**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Tratamiento de riesgos de ciberseguridad en la micro, pequeña y mediana empresa |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501099 - Probar la solución del *software* de acuerdo con parámetros técnicos y modelos de referencia. | RESULTADOS DE APRENDIZAJE | 220501099-01. Planificar la evaluación de la ciberseguridad de acuerdo con las necesidades de las MiPymes. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 007 |
| NOMBRE DEL COMPONENTE FORMATIVO | Auditorías a las estrategias de ciberseguridad |
| BREVE DESCRIPCIÓN | Este componente formativo aborda aspectos clave de las estrategias de seguridad de los activos más importantes para las organizaciones. Con su estudio responsable, el aprendiz se afianzará en lo relacionado con enfoques y cambios para seguridad, prevención de incidentes de ciberseguridad, atención, programas de auditoría y monitoreo efectivo. |
| PALABRAS CLAVE | Aseguramiento de ciberseguridad, auditorías cibernéticas, controles de ciberseguridad, riesgos cibernéticos |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | 2 - Ciencias naturales, aplicadas y relacionadas |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:** 
   * + 1. **La auditoría cibernética**
   1. Técnicas de auditoría
   2. Tipos de auditoría
   3. Definiciones y elementos fundamentales de la auditoría
   4. Consideraciones importantes para una auditoría
   5. Principios de la auditoría
   6. Fases de la auditoría
2. **Pruebas de vulnerabilidad cibernética**
   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
3. **INTRODUCCIÓN**

Aquí inicia el estudio del componente formativo “**Auditorías a las estrategias de ciberseguridad**”. En este punto, visualice con atención el video que se muestra en seguida y comience esta experiencia de aprendizaje, en la que se le desean todos los éxitos. ¡**Adelante**!

DI\_CF07\_0\_Video\_Introduccion

1. **DESARROLLO DE CONTENIDOS:**

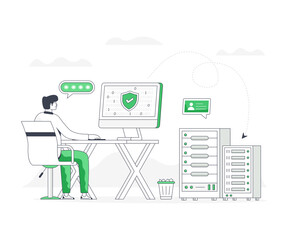
Los contenidos de este CF07, reusará elementos temáticos ya trabajados y producidos del programa 228124 Implementación y operación de la ciberseguridad. FAVOR PRESTAR ATENCIÓN A LOS COMENTARIOS EN CADA PUNTO.

Enlace al CF09 (228124) en la carpeta “FinalXVirtualizar” es: <https://drive.google.com/drive/folders/1F8MEEYhgBnJNCfgT9_QqQnhav-OiX26s>

Enlace al CF10 (228124) en la carpeta “FinalXVirtualizar” es: <https://drive.google.com/drive/folders/126RW4JF3oCuXmKQAekJmUTOsU0xfsecX>

* + - 1. **La auditoría cibernética**

A medida que las organizaciones adoptan nuevas tecnologías digitales, aumenta el riesgo de ser objeto de ciberataques. La mayor complejidad de la red que surge como resultado de la innovación digital, a menudo crea nuevas brechas en la red para que las exploten los ciberadversarios.



Si no se controlan, estos riesgos pueden socavar los objetivos organizacionales, por lo que es fundamental que las empresas cuenten con programas efectivos de ciberseguridad.

Se debe tener presente que:

* Un componente clave para el éxito de estos programas es la administración de auditorías de ciberseguridad.
* La administración periódica de auditorías de ciberseguridad ayuda a las organizaciones a identificar brechas en su infraestructura de ciberseguridad.
* Las organizaciones también pueden utilizar las auditorías para evaluar su cumplimiento de diversas leyes y reglamentos.
* Con un programa de auditoría de seguridad cibernética establecido, las empresas pueden monitorear de manera efectiva su postura de seguridad a medida que sus redes crecen y se vuelven más complejas.

