**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Implementación y operación de la ciberseguridad |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501099. Probar la solución del *software* de acuerdo con los parámetros  técnicos y los modelos de referencia. | RESULTADOS DE APRENDIZAJE | 220501099-1. Planificar la evaluación de la ciberseguridad de acuerdo con los requisitos organizacionales establecidos y normatividad vigente. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 09 |
| NOMBRE DEL COMPONENTE FORMATIVO | Planificación de la evaluación de la seguridad digital |
| BREVE DESCRIPCIÓN | Mediante este componente, el aprendiz se capacitará en la identificación de aspectos clave del proceso de evaluación de estrategias de seguridad en organizaciones, fase orientada por el estándar ISO/IEC 27001:2013. Se afianzará en verificar la efectividad de controles de seguridad implementados y, a partir de esta evaluación, establecer propuestas de mejoramiento de la seguridad de activos de información. |
| PALABRAS CLAVE | Auditoría, cumplimiento, evidencia, métrica, registro. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | Servicios |
| IDIOMA | Español |

1. **TABLA DE CONTENIDO:**

**Introducción**

1. Fases Sistema de gestión de seguridad de la información
2. Técnicas de auditoría
3. Tipos de auditoría
4. Definiciones y elementos fundamentales de la auditoría
5. Consideraciones importantes para una auditoría
6. Principios de auditoría
7. Fases de la auditoría
8. Clasificación de auditoría informáticas
9. Perfil del auditor
10. Metodología para la auditoría en sistemas
11. Aplicación de mediciones de seguridad
12. **DESARROLLO DE CONTENIDO:**

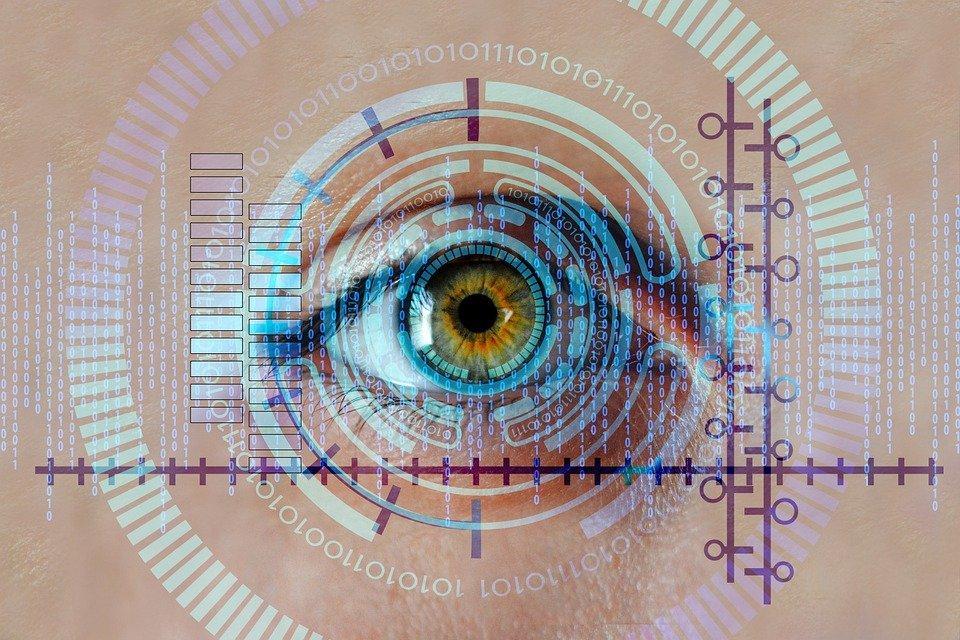
**Introducción**

Le invitamos a adentrarse en el estudio de este componente, reconociendo el valor fundamental que tiene para su formación como tecnólogo/a en implementación y operación de la ciberseguridad.

