**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 | 220501108-01 - Apropiar conceptos de ciberseguridad de acuerdo con procesos, políticas, normas, protocolos y procedimientos internos de la organización. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF01 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Introducción a la ciberseguridad y delitos informáticos |
| BREVE DESCRIPCIÓN | En este componente formativo se tratarán los temas de normatividad en la ciberseguridad, pilares de la seguridad informática y buenas prácticas en la navegación. |
| PALABRAS CLAVE | Buenas prácticas, ciberseguridad, información, navegación segura, protección |

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

1. **TABLA DE CONTENIDOS**

**Introducción**

* 1. **Componentes y normatividad asociados a la ciberseguridad**

1.1. Normatividad aplicada a la ciberseguridad

1.2. Componentes de la ciberseguridad

* 1. **Pilares de la seguridad informática**
  2. **Navegación segura**

3.1 La navegación en los diferentes entornos virtuales

3.2 Protocolos aplicados para una navegación segura

3.3 Buenas prácticas al momento de navegar en la Internet

**Síntesis**

1. **INTRODUCCIÓN**

El componente formativo “Introducción a la ciberseguridad y delitos informáticos” pretende brindar los conocimientos iniciales para realizar una adecuada comprensión sobre la caracterización de los componentes de la ciberseguridad en un ambiente empresarial y productivo. A continuación, se explicarán las temáticas a desarrollar y la importancia de las mismas:



|  | Se espera que al finalizar este componente tenga la habilidad para identificar y aplicar los pilares de la seguridad informática, manejar la normatividad de la ciberseguridad y aplicar prácticas de navegación segura. |
| --- | --- |

1. **DESARROLLO DE CONTENIDOS**
   1. **Componentes y normatividad asociados a la ciberseguridad**

La seguridad de la información está dirigida por una normatividad que permite establecer los límites de uso y manipulación de la información.

| Cultivar colegas usando una computadora portátil en la mesa Foto gratis | La información se ha convertido en el activo más importante para las organizaciones del Siglo XXI, pues permiten desarrollar la competitividad de las empresas y realizar sus procesos misionales de manera óptima. |
| --- | --- |

La ciberseguridad, entonces, se encarga de que esa normatividad se aplique de manera correcta. La información se encuentra caracterizada en privada, pública y sensible; para cada una se debe realizar un manejo específico, tal como se aprecia en el siguiente recurso:



**1.1. Normatividad aplicada a la ciberseguridad**

En Colombia se han realizado grandes esfuerzos por implementar normas y procedimientos que garanticen el acceso de la información y la protección de los datos de quienes utilizan la misma. Las políticas de seguridad de la información deben estar sujetas al tratamiento y distribución de los datos a través de los diferentes mecanismos de distribución, ya sea en redes de dominio local o internacional.

Existe un marco legal en Colombia que rige los diferentes riesgos y sanciones que se pueden presentar al momento de violar la soberanía de quien posee la legítima autoría de la información y los datos. Un ejemplo de ello, es la Ley 1273 de 2009, la cual hace parte de la estrategia de articulación de la Policía Nacional de Colombia para el manejo de los delitos informáticos. La siguiente figura presenta brevemente en qué consiste esta ley:

**Figura 1**

*Ley 1273 de 2009, delitos informáticos*



|  |  |
| --- | --- |
| La Ley 1273 crea un bien jurídico llamado “De la protección de la información y de los datos”, el cual está contemplado en el Código Penal colombiano donde la información y los datos se convierten en un activo propio de cada individuo. Por lo tanto, se debe cumplir con las características para ser determinante con las sanciones y multas establecidas. | |

El documento Conpes, por su parte, comprende los diversos grupos que conforman la Policía Nacional de Colombia para el manejo de las diferentes normatividades que se aplican en el país. En la figura que podrán apreciar a continuación, se ilustran las diferentes asistencias y apoyo que se brinda en caso de existir un delito que viole la privacidad de los datos o información de una persona o ciudadano:

