**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Desarrollo de habilidades digitales para experiencias seguras en línea |
| --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 2 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Herramientas y estrategias de protección digital |
| BREVE DESCRIPCIÓN | Este componente formativo presenta las herramientas y estrategias a utilizar en el caso de protección digital, con el fin de evitar amenaza y riesgo que afecte la experiencia al momento de utilizar recursos digitales. |
| PALABRAS CLAVE | Antivirus, contraseña, delito informático, huella digital, internet, *software* |

| COMPETENCIA | 220501110. Implementar el sistema de seguridad de la información según modelo y estándares técnicos. | RESULTADOS DE APRENDIZAJE | 220501110-02. Aplicar las estrategias de ciberseguridad conforme a los recursos y servicios digitales utilizados. |
| --- | --- | --- | --- |

| AREA OCUPACIONAL | No aplica |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:**

**Introducción**

**1. Herramientas y estrategias de protección**

1.1 Clasificación y características de las herramientas de protección

1.2 Antivirus gratuitos

1.3 Gestión de contraseñas

1.4 Fuentes de descarga segura de *software*

1.5 Datos personales y datos de terceros

1.6 Compras por internet

**2. Huella digital**

2.1 Importancia de la huella digital

2.2 Identidad digital

**3. Delitos informáticos**

3.1 Legislación actual

3.2 Tipología, sanciones y penalizaciones de los delitos informáticos

1. **DESARROLLO DE CONTENIDOS:**

**Introducción**

**¿Qué se debe hacer para enfrentar un riesgo digital?**

Es una pregunta muy común entre las personas. Lo primero que debe tener presente es que no está solo, existen múltiples herramientas en las que tendrá apoyo, tanto en la generación de protección como en la conciencia de que todo depende del buen uso que se les dé a los dispositivos y servicios en red, y eso es lo que se aprenderá en este componente formativo.

Se explicarán conceptos que debemos tener presentes y conocer a la perfección qué es la identidad digital para así saber dónde dejar la huella.

**¡Bienvenido!**

* 1. **Herramientas y estrategias de protección**

Se denomina herramientas de protección a todas las herramientas que nacen para cubrir las necesidades de seguridad, digital en este caso; son aquellas que presentan un alivio en el uso de los contenidos digitales y se caracterizan por ser de carácter pago o gratuito, según se establezca por parte de cada fabricante.

* 1. **Clasificación y características de las herramientas de protección**



¿Sabía que las herramientas y estrategias de protección son tan variables y distintas como las diferentes herramientas digitales y tecnológicas que se pueden usar?

Su número es tan extenso que se clasifican en dos grandes áreas:

**1. Las que trabajan a nivel de usuario**

Son las herramientas que se requieren para la protección personal y las buenas prácticas de seguridad, con contenidos digitales para aplicativos personales como redes sociales.

**2. Las que trabajan a nivel técnico o empresarial**

Obedecen más a políticas institucionales tendientes a la protección de los recursos tecnológicos corporativos, dentro de los cuales se integran todos los datos que deben protegerse por parte de los usuarios o empleados de las diferentes organizaciones en sus diferentes roles.

Gráficamente se puede explicar así:

**Figura 1**

*Herramientas de protección*



Cada usuario debe seguir siempre estas recomendaciones y buenas prácticas:



Ahora, desde el punto de vista empresarial, las recomendaciones son:



**1.2 Antivirus gratuitos**

El siguiente video explica qué es un antivirus y la diferencia entre los comerciales y los gratuitos.



También podemos encontrar otras diferencias, como son:

**Consumo de recursos *hardware* y *software***

Generalmente, los antivirus de pago o comerciales tienen interfaces más sencillas que consumen menos recursos que los gratuitos.

**Soporte técnico**

El soporte por parte del fabricante de un antivirus gratuito es más limitado en cuanto a actualizaciones, definiciones de nuevos virus entre los dos modelos.

**Anuncios**

Los antivirus gratuitos disponen de una serie de anuncios o publicidad de parte del fabricante o de terceros, esto puede resultar algo molesto.