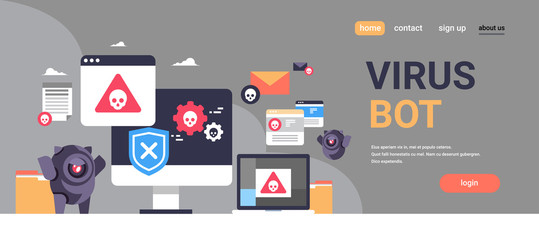
Para los subnumerales (1.1 al 1.6) de este componente, se tomarán elementos del CF09 del programa (228124), como se explica en los comentarios siguientes.

Enlace al CF09 (228124) en la carpeta “FinalXVirtualizar” es: <https://drive.google.com/drive/folders/1F8MEEYhgBnJNCfgT9_QqQnhav-OiX26s>

* 1. **Técnicas de auditoría**
  2. **Tipos de auditoría**
  3. **Definiciones y elementos fundamentales de la auditoría**
  4. **Consideraciones importantes para una auditoría**
  5. **Principios de la auditoría**
  6. **Fases de la auditoría**

1. **Pruebas de vulnerabilidad cibernética**

Las empresas se enfrentan a una amplia gama de amenazas de ciberseguridad al volverse más dependientes de internet, el acceso remoto y la tecnología en general. Para mantener seguros sus datos y aplicaciones esenciales, deben identificar las vulnerabilidades potenciales que los ciberdelincuentes podrían explotar en nombre de sus objetivos.



Mediante el uso de una combinación de herramientas de prueba de vulnerabilidades y técnicas de escaneo, los expertos en seguridad cibernética pueden ayudarlos a identificar y reforzar las brechas y debilidades de seguridad.



¡**Importante**!

¡**Atención**!

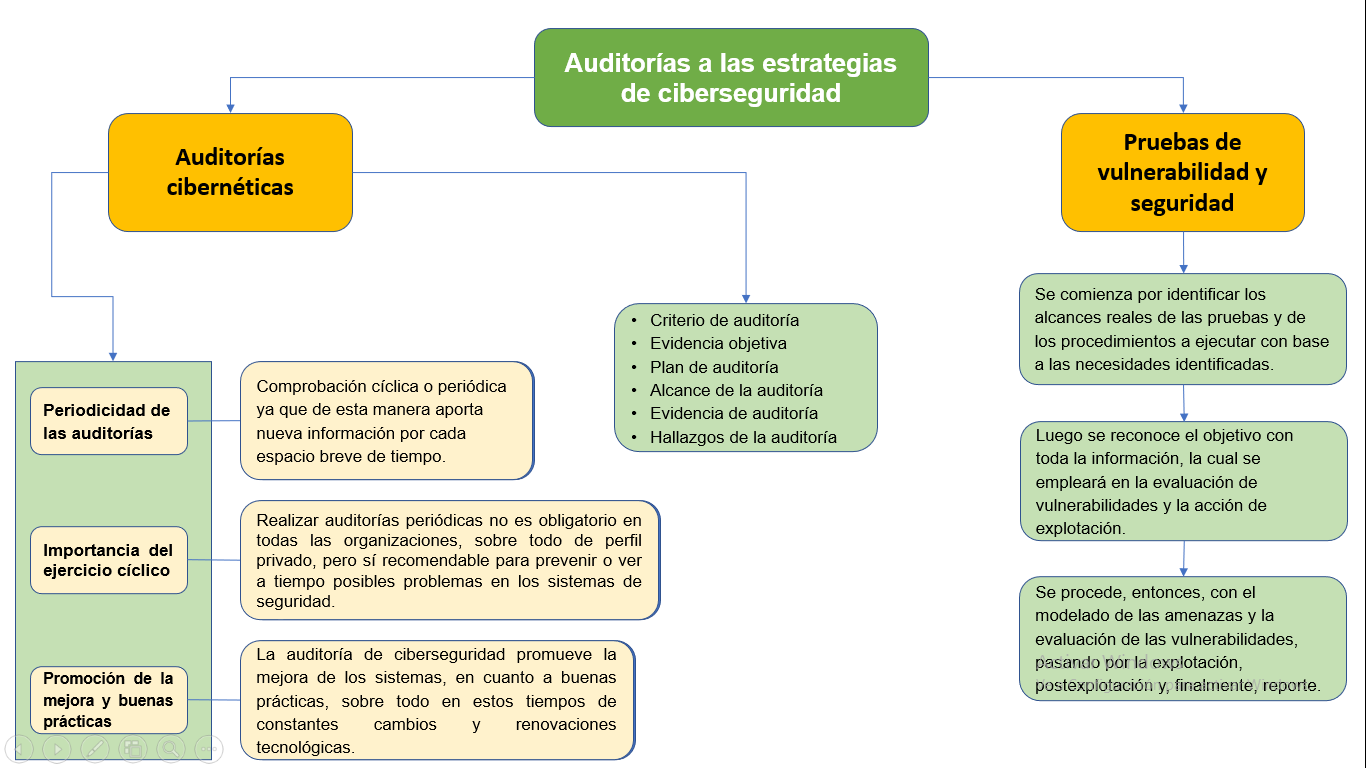
Para los subnumerales (2.1 al 2.6) de este componente, se tomarán elementos del CF10 del programa (228124), como se explica en los comentarios siguientes.