CF09\_Introducción\_formato\_9\_acordeon\_DI\_2023

* + - 1. **Fases Sistema de gestión de seguridad de información**

Para comenzar con la profundización en los contenidos de este componente formativo, recuerde las fases de un Sistema de Gestión de la Seguridad de la Información. Tenga presente que ella contempla el planear, el hacer, el verificar y el actuar. En este componente, se enfocará la atención en la fase del verificar, en la cual se realizan las diferentes actividades de evaluación de los controles implementados, a partir de unos ejercicios los cuales pueden ser internos, motivados por la misma compañía, o a través de un tercero de acuerdo a las circunstancias y estado de la implementación en la organización.



Nota. <https://bit.ly/3zmZkJD>

Reafirme sus conocimientos en lo referente a las fases del Sistema de Gestión de Seguridad de la Información (SGSI), en la siguiente infografía:

CF9\_1\_Fases\_SGSI\_formato\_2\_infografia\_interactiva\_DI\_2023

* + - 1. **Técnicas de auditoría**

Las auditorías son un “*proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas, de manera objetiva, con el fin de determinar el grado en que se cumplen los criterios de auditoría*” (ISO, 2018). Las auditorías se convierten en el proceso mediante el cual se valida y corrobora, con algún proceso de observación, indagación o verificación, si un criterio de evaluación se está cumpliendo, de acuerdo con los parámetros establecidos.



Nota. ghttps://bit.ly/3nOfEBf

**3. Tipos de auditoría**

De acuerdo con el momento en que se realiza la auditoría, del alcance de la misma y del auditor que la realiza, estas se pueden clasificar en 3 tipos: de primera parte, de segunda parte o de tercera parte.

**Tabla 1**

*Tipos de auditoría*

|  |  |  |
| --- | --- | --- |
| Auditoría de primera parte | Auditoría de segunda parte | Auditoría de tercera parte |
| Auditoría interna | Auditoría externa de proveedor | Auditoría de certificación y/o Acreditación |
|  | Otra auditoría externa de parte interesada | Auditoría legal, reglamentaria o similar |

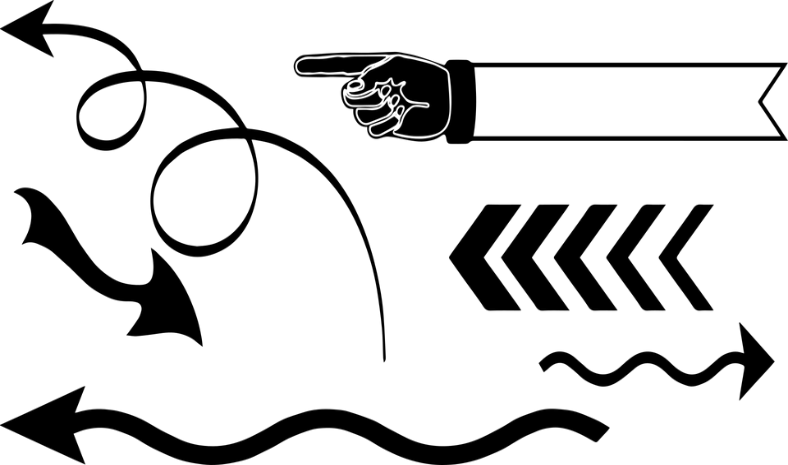
Nota: tomado de ISO, 2018.

Pero, ¿cuáles son las especificidades de cada tipo de auditoría? Aquí se los presentamos; revise la siguiente infografiay descúbralo; le sugerimos tomar nota de ello en su libreta personal de apuntes. ¡Adelante!

CF9\_3\_TiposDeAuditoria\_formato\_2\_infografia\_interactiva\_DI\_2023

1. **Definiciones y elementos fundamentales de la auditoría**

Para establecer o entender un ejercicio de auditoría es necesario referirse a la norma GTC-ISO 19011:2018, la cual establece las directrices para la auditoría de los sistemas de gestión.



