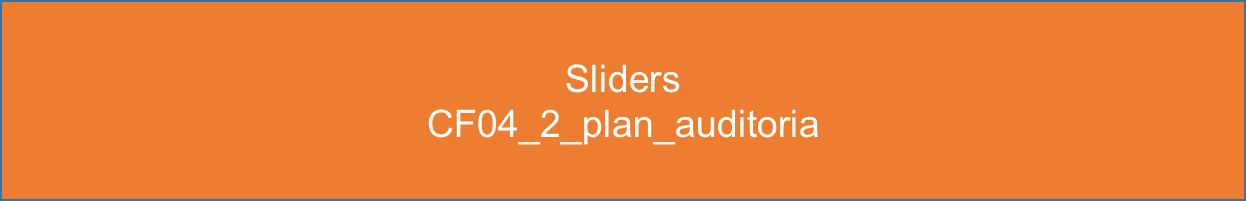
*La entrevista*



Nota. Tomado y adaptado de Icontec, 2013.

**2. Desarrollar y mantener la competencia de los auditores**

Dentro de las auditorías *in situ,* el auditor líder debe contar con un plan de auditoría, que debe contener la siguiente información:



A continuación, se presenta un formato de ejemplo para el control de auditoría.

**Tabla 1**

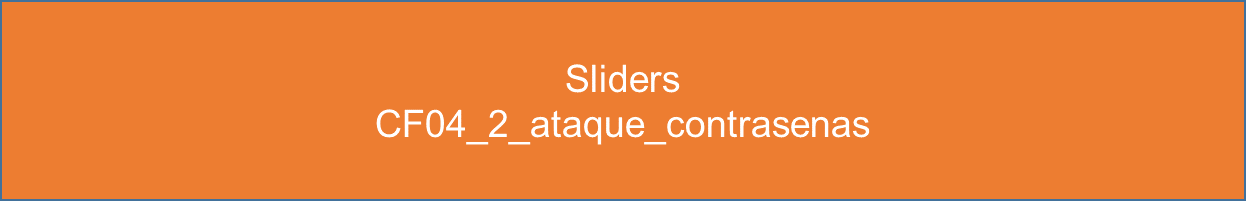
*Formato control de auditoría*

| Objetivo |  | | | | |
| --- | --- | --- | --- | --- | --- |
| Alcance |  | | | | |
| Criterios |  | | | | |
| Auditor líder |  | | Equipo auditor |  | |
|  | | | | | |
| Reunión de apertura |  | | Reunión de cierre |  | |
|  | | | | | |
| Fecha | Hora | Proceso/Actividad | Observaciones | Auditado | Auditores |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | | | | | |
| Observaciones |  | | | | |
| Elaborado por | | | Aprobado | Fecha | |

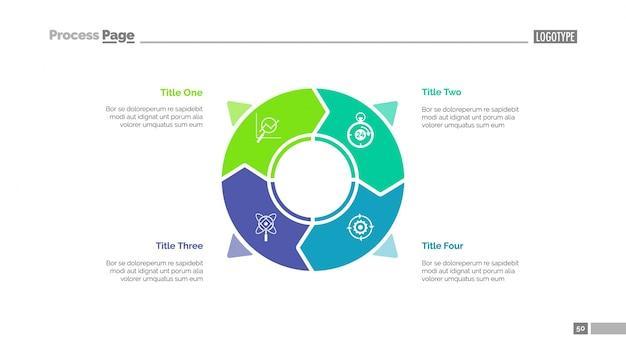
El auditor de seguridad de la información debe establecer píldoras o programas de concienciación, en la que por ejemplo se concientice sobre la importancia de crear contraseñas seguras.



Dentro de los tipos de ciberataques también se encuentra el ataque a las contraseñas:



Nota. Adaptado de Instituto Nacional de Ciberseguridad (INCIBE)



Otra actividad para realizar es aplicar la lista de verificación el ciclo PHVA, donde se ponen en práctica los conceptos de auditoría de SGSI. En ese proceso se debe coordinar la planificación, analizar los resultados y avances del plan de mejora, se puede implementar una lista y un listado de verificación.

