**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Desarrollo e implementación de soluciones para la transformación digital |
| --- | --- |

| COMPETENCIA | 220501108 - Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501108-01 - Determinar métodos de análisis y valoración de riesgos de ciberseguridad, de acuerdo con estándares internacionales y normatividad nacional. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF01 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Análisis y valoración de riesgos de ciberseguridad |
| BREVE DESCRIPCIÓN | Con este componente, el aprendiz profundizará en los fundamentos necesarios para realizar el análisis y valoración de riesgos, diagnosticando el estado actual de la seguridad de la información en una organización, como elementos fundamentales para definir un plan de tratamiento adecuado. |
| PALABRAS CLAVE | Auditoría forense, ciberseguridad, *hacking*, informática forense, seguridad digital |

| ÁREA OCUPACIONAL | 6 - Ventas y servicios |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:**

**Introducción**

**1. Fundamentos de redes y *networking***

1.1 Conceptos

1.2 Características

1.3 Tipos de redes

1.4 Modelo OSI

1.5 Protocolo TPC/IP

1.6 Protocolos IPv4 e IPv6

1.7 Enrutamiento IP

**2. Normatividad y estándares: ciberseguridad**

**3. Normatividad y estándares: seguridad de la información**

**4. Marco legal**

**5. Marco jurídico**

**6. Tipificación de delitos informáticos en Colombia**

**7. Activos de Información**

7.1 Características de los activos de información

7.2 Tipos de activos de información

7.3 Técnicas de valoración de activos

**8. Amenazas y vulnerabilidades**

8.1 Características y tipos de amenazas y vulnerabilidades

8.2 Vulnerabilidades del sistema

8.3 Amenazas de ataques de denegación de servicio

8.4 Vulnerabilidades producidas por contraseñas

8.5 Vulnerabilidades producidas por usuarios

8.6 Otras amenazas informáticas

**9. Riesgos**

9.1 Niveles de riesgo

9.2 Características, impacto y análisis de riesgo

9.3 Técnicas de tratamiento de riesgos

**10. *Ethical hacking***

10.1 Objetivos del *ethical hacking*

10.2 Tipos de pruebas de penetración

1. **INTRODUCCIÓN**

En este componente se abordarán los conceptos y fundamentos de las tecnologías de información y la seguridad de la información, reconociendo la normatividad, marcos y estándares para una adecuada gestión de riesgos de ciberseguridad y la tipificación de delitos informáticos en el contexto colombiano.

Por lo anterior, a través del siguiente video se presentan las temáticas que se abordarán en el componente formativo, destacando la importancia en los entornos empresariales, de esta manera se invita al aprendiz a disponerse para el proceso de aprendizaje:



1. **DESARROLLO DE CONTENIDOS:**

1. Fundamentos de redes y *networking*

1.1 Conceptos

1.2 Características

1.3 Tipos de redes

1.4 Modelo OSI

1.5 Protocolo TPC/IP

1.6 Protocolos IPv4 e IPv6

1.7 Enrutamiento IP

2. Normatividad y estándares: ciberseguridad

3. Normatividad y estándares: seguridad de la información

4. Marco legal

5. Marco jurídico

6. Tipificación de delitos informáticos en Colombia

7. Activos de Información

7.1 Características de los activos de información

7.2 Tipos de activos de información

7.3 Técnicas de valoración de activos

8. Amenazas y vulnerabilidades

8.1 Características y tipos de amenazas y vulnerabilidades

8.2 Vulnerabilidades del sistema

8.3 Amenazas de ataques de denegación de servicio

8.4 Vulnerabilidades producidas por contraseñas

8.5 Vulnerabilidades producidas por usuarios

8.6 Otras amenazas informáticas

9. Riesgos

9.1 Niveles de riesgo

9.2 Características, impacto y análisis de riesgo



**9.3 Técnicas de tratamiento de riesgos**

La etapa de tratamiento de los riesgos consiste en comparar los niveles del riesgo encontrados durante los procesos de identificación y análisis, con los criterios previamente establecidos. En esta etapa se realiza la priorización de los riesgos para futuras acciones, igualmente se contemplan las decisiones a tomar, conforme a las consideraciones de apetito o tolerancia al riesgo desde la alta dirección.

