

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.

Noviembre 2023

Tabla de contenido

Introducción	1
1. Fases Sistema de gestión de seguridad de información.....	1
2. Técnicas de auditoría	3
3. Tipos de auditoría	3
4. Definiciones y elementos fundamentales de la auditoría.....	5
5. Consideraciones importantes para la auditoría	7
6. Principios de auditoría	8
7. Fases de la auditoría	9
8. Clasificación de auditorías informáticas	11
9. Perfil del auditor	12
10. Metodología para la auditoría en sistemas	13
11. Aplicación de mediciones de seguridad	18
Síntesis	20
Material complementario.....	21
Glosario	22
Referencias bibliográficas	23

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.

Dentro del ciclo que enmarca la norma ISO/IEC 27001:2013, se establece una fase que permite evaluar el rendimiento del sistema de seguridad de la información y, en especial, los controles que fueron propuestos para mejorar la seguridad de los activos de información de la organización, esta fase implica establecer una métrica, bajo la cual se identifiquen los rangos de valores aceptables y no aceptables, de cada control.

A partir de esta evaluación se podrán establecer los mecanismos de mejora de los mismos controles, o de cambio completo de un determinado control, en caso de ser necesario.

“Lo que no se mide no se puede mejorar. Lo que no se mejora, se degrada siempre” William Thomson Kelvin

Se considera que la evaluación de la estrategia de seguridad deba realizarse de manera periódica, convirtiéndose en punto de partida para la adopción de la mejora continua.

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.

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

- **Fase 1. Establecer el SGSI**
 - Diseñar SGSI
 - Análisis de procesos
 - Definir alcance
 - Elaborar política de seguridad
 - Identificar y evaluar inventario de activos
 - Realizar análisis de riesgos
 - Generar SoA
- **Fase 2. Implementar y operar el SGSI**
 - Generar plan de mitigación de riesgos
 - Aplicar plan de mitigación de riesgos
 - Implementar controles seleccionados
 - Administración de cambio
- **Fase 3. Monitorear y revisar el SGSI**
 - Revisiones gerenciales
 - Revisiones independientes
 - Auditorías internas

- Revisiones técnicas
- **Fase 4. Mantener y mejorar el SGSI**
 - Implementar mejoras
 - Tomar acciones preventivas y correctivas
 - Comunicar resultados de las acciones tomadas

2. 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.

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

Auditoría de primera parte	Auditoría de segunda parte	Auditoría de tercera parte
	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 información:

Los tipos de auditoría

Las auditorías son de un tipo o de otro, según el momento en que se realiza, según el alcance que esta tiene y según el auditor que la realiza.

I. Auditoria de primera parte

Estas son realizadas por la misma organización o también llamadas Auditorías Internas. buscan verificar que se estén aplicando y cumpliendo los requisitos establecidos en la estrategia de seguridad.

II. Auditoria de segunda parte

Se denominan también auditorías externas; este tipo de auditoría externa es la que evalúa que se estén cumpliendo los requisitos con los proveedores, en relación al cumplimiento de la estrategia de seguridad.

III. Auditoria de tercera parte

Son las auditorías realizadas por partes externas con fines de certificación o acreditación, aunque también se pueden dar para verificación de cumplimiento legal, reglamentario entre otras.

IV. Enfoque en su organización

En este componente formativo, se enfocará la mirada hacia las auditorías de primera parte o auditorías internas, ya que las demás auditorías son realizadas por terceros. Con este énfasis, usted se fortalecerá en la identificación de aspectos clave del proceso de evaluación de estrategias de seguridad para su propia organización.

4. 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.

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, esto es:

Video 1. Definiciones y elementos de la auditoría



Enlace de reproducción del video

Síntesis del video: Definiciones y elementos de la auditoría

Definiciones y directrices para la auditoría de los sistemas de gestión, según la norma GTC-ISO 19011:2018.

Criterio de auditoría: es un conjunto de requerimientos, que han sido establecidos como referente y frente a los cuales se va a verificar su evidencia objetiva.

Evidencia objetiva: es cualquier dato, recurso o información que respalda la veracidad de algo.

Alcance de auditoría: establece los límites sobre los cuales se va a realizar un ejercicio de auditoría, este alcance puede determinarse en términos de organizaciones, procesos, sedes, tiempo, entre otras.

