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.

Junio 2024

Tabla de contenido

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 consultar el siguiente video, para conocer el abordaje conceptual del componente:

Video 1. Riesgos asociados al uso prolongado de las nuevas tecnologías

Enlace de reproducción del video

Síntesis del video: Riesgos asociados al uso prolongado de las nuevas tecnologías
Las personas generalmente no tienen conciencia de las múltiples amenazas y consecuencias tanto a nivel personal o legal a las que se ven inmersos por utilizar plataformas digitales ya que muchos de sus datos personales, empresariales y privados se ponen a disposición pública y de terceros; estos datos pueden ser utilizados con fines delictivos que llegan a desprestigiar la imagen de aquellos que usan frecuentemente las herramientas tecnológicas en línea, al hacer uso de información sensible para otro tipo de fines diferentes a los iniciales. Los riesgos en internet se encuentran asociados al uso de las nuevas herramientas tecnológicas por lo que se hace necesario explicar detalladamente las amenazas a las cuales se encuentran las personas expuestas; es así como es muy acertado educar y concienciar en lo digital a los usuarios para potenciar el uso seguro y responsable de la información y de las herramientas que se encuentran hoy en día en los ecosistemas digitales y entornos virtuales. Para apoyar el desarrollo de habilidades digitales en cuanto a experiencias seguras en línea, este componente está dirigido para concienciar a los usuarios que están inmersos en el uso de herramientas tecnológicas; podrán encontrar información relevante y pertinente en el uso seguro y responsable de la información junto con la normatividad vigente.

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

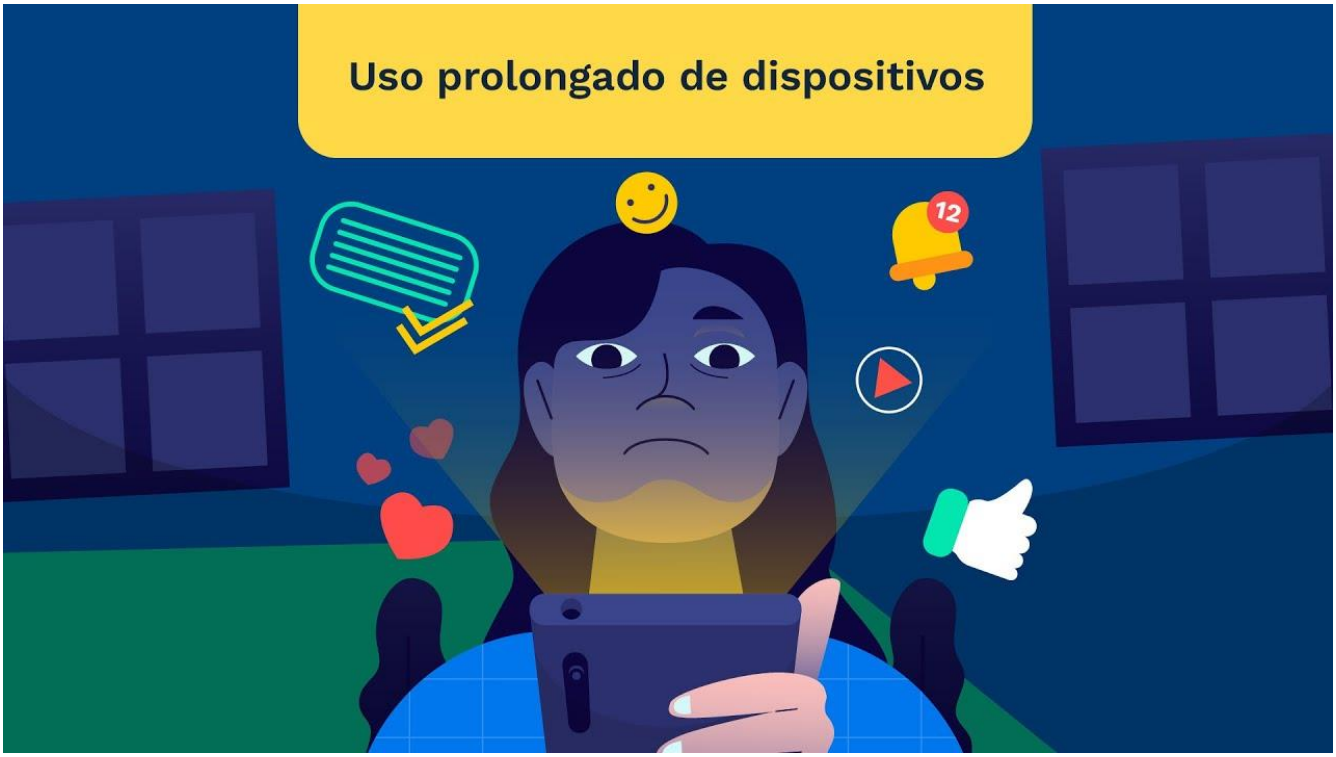
Las nuevas herramientas tecnológicas brindan oportunidades de comunicación, así, las redes sociales son de las más importantes porque se enfocan en el ocio y entretenimiento, permiten una comunicación permanente síncrona y asíncrona con amigos y familiares e, incluso, con personas totalmente desconocidas,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