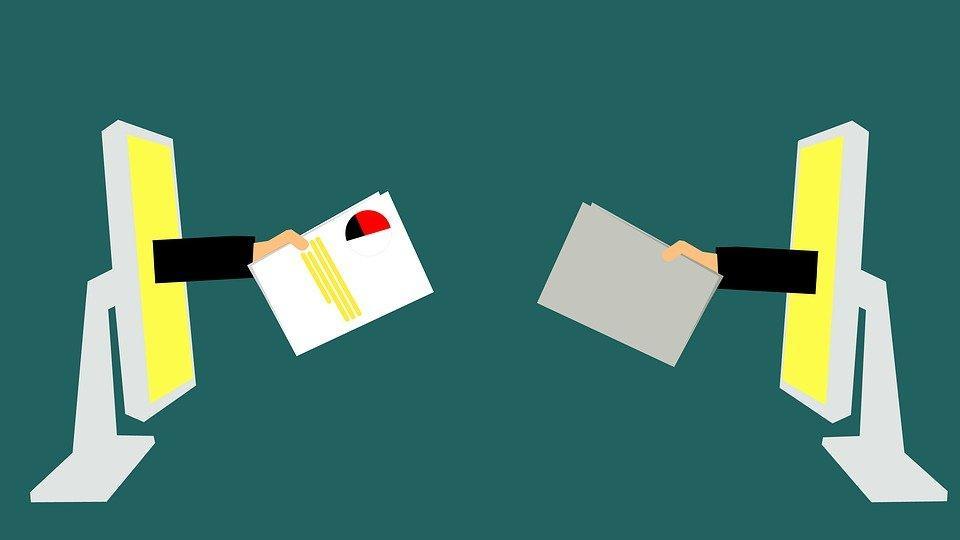
Nota. <https://bit.ly/3Csp0qn>

Entérese de algunas definiciones y lineamientos que da la norma y que aseguran que el proceso de evaluación y auditoría del sistema de gestión de seguridad de información, en las organizaciones, sea efectivo:

CF9\_4\_Definiciones\_y\_Elementos\_Auditoria\_formato\_4\_video\_DI\_2023

1. **Consideraciones importantes para la auditoría**

De acuerdo a la norma GTC-ISO 19011:2018, una auditoría de sistemas de gestión se debe establecer bajo ciertas condiciones que permitan la construcción y desarrollo de la misma, en la organización.



Nota. https://bit.ly/3lHNNjx

**Consideraciones Importantes Auditoría**

Las auditorías de los sistemas de gestión de la seguridad de la información, deben ser establecidas teniendo en cuenta algunas condiciones que favorecerán, rotundamente, tanto su construcción como su desarrollo.

Diagrama

Descripción generada automáticamente

El esquema de auditoría contempla:

1. El establecimiento de los objetivos del programa.
2. La determinación y evaluación de los riesgos y oportunidades.
3. El establecimiento del programa de auditoría.
4. La implementación del programa de auditoría.
5. El seguimiento que se hará a ese programa de auditoría.
6. La respectiva revisión y mejora del programa.

Los elementos más significativos, que deben incorporarse para el exitoso desarrollo de la auditoría; incorporan al ciclo PHVA: planificar, hacer, verificar, actuar, ciclo común en todos los sistemas de gestión.

Una vez construido el esquema de auditoría se da inicio a la auditoría en la cual se preparan las actividades para la misma, se ejecutan tales actividades, se prepara y distribuye el informe, con el cual se cierra el proceso de auditoría.

Importante tener en cuenta que lo que hace que la auditoría sea un proceso completo es la realización de las actividades de seguimiento de la misma. Acción que está dentro de la fase Actuar del ciclo PHVA.

1. **Principios de auditoría**

Entiéndase como principios de auditoría a los elementos y aspectos fundamentales, para desarrollar un ejercicio de auditoría y obtener resultados confiables, objetivos, pertinentes y suficientes para que la organización tome las decisiones apropiadas en el futuro.

