**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Caracterización de componentes en ciberseguridad |
| --- | --- |

| COMPETENCIA | 220501108 - Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501108-04 - Proponer estrategias de mejora continua de acuerdo con el análisis realizado. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF04 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Dispositivos de control e informática forense |
| BREVE DESCRIPCIÓN | En este componente formativo, se abordarán los diferentes dispositivos de control utilizados para evitar ataques informáticos y la aplicación de la informática forense. |
| PALABRAS CLAVE | ciberseguridad, *firewall*, forense, IPS, parchado virtual |

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

1. **Tabla de contenidos**

**Introducción**

* 1. **Dispositivos de control y monitoreo**
  2. **Informática forense**
  3. **Análisis de evidencia digital**
  4. **Certificaciones profesionales en ciberseguridad**

**Síntesis**

1. **Introducción**

La seguridad de la información es un aspecto importante dentro de las organizaciones, a tal punto que muchas de ellas destinan millones de dólares en la aplicación y puesta en marcha de procesos que aseguren los tres componentes de riesgo establecidos en la norma ISO 27001: integridad, disponibilidad e integridad de la información, factores determinantes para el manejo de la información dentro de una organización. En el siguiente video, se aprecia de manera genérica cada una de las temáticas a desarrollar alrededor de los dispositivos de control y su aplicación en la informática forense.



**C. Desarrollo de contenidos**

1. **Dispositivos de control y monitoreo**

| La seguridad de la información está tomando una importancia bastante significativa en las organizaciones. Cabe destacar que, hasta no hace muchos años, este aspecto solo era un valor agregado en las organizaciones. Sin embargo, dejó de serlo para convertirse en uno de los pilares de la organización, ya que esta protege uno de los activos más valiosos: la información. De ahí, la necesidad de implementar herramientas y procesos para procurar su protección y buen manejo. |  |
| --- | --- |

Una de las principales tecnologías de protección y fundamental en la implementación para la ciberseguridad es el *firewall* o también llamado cortafuegos. El video que se presenta a continuación desarrolla en qué consiste su uso.



De igual forma, los IPS, *sistemas de protección de intrusos*, se encuentran en dos presentaciones: *hardware* y *software.* Estos se encargan de realizar un escaneo en la red de información de una organización y son capaces de detectar alguna situación sospechosa y dar alertas sobre la situación que se esté presentando, mediante el envío de correo electrónico o, en algunos casos, mensajes de texto, dependiendo de su configuración. Es importante destacar que los IPS están en la capacidad de bloquear o controlar el tráfico de la red de acuerdo con situaciones detectadas.

| Mujer trabajando en superposición gráfica de red informática Foto gratis | En la actualidad, los IPS utilizan algoritmos de inteligencia artificial para poder predecir una situación de riesgo, o, de acuerdo con unos patrones detectados, bloquear el acceso a ciertos dispositivos o segmentos de la red de datos donde se encuentran los dispositivos críticos o con la información que debe estar protegida. |
| --- | --- |

Estos sistemas tienen la capacidad de detectar y guardar en una base de datos la información de cierto usuario y su comportamiento, lo que le permite en próximas ocasiones verificar si se trata del mismo usuario y automáticamente detectarlo y/o bloquearlo. Lo anterior se conoce como *Machine Learning,* que permite a una máquina utilizar algoritmos de aprendizaje; almacenan información y luego la utilizan para ejecutar funciones específicas.

Los IPS se clasifican de la siguiente manera.



Ahora bien, adicionales a las herramientas anteriormente expuestas, existen otros procesos que permiten monitorear y controlar el manejo que se le da a la seguridad de la información en una organización.