**Figura 2**

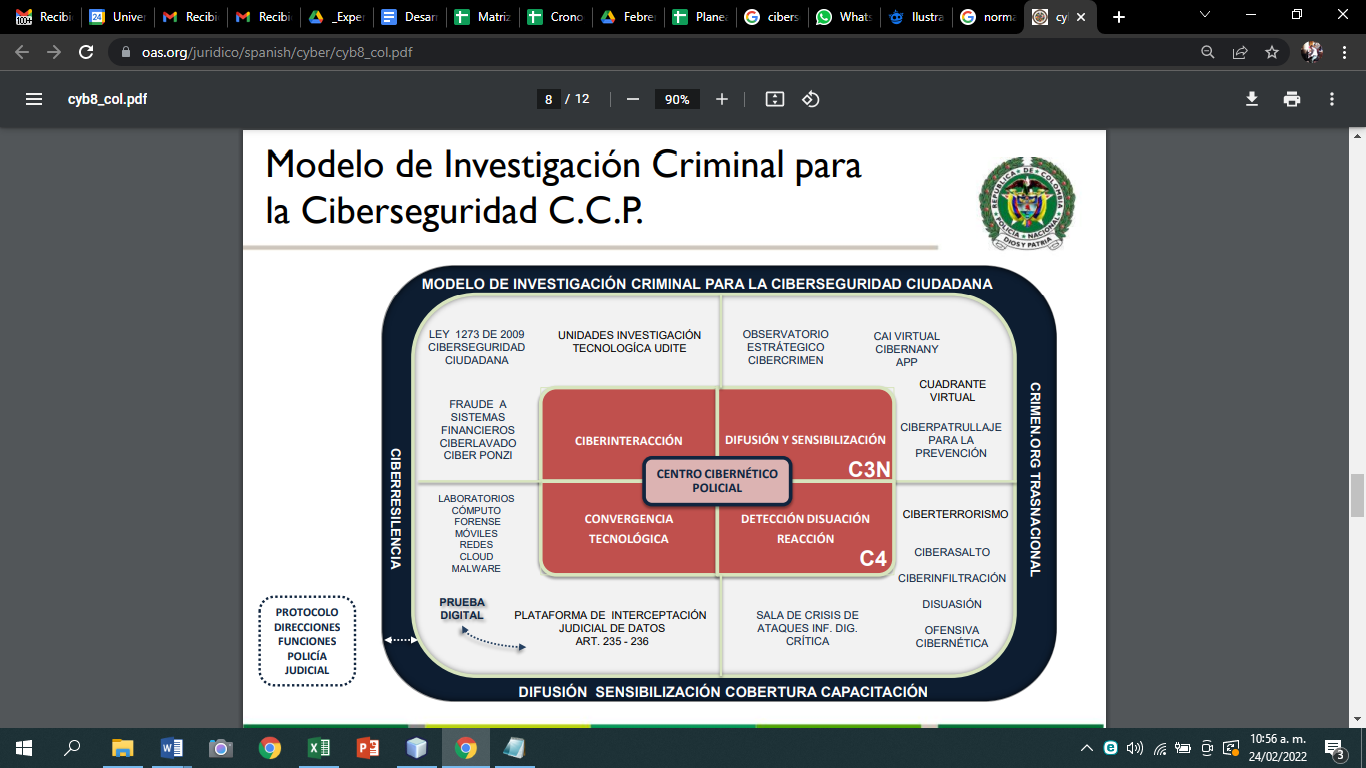
*Comisión intersectorial*



Ahora bien, existe un modelo de investigación criminal para la ciberseguridad en el cual se puede comprender el alcance y magnitud que pueden tener los delitos a la ciberseguridad. A continuación, se puede observar los diferentes tipos de fraudes cometidos en las organizaciones, que también atentan contra los ciudadanos:

**Figura 3**

*Modelo de investigación criminal*



Nota. Tomado de Policía Nacional (2014).