**Tecnologías de punta**

Para la búsqueda, detección y eliminación de los virus, en los antivirus de pago se utilizan varias tecnologías que permiten identificar y detectar nuevos virus o mutaciones de acuerdo con los comportamientos de virus ya conocidos, mientras que en los antivirus gratuitos operan con una única tecnología que reconoce los antivirus más conocidos.

A continuación, se enumeran algunas de las soluciones de antivirus gratuitos más conocidas o utilizadas y sus páginas web oficiales **desde donde se pueden descargar**. Por favor, valide el que se adapte a su necesidad e instale, **no se recomienda instalar más de uno** por dispositivo.

Avast <https://www.avast.com/es-co/download-thank-you.php?product=FAV-PPC&locale=es-co> 



Panda <https://repository.pandasecurity.com/Panda/FREEAV/191048/PANDAFREEAV.exe?_ga=2.263797774.385325174.1631032485-1932197500.1631032485&_gac=1.86366570.1631032485.Cj0KCQjwm9yJBhDTARIsABKIcGYHvo_5V8gGhbVafeBE2tNCWhyUMAXmOUpdoDsRmIq2v0QkerIUZjIaAmO3EALw_wcB>

AVG

<https://www.avg.com/es-co/download-thank-you.php?product=FREEGSR>



Windows Defender: es un antivirus propio del sistema operativo Microsoft el cual solo debe activarse y mantenerse actualizado.

**1.3 Gestión de contraseñas**



Esta es una de las mejores prácticas a implementar como usuarios regulares de herramientas tecnológicas, donde se requiere para el acceso o uso ingresar con una cuenta de usuario y una contraseña.

Una mala práctica en este sentido puede comprometer la privacidad, lo que deriva en vulnerabilidad por parte de un tercero que puede editar, borrar o manipular la información personal de cada persona. Para el caso de los correos electrónicos, datos bancarios y redes sociales, el uso de estos elementos conocidos como *password* es fundamental y se debe tener cuidado extremo a la hora de su generación y uso.

A continuación, se amplía en el siguiente video, el concepto de contraseña.



Se deben tener siempre presente las siguientes recomendaciones, sean en el plano personal o corporativo, para evitar una mala práctica en la gestión de contraseñas.



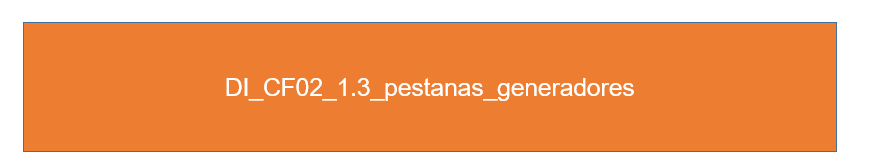
En el caso puntual de los generadores de contraseñas, se aconseja el uso de cualquiera de los siguientes recursos gratuitos en línea:

**Tabla 1**

*Gestor de contraseñas*

| **Gestor de contraseñas** | **Sitio web** |
| --- | --- |
| KeePass: es una solución de código abierto muy utilizada y potente. | <https://keepass.info/> |
| 1Password: es una muy buena alternativa de uso comercial, quizá la más recomendada. | <https://1password.com/> |
| Dashlane: es una herramienta con excelente diseño y es sencilla de utilizar, aunque es de pago ofrece muy buenas funcionalidades. | <https://www.dashlane.com/es> |
| Keeper: es una muy buena alternativa que, aunque no tiene un muy buen diseño, tiene aplicaciones para escritorio, móvil y navegadores. | <https://www.keepersecurity.com/es_ES/pricing.html?t=b> |

Se propone utilizar un generador de contraseñas en el que, eligiendo los niveles de complejidad, puedan generarse las contraseñas. A continuación, se mencionan algunos de los sitios que pueden ser utilizados para esta labor:



**1.4 Fuentes de descarga segura de *software***

En la cotidianidad, se utiliza internet y otras herramientas tecnológicas a diario y es común que encontrar algunas soluciones de aplicaciones y/o servicios que pueden potencializar el uso de las TIC (Tecnologías de la Información y Comunicación), eso hace que se haga obligatorio prestar especial atención a los sitios desde los cuales se hacen las descargas de cualquier tipo de aplicación. Lo primero, al momento de tratar de descargar una aplicación o archivo, es reconocer si la descarga se hace desde un sitio seguro y para ello se presentan las siguientes recomendaciones las que cada usuario de las redes, puede aplicar a conveniencia.

