**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

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

| COMPETENCIA | 220501110. Implementar el Sistema de Seguridad de la Información según modelo y estándares técnicos. | RESULTADOS DE APRENDIZAJE | 220501110-03. Realizar un uso adecuado y responsable de los recursos tecnológicos para garantizar la integridad de la persona. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 003 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Riesgos asociados al uso prolongado de las nuevas tecnologías |
| BREVE DESCRIPCIÓN | El mundo digital brinda herramientas y servicios para el desarrollo personal y profesional de las personas, pero es indispensable conocer los riesgos asociados del uso de tecnologías que están en tendencia; este componente busca identificar y establecer los riesgos asociados al uso prolongado de la tecnología, su uso responsable, las repercusiones en la salud y los delitos, fraudes y amenazas. |
| PALABRAS CLAVE | Amenaza, ciberbullying, delitos, fraude, riesgo |

| ÁREA OCUPACIONAL | 4 - Ciencias sociales, educación, servicios gubernamentales y religión |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:**

**Introducción**

* 1. **Riesgos o amenazas asociados al uso de las nuevas tecnologías**
  2. Uso prolongado de dispositivos
  3. Riesgos y recomendaciones de buen uso
  4. Uso prolongado de redes sociales
  5. **Fraude electrónico**
  6. **Delitos contra la propiedad intelectual**
  7. **Amenazas a la privacidad**
  8. **Ciberbullying o ciberacoso**

1. **DESARROLLO DE CONTENIDOS:**

**Introducción**

Las tecnologías de información y comunicación han crecido vertiginosamente en los últimos años, pero, ¿se conocen las implicaciones que tiene acceder a esas tecnologías e intercambiar información con otras personas?

Por ello, se invita a observar el video para conocer el abordaje conceptual del componente:

****

* + - 1. **Riesgos o amenazas asociados al uso de las nuevas tecnologías**

Las nuevas herramientas tecnológicas brindan oportunidades de comunicación, así, las redes sociales son de las más importantes porque se enfocan en el ocio y entretenimiento, permiten una comunicación permanente síncrona y asíncrona con amigos y familiares e, incluso, con personas totalmente desconocidas, pero...

| Las TIC no solo aportan innumerables ventajas y oportunidades, están acompañadas de diversos inconvenientes y peligros que afectan directamente la integridad y privacidad de la información que se comparte. |  |
| --- | --- |

* 1. **Uso prolongado de dispositivos**

El uso abusivo y prolongado de dispositivos electrónicos afectan tanto física como mentalmente a las personas, generando depresión, ansiedad, riesgo de suicidio y adicciones; así como fallas en la atención, memoria y aprendizaje. El siguiente recurso ampliará la información con respecto al uso prolongado de los dispositivos:



* 1. **Riesgos y recomendaciones de buen uso**

Es importante conocer los riesgos de utilizar tecnologías digitales, y ser conscientes que hacer frente a ellos es un componente clave para tener una identidad digital. Las habilidades digitales no solo consisten en saber manejar un dispositivo a la perfección, sino también tener conciencia de que la seguridad de la información es igual a cuando se transita por un sector que no genera confianza y se toma las medidas necesarias para protegerse. En el mundo digital no es diferente, se debe cuidar que el uso de los dispositivos no genere una adicción digital, ya que en los últimos años ha desencadenado múltiples problemas físicos y mentales; entre los riesgos más comunes están:



¿Sabía que los riesgos ante el uso de los dispositivos podrían ser interminables?

Esto debido a que el uso excesivo de la tecnología se ve sesgado por el autocontrol por la cantidad de información que recibe a diario el cerebro. Por ello, es importante tomar en cuenta algunas consideraciones para evitar problemas físicos y psicológicos que harán que la tecnología esté bajo el control del usuario y no al contrario.

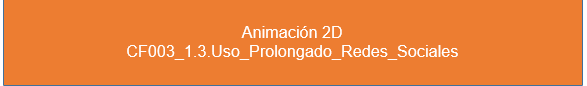
| El ser humano es pensante y racional, capaz de discernir cuando es el momento de hacer un alto y no depender de un aparato electrónico. |
| --- |

A continuación, se enlistan las recomendaciones para un buen uso de la tecnología:

****

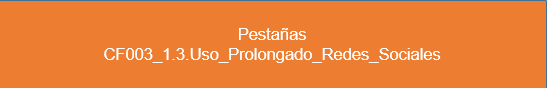
* 1. **Uso prolongado de redes sociales**

El uso excesivo de los perfiles en redes sociales y el aumento de las mismas en la era digital es cada vez más común. A continuación, se expone un recurso que permitirá conocer más sobre el tema:



Ese exceso del uso de redes sociales, se puede dar por entendido cuando la cantidad de horas de uso afecta al normal desarrollo de la vida cotidiana (Castellana, Sánchez-Carbonell, Graner y Beranuy, 2007; Viñas, 2009) y no solo por lo que se refiere al tiempo invertido, sino también por el impacto que causa en aspectos personales y sociales de la vida, donde se acerca a los que están lejos y se aleja a los que están cerca, tal como suelen decir los eruditos en el tema.

