**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 | 220501099-2. Ejecutar la evaluación de las estrategias de ciberseguridad con base en la planificación de la misma. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 10 |
| NOMBRE DEL COMPONENTE FORMATIVO | Evaluación de los controles de ciberseguridad. |
| BREVE DESCRIPCIÓN | Mediante el estudio juicioso de este componente formativo, el aprendiz estará capacitado para reconocer aspectos importantes de la evaluación de las estrategias de ciberseguridad y su aplicación, estimando el diagnóstico, diseño, monitoreo y operación de la misma. Así mismo, podrá realizar un informe basado en la auditoría de dicha operación. |
| PALABRAS CLAVE | Alcance de pruebas, amenazas, auditoría, manuales, pruebas de efectividad. |

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

1. **TABLA DE CONTENIDO:**

**Introducción**

1. Finalidad de las pruebas
2. Pruebas y análisis
3. Tipos de pruebas de efectividad
4. Procedimiento de ejecución de pruebas de efectividad
5. Alcance de las pruebas
6. La auditoría en la ciberseguridad
7. Pasos de la auditoría en ciberseguridad
8. Tipos de auditorías
9. **INTRODUCCIÓN:**

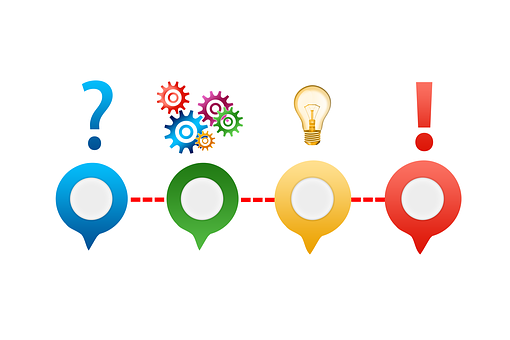
Para iniciar el desarrollo temático y conceptual de este componente formativo, es importante tener un contexto sobre lo que se tratará en este, por tal motivo, a continuación, se presenta una breve introducción, que lo contextualizará en este aprendizaje:



1. **DESARROLLO DE CONTENIDOS**

**1. Finalidad de las pruebas**

El enfoque de las pruebas de efectividad, significa comprobar o medir la eficiencia de la ejecución del modelo de seguridad en las organizaciones, para esto se han desarrollado metodologías que favorecen la comprensión y el desarrollo de las pruebas, el alcance de objetivos y el beneficio que se gana al identificar sus etapas y gestionarlas.



Nota. https://bit.ly/3o36m4j

Tales metodologías se desarrollan en diferentes etapas, ayudando a definir qué tanto ha avanzado la organización con la implementación del modelo. Así pues, por medio de la valoración de diferentes aspectos, se podrán identificar también vulnerabilidades y amenazas, a las cuales está expuesta la organización, de igual manera que las debilidades de los controles implementados.

A continuación, se presentan las etapas del procedimiento de las pruebas, según lo estipulado por la Guía metodológica de pruebas de efectividad, del MINTIC:

* **Etapas de las pruebas de efectividad**
  + **Fase de levantamiento de información**

Etapa en la que la organización hace recopilación de toda la información requerida para dar inicio a la actividad; esta información podrá estar organizada por el equipo de seguridad con el que cuente la empresa o compañía.

Con la información recolectada se buscará identificar los activos de mayor importancia en la organización, activos que tienen relación con los procesos institucionales, que serán de carácter misional o de apoyo. Otro aspecto que debe ser favorecido o facilitado por la información recopilada, es el hecho de permitir conocer el contexto de la entidad, en otras palabras, el entorno en donde serán proyectados los objetivos institucionales.

La recolección de la información es realizada por un equipo de personas que debe estar integrado al organigrama de la entidad, al mapa de procesos, política de seguridad, manual de políticas, metodología de riesgos, identificación de riesgos, planes de gestión de riesgos, entre otros. Este compendio de información es cimiento para lograr identificar la brecha de seguridad que tenga la organización.

* **Etapa de revisiones de manuales**

Cuando se habla de revisiones, se está haciendo referencia a aquellos procesos de inspección de los distintos manuales que la organización ha de realizar, para lograr la identificación de lo comprendido por los servidores públicos en seguridad, de lo realizado en seguridad en los procesos y, adicionalmente, el estado en que se encuentran las políticas institucionales.

Tales revisiones, se llevan a cabo a la vez que se analiza la documentación, mediante encuentros o reuniones con quienes están a cargo de dichos temas, con los encargados de los procesos. Se trata de una forma efectiva porque mediante las inspecciones se logra hacer identificación del porqué de las implementaciones de seguridad y los controles aplicados en la organización.