1. **Informática forense**

La informática forense es una rama de la ciencia de la computación que se especializa en el análisis y toma de evidencia en los escenarios donde se cometen delitos informáticos. En muchos aspectos, se puede comparar la informática forense con las labores que se ven dentro de las películas, donde se examinan escenarios y se perfilan personas, se toma evidencia en equipos, etc. Todo esto puede sonar un poco a ciencia ficción, pero muchos de esos procesos son reales y hacen parte de esta disciplina.

| Cibernético, Seguridad, Internet, Red, Tecnología | Hoy la informática forense ha tomado un nivel de aceptación en el que es uno de los procesos llevados a cabo en miles de organizaciones a lo largo del mundo, ya que permite establecer las causas, motivos y condenar los diferentes actos vandálicos que se cometen contra la infraestructura tecnológica de una organización. |
| --- | --- |

Dentro de la informática forense, se encuentran diferentes actividades y procesos que se realizan, los cuales tienen como objetivo principal esclarecer las causas de un delito informático y armar una hipótesis de cómo ocurrieron los hechos.

|  |  |
| --- | --- |
| En la actualidad, la Policía Nacional es el organismo encargado de realizar estas labores mediante los peritos informáticos, los cuales se encargan de recolectar y realizar las actividades forenses a nivel nacional. | |

En el caso de Colombia, país regido por leyes, tanto a nivel penal como administrativas, los delitos informáticos están estipulados en la Ley 1273 de 2009, llamada también Ley de delitos informáticos, en la cual se modifica el Código Penal para sancionarlos. Se instauran diferentes tipos de cláusulas, multas y hasta sanciones de tipo carcelario, dependiendo del tipo de delito cometido, expresadas en los diferentes artículos de esta Ley. A continuación se mencionan algunos de ellos, los cuales están distribuidos en dos capítulos.

**Figura 1**

*Atentados informáticos en la Ley 1273 de 2009*



|  |  |
| --- | --- |
| Gracias a estos mecanismos impuestos en la ley penal, se ha logrado establecer el principio fundamental para el acceso de la información y de los datos. Las empresas de cualquier tipo de proceso administran y manejan determinada información, ya sea desde un hospital hasta la misma Registraduría. La implementación de esta ley permite regular el uso de la información de los usuarios y personas, las cuales son dueñas y propietarias de la misma. En otras palabras, quiere decir que todas las empresas que utilicen información de terceros deben velar por resguardar la información de manera tal que no infrinjan ninguno de los artículos antes expuestos. | |

| Educados, Libro, Libro Club De Discusión imagen png - imagen transparente  descarga gratuita | LEY 1273 de enero de 2009  Se sugiere explorar los demás artículos contemplados en esta Ley, recurso que se encuentra en el material complementario. |
| --- | --- |

Ahora bien, en el caso de la informática forense, se pueden encontrar diversos factores fundamentales que permiten realizar un seguimiento a los procesos en delitos informáticos. Cabe decir que el proceso de la informática forense incluye un conjunto de actividades que se deben realizar y protocolos que también se deben llevar a cabo para efectuar este proceso; no obstante, aunque los procesos por delitos de la seguridad de la información en algunos casos quedan impunes, se resalta el hecho de que los procesos que se llevan a cabo para poder esclarecer los sucesos son rigurosos y muy aplicables, tal como se presenta en el siguiente gráfico interactivo.

**Figura 2**

*Proceso forense*



**3**. **Análisis de evidencia digital**

El procedimiento en la toma de evidencias debe estar dentro de un marco de manejo para evitar dañar o corromper los datos y que luego no puedan ser usados en procesos legales. Las evidencias requieren un proceso de manejo muy riguroso, ya que de esta dependen los procesos que se tomarán y que pueden generar inocencia o culpabilidad en una persona, de acuerdo con los hallazgos que se realicen.

| Evidencia digital | Es todo elemento o parte utilizada en un sistema de tratamiento de información que provee acceso a un medio tecnológico o una parte en él, tales como archivo, fichero, memoria usb, equipo de computo, llave de acceso, usuario, contraseña, etc. Una evidencia digital es todo aquello que se almacena o procesa mediante medios digitales o sistemas informáticos. |
| --- | --- |

A continuación, se presentan algunas características específicas que toda evidencia digital contiene.