Sabiendo lo anterior, es preciso conocer que existen diferentes modalidades de fraude como se puede evidenciar; sin embargo, se abordaran los más comunes, encontrando:



**1.2. Componentes de la ciberseguridad**

Dentro de los componentes de la ciberseguridad se encuentra que para realizar un proceso correcto de gestión de la información se debe involucrar tres agentes importantes que son las personas, la tecnología y los servicios tecnológicos soportados. En la siguiente figura se expone en qué consiste cada uno:

**Figura 4**

*Componentes de la ciberseguridad*



|  |  |
| --- | --- |
| Estos componentes deben estar debidamente alineados con la política de seguridad establecida por la empresa, es decir, se deben establecer protocolos, planes y procesos que permitan tomar decisiones en un momento determinado. | |

Los componentes de la ciberseguridad juegan un papel importante dentro de las organizaciones, debido al impacto que pueden ocasionar en un ataque informático o incidente de seguridad.

|  | En este caso, se debe tener en cuenta que la capacitación del personal y los recursos tecnológicos para prevenir estas acciones, las cuales no se pueden percibir como un gasto sino como una inversión que permite asegurar la continuidad del negocio. |
| --- | --- |

* 1. **Pilares de la seguridad informática**

Son elementos que comprenden los dominios del sistema y las reglas que se deben seguir para asegurar la información. Estos pilares son el fundamento esencial de cualquier sistema informático, que en sus funciones está la preservación de los datos y la información.

El uso de la información pasa a ser uno de los procesos críticos dentro de una organización, ya que salvaguardar la misma es esencial en la mayoría de ocasiones con la continuidad del negocio. Estos pilares no solo garantizan una política de seguridad de la información, sino que abren un espectro mucho más grande que son los planes de recuperación de desastres, que buscan evitar que esto suceda, pero en caso de que llegase a darse esta situación se pueda tener un punto de partida de protocolos a activar para empezar la recuperación del mismo. Vea la descripción de cada uno de estos pilares:



|  |  |
| --- | --- |
| Los pilares de la seguridad de la información son una base inicial para entender los niveles de acceso y tratamiento que puede sufrir la información al momento de ser ingresada a un sistema de tratamiento de datos; es importante resaltar que estos pilares aplican para cualquier sistema de información y garantizan que la información sea manejada de una manera adecuada. | |

Los pilares de la información son un eje principal para garantizar la protección no solo de los activos de la organización, sino también se convierten en un instrumento de valoración a los servicios prestados por un sistema a una organización donde la información es protagonista de este proceso. Existen muchos factores que pueden evitar el correcto desempeño de estos pilares, los cuales se pueden ver inmersos en intereses externos o internos que no favorecen la calidad y procesos de negocio que realiza la organización.

| Concepto de gestión de datos de cloud computing Foto gratis |
| --- |
| Un ejemplo de ello puede ser un empleado insatisfecho o que no está de acuerdo con las políticas o ha sido despedido; este suceso puede desencadenar muchas variantes que pueden colocar en riesgo la información y los activos de la empresa, por eso se debe tener en cuenta que el acceso solo debe ser permitido mediante protocolos y mecanismos de autenticación certificados y que garanticen una integridad adecuada a la información almacenada. |

| “Tenemos más de diez mil riesgos diferentes cada año, eso equivale a miles de amenazas supuestamente de alto riesgo a las que debemos responder” (Ortiz, 2020). |
| --- |

* 1. **Navegación segura**

Internet es un mar de conocimiento e información que millones de personas usan a diario para sus actividades personales o empresariales, pero más allá de la búsqueda y procesamiento de esta información se encuentran con diferentes tipos de técnicas de *hacking* que colocan en riesgo los datos que utilizan en los diferentes portales y sitios que visitan.

| Mujer asiática hermosa que usa el teléfono inteligente que compra compras en línea Foto gratis | La mayoría de personas realizan transacciones bancarias, consultan redes sociales, compras *online,* entre otras actividades; pero poco saben del tratamiento que se le puede dar a la información que allí se suministra y cómo se almacena. |
| --- | --- |

Es importante tener en cuenta que cuando se ingresa a un portal web o sitio en Internet los datos de navegación y la información que se suministra en el mismo se ve comprometida en todos los sentidos; por ello, es necesario abordar desde las características técnicas hasta las funcionales, como manejar y proteger de estos problemas de seguridad.