Enlace al CF10 (228124) en la carpeta “FinalXVirtualizar” es: <https://drive.google.com/drive/folders/126RW4JF3oCuXmKQAekJmUTOsU0xfsecX>

* 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

1. **Síntesis**

Con este punto, se finaliza el estudio de los contenidos de este componente formativo. Es momento de hacer síntesis, para lo cual se debe analizar el esquema que se muestra a continuación y registrar esta síntesis en la libreta personal de apuntes. Además, se deben repasar los temas que considere necesario. ¡**Adelante**!



1. **ACTIVIDADES DIDÁCTICAS**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Auditando la ciberseguridad |
| Objetivo de la actividad | Reafirmar los conceptos y procedimientos para las auditorías a estrategias de ciberseguridad de la empresa, con base en los contenidos estudiados en este componente formativo. |
| Tipo de actividad sugerida | Selección de única respuesta. |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Actividad\_Didactica\_1  (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 |
| Procedimiento de ejecución de pruebas de efectividad. | 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> | Otro: Guía técnica | <https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf> |
| Principios de la auditoría | Organización Internacional de Normalización (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad. (ISO 27001).* ISO.<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. |
| Auditoría | 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. |
| Escala | rango de valores organizados con los cuales se evalúa un atributo. |
| Evidencia | información suficiente que respalda alguna acción. |
| Indicador | unidad 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. |
| Modelado de amenazas | acción que 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. |
| SGSI | Sistema de Gestión de la Seguridad de la Información. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

Avansis (2020). *Auditoría de ciberseguridad*. Avansis. <https://www.avansis.es/ciberseguridad/auditoria-de-ciberseguridad/>

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

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

ISO (2020). *Fase 8 auditoría interna según ISO 27001. (ISO 27001).* ISO. [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).* ISO. [https://e-collection-icontec-org.bdigital.sena.edu.co/normavw.aspx?id=75245](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.* Ministerio de Tecnologías de la Información y Comunicaciones <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.* Ministerio de Tecnologías de la Información y Comunicaciones <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).* ISO. <https://www.iso.org/standard/54534.html>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha |
| Autor (es) | Ronald Alexander Vacca Ascanio | Experto Temático | Regional Norte de Santander - Centro | 15/09/2022 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Regional Norte de Santander – Centro de la Industria, la Empresa y los Servicios | Octubre de 2022 |
| Carolina Coca Salazar | Asesora Metodológica | Regional Distrito Capital- Centro de Diseño y Metrología | Octubre de 2022 |
|  | Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander – Centro Industrial del Diseño y la Manufactura | Octubre de 2022 |
|  | José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Noviembre del 2022. |

1. **CONTROL DE CAMBIOS**

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