1.1. Uso prolongado de dispositivos

El uso abusivo y prolongado de dispositivos electrónicos afecta 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 video ampliará la información con respecto al uso prolongado de los dispositivos:

Video 2. Uso prolongado de dispositivos



Enlace de reproducción del video

Síntesis del video: Uso prolongado de dispositivos
Hace mucho tiempo que la tecnología forma parte del diario vivir de las personas, incluso los dispositivos se convirtieron en un componente importante en el desarrollo social y cognitivo del ser humano. No obstante, estos aparatos causan serios problemas de salud y tienen consecuencias negativas, incluso mucho más afianzados en los nativos tecnológicos, ya que desde su nacimiento han tenido contacto directo con un mundo totalmente digitalizado sin dejar de lado a aquellos que han afrontado el cambio generacional y tecnológico a través del tiempo. Científicos han revelado que el uso abusivo de los dispositivos electrónicos es

potencialmente peligroso para la salud humana. En el año 1987 se realizó un experimento con animales de laboratorio en el que se expuso a hembras embarazadas y a machos a el efecto electromagnético de estos dispositivos, el resultado fue crías de menor peso y talla y en los machos testículos más pequeños. Asimismo, se pudo comprobar que la exposición abusiva a la tecnología disminuye la cantidad de sodio en la corteza cerebral y el hipotálamo.

El uso desmedido de estos dispositivos móviles provoca falta de concentración y un bajo rendimiento en el trabajo, además el insomnio, la ansiedad y los dolores musculares son algunas consecuencias para la salud del uso abusivo del teléfono móvil, pero no solo produce problemas para conciliar el sueño, se está procurando establecer que el teléfono móvil también incrementa las posibilidades de padecer cáncer de próstata y de mama e infertilidad. En cuanto al insomnio, con el uso continuo del teléfono móvil y las luces encendidas hasta altas horas de la noche al parecer la glándula pineal se activa mucho y el cerebro que es de día lo cual perpetúa la falta de sueño, también al recibir o esperar recibir mensajes o no recibirlos genera ansiedad y acentúa el insomnio.

1.2. 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 que la seguridad de la información es igual a cuando se transita por un sector que no genera confianza y se toman 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, porque en los últimos años, se han desencadenado múltiples problemas físicos y mentales; entre los riesgos más comunes están:

Figura 1. Riesgos por el uso de dispositivos

Figura 2. Otros riesgos por el uso de dispositivos

¿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:

- Realiza actividades de ocio diferentes a las ofrecidas por las tecnologías.

- Apaga o silencia tus dispositivos al menos dos horas antes de ir a descansar en la noche.
- Controla la información que se observa, evita páginas que no ayudan ni apoyen a tu autoestima.
- Accede a contenidos que ayuden al desarrollo cognitivo y emocional.
- Fija horarios y estipula prioridades.
- Deja a un lado los dispositivos cuando realices actividades como alimentarte, dormir y hacer ejercicio.
- Socializa de manera directa y guarda los dispositivos cuando estés en interacción con personas.
- Identifica cualquier síntoma de adicción digital o necesidad excesiva del uso de las tecnologías.

1.3. 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:

Video 3. Riesgos o amenazas asociados al uso de las nuevas tecnologías: uso prolongado de redes sociales

Enlace de reproducción del video

Síntesis del video: Riesgos o amenazas asociados al uso de las nuevas tecnologías: uso prolongado de redes sociales
La presencia de la tecnología ha formado adeptos en la personalidad que conducen a la aceptación social y desarrollo emocional, pues la utilización permanente de redes sociales puede conllevar al uso excesivo, lo que ocasiona un problema de salud pública; muchas personas que se encuentran con perfiles digitales en la red deben asumir los riesgos a los cuales están continuamente expuestos el principal es la adicción y su uso abusivo, además del acceso a contenidos

inapropiados el ciber bullying o la transgresión de la intimidad; esto puede fomentar riesgos asociados a la salud física y mental; tales como la anorexia y el suicidio.