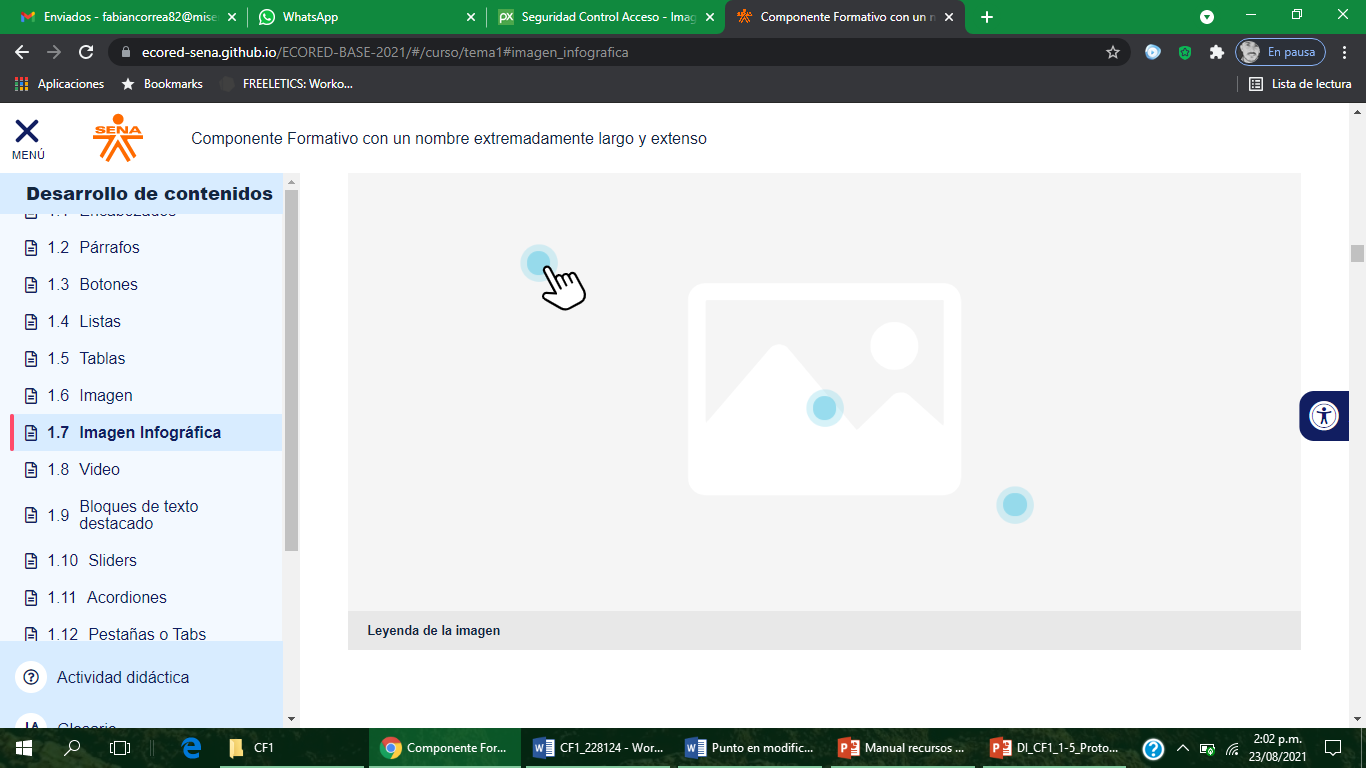


Nota. https://bit.ly/3krdHs9

Adicional de las técnicas, tipos, definiciones y consideraciones, relacionadas con el proceso de auditoría, hay que tener en cuenta que toda acción en pos de la auditoría, ha de estar orientada por estos principios. Conózcalos a continuación:

CF9\_6\_Principios\_de\_Auditoria\_​

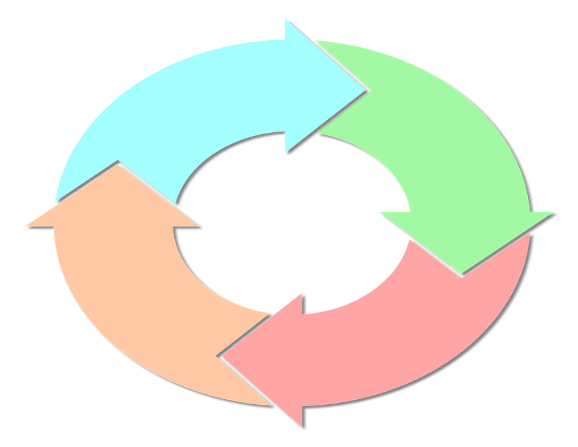
formato\_11\_linea\_tiempo\_DI\_2023



**¡Importante!**

1. **Fases de la auditoría**

De acuerdo al diagrama de flujo presentado por la metodología de la norma GTC-ISO 19011:2018, se pueden establecer tres fases para el desarrollo de una auditoría: la planeación, la implementación y el monitoreo de la misma.