Por otra parte, ayuda a hacer comprobación de si las personas y equipos de trabajo comprenden los distintos procesos de la seguridad institucional y si se ha logrado generar y tomar conciencia de las distintas políticas de seguridad y de privacidad que la empresa tiene.

* **Etapa de identificación de amenazas**

Se refiere a la evaluación misma del riesgo de seguridad en la organización. En otras palabras, es la evaluación de las distintas acciones y actividad en donde se han visto implicadas las personas, la infraestructura y los procesos. Todo ello, con el objetivo de lograr la identificación de las distintas amenazas que sobre la entidad pueden ocurrir.

Lo que resulte de la aplicación de estas actividades favorece que se desarrollen diferentes planes de mitigación de vulnerabilidades halladas; también ayuda a orientar mejor los recursos y la ayuda a las áreas de la organización que más lo estén necesitando. Buscar estas amenazas se debe dar desde el momento en que se crean los procesos y durante todo el ciclo de vida.

El enfoque que deben tener estas actividades debe ser simple, en otras palabras, se deben descomponer los procesos a través de la evaluación manual, así se podrá tener conocimiento del funcionamiento y su interrelación con las demás actividades, como:

* Definir y clasificar los activos de la entidad, evaluando su criticidad, sus posibles vulnerabilidades técnicas, operacionales y de gestión.
* Desarrollar una matriz con las amenazas potenciales, con sus vectores de ataque.
* Elaborar planes de mitigación para cada amenaza real.

El resultado de todo esto puede ser una serie de documentos, listas o diagramas, en los cuales se plasman los análisis de riesgo de la entidad y sus planes de mitigación a través de los controles sugeridos.

1. **Pruebas y análisis**

Mediante las pruebas y análisis, las entidades identifican los diferentes riesgos que se muestran por las debilidades en la implementación del modelo de seguridad y de privacidad de la información y las vulnerabilidades que se manifiestan dada la ausencia de controles de seguridad que logren mitigar riesgos.

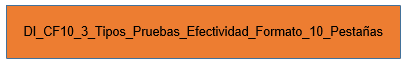


Nota. https://bit.ly/3AyDWTh

Este tipo de pruebas están orientadas a la evaluación de la estructura de seguridad de la organización; para ello, las organizaciones han de revisar diferentes frentes de trabajo como, por ejemplo, el Anexo A de la ISO 27001:2013, el ciclo de vida de la seguridad (PHVA), el nivel y estado de madurez de la organización en correspondencia con los niveles expuestos en el modelo de seguridad y privacidad y las recomendaciones para que la organización logre plasmar el concepto de **ciberseguridad**.

1. **Tipos de pruebas de efectividad**

Existen tres tipos de pruebas de efectividad, , basados en el nivel de conocimiento del entorno o de la infraestructura de la organización objetivo, estos tres tipos de prueba son los siguientes:



1. **Procedimiento de ejecución de pruebas de efectividad**

Las pruebas de efectividad pueden realizarse por medio de las siguientes acciones de manera secuencial:

A continuación, se especifican las acciones con las que se aplican las pruebas de efectividad; comprenda los aspectos importantes de cada una de ellas a través de la siguiente información:



De la aplicación procedente, responsable y oportuna de las pruebas, depende en gran medida su efectividad y su potencial aprovechamiento. Las pruebas de efectividad han de realizarse con las acciones mencionadas, siendo cada una de estas, una acción vinculada consecuentemente con las anteriores o con las posteriores.