* La mejor recomendación es descargar alguna aplicación, juego o archivo desde los sitios oficiales del fabricante.
* Si la descarga se va a hacer a partir de un *link* recomendado por alguna persona o página, se deben de validar los comentarios de otros usuarios que hallan hecho la descarga e identificar las credenciales y reputación de quien publica algún comentario, ya que puede haber comentarios falsos dispuestos solo para generar una falsa confianza en la persona que va a descargar.
* Si se desea comprar alguna aplicación utilizar las tiendas oficiales; por ejemplo en el tema de las aplicaciones móviles recurrir a las apps store según el dispositivo utilizado y siempre validar los comentarios y recomendaciones de otros usuarios.
* Desconfiar de aplicaciones gratuitas, antes de descargar e instalar alguna aplicación de este tipo se debe verificar su origen e idoneidad, pues se puede incurrir en el uso de *software* falso que simula realizar acciones de protección y mejora del rendimiento del equipo, pero en realidad lo que hace es infectar o afectar los equipos con virus, *malware* y *adware*.
* No utilizar *software* falso o pirata, normalmente se tiende a utilizar *software* de manera ilegal sin licencia lo que obliga a utilizar los llamados *cracks* de activación, estos normalmente vienen infectados con algún tipo de virus lo que ocasionará que los equipos donde se instale el *software* de manera ilegal se infecten y queden expuestos a robo de información.
* No acceder a descarga de apps a través de *links* dispuestos en páginas donde se promocionan estas aplicaciones o *software*, normalmente este tipo de *links* llevará a un sitio predeterminado o previamente configurado para que se descarguen las apps con algún tipo de infección con *malware* o virus.
* Cuando se realicen descargas de aplicaciones tener siempre activo el antivirus, esto permitirá hacer una revisión de la descarga a fin de examinar e identificar posibles virus, *malware* y *spyware*.

**1.5 Datos personales y datos de terceros**

Los datos personales son todos aquellos que relacionan o permiten identificar y caracterizar a una persona, permitiendo ser identificados o identificables.

Algunos ejemplos de los datos personales son:

* Nombres y apellidos.
* Edad.
* Dirección o domicilio.
* Correo electrónico.
* Número de teléfono.
* Educación o perfil académico.
* Patrimonio.
* Estado de salud.
* Origen étnico.
* Creencia religiosa.
* Ideología política.
* Preferencias sexuales.
* Documento de identidad.

Es muy útil reconocer la importancia que tiene la protección de los datos personales, para evitar que estos datos sean utilizados con una finalidad distinta a la que inicialmente fueron suministrados, evitando que se vulneren los derechos y libertades de los usuarios en red; esto implica que siempre que se use un sitio físico o virtual, que requiera de un registro, es necesario poner especial atención en que se identifique claramente cuál será el propósito o finalidad que tienen para el manejo de los datos personales registrados.

Para este propósito, el Estado colombiano desarrollo la Ley Estatutaria 1581 de 2012 que constituye el marco general de la protección de los datos personales en Colombia, entre otras cosas, esta Ley manifiesta el derecho que tienen todas las personas a autorizar el uso de la información personal almacenada en bases de datos y archivos administradas por personas naturales o jurídicas, públicas o privadas, así como su posterior actualización, modificación y rectificación.

**Para recordar:** toda empresa, sitio, página o portal web que requiera el registro de los datos personales, debe (sin ninguna excepción), solicitar la autorización a todas las personas para el tratamiento de sus datos personales.

Esta autorización requiere:

* Tener un **consentimiento informado,** lo que significa que antes de solicitar datos personales, debe ser expresada e informada la solicitud de tratamiento de los datos personales.
* Determinar de manera clara para que serán usados los datos que buscan ser obtenidos.
* Especificar claramente los derechos y los medios a través de los cuales puede el usuario ejercerlos.
* Respetar las condiciones de seguridad y privacidad de la información, sin obviar el trámite de consultas, solicitudes y reclamos por parte de los sujetos que se puedan ver afectados por la obtención de sus datos personales sin previa autorización.