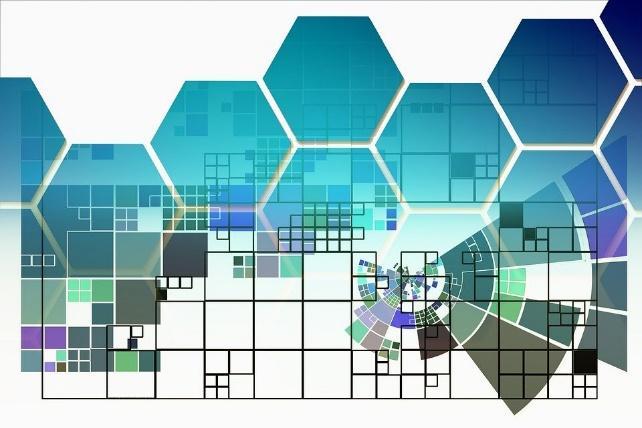
Nota. https://bit.ly/39mOPLR

Revise la siguiente infografía, y profundice en las fases de la auditoría. Le recordamos que puede llevar registro de los aspectos más destacados, en su libreta personal de apuntes.

CF9\_7\_FasesDeLaAuditoria\_formato\_2\_infografia\_interactiva\_DI\_2023

1. **Clasificación de auditorías informáticas**

Las auditorías, dependiendo del alcance y de los activos a evaluar, se pueden clasificar en: auditoría informática y auditoría de sistemas. Ambas clases de auditorías cuentan con aspectos, principios y elementos específicos en sus fases.



Nota. https://bit.ly/3EDKQsX

Aquí se las presentamos:

CF9\_8\_Clasificacion\_Auditorias\_Informaticas\_​

formato\_10\_tabs\_horizontales\_DI\_2023

1. **Perfil del auditor**

El auditor juega un papel importante en el desarrollo del ejercicio de auditoría, ya que además de tener un conocimiento de la organización y los procesos, es quien da fe de la verificación en relación al cumplimiento de las políticas y controles de seguridad, objeto de evaluación.

Además, el auditor debe contar con las siguientes cualidades y capacidades para lograr los objetivos del ejercicio:

**Tabla 2**

*Cualidades y capacidades de un auditor*

|  |  |
| --- | --- |
| Capacidades y cualidades de un auditor | |
| Conocimiento de los procesos de la organización. | Cuenta con habilidades y destrezas. |
| Ser diplomático y respetuoso. | Ser objetivo. |
| Conocer y aplicar metodología para auditoría. | Ser imparcial y sincero. |
| Conocimiento de herramientas, métodos y temas afines. | Tener valores y principios éticos. |
| Manejo de técnicas de auditoría. | Ser discreto y manejar el principio de confidencialidad. |
| Tener experiencia en temas a evaluar. | Tener capacidad de observación. |

Nota: adaptada de Guía de auditoría. MINTIC. (2016).

1. **Metodología para la auditoría en sistemas**

La aplicación de las auditorías en sistemas debe estar regida por una metodología que oriente los procesos necesarios a desarrollar y que explique los pasos que se deben de realizar. La *Guía de Auditoría* N.° 15 del MINTIC, propone una metodología para el desarrollo de una auditoría de sistemas.



Nota. https://bit.ly/3lGeYel

A continuación, puede revisar la metodología para una auditoría de sistemas.

Diagrama

Descripción generada automáticamente

La metodología para la realización de una auditoría de sistemas, contempla pasos cabales que aseguran efectividad y oportunidad en el proceso mismo de la auditoría.

* Planear cómo se llevará a cabo la auditoría.
* Razones de la auditoría.
* Objetivos generales y específicos.
* Métodos, técnicas y procedimientos.
* Hasta la elaboración de la documentación de planes, programas y presupuestos.