Si el riesgo resultante es considerado bajo o aceptable, debe ser controlado con un mínimo tratamiento, sin dejar de ser monitoreado periódicamente, para asegurar que se mantengan en niveles aceptables.

Una vez se obtiene el mapa de riesgos, se sigue con el paso de tratamiento, donde se derivan planes de mejora a desarrollar, reconociendo cuáles serán las acciones para el tratamiento del riesgo, valorando estas opciones y preparando los planes de tratamiento del riesgo e implantarlos.

Los siguientes son los mecanismos para el tratamiento de los riesgos:



Una vez identificadas las acciones a realizar, es necesario llevar a cabo la implementación de los planes de tratamiento; lo ideal es que la responsabilidad por el tratamiento del riesgo recaiga en aquellos más capaces de controlar el riesgo o que puedan tomar decisiones sobre estos.

Llevar a feliz término la implementación de un plan de tratamiento del riesgo requiere un mecanismo gerencial muy efectivo con la suficiente jerarquía en la organización, de modo que puedan asignarse las responsabilidades individuales de las acciones y monitorearlas de acuerdo con el criterio especificado.

En las técnicas del sistema de tratamientos de riesgos se debe garantizar lo siguiente:

• Un funcionamiento correcto de la organización.

• Revisiones internas efectivas.

• Controles legales actualizados con las leyes y reglamentos vigentes.

Además, se pueden establecer estrategias para evitar los riesgos y minimizar el impacto o la frecuencia de ocurrencia del riesgo; así, al analizar el nivel del riego se podrá tomar la decisión para el mecanismo de tratamiento y la implementación del control para mitigarlo, articulando todo esto, mediante la política de control y con el plan de mejora de la organización.

| Es importante destacar que el paso final de la gestión de riesgos está asociado al monitoreo y revisión, donde es necesario monitorear los riesgos, la efectividad del plan de tratamiento del riesgo, las estrategias y el sistema gerencial establecido para controlar la implementación. |  |
| --- | --- |

Las revisiones continuas son esenciales para asegurar que el plan de tratamiento permanezca consistente con la realidad, por lo que es necesario implementar mecanismos periódicos de monitoreo, tanto para las implementaciones de tratamiento, controles y riesgos de niveles altos, como para la definición y el seguimiento a todo en un mapa de riesgos.

10. *Ethical hacking*

10.1 Objetivos del *ethical hacking*

10.2 Tipos de pruebas de penetración



1. **SÍNTESIS**

A continuación, se presenta el diagrama que representa el resumen de las temáticas que están desarrolladas en el componente formativo:



1. **ACTIVIDADES DIDÁCTICAS (Se debe incorporar mínimo 1 – no es opcional)**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Autoevaluación de conceptos de análisis y valoración de riesgos de ciberseguridad |
| Objetivo de la actividad | Identificar los conceptos acerca del análisis y valoración de riesgos de ciberseguridad con el fin de afianzar los conocimientos adquiridos en el componente. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo\_CF01\_ActividadDidactica |

**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 |
| --- | --- | --- | --- |
| 2. Normatividad y estándares: ciberseguridad  3. Normatividad y estándares: seguridad de la información | ISO. (2018). *Seguridad de la información, ciberseguridad y protección de la privacidad* (ISO 27005)*.* | Norma / Documento | <https://www.iso.org/standard/75281.html> |
| 2. Normatividad y estándares: ciberseguridad  3. Normatividad y estándares: seguridad de la información | ISO. (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad* (ISO 27002). | Norma / Documento | <https://www.iso.org/standard/54533.html> |
| 8. Amenazas y vulnerabilidades | Gómez, V., Á. (2015). *Auditoría de seguridad informática*. RA-MA Editorial. | Libro | <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/62464?page=14> |
| 9. Riesgos | Gómez V., Á. (2015). *Seguridad en equipos informáticos*. RA-MA Editorial. | Libro | <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/62466?page=1> |
| 9.2. Características, impacto y análisis de riesgos | ISO (2018). *Gestión del riesgo. Directrices (*ISO 31000). | Norma / Documento | <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es> |
| 10. *Ethical Hacking* | Astudillo, B. K. (2019). *Hacking ético: ¡Cómo* *convertirse en hacker ético en 21 días o menos!* Ediciones de la U. | Libro | <https://www-ebooks7-24-com.bdigital.sena.edu.co/?il=10047&pg=19> |