Ahora bien, para el caso de la estandarización de las respuestas a incidentes, se establece la generación de una forma, protocolo o procedimiento que se debe realizar para garantizar la respuesta adecuada al usuario o al proceso que se lleva a cabo; es decir, se tiene que seguir un lineamiento de acuerdo con unos objetivos definidos, los cuales se tratan en el siguiente recurso.



El proceso de análisis de una evidencia digital, en el caso de ocurrir un incidente, se puede sintetizar de esta manera.

**Figura 3**

*Gestión de incidentes*



La gestión de incidentes se puede abordar desde los siguientes estándares de proceso:

**Figura 4**

*Estándares de gestión*



**4. Certificaciones profesionales en ciberseguridad**

El mercado laboral hoy día es bastante exigente, a diferencia de otros momentos y circunstancias en que solo bastaba con un entrenamiento donde los profesionales adquirían un conocimiento teórico - práctico para luego ejercer y colocarlo en práctica en la industria. Hace unos años, por el tema de competitividad en las empresas a nivel mundial, se creó la figura de certificación, la cual no solo dice que una persona es competente en un área o conocimiento específico, sino que está avalado por una empresa que da fe de la aplicación de normas y estándares de calidad al momento de ejecutar una labor.

|  | Como bien se sabe, las normas y estándares se crean para mejorar los niveles de calidad de un producto o servicio; por eso, la certificación es un *plus* que recibe un profesional en su área de desempeño. |
| --- | --- |

El mercado laboral, para aquellos que se dedican o quienes están interesados en incursionar, ofrece en la ciberseguridad un panorama bastante interesante, ya que se carece de personal certificado que sepa aplicar sus normas y componentes de manera adecuada; por tanto, existen posibilidades de encontrar buenas ofertas y oportunidades de empleo, ya que, además, por su tendencia, se considera de alta demanda en las organizaciones, en parte porque estas deben certificarse en el manejo y tratamiento de la información. De tal forma que su personal encargado y, por ende, su departamento de seguridad velen correctamente tanto por la seguridad como por el buen uso de la información que utiliza la empresa en sus procesos de negocio.

Actualmente, existe una gama bastante variada de certificaciones en cuanto a la ciberseguridad y la seguridad informática. A continuación, se comentan algunas de ellas y los respectivos enfoques para los profesionales que deseen ingresar en este mundo de la ciberseguridad.

**Figura 5**

*Certificaciones*

|  |  |
| --- | --- |
| Estas son las certificaciones con las que más profesionales cuentan, por lo tanto, son unas de las más demandadas por las organizaciones. Sin embargo, también cabe decir que estas certificaciones se encuentran a nivel esencial en las organizaciones, es decir, contienen los conocimientos técnicos y prácticos para la administración de la información y, por ello, se utilizan mucho en las organizaciones. Un profesional certificado trae consigo un impacto positivo en las oportunidades de empleo y salarios, este último se ve reflejado en mayor medida en países como Estados Unidos y países asiáticos. | |

Ahora bien, por otra parte, se debe tener presente que todas estas certificaciones tienen un grado de complejidad para su obtención, lo cual depende del nivel de conocimiento de cada profesional. A modo de resumen, se presenta cómo un profesional puede ir escalando en su formación hasta lograr las certificaciones más apetecibles en el mercado.



De acuerdo con lo mencionado anteriormente, se puede llegar a la conclusión de que las certificaciones están orientadas no solo al fortalecimiento de los conocimientos del profesional, sino que adicionalmente mejora sus condiciones de oportunidad laboral y mejoramiento salarial, aunque no se puede dejar de lado que las empresas, hoy día, por temas de calidad, deben contar con personal no solo profesional, sino certificado, para que estas puedan alcanzar, a su vez, certificaciones que les exige el mercado actual. Por lo tanto, esto se convierte en un beneficio para ambas partes.