**3.1 La navegación en los diferentes entornos virtuales**

Los entornos virtuales comprenden las diferentes plataformas y medios que se utilizan a diario para realizar los procesos de negocio u ocio en particular. Un ejemplo de ello son las redes sociales, plataformas de comercio electrónico, sitios de banca financiera, las computadoras o dispositivos, para poder acceder a estos sitios o entornos virtuales. En la mayoría de ocasiones se debe suministrar información, que como se describió en temas anteriores, puede ser pública, privada o sensible, dependiendo del entorno y situación que se presente. Frente a este aspecto se debe tener en cuenta los siguientes aspectos:

**Figura 5**

*Aspectos importantes al suministrar información*



Se comprende como entorno virtual a todo aquel proceso que utiliza medios tecnológicos para el procesamiento y manejo de la información, los cuales son utilizados en los procesos de negocio y público en general. Estos sistemas, en la mayoría de ocasiones, se encuentran instalados en servidores y equipos que centralizan la información, es decir, se encuentran con acceso a nivel mundial, para ser precisos Internet. **Al estar expuestos al acceso mundial se convierten en una ventaja para las personas que los utilizan, pero también en una amenaza para los más descuidados.** En el siguiente videose explica la técnica de fraude más conocida como *phishing*:



**3.2 Protocolos aplicados para una navegación segura**

Los protocolos de navegación segura aplicados van desde configuraciones del sistema, hasta la aplicación de modelos informáticos que garanticen el acceso de los diferentes sitios y portales de Internet, sin necesidad de comprometer la información de los usuarios de los mismos; dichos protocolos permiten minimizar los riesgos de ser víctimas de ataques informáticos, pero siempre se debe tener en cuenta el factor humano, quien es el usuario que utiliza el sistema.

Por otra parte, los protocolos de navegación segura incluyen una verificación por parte del usuario donde incluye tanto *software* como *hardware*, es decir, uno de los puntos importantes para que esto se convierta en una política de uso de la información es verificando los siguientes componentes:



**3.3 Buenas prácticas al momento de navegar en la Internet**

De la navegación segura existen muchas técnicas, procedimientos y *software* que permiten garantizar que esta se dé dentro de los procesos de navegación en la Internet, pero se debe también tener en cuenta que la navegación segura involucra como actor del proceso al usuario que utiliza el sistema, ya que es quien da las órdenes a la aplicación para que realice las funciones requeridas. Siendo así, vea cómo se presentan algunos métodos comunes:



|  |  |
| --- | --- |
| Es importante destacar que estos son algunos protocolos y herramientas a utilizar para realizar la navegación segura en Internet; pero actualmente se puede encontrar muchos mecanismos que serán abordados en este curso y que serán de gran ayuda para mejorar los niveles de seguridad en las organizaciones y la ciudadanía en general. | |

1. **SÍNTESIS**

En este componente se abordaron distintas temáticas que iniciaron desde la introducción a la ciberseguridad, pasando por sus componentes, normatividad y pilares de la seguridad de la información, hasta los diferentes entornos virtuales y buenas prácticas en la navegación, tal como lo presenta el siguiente esquema:

**Figura 8**

*Síntesis*



1. **ACTIVIDADES DIDÁCTICAS**

| DESCRIPCIÓN DE LA ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Conociendo la ciberseguridad |
| Objetivo de la actividad | Validar conocimientos y conceptos aprendidos. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Se encuentra en la carpeta Formatos DI con el nombre “CF01\_Actividad didáctica” |