**Métricas**

Las métricas permiten establecer un nivel de medición cuantitativo en relación al cumplimiento de un requisito, de un control que implementó la organización para alcanzar un objetivo. Estas métricas están organizadas en dos categorías: métrica directa y métrica indirecta.

En el caso de métricas enfocadas en seguridad, estas permiten evaluar los controles implementados, cómo se cumplen los objetivos de seguridad establecidos por la organización, permitiendo identificar el grado de afectación que puede recibir un activo de información por la materialización de alguna amenaza.

Las métricas de seguridad son usadas, en las auditorías, para:

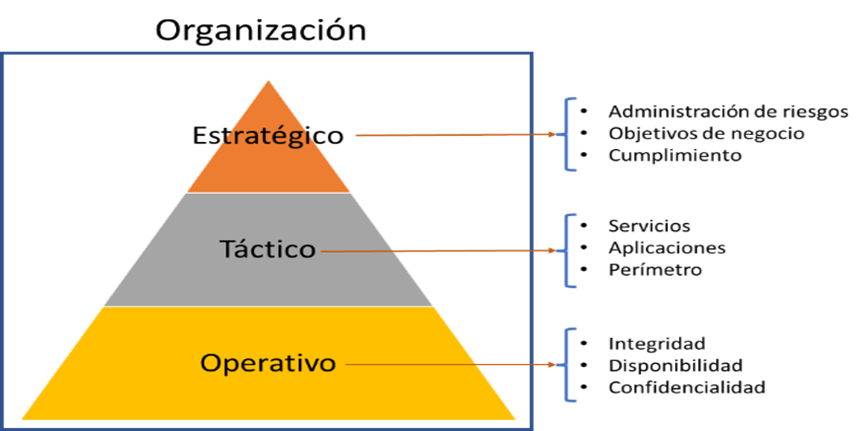
* Gestión de la seguridad de la información en una organización.
* Brindar la información necesaria para la generación de informes.
* Cumplir con legislación, reglamentación y normas que rigen una organización.
* Apoyar la gestión de riesgos.

Las métricas deben conservar las algunas características:

* Deben ser alcanzables.
* Debe ser expresadas en escalas de porcentaje o escalas numéricas.
* Deben explicar los componentes evaluados.
* Deben permitir identificar puntos débiles.
* Debe permitir conocer los riesgos a los que se enfrenta la organización.

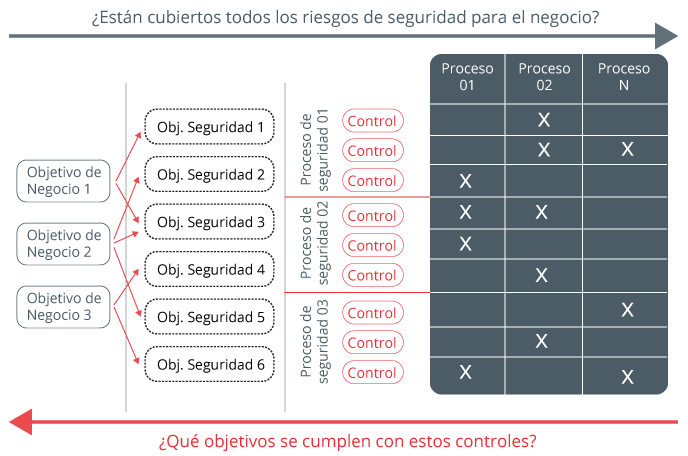
**Medición de la seguridad en la organización**

**Gráfico N.º Niveles de decisión de una organización**

****

Uno de los objetivos de las estrategias de seguridad es garantizar los pilares de la seguridad de la información a partir de la implementación de estrategias, acciones y controles… pero, anteriormente, estos deben poder medirse para conocer el grado de eficiencia; es aquí donde se hace uso de las métricas, las cuales favorecen la identificación del nivel de apropiación en lo operativo, lo táctico y lo estratégico: los tres niveles de decisión, calves, en la organización.

**Cómo se mide la seguridad en una organización**



Los objetivos de seguridad de la organización deben alinearse con los objetivos de negocio de la organización, de tal manera que se identifiquen los procesos que se deben cubrir, permitiendo identificar y establecer los controles necesarios.