Es importante mencionar que las empresas que reciben los datos a través de registros realizados por terceros, tienen que cumplir con los mismos criterios de solicitud de autorización, pero adicionalmente se deben priorizar las siguientes actividades.

* Creación de la política de protección de datos personales.
* Creación del consentimiento informado.
* Levantamiento de las bases de datos.
* Registro nacional de las bases de datos ante la súper intendencia de industria y comercio.

**1.6 Compras por internet**



Internet y la masificación del uso de las Tecnologías de la Información y las Comunicaciones (TIC) ha potenciado e incrementado el mercado digital; cada vez es mayor y mejor el acceso a la oferta y compra de productos y servicios en línea, lo que conlleva a identificar cuál o cuáles serán las mejores prácticas o recomendaciones a tener en cuenta al momento de realizar algún tipo de transacción que incluya movimientos financieros.

En la actualidad, gran parte de las transacciones diarias se realizan por internet desde dispositivos móviles o electrónicos. Algunas de las transacciones que se pueden hacer en línea son:



Cuando se realizan compras por internet, es importante tener presente las siguientes buenas prácticas o consejos, a saber:

**Saber exactamente qué tipo de producto o servicio se requiere**

Al momento de hacer la compra se debe tener claridad frente a las características del producto o servicio que se desea adquirir, debido a la gran oferta existente no siempre el mejor precio corresponde a productos más confiables.

**Revisar y comparar las referencias y comentarios**

Estos son hechos por otros compradores del mismo producto, para validar la calidad y cumplimiento y seriedad del proveedor.

**Navegar e interactuar con las plataformas o sitios donde se hará la compra**

Se recomienda hacer una navegación detallada dentro de las plataformas para identificar sus contenidos, periodos de actualización, comentarios o algo que permita identificar si efectivamente es un sitio válido, confiable y seguro.

**Validación de la seguridad básica de la plataforma o sitio de comercio**

Todo sitio serio debe contar con unas medidas de seguridad técnicas que son básicas y requeridas, por ejemplo se debe validar que cuente con un certificado digital que garantice que la información, datos o transacciones se hagan protegidas y cifradas, para esto se valida que la URL cuente con un protocolo seguro como lo es **https://,** si se cuenta con este requisito básico en la URL previo al nombre, debe mostrar un candado lo cual indica que el sitio es seguro.

**Pagos seguros**

El momento de realizar el pago por el producto o servicio adquirido se debe realizar la validación de que se cuenta con una pasarela de pagos reconocida y certificada, entre otras, las siguientes son pasarelas de pago certificadas y aprobadas en el país: PayU, Mercado Pago, En Línea Pagos, Pagos Inteligentes, Opacó, Interpagos, Pago Digital, Recaudo Express, Mercado Libre, PSE, Paypal, entre otros.

**Política de privacidad y devoluciones**

En toda plataforma de comercio se debe contar una clara política de privacidad y devoluciones y de fácil acceso que facilite al usuario en un momento determinado saber cuál es el proceso para una devolución que debe hacer y tener claridad frente al manejo de sus datos personales que sean autorizados.

**Acceso a canales de soporte y servicio al cliente**

Una página o sitio confiable donde se pueden realizar compras *online* debe contar con las estrategias y canales de atención como redes sociales, página web, teléfonos, direcciones, esto permitirá determinar si el sitio es seguro, operativo y confiable.

**Términos y condiciones**

El sitio el sitio o plataforma donde se realicen las compras debe contar con espacio claramente determinado con los términos y condiciones donde se especifique claramente las condiciones para los pagos, políticas de devoluciones y reembolsos, envíos, costos de transporte, tiempos de entrega, entre otros, de esta manera se evitará tener inconvenientes y experiencias no favorables con la compra.

* 1. **Huella digital**

¿Sabía que la huella digital puede ser vista desde dos frentes?

1. El primero corresponde a los rastros y huellas de identidad que un usuario deja al utilizar internet o dispositivos digitales.
2. El segundo está relacionado con la utilización de la huella dactilar en dispositivos de autenticación y verificación de identidad.