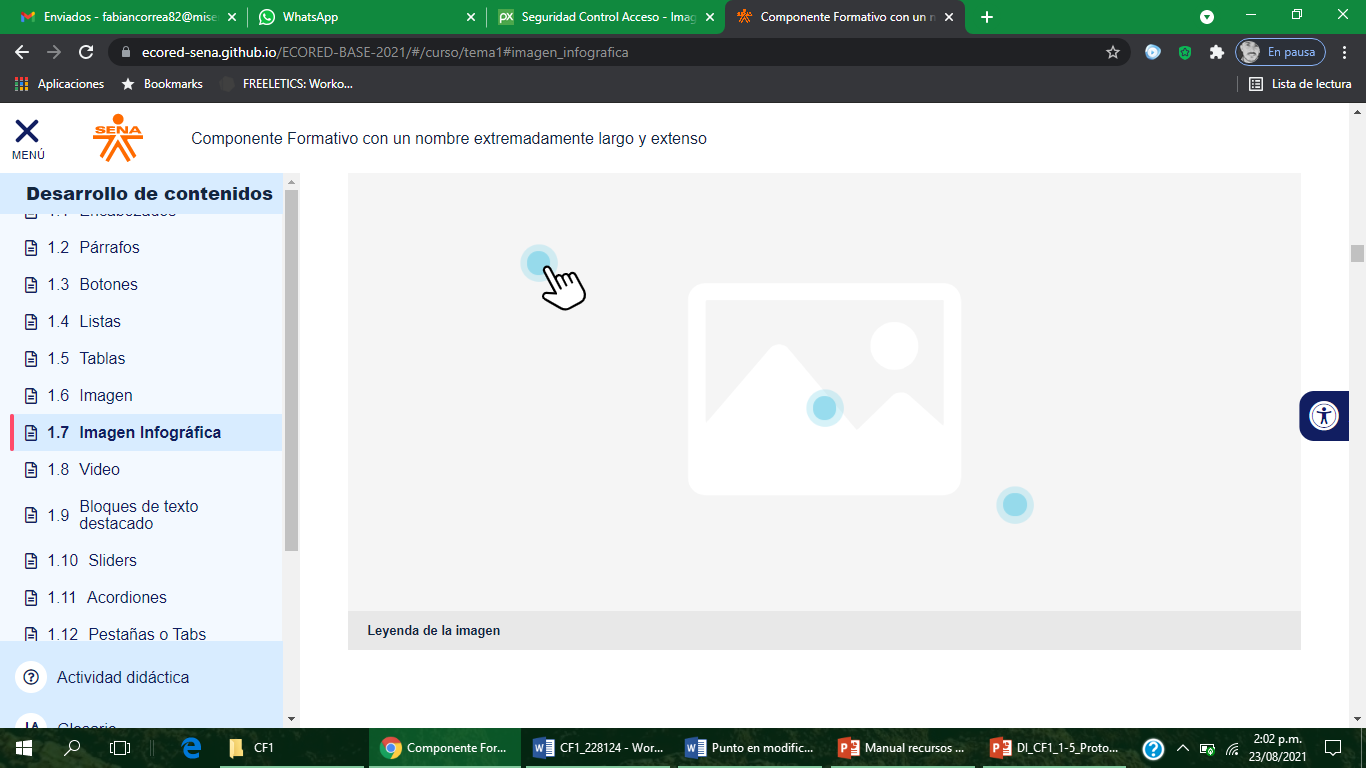
Para ahondar en los aspectos importantes relacionados con pruebas de efectividad y su procedimiento, le recomendamos estudiar la Guía No 1. **Guía metodológica de pruebas de efectividad del MinTIC**.

1. **Alcance de las pruebas**

Deberán existir una serie de reglas y otros elementos importantes para la aplicación de las pruebas de efectividad técnicas, con el fin de asegurar que tales actividades no lleguen a incurrir en fallas mayores y que, también, sea posible la afectación de la infraestructura o de las distintas operaciones de la organización.

Dentro del alcance, es posible definir aspectos como los que se muestran a continuación:





**¡Importante!**

1. **La auditoría en la ciberseguridad**

Una auditoría de ciberseguridad se considera una de las partes más importantes de un sistema de bloqueo frente a posibles ciberataques, por lo cual percibe especial interés para conocer en qué consiste y cómo proceder para mantener tales ciberataques lejos de los intereses de la organización.



Nota. https://bit.ly/3hYA6f3

Es importante realizar este tipo de auditoría, tanto interna como externa, para verificar el estado de la seguridad de la organización. En estas auditorías se inspeccionan los sistemas frente a los ataques o posibles brechas de seguridad que puedan existir.

Las siguientes, son algunas particularidades importantes que se han de tener en cuenta, en lo referente a periodicidad e intensidad, en procesos de auditorías de ciberseguridad, esto es:

DI\_CF10\_6\_LaAuditoriaEnLaCiberseguridad

1. **Pasos de la auditoría en ciberseguridad**

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

Profundice en los pasos que se deben seguir para la auditoría en ciberseguridad, explorando la información que se expone a continuación:

DI\_CF10\_7\_Pasos\_Auditoria\_Ciberseguridad\_Formato\_1\_Infografía

Cumplidos estos pasos, se explicarán, además, las acciones recomendadas que debe realizar la empresa u organización en cada uno de los puntos críticos (ante ciberataques) que se han encontrado.

1. **Tipos de auditorías**

Las auditorías pueden ser de tipo externas o internas. Se diferencian dependiendo de quién realiza la auditoría; si lo realizan compañías independientes de la organización se consideran auditorías externas y cuando son realizadas por personas que trabajan en la propia organización se denominan auditorías internas.