Plan de auditoría: este plan describe las actividades que se realizarán en el marco de la auditoría, y debe ser presentado a las partes (auditor – auditado) para su aprobación.

Evidencia de auditoría: son todos los registros y material que respalde el ejercicio de auditoría, estas evidencias deben ser cuantificables y calificables.

Hallazgos de auditoría: se trata de los resultados de la evaluación aplicada, de acuerdo a los criterios auditados.

5. 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.

Consideraciones importantes de una 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, esto es:

- a.** El establecimiento de los objetivos del programa.
- b.** La determinación y evaluación de los riesgos y oportunidades.
- c.** El establecimiento del programa de auditoría.
- d.** La implementación del programa de auditoría.
- e.** El seguimiento que se hará a ese programa de auditoría.
- f.** 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.

6. 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.

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 los principios que se mencionan a continuación:

- 1) Integridad:** el auditor debe realizar el ejercicio a partir de su honestidad, imparcialidad, diligencia y responsabilidad, durante toda la auditoría.
- 2) Presentación ecuánime:** los resultados de la auditoría deben reflejar la veracidad y exactitud de la información que se pudo evaluar durante la auditoría.
- 3) Debido cuidado profesional:** el auditor debe tener la capacidad de formular juicios de valor razonables durante toda la auditoría.
- 4) Confidencialidad:** la seguridad de la información, durante el ejercicio de la auditoría, es un factor de sumo cuidado. Se debe garantizar que la información, su uso y protección, serán aplicados de manera apropiada.
- 5) Independencia:** el auditor se debe considerar y sentir independiente y libre de sesgo y conflicto de intereses, durante todo el ejercicio de la auditoría, lo cual permite realizar una evaluación objetiva.

6) Enfoque basado en la evidencia: los criterios evaluados deben contar con la presentación y verificación de las evidencias correspondientes, lo cual da fe del ejercicio de auditoría dando fiabilidad a ésta.

¡Importante!

Con los anteriores principios, se busca objetividad, confianza y contar con un insumo para identificar el rendimiento de la estrategia de seguridad de la información y poder tomar decisiones.

7. 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.

A continuación, podrá profundizar en las fases de la auditoría con la siguiente información:

Fase 1. Planeación de la auditoría:

- La auditoría debe ser programada, aprobada e informada a todos los líderes de procesos e interesados con tiempo de antelación.
- Para las auditorías, es necesario que todos los líderes de procesos y equipos estén informados y alineados en atención a los requerimientos de los auditores, de tal manera que pueda ser presentada cualquier evidencia o requerimiento que sea solicitado por el auditor.

- De acuerdo con el ciclo PHVA, las auditorías deben de realizarse por lo menos una vez en el año, aunque si la organización considera, debido a la criticidad de sus procesos, o con el fin de determinar alguna verificación, que deban hacer más en este periodo de tiempo, también es válido; esto ayudaría a evaluar e identificar falencias en los criterios de auditoría.
- Para cada auditoría se debe contar con los informes de las auditorías anteriores, tanto internas como externas, y revisiones de la alta dirección. Además, estas auditorías deben realizarse antes de las auditorías de certificación y/o acreditación, ya que estas auditorías internas pueden detectar falencias que pueden corregirse para dicha evaluación.

Fase 2. Implementación de la auditoría

- En este evento se realiza la apertura de la auditoría en la cual se presenta la metodología, tiempos, procesos, sistemas o cualquier detalle que permita identificar el alcance de la misma, se hace entrega de la información existente o de auditorías anteriores, y se da inicio al ejercicio de acuerdo a la programación establecida.
- Una vez se finalice el ejercicio, el auditor realiza el informe, el cual es presentado durante el cierre de la auditoría.
- Con el informe del auditor, la alta dirección establecerá las acciones de mejora a futuro, a través de un plan de mejoramiento; estas acciones pueden ser correctivas, preventivas o de mejora.

Fase 3. Monitoreo a la auditoría

- En esta fase, se busca realizar el seguimiento a las acciones establecidas en el último ejercicio, con el fin de validar su efectividad en la corrección de falencias o la adecuada implementación de nuevos controles.
- Este seguimiento debe realizarse de manera permanente con el fin de reportar avances y fortalecer aquellas acciones que pueden retrasar el cumplimiento de los objetivos.