Es así como se posibilita un mejor proceso de medición de la seguridad en una organización.

**Métricas de seguridad para cada uno de los niveles de decisión**

A continuación, se describen los diferentes niveles de decisión en las métricas de seguridad:

CF9\_10\_Metricas\_de\_seguridad\_ 10\_tabs\_verticales(pasos)\_DI\_2023

1. **Aplicación de mediciones de seguridad**

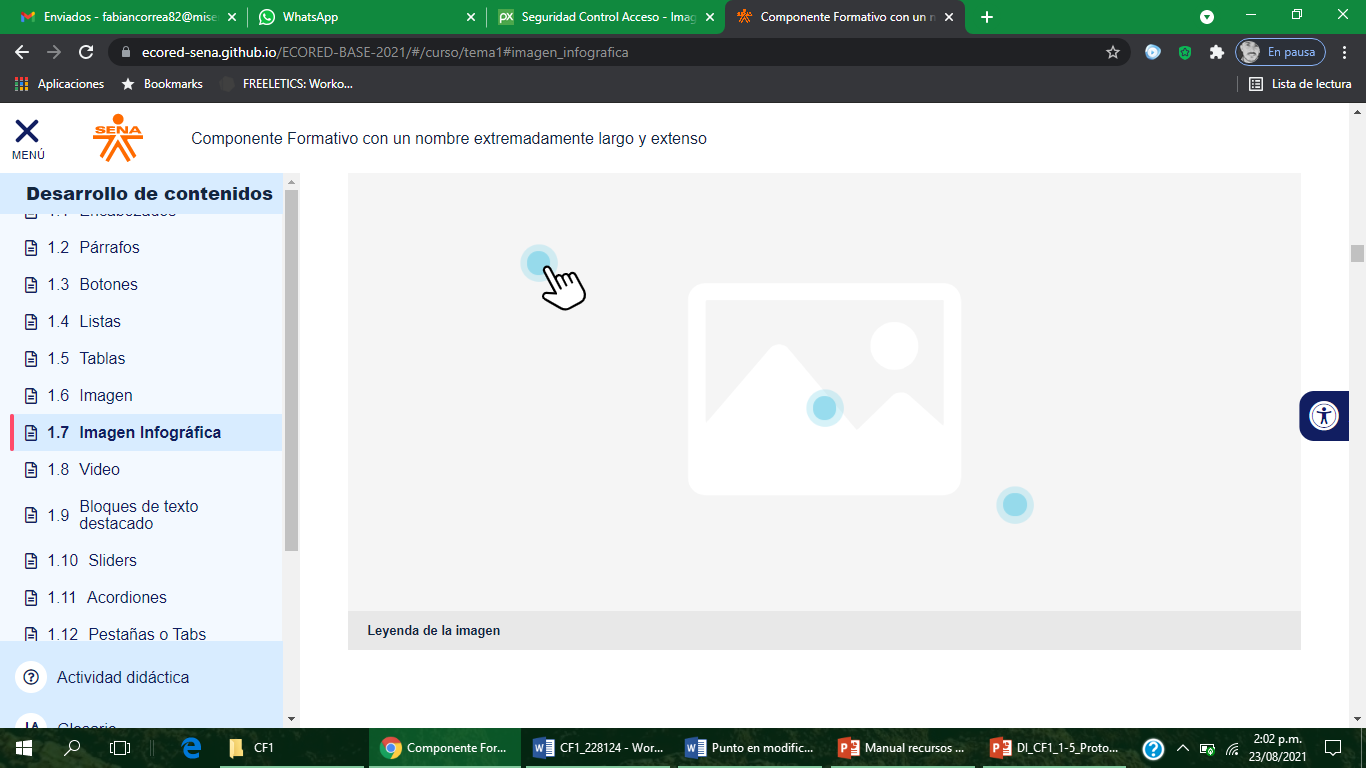
Los líderes de procesos deben estar informados sobre cuáles son las métricas establecidas, y cómo éstas ayudan a cumplir los objetivos de seguridad, con el fin de que se desarrollen y documenten las acciones encaminadas al cumplimiento de dichos objetivos.