Por ello, se relacionan las consecuencias del uso prolongado frente a la utilización prolongada de las redes sociales, a saber:

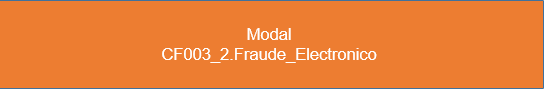


* + - 1. **Fraude electrónico**

Como una de las costumbres más marcadas dentro de la actual sociedad, está el uso de las herramientas informáticas, lo que hace que sea más vulnerable a ataques cibernéticos y a los fraudes electrónicos, pues normalmente se comparten información revelando datos importantes de identidad, lo que es un espacio propicio para delincuentes.

|  | La virtualización de muchas actividades ha transformado las bases de la sociedad y es comúnmente conocida como *sociedad de la información y del conocimiento,* que radica su fundamento en utilizar dispositivos digitales para las tareas diarias tales como comprar, vender, realizar operaciones financieras entre otras, a través de un solo clic. |
| --- | --- |

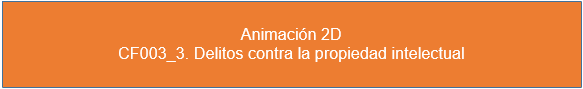
A continuación, se relacionan los fraudes electrónicos más populares que segundo a segundo se están cometiendo detrás de una pantalla, como el robo de identidad, el *phishing*, el *vishing* y el *smishing*:



* + - 1. **Delitos contra la propiedad intelectual**

En la Carta Magna de Colombia de 1991, en el artículo 61, reza: “El Estado protegerá la propiedad intelectual, por el tiempo y mediante las formalidades que establezca la ley”.

Quiere decir esto que se deberá proteger jurídicamente todos los derechos de autor y dar reconocimiento a aquellos que investigan, crean y brindan información importante reconocida y verificada. Es importante conocer cuáles son los tipos de propiedad intelectual para que no incurrir en posibles delitos por falta de conocimiento y se generen apuros por compartir información que no es propia, entre los más destacados, según la OMPI (Organización Mundial de la Propiedad Intelectual), se encuentran:

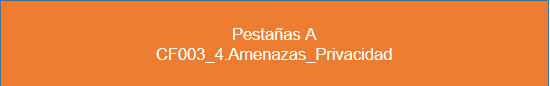


* + - 1. **Amenazas a la privacidad**

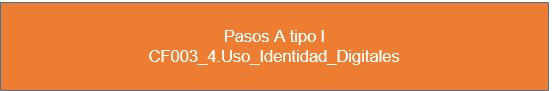
Tanto en las redes sociales como en internet en general, se está propenso a que se filtren los datos personales debido a que se acepten términos y condiciones sin leer previamente como en un ciberataque realizado por un pirata informático o los tan mencionados *hackers*; la privacidad en sí comprende las actividades que se llevan a cabo en un ámbito reservado; en internet se entiende como el control sobre la información para limitar la cantidad de personas autorizadas a acceder a la misma. Esto incluye datos personales, fotografías, documentos, conversaciones, entre otras.

| Cuanta más información proporcionas en Internet, más difícil es preservar tu privacidad. | Los sitios que se frecuentan en internet muchas veces modifican las condiciones y políticas de privacidad y en la era actual, hay una cultura de aceptar sin lectura previa es más común de lo que parece exponiendo datos que antes estaban con acceso restringido. |
| --- | --- |

El mundo digital no es ajeno a riesgos y amenazas a las cuales un usuario está expuesto, pues la información es muy susceptible a que sea usada por terceros para sus propios fines y que son delictivos, esto hace que la privacidad sea un flanco para personas inescrupulosas que están prestas para vulnerar la seguridad digital; entre las prácticas más comunes que pueden afectar la seguridad y privacidad, se pueden listar:



Es así como, frecuentemente, se descuida la forma cómo y a quién se entrega información y datos importantes, lo cual repercute en cómo se usa la identidad digital en la red, es por ello que se debe de tener en cuenta:

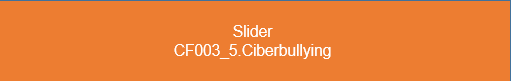


* + - 1. **Ciberbullying o ciberacoso**

Según la Unicef (2010), para iniciar a describir este fenómeno muy popular, se hace indispensable conocer la definición del término “*bullying*”, que se traduce en sinónimos como atemorizar, excluir, golpear, insultar, intimidar, ridiculizar, provocar o incomodar a una persona, es por ello que hay que estar atentos a los signos de alerta que pueden presentar los niños, niñas, adolescentes y hasta adultos frente a estos temas de interés para el buen desarrollo socio emocional de una persona, más aún cuando los medios electrónicos presentes están en el diario vivir de una persona por medio de redes sociales y otras herramientas que son de uso cotidiano.