8. 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 que a continuación se presentan:

A. La auditoría informática

Esta auditoría busca recolectar, consolidar y evaluar las evidencias que demuestren si la organización realizó la implementación de controles, y acciones para la protección de los activos de información.

Auditoría informática y objetivos

La aplicación de controles y acciones para la protección de activos de información, se evidencia a partir del logro de los objetivos de la auditoría, como son:

- ✓ Protección de activos e integridad de datos.
- ✓ Gestión de protección de activos, de manera eficaz y eficiente.

Las auditorías informáticas y su tipo

Este tipo de auditorías se puede ser de tipo interno o externo con el objetivo de obtener un informe objetivo.

B. La auditoría de sistemas

En este tipo de auditoría se busca evaluar el manejo de la protección de los activos de información que son administrados en los sistemas de información de la organización, incluyendo las capacidades del recurso humano para una adecuada gestión de estos activos.

Auditorías de sistemas y su tipo

Estas auditorías son de tipo preventivo, y abarca la revisión de dispositivos de hardware como sistemas de información.

9. 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.

10. 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 No. 15 del MINTIC, propone una metodología para el desarrollo de una auditoría de sistemas.

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: 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:** esta métrica se enfoca en velocidad de ejecución, defectos encontrados en una cantidad de tiempo, costo, tamaño de memoria usada, número de líneas de código, entre otros.
- ❖ **Métrica indirecta:** esta se enfoca en la calidad, complejidad, fiabilidad, eficiencia, funcionalidad, facilidad de mantenimiento, entre otros.

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

Figura 1. Niveles de decisión de una organización



Estos niveles son:

- **Estratégico.** Compuesto por
 - Administración de riesgos
 - Objetivos de negocio
 - Cumplimiento
- **Táctico.** Compuesto por
 - Servicios

- Aplicaciones
- Perímetro
- **Operativo.** Compuesto por
 - Integridad
 - Disponibilidad
 - Confidencialidad

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, claves, en la 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:

A. Métricas de nivel estratégico

- ✓ Conocer el % (tanto por ciento) de las cuentas inactivas de usuario, deshabilitadas. respecto al total de cuentas inactivas.

- ✓ Conocer el valor total de los incidentes de seguridad informática respecto al presupuesto total de seguridad informática.
- ✓ Conocer el % (tanto por ciento) de los nuevos funcionarios que completaron su entrenamiento de seguridad respecto al total de los nuevos funcionarios que ingresaron.

El propósito de esta métrica es el desempeño de personas y procesos.

B. Métricas del nivel táctico

- ✓ Conocer el número de mensajes salientes con spyware o virus.
- ✓ Número de mensajes de spam detectado, respecto al número total de mensajes ignorados.
- ✓ Número de estaciones de trabajo en funcionamiento, configuradas correctamente, respecto al total de estaciones de trabajo.
- ✓ Número de spyware o virus detectados en estaciones de trabajo o servidores.

El propósito de esta métrica es el desempeño de las tecnologías de seguridad informática.

C. Métricas del nivel operativo

- ✓ Número de incidentes asociados con la disponibilidad respecto al total de incidentes.
- ✓ Número de incidentes asociados con la confidencialidad respecto al total de incidentes.

Propósito de esta métrica: desempeño de la administración de incidentes.

11. 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.

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

Aplicar mediciones busca

- ✓ Representar los valores del nivel de seguridad de la organización.
- ✓ Evaluar la eficiencia del SGSI en la organización.
- ✓ Incluir niveles de seguridad que sirvan de guía para las revisiones del SGSI.
- ✓ Evaluar la efectividad de los controles de seguridad en la organización.

Según método de evaluación de atributos

- ✓ Estos son objetivos: los que se centran en una regla numérica (por ejemplo, de 1 a 5), que se pueden aplicar a las personas o a los procesos, se recomienda que se realice primero a los procesos.
- ✓ Estos son subjetivos: los que se centran en el criterio de los empleados o de los evaluadores externos.

Métodos de recolección de información

Según forma de aplicar mediciones a atributos, es común realizar:

- ✓ Cuestionarios.
- ✓ Inspección visual.

- ✓ Toma de notas.
- ✓ Comparación de datos de diferentes momentos.
- ✓ Muestreo.
- ✓ Consulta directa a sistemas de información.
- ✓ Entre otros.