1. **GLOSARIO:**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Activos de información | están relacionados con la seguridad de la información, hacen referencia a cualquier información o dispositivo que tenga que ver con el tratamiento de esta y que sea de valor para la organización. |
| Auditoría | acción que consiste en emitir criterios y opiniones profesionales acerca de cualquier objeto de análisis, del cual se espera que represente de manera adecuada la realidad que pretende reflejar; también sobre si cumple o no con las condiciones y funcionalidades que se han acordado en el nivel de servicio. |
| Auditorías internas de SGSI | el principal objetivo de la auditoría de SGSI es investigar, de manera objetiva, si existe algo que esté mal realizado. El auditor interno tiene que ser una persona capacitada, con su conocimiento debe poder descubrir si algo se hace mal dentro de la organización. Realizando un buen trabajo, correctivo y/o preventivo, entonces la auditoría interna de SGSI mejorará su seguridad. |
| Ciberseguridad | conjunto de metodologías, medidas y controles destinados a gestionar la seguridad de la información de una organización y/o de la información en general. |
| *Ethical hacking* | proceso que se da al interior de las organizaciones a través del cual se exploran las vulnerabilidades existentes en los sistemas, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc. |
| *Malware* | *software* diseñado para comprometer la seguridad de la información, como la utilidad y preservación del equipo. |
| Riesgo | posibilidad de sufrir una afectación por causa de factores externos o internos. El riesgo es un peligro latente que puede o no materializarse. En el orden informático y de ciberseguridad, los riesgos no son distintos, contemplan las vulnerabilidades y las amenazas y pueden ser controlados, tratados, mitigados, prevenidos y, en algunos casos, eliminados. |
| Seguridad informática | rama del saber que tiene ocupación en el diseño de normas y criterios, procedimientos y métodos, técnicas y estrategias, dirigidos a lograr seguridad y confiabilidad en un sistema de información. |
| Tratamiento de riesgos | medidas y controles que se implementan para mitigar el impacto o la frecuencia de ocurrencia de un riego. |
| Virus informático | *software* que se instala en un dispositivo sin el consentimiento del usuario, con el fin de alterar el funcionamiento. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Cloud Education. (2021). *Redes.* IBM. <https://www.ibm.com/co-es/cloud/learn/networking-a-complete-guide#toc-trminos-y--ZhqcZz4r>

Corporation and/or its affiliates. (2010). *Modelo de referencia OSI*. ORACLE. <https://docs.oracle.com/cd/E19957-01/820-2981/ipov-8/index.html>

Ministerio de Hacienda y Administraciones Públicas de España. (2012). *Metodología de análisis y gestión de riesgos de los sistemas de información*. <https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf>

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2017). *Guía de transición IPv4 a IPv6 para Colombia*. <https://www.mintic.gov.co/portal/715/articles-162301_guia_transicion_ipv4_ipv6.pdf>

Organización de Estados Americanos. (2019). *Ciberseguridad marco NIST. Un abordaje integral de la ciberseguridad*. <https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf>

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

Projete. (s.f.). *Amenazas y vulnerabilidades*. <https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/>

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 | Agosto de 2021 – CF de reúso |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Centro agropecuario La Granja, Regional Tolima | Agosto de 2021 – CF de reúso |
| Carolina Coca Salazar | Revisora metodológica y pedagógica | Regional Distrito Capital- Centro de Diseño y metrología | Agosto de 2021 – CF de reúso |
| Cesar Antonio Villamizar Núñez | Experto Temático | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Septiembre de 2022 |
| Giovanna Andrea Escobar Ospina | Diseñador Instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Septiembre de 2022 |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital – Centro de Diseño y Metrología | Septiembre de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura. | Septiembre de 2022 |
|  | José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital – Centro de Diseño y Metrología. | Octubre del 2022. |

1. **CONTROL DE CAMBIOS**

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

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

**Nota:**Para la propuesta instruccional se deben tener en cuenta las métricas desarrolladas en el equipo:

<https://drive.google.com/drive/u/1/folders/1UiJvaklSCICR4BaQ7ga_q04JFa53h_u_>