Para ampliar la información, invitamos a ver el siguiente video.





Cuando se utiliza internet y los diferentes medios y dispositivos digitales, se comparte información sobre gustos, preferencias, datos personales, incluso la posición geográfica de las personas, y toda esta información puede ser usada para construir una imagen del perfil de la persona con actividades e intereses. Es importante pensar, entonces, en quién puede ver esa información, incluso si se tiene una buena configuración de privacidad, se puede copiar el contenido y transmitirlo para el mundo en general.

Por este motivo, se debe pensar muy bien antes de publicar opiniones, intereses, gustos, posiciones religiosas o políticas, porque una vez publicadas se pierde el control sobre este contenido y puede ser copiado o multiplicado de manera exponencial e incluso generar reacciones inoportunas.

**Huella dactilar**

Ahora, las huellas dactilares son una marca única con un patrón específico para cada persona.

Según Interpol (s.f.): “No hay dos personas con las mismas huellas dactilares; ni siquiera los gemelos homocigóticos. Las huellas dactilares no cambian nunca, ni con la edad, a menos que la capa profunda o basal se destruya o se modifique intencionadamente por medio de cirugía plástica”.

Todo esto indica que cada una de las huellas de los dedos y pies es única e irrepetible.

Este patrón único permite relacionar una serie de datos asociados a una persona como son:

* El nombre.
* La identificación.
* La fecha de nacimiento, entre otros.

**2.1 Importancia de la huella digital**

Para efectos de este curso, se enfatizará en el estudio de la huella digital como el rastro que se construye al hacer uso de internet y de sus diferentes herramientas o dispositivos digitales.

Es importante entender que dependiendo del uso que se hace de:



Las herramientas tecnológicas e internet



Tipo de búsquedas



Publicaciones



Compras



Tipos de consumo

se va a ir construyendo una huella digital que contendrá los datos sobre todas las actividades antes planteadas.

Cuando se realiza algún tipo de comentario o publicaciones en algunas plataformas tecnológicas como:

* Blogs.
* Webs y redes sociales.
* Uso de aplicaciones.
* Registros de correo electrónico.
* Compras.
* Consumo de plataformas de entretenimiento, entre otras.

Esta es información que forma parte del historial en línea de una persona y, potencialmente, puede ser vista, compartida o comentada por otras personas o incluso ser almacenada en una base de datos, por lo que es importante tener presente que, de una forma u otra, **todo lo que se hace queda grabado**.

De acuerdo con lo anterior:

Es prácticamente imposible borrar la huella digital, porque así se borre una publicación o un comentario, siempre existe la posibilidad de que haya sido compartido, almacenado o registrado.

Después de lo estudiado, surge esta pregunta:



**¿Y por qué es importante la construcción de la huella digital?**



La importancia de construir una muy buena huella digital radica, entre otras cosas, que en la actualidad las empresas de selección de talento humano acuden a las redes sociales y en general a internet para investigar e identificar comportamientos y posiciones de posibles candidatos que se presentan o que son requeridos en el mundo laboral.

**2.2 Identidad digital**

Como se ha mencionado, la huella digital permite con el tiempo y de acuerdo con las acciones, construir la **identidad digital,** que se trata de un **“yo”** en la red, que determina los datos que cada persona va dejando en la red a partir del consumo de productos y servicios, publicaciones. La identidad digital determina qué ven los demás usuarios en términos de uso de recursos tecnológicos en los que se reconocen los perfiles aunque se puede dar que en muchos casos la identidad digital obedezca a un seudónimo.

Algunas de las amenazas que afectan la identidad digital, como parte de la utilización de internet y los recursos tecnológicos, son:



**3. Delitos informáticos**

Se definen como aquellos actos ilícitos en los que se usan las tecnologías de la información, como las computadoras, los programas informáticos, los medios electrónicos, internet, entre otros, como medio o como fin.