El formato se muestra a continuación:



**3. Conocer y aplicar conceptos y técnicas de auditoría a los requisitos y controles de un SGSI**

Al establecer técnicas de auditoría como la implementación de las políticas de seguridad de la información, se definen principios generales, pero no se definen las tecnologías o formas específicas de realizar las actividades.

En tal sentido, se deben establecer roles y responsabilidades en cada fase, estos deben ser auditados y se debe describir cómo cumplir la política de seguridad de la Información.

Para mayor ilustración sobre roles y responsabilidades del SGSI se invita al aprendiz a consultar la guía del MINTIC (Roles y Responsabilidades – Seguridad y Privacidad de la Información), en el material complementario.

La siguiente figura representa elementos involucrados en la política de seguridad de la información:

**Figura 4**

*Control de Información documentada*

****

Nota. Tomado de Icontec, 2013.

En relación con las políticas de seguridad de la información, es importante indicar que tienen la siguiente estructura:



Esta estructura debe contener detalles como:

* **Condiciones obligatorias**: explica lo que se debe cumplir.
* **Responsabilidades**: identifica quiénes tienen obligaciones sobre la política.
* **Seguimiento y control**: identifica cómo se revisan las políticas.
* **Procedimientos**: identifica los procedimientos que implementan la política.

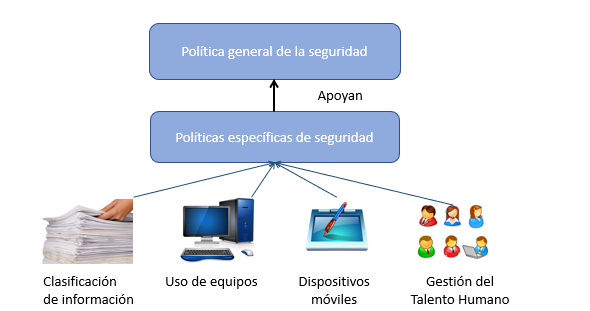
A continuación, se presenta el ejemplo de cómo podría ser una política:



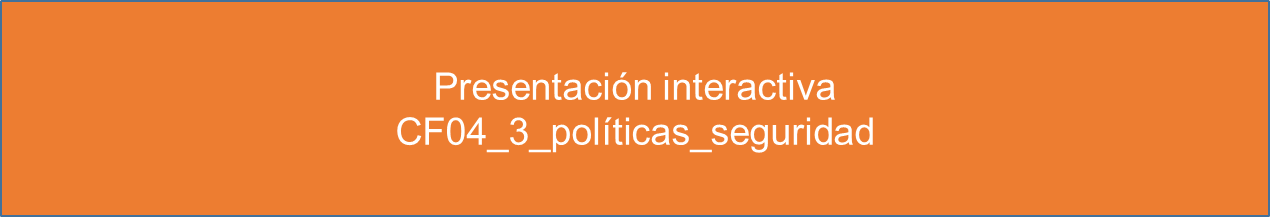
Ahora, la política general de seguridad es la información de más alto nivel de la organización, en ella se expone el compromiso e intención de la organización para lograr la seguridad de la información, las demás políticas apoyan el objetivo de dicha política, allí se pueden encontrar el avance y mejoras implementadas. A continuación, se relacionan algunos ejemplos de políticas de seguridad de la información específicas:

**Figura 5**

*Políticas específicas*



Algunas de estas políticas específicas, se presentan a continuación:



Los formatos necesarios para realizar solicitudes con relación a los datos recolectados durante la auditoría se presentan a continuación:

**Tabla 2**

*Solicitud de Cambio en componentes de infraestructura tecnológica*

| **Fecha de esta solicitud**  (día/mes/año) | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Número de solicitud**  [Este Campo se diligencia en forma consecutiva] | |  | | **Fecha solicitada para ejecutar el cambio**  (día/mes/año) | | | | | | |  |
| **Nombre del Jefe de dependencia solicitante** | |  | | **Estado de la solicitud**  [Campo es diligenciado por responsable del proceso, área o sistema de información]  Los estados pueden ser: Aprobado, Rechazado, Ejecutado | | | | | | |  |
| **Email** | | | | | |  | | | | | |
| **Nombre del Solicitante del cambio** |  | | | | | | **Teléfono** | |  | | |
| **Email** | | | | | |  | | | | | |
| **Descripción detallada del cambio que se solicita**  [describir de la forma más precisa posible el componente tecnológico o sistema de información que se desea cambia] |  | | | | | | **Teléfono** | |  | | |
|  | | | | | | | | | | | |
| **Justificación del cambio**  [Escriba las razones por las cuales es necesario el cambio, las razones pueden incluir: Solución de errores conocidos, Desarrollo de nuevos servicios. Mejora de los servicios existentes, otras] | | | | | | | | | | | |
|  | | | | | | | | | | | |
| **Nivel Riesgo identificado para el cambio**  (describa qué posibles riesgos puede implicar el cambio) | | | | | | | | | | | |
| **Nivel Impacto identificado para el cambio**  (describa qué posibles riesgos puede implicar el cambio) | | | | |  | | | | | | |
| **Si el cambio requiere proveedores externos incluya los datos de contacto** | | | | |  | | | | | | |
| **Nombre** | | | | | | | | | | | |
|  | | | **Correo** | | | | | **Teléfono Fijo** | | **Móvil** | |
|  | | |  | | | | |  | |  | |
|  | | |  | | | | |  | |  | |
|  | | |  | | | | |  | |  | |

Nota. esta sección debe ser diligenciada por el solicitante del cambio.

**Tabla 3**

*Aprobación del cambio*

| **Fecha de evaluación del cambio**  (día/mes/año) | | | |  | | **Aprobado**  (SI / NO) |  | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Si es rechazado (justificación del rechazo)** | | | | | | | | | |
|  | | | | | | | | | |
|
|
| **Si el cambio es aprobado indicar:** | | | | | | | | | |
| **Prioridad**  Inmediato/ No inmediato |  | | | **Clasificación**  Estándar, NO estándar, Emergencia | | | |  | |
| **Autorización del cambio (datos de quienes autorizan)** | | | | | | | | | |
| **Nombre** | | **cargo** | | | **email** | | | **teléfono** | |
|  | |  | | |  | | |  | |
| **Responsable de la ejecución del cambio**  (Escribir los datos de contacto de las personas que serán designadas como responsables del cambio. Pueden ser el personal de mesa de ayuda, administradores de equipos o sistemas de información o proveedores externos) | | | | | | | | | |
| **Nombre** | | | **email** | | | **Móvil** | | | **fijo** |
|  | | |  | | |  | | |  |
|  | | |  | | |  | | |  |

Nota. Esta sección debe ser diligenciada por el responsable del proceso, área TIC o sistema de información.

**Tabla 4**

*Plan de trabajo del cambio*

| **Detalle de las actividades a realizar ANTES del cambio** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Fecha programada** | **Hora programada** | **Actividad** | **Responsable** | **Recursos** | **Resultados**  **esperados** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Detalle de las actividades a realizar DURANTE el cambio** | | | | | | |
| **No.** | **Fecha programada** | **Hora programada** | **Actividad** | **Responsable** | **Recursos** | **Resultados**  **esperados** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Detalle de las actividades a realizar después del cambio** | | | | | | |
| **No.** | **Fecha programada** | **Hora programada** | **Actividad** | **Responsable** | **Recursos** | **Resultados**  **esperados** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Plan de vuelta atrás** | | | | | | |
| **No.** | **Fecha programada** | **Hora programada** | **Actividad** | **Responsable** | **Recursos** | **Resultados**  **esperados** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Nota. Esta sección debe ser diligenciada por las personas que son responsables del cambio o quienes lo ejecutarán.