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 |
| --- | --- | --- | --- |
| Componentes y normatividad asociados a la ciberseguridad | Baca, G. (2016). *Introducción a la seguridad informática*. Grupo Editorial Patria. <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_elibro_books_ELB40458> | Libro | <https://sena-primo.hosted.exlibrisgroup.com/permalink/f/1i756fj/TN_cdi_elibro_books_ELB40458> |
| Normatividad aplicada a la ciberseguridad | Policía Nacional. (2014). *Ciberseguridad entorno colombiano*. <https://www.oas.org/juridico/spanish/cyber/cyb8_col.pdf> | Presentación | <https://www.oas.org/juridico/spanish/cyber/cyb8_col.pdf> |
| Pilares de la seguridad informática | Calderón, L. (s.f.). *Seguridad informática y seguridad de la información*. Universidad Piloto de Colombia. <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2821/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y> | Artículo | <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2821/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y> |
| Buenas prácticas al momento de navegar en la Internet | Centro transparencia Google. (s.f.). *Informe de transparencia de Google*. <https://transparencyreport.google.com/safe-browsinzzg/search> | Página web | <https://transparencyreport.google.com/safe-browsinzzg/search> |

1. **GLOSARIO**

| Término | Significado |
| --- | --- |
| Ciberseguridad | Son todos los protocolos y políticas que se implementan para realizar un uso adecuado de la tecnología, lo cual pretende evitar que la información y los sistemas informáticos sean vulnerados. |
| Confidencialidad | Proveer mecanismos de autenticación para garantizar que la información solo será accedida por quien tenga el legítimo derecho a accederla. |
| Disponibilidad | Establecer los tiempos en los cuales la información estará disponible, por ejemplo, 24/7, 5/24, entre otros. |
| Entornos virtuales | Es un espacio cibernético en el cual se ejecuta una aplicación o conjunto de aplicaciones informáticas, que debe proporcionar los mecanismos necesarios para su acceso y manejo adecuado. |
| Información privada | Conjunto de datos que puede contener componentes específicos sobre la información personal de un ciudadano, y por encontrarse en un ámbito privado, solo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. |
| Información pública | Es aquella que puede ser almacenada y tratada con poca restricción en un sistema informático. |
| Información sensible o confidencial | Es una clasificación específica de la información privada de un individuo, la cual puede generar momentos de peligro o de ausencia de seguridad para su integridad física o financiera. |
| Integridad | Método o manera en la cual será accedida la información y qué procesos internos debe llevar a cabo. |
| *Phishing* | Técnica utilizada para hacerse pasar por una entidad de confianza y solicitar información a los usuarios de estos servicios, y así engañar a la víctima para que acceda a sitios o portales para suministrar información de cuentas bancarias, usuarios, contraseñas, entre otro tipo de información. |
| Políticas de seguridad | Una política de seguridad es la manera en la que se establecen las reglas y mecanismos para la protección y manejo de la información en una organización. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Conpes 3701. (2011). *Lineamientos de política para ciberseguridad y ciberdefensa*. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

Ortiz, A. (2020). *¿Cuáles son los tres pilares de la seguridad informática?* HostDimeBlog. <https://www.hostdime.com.pe/blog/cuales-son-los-tres-pilares-de-la-seguridad-informatica/>

Policía Nacional. (2014). *Ciberseguridad entorno colombiano*. <https://www.oas.org/juridico/spanish/cyber/cyb8_col.pdf>

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Dulfran Antonio Montaño Montaño | Experto temático | Regional Distrito Capital - Centro de Diseño y Metrología | Febrero 2022 |
| Miroslava González Hernández | Diseñadora instruccional | Regional Norte de Santander – Centro de la Industria, la Empresa y los Servicios | Febrero 2022 |
| Andrés Felipe Velandia Espitia | Asesor metodológico | Regional Distrito Capital – Centro de Diseño y Metrología | Marzo 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo desarrollo curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Marzo 2022 |
|  | Julia Isabel Roberto | Correctora de estilo | Regional Distrito Capital – Centro de Diseño y Metrología | Marzo 2022 |

1. **CONTROL DE CAMBIOS**

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

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