**3.1 Legislación actual**

En Colombia, la legislación frente a los delitos informáticos, su tipificación y tipos de sanciones han tenido una evolución lenta en el tiempo, sin embargo, se ha legislado al respecto. A continuación, se realizará un resumen general de las leyes que marcaron el inicio y evolución de la legislación colombiana en esta temática:

* Ley 527 de 1999: por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
* Ley 599 de 2000: el Código Penal Colombiano no habla explícitamente de delitos informáticos, sin embargo, algunos artículos protegen los bienes jurídicos de vulneraciones cometidas a través de la red informática.
* Ley 603 de 2000: ley que ampara los derechos de autor, que protege la propiedad y producción intelectual.
* Ley 679 de 2001: entre otras cosas establece las normas atinentes para contrarrestar el abuso sexual de menores, a través de medios electrónicos.
* Ley 1266 de 2008: ley de habeas data regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros.
* Ley 1273 de 2009: establece nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos.

**3.2 Tipología, sanciones y penalizaciones de los delitos informáticos.**

Para hablar de la tipología y tipos de sanciones que actualmente están vigentes en Colombia, se debe tomar como referente la Ley 1273 de 2009, la cual está compuesta por dos capítulos. A continuación, se desglosan cada uno de ellos.

**Capítulo 1  
De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos**

**Artículo 269A - Acceso abusivo a un sistema informático**

El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

**Artículo 269B - Obstaculización ilegítima de sistema informático o red de telecomunicación**

El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

**Artículo 269C - Interceptación de datos informáticos**

El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

**Artículo 269D - Daño Informático**

El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

**Artículo 269E - Uso de *software* malicioso**

El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional *software* malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

**Artículo 269F - Violación de datos personales**

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

**Artículo 269G - Suplantación de sitios web para capturar datos personales**

El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

**Artículo 269H - Circunstancias de agravación punitiva**

Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

* Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
* Por servidor público en ejercicio de sus funciones.
* Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
* Revelando o dando a conocer el contenido de la información en perjuicio de otro.
* Obteniendo provecho para sí o para un tercero.
* Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
* Utilizando como instrumento a un tercero de buena fe.
* Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

**Capítulo 2  
De los atentados informáticos y otras infracciones**

**Artículo 269I - Hurto por medios informáticos y semejantes**

El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

**Artículo 269J - Transferencia no consentida de activos**

El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Ahora bien, si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Para entender mejor los delitos informáticos observe el siguiente ejemplo:

PEDRO MARTÍNEZ es un ingeniero de sistemas que se desempeña como administrador de la red en la empresa ABASTOS LTDA.

Este señor es amigo de ULISES PINTO quien fuera novio de MARTHA SÁNCHEZ funcionaria de la empresa.

Un día cualquiera ULISES le dice a PEDRO que desea saber los números de teléfono y la dirección de MARTHA, para lo cual PEDRO aprovechando su perfil, le entrega en una memoria USB dicha información, así mismo, le hace entrega de unas fotografías de la señora SÁNCHEZ que posteriormente son publicadas en internet.

¿Existe algún delito y cuál es la pena máxima?

Según la Ley 1273 del 2009 los artículos que hacen parte del presente caso son:

* Artículo 269A.
* Artículo 269F.
* Artículo 269H.

Estos artículos son aplicados tanto para PEDRO como para ULISES, puesto que ellos cometieron una conducta punible, de diferente agravación.

Para PEDRO se tipifica el artículo 269A, ya que este habla sobre el acceso abusivo a un sistema informático, porque pueda que él sea ingeniero de sistemas, pero su papel es administrador de la empresa y no debería estar utilizando su conocimiento en sacar información que no debe, para dársela a otra persona y mucho menos sin consentimiento del gerente o dueño de la empresa.

Para ULISES se tipifica el articulo 269F, ya que esta habla de la violación de datos personales, porque él, en vez de guardar esa información y datos de MARTHA para él solo, lo que hizo fue publicarlas, independientemente de las razones por las cuales lo hizo.

El artículo 269H, habla de las agravaciones que tienen cada una de sus acciones tanto de PEDRO como de ULISES, las cuales son:

* Tercera: aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
* Cuarta: revelando o dando a conocer el contenido de la información en perjuicio de otro.
* Octava: si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

La tercera y cuarta agravación la cumple ULISES y la octava agravación la cumple PEDRO. Con respecto a la pena, para PEDRO según la conducta que tuvo (artículo 269 A) es de 48 a 96 meses y según su agravación (artículo 269 H), esta pena se aumentará a la mitad o las tres cuartas (3/4) partes, por lo tanto, la pena la dictará el juez, dependiendo del aumento que le vaya a dar según los datos mencionados.