Nota. https://bit.ly/3Arq7pK

Algunas generalidades de suma importancia y que debe tener en cuenta para la aplicación de mediciones de seguridad son:

CF9\_11\_Aplicación\_de\_Mediciones\_de\_Seguridad\_formato\_10\_tabs\_verticales(pasos)\_DI\_2023



**¡Atención!**

# Síntesis

La planificación de la evaluación de la seguridad digital es un proceso fundamental para garantizar la protección de la información y los activos digitales en cualquier organización. Esta planificación implica una serie de pasos esenciales que aseguran que se identifiquen y aborden adecuadamente las vulnerabilidades y amenazas a la seguridad digital.

**Imagen que contiene Diagrama

Descripción generada automáticamente**

1. **ACTIVIDADES DIDÁCTICAS (OPCIONALES SI SON SUGERIDAS)**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la actividad | Planeación seguridad digital |
| Objetivo de la actividad | Identificar términos para la planificación de la evaluación de la ciberseguridad según normatividad. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | CF09\_actividad\_didáctica\_completar\_espacios |

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 |
| 6. Principios de auditoría | Organización Internacional de Normalización (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad.* (ISO 27001). <https://www.iso.org/standard/54534.html> | Norma técnica | <https://www.iso.org/standard/54534.html> |

1. **GLOSARIO**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Atributo: | cualquier propiedad o característica que permite distinguir un objeto de otro. |
| Escala: | rango de valores organizados con los cuales se evalúa un atributo. |
| Evidencia: | información suficiente que respalda alguna acción. |
| Indicador: | son unidades que permiten medir el desempeño o desarrollo de alguna acción o de algún control. |
| Métrica: | conjunto de criterios y condiciones necesarios para medir un control o una acción |
| SGSI: | Sistema de Gestión de la Seguridad de la Información. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Instituto Nacional de Ciberseguridad (2015). *¿Sabes cómo se mide la seguridad de la información en tu empresa?* INCIBE. <https://www.incibe.es/protege-tu-empresa/blog/mide-seguridad-informacion>

ISO (2020). *Evaluación del desempeño en ISO 27001.* (ISO 27001). <https://normaiso27001.es/evaluacion-del-desempeno-en-iso-27001/>

ISO (2020). *Fase 8 auditoría interna según ISO 27001.* (ISO 27001). [https://normaiso27001.es/fase-8-auditoría-interna-segun-iso-27001/](https://normaiso27001.es/fase-8-auditoria-interna-segun-iso-27001/)

ISO (2018). *Directrices para la auditoría de los sistemas de gestión*. *(ISO 19011).* <https://e-collection-icontec-org.bdigital.sena.edu.co/normavw.aspx?ID=75245>

Ministerio de Tecnologías de la Información y Comunicaciones (2016). *Guía de Auditoría*. MINTIC. [https://www.mintic.gov.co/gestionti/615/articles-5482\_G15\_Auditoría.pdf](https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf)

Organización Internacional de Normalización (ISO, 2013). *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos*. (ISO 27001). <https://www.iso.org/standard/54534.html>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| Autor (es) | Hernando José Peña Hidalgo | Experto Temático | Cauca - Centro de Teleinformática y Producción Industrial | Septiembre 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Centro agropecuario La Granja, Regional Tolima | Septiembre 2021 |
| Carolina Coca Salazar | Revisora Metodológica y Pedagógica | Regional Distrito Capital- Centro de Metrología y Diseño | Septiembre 2021 |
| Sandra Patricia Hoyos Sepúlveda | Revisión y corrección de estilo | Centro para la Industria de la Comunicación Gráfica – Regional Distrito Capital | Septiembre 2021 |

1. **CONTROL DE CAMBIOS**

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del cambio |
| Autor (es) | Nelly Parra | Adecuadora Instruccional | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
|  | Alix Cecilia Chinchilla Rueda | Asesora Metodológica | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |
|  | Liliana Victoria Morales Guadrón | Responsable Línea de Producción Distrito Capital. | Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información. | Octubre de 2023 | Adecuación de contenidos de acuerdo con la directriz de Dirección General. |