Asociación con tipo de escala

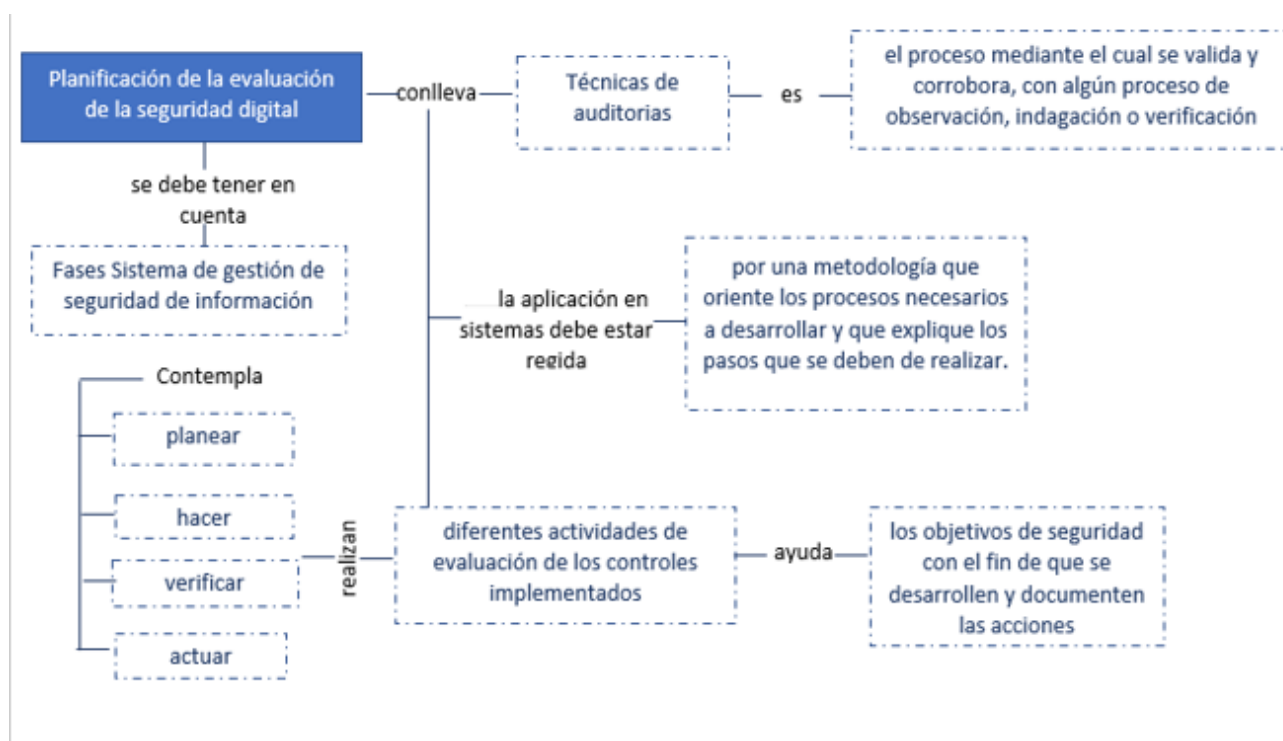
Realizada la medición de atributos, esta se asocia a un tipo de escala:

- ✓ Ratio.
- ✓ Nominal.
- ✓ Intervalos.
- ✓ Ordinal.

¡Atención! Para este ejercicio se puede hacer uso de instrumentos (formatos de evaluación) que permitan registrar y automatizar el proceso y la aplicación de fórmulas de comparación, en caso de ser necesario.

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:



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
6. Principios de auditoría	Ministerio de Tecnologías de la Información y Comunicaciones (s.f). <i>Modelo de seguridad y privacidad de la información.</i>	Documento normativo	https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Glosario

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.

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-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>

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Líder del equipo	Dirección General
Liliana Victoria Morales Gualdrón	Responsable de línea de producción	Centro de Gestión de Mercados, Logística y Tecnologías de la Información - Regional Distrito Capital
Nelly Parra Guarín	Adecuación instruccional - 2023	Centro de Gestión de Mercados, Logística y Tecnologías de la Información - Regional Distrito Capital
Alix Cecilia Chinchilla Rueda	Metodología para la formación virtual	Centro de Gestión de Mercados, Logística y Tecnologías de la Información - Regional Distrito Capital