**D. Síntesis**

Se ha llegado al final del componente, en el cual se abordaron temas relacionados con la importancia de los procesos forenses, el manejo de evidencias y el procedimiento que se debe llevar a cabo por parte del personal técnico para garantizar la calidad e integridad de las mismas. También se trataron temáticas relacionadas con las certificaciones de la seguridad de la información y su importancia actual para las organizaciones. A continuación, se presenta un resumen visual de lo abarcado.

**Figura 6**

*Síntesis*

**E. Actividades didácticas**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Cuestionario |
| Objetivo de la actividad | Validar conocimientos y conceptos aprendidos en el componente. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | *Formatos DI: CF03\_Actividad didáctica* |

**F. 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 |
| --- | --- | --- | --- |
| Informática forense | Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los  datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*.* Enero 5 de 2009. | Ley | <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf> |
| Informática forense | UNIR | La Universidad en Internet. (2018). *La práctica de la Informática Forense | UNIR OPENCLASS* [Video]. YouTube. <https://www.youtube.com/watch?v=VKVu3_SLqwM> | Video | <https://www.youtube.com/watch?v=VKVu3_SLqwM> |
| Análisis de evidencia digital | Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (s. f.). *CSIRT Gobierno*. Gov.co. <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/> | Sitio web | <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/> |
| Certificaciones profesionales en ciberseguridad | Harán, J. (2020). *Certificaciones en seguridad informática más populares*. Welivesecurity. <https://www.welivesecurity.com/la-es/2020/11/19/certificaciones-seguridad-informatica-mas-populares/> | Artículo | <https://www.welivesecurity.com/la-es/2020/11/19/certificaciones-seguridad-informatica-mas-populares/> |
| Certificaciones profesionales en ciberseguridad | Jiménez, M. (2016). *La certificación en ciberseguridad es clave para competir*. Prisacom*.* <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_proquest_newspapers_1827856119> | Artículo | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_proquest_newspapers_1827856119> |

**G. Glosario**

| Término | Significado |
| --- | --- |
| *Antispam* | Sistema que se instala en los sistemas de correo electrónico para evitar que correos no certificados o de dudosa procedencia coloquen en riesgo la información de la organización. |
| Certificación | Proceso que realiza un profesional para validar el conocimiento de acuerdo con un examen avalado por organismos de certificación. |
| *Firewall* | Control de seguridad, que puede ser *hardware* o *software,* para evitar instrucciones a personas no deseadas. |
| IPS | Sistema de protección de usuario, el cual permite poner reglas de protección para evitar que los usuarios no comentan plagios o comportamientos indebidos en la infraestructura de la empresa. |
| Ley 1273 de 2009 | Ley de delitos informáticos que establece sanciones en el ámbito de la seguridad de la información. |
| Parchado virtual | Es la manera como se actualizan los dispositivos de seguridad. Estas actualizaciones están conectadas con los repositorios de los fabricantes y, de esta forma, los dispositivos se encuentran constantemente actualizados. |

**H. Referencias bibliográficas**

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de losdatos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*.* Enero 5 de 2009. <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>

**I. Control del documento**

|  | Nombre | Cargo | Dependencia | Fecha |
| --- | --- | --- | --- | --- |
| Autor(es) | Dulfran Antonio Montaño Montaño | Experto Temático | Regional distrito capital- Centro de diseño y metrología. | 18 de marzo de 2022 |
| Miroslava González Hernández | Diseñador y evaluador Instruccional | Regional Norte de Santander- Centro de la Industria, la Empresa y los Servicios | Marzo 2022 |
| Silvia Milena Sequeda Cárdenas | Asesora metodológica | Regional distrito Capital- Centro de diseño y metrología | Marzo 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable equipo de desarrollo curricular | Regional Santander - Centro industrial de diseño y la manufactura | Marzo 2022 |
| Darío González | Corrección de estilo | Regional Distrito Capital – Centro de Diseño y Metrología | Abril 2022 |

**J. Control de cambios**

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