|  | Es importante estar atentos a los cambios en comportamiento, lenguaje o pensamiento, ya que el hostigamiento *online* es una práctica bastante común entre los usuarios de internet, incluso se presenta de forma pasiva sin darnos cuenta. El ciberbullying tiene bastantes semejanzas con el *bullying* tradicional (discriminación), aunque su manifestación y características son propias y es fundamental conocerlas para una sana convivencia social-digital pacífica y libre de discriminación. |
| --- | --- |

Las personas no pueden dimensionar los alcances que pueden llegar a tener lo que se publica en la red y que puede llegar a millones de usuarios en cuestión de segundos. El ciberacoso se ha vuelto una normalidad cuando se navega en internet, puesto que se presenta de manera pasiva (cuando se ve alguna imagen cuyo fin sea hacer gracia) y de manera activa (cuando ven comentarios xenófobos y ofensivos en comentarios o reseñas) por lo cual ya no es ningún tabú y, de hecho, se divide en varias facciones para identificar su tipo, tal como se relaciona a continuación:



El ciberbullying tiene diferentes características las cuales permite serconsciente que esta práctica es más común de lo que crees, la era digital es un hecho y ha cambiado muchas formas de pensamiento, es importante conocer cuáles son sus características más relevantes y poner “*stop*” a esas malas prácticas de uso de las nuevas tecnologías emergentes y construir una identidad digital pertinente y segura para todas las personas. A continuación, se relacionan estas características:

| Viralización | No hay olvido | Múltiples dispositivos |
| --- | --- | --- |

El acoso incorpora diferentes actores en los cuales se relacionan roles específicos, esto para que se materialice y de lo cual depende la forma cómo se lleve a cabo, ya sea por:



Usualmente los agresores se esconden bajo el anonimato, perfiles con datos falsos con o sin experticia en temas informáticos y la huella digital con la que actúan siempre es con información no real, es por ello que se hace necesario aprender a identificar los actores que intervienen en el ciberacoso:

|  |
| --- |

1. **ACTIVIDADES DIDÁCTICAS**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Quiz de conocimientos |
| Objetivo de la actividad | Apropiar conocimientos de los riesgos y amenazas a los cuales se exponen los usuarios digitales al hacer uso de las nuevas herramientas tecnológicas. |
| Tipo de actividad sugerida | Opción múltiple |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo documento en Word llamado Actividad didáctica 1 |

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 |
| --- | --- | --- | --- |
| Riesgos y Amenazas, redes sociales | Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2017). *Cartillas de Seguridad para Internet.* https://cartilla.cert.br | Cartilla | https://cartilla.cert.br |
| Fraudes electrónicos | Sánchez, G. (2012). Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos. *Boletín de Información, 324*, 67-88. <https://dialnet.unirioja.es/descarga/articulo/4198948.pdf> | Artículo | <https://dialnet.unirioja.es/descarga/articulo/4198948.pdf> |
| Ciberbullying | Molina, M., Furnari, A., y Hagelstrom, I. (2017. *Guía de sensibilización sobre convivencia digital*. https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia\_ConvivenciaDigital\_ABRIL2017.pdf | Cartilla | https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia\_ConvivenciaDigital\_ABRIL2017.pdf |
| Edusalta. (2015). *Cyberbullying - Guía práctica para adultos.* http://www.edusalta.gov.ar/index.php/docman/secretaria-de-planeamiento-educativo/buenas-practicas-de-convivencia-institucional/2728-cyberbullying-guia-practica-para-adultos | Cartilla | http://www.edusalta.gov.ar/index.php/docman/secretaria-de-planeamiento-educativo/buenas-practicas-de-convivencia-institucional/2728-cyberbullying-guia-practica-para-adultos |
| Fernández, J. (2018). *CiberBullying. Guía rápida para la prevención del acoso.* https://www.ararteko.eus/RecursosWeb/DOCUMENTOS/1/1\_1218\_3.pdf | Cartilla | https://www.ararteko.eus/RecursosWeb/DOCUMENTOS/1/1\_1218\_3.pdf |