**Tabla 5**

*Evaluación de resultados del cambio*

| **Fecha real de ejecución del cambio** (día/mes/año) | | | |  | |
| --- | --- | --- | --- | --- | --- |
| **Problemas encontrados durante la ejecución del cambio** | | | | | |
|  | | | | | |
|
|
| **Se aplicó plan de vuelta atrás**  (SI/NO) |  | **Quién autorizó la ejecución del plan de vuelta atrás** |  | | |
| **Fecha de ejecución del plan de vuelta atrás**  (día/mes/año) | | |  | | |
| **Revisión de resultados del cambio** | | | | | |
| **El cambio se ejecutó en la fecha prevista** (SI/NO) | | | | |  |
| **El cambio se ejecutó según el plan propuesto** (SI/NO) | | | | |  |
| **Fue necesario aplicar el plan de vuelta atrás** (SI/NO) | | | | |  |
| **Los resultados del cambio resolvieron el problema/necesidad** (SI/NO) | | | | |  |
| **Comentarios sobre el cambio** | | | | | |
|  | | | | | |
| **Calificación final del cambio** EXITOSO/ NO EXITOSO | | | | |  |

Nota. Esta sección debe ser diligenciada por la oficina de información sectorial.

Dentro de la evaluación de desempeño del SGSI, la organización debe valorar el ejercicio de seguridad de información y la eficacia del Sistema de Gestión de Seguridad de la Información, mediante:

* Procesos de alineación de TI y negocios.
* Proceso de gestión de riesgos de seguridad de la información.
* Procesos de cumplimiento legal o normativo.
* Proceso de sensibilización y comunicación.
* Procesos de auditoría del sistema.

Para más información se recomienda al aprendiz consultar Evaluación del Desempeño en ISO 27001- Requisitos en detalle, en el material complementario.

La siguiente tabla es un ejemplo de cronograma, donde el auditor puede ajustar la duración dependiendo del parque computacional de la organización.

**Tabla 6**

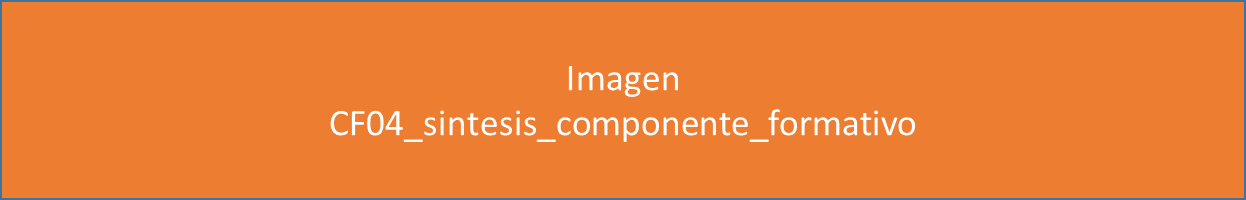
*Cronograma auditoría*

| **Implementación del SGSI** | **Duración** | **Comienzo** | **Fin** |
| --- | --- | --- | --- |
| Fase 1: Situación actual contextualización | 70 días |  |  |
| Fase 2: Sistema de gestión documental | 15 días |  |  |
| fase 3: análisis de riesgos | 21 días |  |  |
| fase 4 propuesta de proyectos | 20 días |  |  |
| fase 5: implementación de políticas | 60 días |  |  |
| fase 6: resultados e informes | 45 días |  |  |
| Fase 7: verificación | 30 días |  |  |



Al finalizar el proceso de auditoría se debe entregar un **Informe final** sobre la empresa planteada y siguiendo la continuidad de los informes realizados en las fases anteriores, se diseña e implementa el plan de mejora empresarial previniendo pérdidas de la información empresarial y aplicando como auditor las políticas de SGSI.