Las auditorías en ciberseguridad pueden clasificarse según el objetivo que persiguen o según la información proporcionada, esto es:

* **Auditoría según el objetivo:** este tipo de auditorías las puede revisar más detalladamente a continuación:

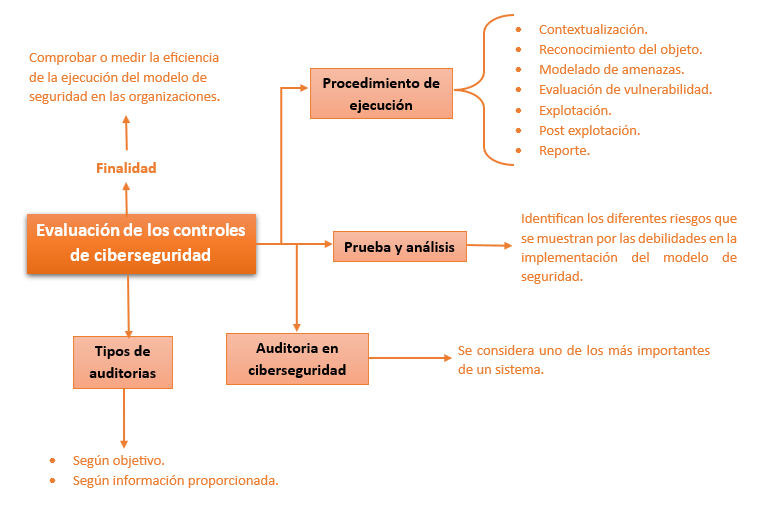


* **Auditorías según información proporcionada**: este tipo de auditorías están clasificadas en tres y las puede detallar a mayor profundidad a continuación:



1. **SINTESIS**

La ciberseguridad es un aspecto muy importante en cualquier organización, por lo que es de suma importancia tener una evaluación constante de los riesgos de algún tipo de ataque en este sentido, se debe conocer muy bien el tipo de estrategias a utilizar, con el fin de detectar las posibles amenazas y con esto implementar acciones que permitan mitigar o corregir los controles de ciberseguridad establecidos por la empresa u organización. Al igual que reconocer los diferentes tipos de auditorías y sus respectivos informes que permitan una mejor toma de decisiones en este aspecto.



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

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la actividad | Evaluación de la ciberseguridad |
| Objetivo de la actividad | Determinar el procedimiento a seguir en posibles casos de ataques que hayan sido detectados luego del seguimiento y evaluación constante a las estrategias de ciberseguridad implementadas como resultado de las auditorías y de la interpretación de los informes respectivos. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Carpeta Anexos |

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 |
| 4. Procedimiento de ejecución de pruebas de efectividad. | Ministerio de Tecnologías de la Información y Comunicaciones (2016). *Guía Metodológica de Pruebas de Efectividad.* | Otro: Guía técnica | <https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf> |

1. **GLOSARIO:**

|  |  |
| --- | --- |
| TÉRMINO | SIGNIFICADO |
| Auditoría: | una auditoría es un proceso de verificación y/o validación del cumplimiento de una actividad según lo planeado y las directrices estipuladas. |
| Auditoría externa: | auditoría realizada por compañías independientes de la organización o aquellas que son realizadas por personas ajenas a la empresa, contratadas para ello. |
| Levantamiento de información: | etapa de las pruebas de efectividad en la que la organización ha de hacer recopilación de toda la información requerida para dar inicio a la actividad; tal información podrá estar organizada por el equipo de seguridad con el que cuente la empresa o compañía. |
| Modelado de amenazas: | esta acción establece la relación entre el atacante y el activo intentando definir el beneficio que puede alcanzar el atacante si logra penetrar el sistema y afectar la información de alguna manera. |
| Pruebas de efectividad: | acciones que se enfocan en establecer una línea base del estado de seguridad de la organización, con el fin de facilitar la identificación de la brecha en la implementación del modelo de seguridad. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Ciberseguridad y riesgos digitales (2020*). Normas ISO en auditoría informática: Cuáles son las más importantes.* EALDE. <https://www.ealde.es/iso-auditoria-informatica/>

Ministerio de Tecnologías de la Información y Comunicaciones (2016). *Guía de Auditoría.* <https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf>

Ministerio de Tecnologías de la Información y Comunicaciones (2016). *Guía Metodológica de Pruebas de Efectividad.* <https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.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) | Pablo Cesar Pardo Ortiz | 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 Diseño y Metrología | Septiembre 2021 |
|  | Sandra Patricia Hoyos Sepúlveda | Revisión y corrección de estilo | Centro para la Industria de la Comunicación Gráfica - 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) | Gloria Amparo López Escudero | 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. |