1. **GLOSARIO:**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Amenaza | peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de manera accidental, se presente con una severidad suficiente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medios de sustento, la prestación de servicios y los recursos ambientales (Ley 1523 de 2012). |
| Amenaza tecnológica | amenaza relacionada con accidentes tecnológicos o industriales, procedimientos peligrosos, fallos de infraestructura o de ciertas actividades humanas, que pueden causar muerte o lesiones, daños materiales, interrupción de la actividad social y económica o degradación ambiental. Algunas veces llamadas amenazas antropogénicas. Ejemplos incluyen contaminación industrial, descargas nucleares y radioactividad, desechos tóxicos, ruptura de presas, explosiones e incendios (Lavell, 2007, en UNGRD, 2017). |
| Bloquear | impedir o restringir el acceso de una persona o usuario concreto a un entorno digital determinado. Este puede ser un videojuego, un canal de chat, o una red social. Cualquier contexto en el que el acoso pueda tener lugar. Para entenderlo en el contexto del ciberacoso, “será importante bloquear a los acosadores” para que no ejerzan el hostigamiento. |
| Ingeniería social | tácticas utilizadas para obtener información y datos sensibles de la víctima. Muchas veces son claves o códigos de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y la falta de precaución de la víctima. |
| Peligro | fuente o situación con capacidad de producir daño en términos de lesiones, daños a la propiedad, daños al medio ambiente o una combinación de ellos (ARL Sura, 2017). |
| *Phishing* | tipo de estafa que combina *e-mails* falsos supuestamente enviados desde instituciones de confianza (bancos, empresas de internet, tiendas, entre otras), y que enlazan con sitios web ficticios. Esto, con el fin de engañar a los consumidores y convencerlos de entregar sus datos financieros como números de tarjeta de crédito, de cuenta bancaria, nombres de usuario y passwords, entre otros (SERNAC, 2021). |
| Privacidad | información sensible y privada que se comparte en internet para preservar la integridad de los datos y la información esta debe ser protegida a través de configuraciones y canales de privacidad de la información. |
| Riesgo | combinación de la probabilidad de que ocurra una o más exposiciones o eventos peligrosos y la severidad del daño que puede ser causada por éstos (ARL Sura, 2017). |
| Sextorsión | una vez alguien posee material sexual sobre otra persona, puede utilizarlo para realizar algún tipo de chantaje bajo la amenaza de publicar ese contenido sexual y privado de la otra persona. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2017) *Cartillas de seguridad para internet*. <https://cartilla.cert.br>

Díaz y García Conlledo, M. (s.f.). Delitos contra la propiedad intelectual e industrial especial atención a la aplicación práctica en España. *Derecho Penal y Criminología, 30*(88), 93-134. <https://revistas.uexternado.edu.co/index.php/derpen/article/view/612>

Edusalta. (2015). *Cyberbullying - Guía práctica para* *adultos.* <http://www.edusalta.gov.ar/index.php/docman/secretaria-de-planeamiento-educativo/buenas-practicas-de-convivencia-institucional/2728-cyberbullying-guia-practica-para-adultos>

Eset. (2014). *Top 5 de riesgos para la privacidad que debes conocer.* <https://www.welivesecurity.com/la-es/2014/08/29/top-5-riesgos-privacidad-debes-conocer/>

Fernández, J. (2018). *Ciberbullying. Guía rápida para la prevención del acoso* <https://www.ararteko.eus/RecursosWeb/DOCUMENTOS/1/1_1218_3.pdf>

Gallego, H. (2021). *¿Sabes en que consiste la tecnotoxicopatología?* [https://clinicalasamericas.lasamericas.com.co/Promoción-y-prevención/Blog/191sabes-en-qu233-consiste-la-tecnotoxicopatolog237a](https://clinicalasamericas.lasamericas.com.co/Promoci%C3%B3n-y-prevenci%C3%B3n/Blog/191sabes-en-qu233-consiste-la-tecnotoxicopatolog237a)

Iniseg. (2018). *Ciberseguridad al día, qué es oversharing, la sobreexposición en redes que nos persigue*. <https://www.iniseg.es/blog/ciberseguridad/oversharing-conocelo-y-frenalo/>

Molina, M., Furnari, A., y Hagelstrom, I. (2017). *Guía de sensibilización sobre convivencia digital.* <https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf>

OMPI, Organización Mundial de la Privacidad. (2021). *¿Qué es la propiedad intelectual?* <https://www.wipo.int/about-ip/es/>

Portafolio. (28 de octubre de 2015). *Amenazas que afectan la privacidad en Internet*. <https://www.portafolio.co/negocios/empresas/amenazas-afectan-privacidad-internet-36348>

Sánchez, G. (2012). Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos. *Boletín de Información, 324*, 67-88. <https://dialnet.unirioja.es/descarga/articulo/4198948.pdf>

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Pedro Javier Lozada Villota | Experto temático | Regional Cauca – Centro de teleinformática y producción industrial. | Agosto de 2021 |
| Paula Andrea Taborda Ortiz | Diseñadora instruccional | Regional distrito capital - Centro de diseño y metrología. | 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**

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