**SÍNTESIS**



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

| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| --- | --- |
| **Nombre de la actividad** | Niveles y conceptos generales de auditoría de riesgos |
| **Objetivo de la actividad** | Identificar niveles y conceptos de auditoría de riesgos dentro de la seguridad de la información |
| **Tipo de actividad sugerida** |  |
| **Archivo de la actividad** | Anexos\Anexo1\_CF04\_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** |
| --- | --- | --- | --- |
| Diseñar, implementar y evaluar un programa de auditoría interna de un SGSI | NQA. (2013). *ISO 27001:2013. Guía de implantación para la seguridad de la información.* <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf> | PDF | <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf> |
| Desarrollar y mantener la competencia de los auditores | Diario oficial. (2009). *Ley 1273 de 2009.* <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf> | PDF | <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf> |
| Desarrollar y mantener la competencia de los auditores | Defensoria.gov.co. (2012). *Ley Estatutaria 1581 de 2012.* <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf> | PDF | <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf> |
| Desarrollar y mantener la competencia de los auditores | CONPES. (2011). *Conpes 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.* <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pd>  f | PDF | <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf> |
| Desarrollar y mantener la competencia de los auditores | CONPES. (2016). *Conpes 3854 de 2016. Política Nacional de Seguridad Digital.* <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf> | PDF | <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pd>  f |
| Desarrollar y mantener la competencia de los auditores | Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia.* <https://www.oas.org/juridico/english/cyb_pry_convenio.pdf> | PDF | <https://www.oas.org/juridico/english/cyb_pry_convenio.pdf> |
| Desarrollar y mantener la competencia de los auditores | ISO 27001. (s.f.). *Evaluación del Desempeño en ISO 27001.* <https://normaiso27001.es/evaluacion-del-desempeno-en-iso-27001> | Página web | <https://normaiso27001.es/evaluacion-del-desempeno-en-iso-27001> |
| Conocer y aplicar conceptos y técnicas de auditoría a los requisitos y controles de un SGSI. | 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> | PDF | <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf> |
| Conocer y aplicar conceptos y técnicas de auditoría a los requisitos y controles de un SGSI | MINTIC. (2016). *Seguridad y privacidad de la información – Roles y Responsabilidades.* <https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf> | PDF | <https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf> |
| Conocer y aplicar conceptos y técnicas de auditoría a los requisitos y controles de un SGSI | MINTIC. (2016). *Guía Gestión de riesgos. Seguridad y privacidad de la información.* <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** | Uno de los significados más acordes se encuentra en educalingo (educalingo, s.f.)  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** | Un significado que no da la empresa (ORACLE, 2022)  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 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 quien, que, cuando, donde 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. |
| **PHVA** | Enfoque de gestión simple e iterativo para probar cambios en procesos o soluciones a problemas, e impulsar su optimización continua a través del tiempo. Por sus siglas Planear, Hacer, Verificar, Actuar. |
| **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. |
| **SGSI** | Sistema de Gestión de Seguridad de la Información. |
| **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). |
| **Riesgo** | En el ámbito informático la definición de riesgo son las amenazas digitales de las que se está expuesto día a día cuando se hace uso de la tecnología. |

**F. REFERENCIAS BIBLIOGRÁFICAS**

Congreso de Colombia. (agosto 21 de 1999). Ley 527 de 1999. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html>

Congreso de Colombia. (enero 5 de 2009). Ley 1273 de 2009. <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

DNP. (abril 11 de 2016). Conpes 3854 de 2016. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

DNP. (julio 14 de 2011). Conpes 3701 de 2011. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

Erb, M. (2009). Gestión de riesgo en la seguridad informática. <https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/>

FGN. (2009). Procedimientos Forenses de Policía Judicial. Bogotá.

Gómez, A. (2006). Enciclopedia de la Seguridad Informática. España: RA-Ma .

ICONTEC. (2013). ISO 27001. <https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf>

ICONTEC. (agosto 19 de 2009). ISO 27005. <https://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001071&ruta=/documentacion/0000001359/0000000107>

Instituto Nacional de Ciberseguridad (INCIBE). Guía de Ciberataques. <https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf>

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

MINTIC, M. d. (abril 1 de 2016). Guía Gestión de riesgos MINTIC. <https://acortar.link/aGHdJn>

*National Institute of Standards and technology.* (2002). <https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf>

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

ORACLE. (2022). ORCALE. <https://www.oracle.com/co/database/what-is-database/>

OWASP Top 10 2021. (2021). <https://owasp.org/Top10>

**G. 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 |
| Sandra Patricia Hoyos Sepúlveda | Corrección de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Mayo de 2022 |

**H. CONTROL DE CAMBIOS**

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

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