Para ULISES, según la conducta que tuvo (artículo 269 F) es de 48 a 96 meses y por su agravación (artículo 269 H), esta pena se aumentará la mitad o las tres cuartas (3/4) partes también.

En conclusión, el juez debe determinar cuál fue de mayor agravación e implantarle a ese la pena aumentada a las tres cuartas (3/4) partes y al otro si aumentarle la mitad de la pena, según la importancia de conducta punible que tuvo.

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

| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| --- | --- |
| Nombre de la Actividad | Sopa de letras |
| Objetivo de la actividad | Afianzar algunos de los conceptos más importantes de la ciberseguridad y las redes sociales. |
| Tipo de actividad sugerida | Encontrar los términos asociados a las temáticas tratadas en este componente formativo. |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** | Anexo documento en Word llamado Actividad didáctica 2 en carpeta Formatos\_DI |

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** |
| --- | --- | --- | --- |
| Gestión de contraseñas | Bastidas, H. (2021). *Gestión de contraseñas.* [Video]. YouTube. <https://www.youtube.com/watch?v=WuO1Fu38yPk> | Video | <https://youtu.be/WuO1Fu38yPk> |
| Huella digital | Bastidas, H. (2021). *Huella digital.* [Video]. YouTube. <https://www.youtube.com/watch?v=-p5HezBeYQE> | Video | <https://www.youtube.com/watch?v=-p5HezBeYQE> |

1. **GLOSARIO:**

| **TÉRMINO** | **SIGNIFICADO** |
| --- | --- |
| **Antivirus** | tipo *software* diseñado específicamente para ayudar a detectar, prevenir y eliminar virus informáticos y *software* malicioso o *malware*. |
| **Contraseña** | clave que permite acceder a un lugar, ya sea en el mundo real o en el virtual. Las contraseñas se utilizan por varios motivos: para preservar la intimidad, para mantener un secreto, como una medida de seguridad o como una combinación de todo ello. |
| **Delito informático** | actos ilícitos en los que se usan las tecnologías de la información, como las computadoras, los programas informáticos, los medios electrónicos, internet, entre otros, como medio o como fin. |
| **Huella digital** | corresponde a los rastros y huellas de identidad que un usuario deja al utilizar la internet o dispositivos digitales. |
| **Internet** | unión de todas las redes y computadoras distribuidas por todo el mundo, por lo que se podría definir como una red global en la que se conjuntan todas las redes que utilizan protocolos TCP/IP y que son compatibles entre sí. |
| **Redes sociales** | estructuras formadas en internet por personas u organizaciones que se conectan a partir de intereses o valores comunes. |
| ***Software*** | conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo informático. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

Avance Jurídico Casa Editorial Ltda. (2021). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad* [Ley 1273 de 2009]. Senado de la República de Colombia. <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html>

Bastidas, H. (2021). *Gestión de contraseñas.* [Video]. YouTube. <https://www.youtube.com/watch?v=WuO1Fu38yPk>

Bastidas, H. (2021). *Huella digital.* [Video]. YouTube. <https://www.youtube.com/watch?v=-p5HezBeYQE>

Interpol. (s.f). *Huellas dactilares*. <https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Huellas-dactilares>

1. **CONTROL DEL DOCUMENTO**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| --- | --- | --- | --- | --- |
| **Autor (es)** | Henry Eduardo Bastidas Paruma | Experto temático | Regional Cauca - Centro de teleinformática y producción industrial. | Septiembre 2021 |
| Luis Fernando Botero Mendoza | Diseñador Instruccional | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica. | Septiembre 2021 |
| Ana Catalina Córdoba Sus | Revisora Metodológica y Pedagógica | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica. | Septiembre 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor pedagógico | Regional Santander - Centro Industrial del Diseño y la Manufactura. | Septiembre 2021 |
|  | José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica. | Septiembre del 2021. |

1. **CONTROL DE CAMBIOS**

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

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