La falta de personalidad de los internautas hace muchas veces que creen innumerables perfiles falsos, que conllevan a la baja autoestima y el autoengaño, donde llevan vidas paralelas desde lo real hasta lo ficticio; creando patrones en la conducta de trastornos bipolares, muchas veces estos perfiles hacen que las personas puedan hacer uso de la información de manera no adecuada, dejando ver datos desde lo más íntimo hasta estar pendientes de los likes o reacciones que hacen en sus posts o publicaciones.

Otro aspecto fundamental es consultar continuamente las huellas digitales de todo lo que publican otras personas, hasta límites como verificar horas de ingreso última conexión o accesos creando brechas comunicacionales entre sí; incluso vulnerando la intimidad de los demás y generando sentimiento de culpa y hasta comportamientos homicidas.

Las adicciones a las redes sociales muchas veces no son detectadas a tiempo, pues se piensa que es normal estar horas y horas pendientes de los dispositivos para chequear si hay notificaciones o nuevos post; pero debes de estar alerta a las siguientes señales que determinan la adicción y uso excesivo de redes sociales; insomnio, descuidar las labores estudiantiles, laborales y familiares, poner más atención a los dispositivos que a la familia o pareja, perder la noción del tiempo de conexión, sentirse irritado o desesperado cuando no hay conexión a internet, creer todo lo que se publica en las redes sociales.

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.

2. 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:

- **Robo de identidad**

  Es de las técnicas más utilizadas, como eres un usuario activo de las diferentes herramientas digitales en línea, ya posees una identidad digital y tus datos circulan por la red como si fueras por la calle de tu ciudad, es allí cuando un tercero puede usurpar tus datos y hacerse pasar por ti y sin aviso o permiso usan tus datos para realizar créditos, compras en línea, abrir cuentas, extorsiones y vulneran tu integridad. Esto sucede muy a menudo, porque se cometen errores como dejar a la vista de todos tus datos, contraseñas y claves que solo son de uso personal.

- **Phishing**

  Este término es acuñado por el anglicismo fishing, que en español significa “pesca”, y lo que hacen los delincuentes o hackers es que te engañan por medios electrónicos para que entregues información; la ingeniería social existente en el mundo digital hace que seas vulnerable y termines entregando contraseñas, cuentas bancarias, tarjetas de crédito sin darte cuenta y estas sean usadas con fines delictivos.

- **Vishing**

  Es una modalidad de fraude, que consiste en robar datos por medio de voz IP, te hacen llamadas haciéndose pasar por entidades bancarias, agencias de viaje, entre otros, engañándote con supuestos beneficios y lograr que les brindes información sensible; ha crecido tanto este sistema de fraude que ya los delincuentes pueden realizar este tipo de llamadas a terceros para poder acceder a tu información.

- **Smishing**

  Es un poco parecida a la anterior, la diferencia es que esta técnica de fraude la realizan por mensajería instantánea o texto en tus dispositivos móviles, donde se invita a la víctima a hacer clic en enlaces que no son verificados, para obtener supuestos bonos, premios y ofertas, y entregues información personal y accedan a tus contraseñas, claves, tarjetas de crédito, entre otras.

  Nadie está exento de caer en estas trampas, porque usan técnicas de ingeniería social y engaño para estafar y robar a las personas, pues existen múltiples formas de robo en plataformas online, es por ello que debes

estar alerta a cualquier signo o alarma de mensajes o llamadas que recibas para poder proteger la información.

3. Delitos contra la propiedad intelectual

En la Carta Magna de Colombia de 1991:

“El Estado protegerá la propiedad intelectual, por el tiempo y mediante las formalidades que establezca la ley”. Artículo 61

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 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:

Video 4. Delitos contra la propiedad intelectual

Enlace de reproducción del video

Síntesis del video: Delitos contra la propiedad intelectual
En el mundo globalizado y donde todo se viraliza en cuestión de segundos en la red porque todos están posteando millones y millones de datos de información, se hace inminente que el plagio esté a la orden del día. Una frase que te gustó, una imagen, un video o cualquier tipo de información, es sensible a que otro la tome y se atribuya derechos que no le corresponden porque se piensa que todo lo que hay en internet es gratis, no es de nadie y se puede reenviar, utilizar y hasta modificarlo según las conveniencias; pero no es así, dentro de cada estado, país o región existen normas y regulaciones que hacen que la actividad frecuente que tiene en internet sea tal vez un delito. Los principios jurídicos nos dicen que el desconocimiento de la ley no exime de su cumplimiento, muchas veces por ignorancia se toma información de terceros cuando esta está protegida y tiene derechos de autor; esto dentro del Código Penal está catalogado como plagio y puede generar serios problemas si no se da la atribución necesaria a sus autores. Son los derechos adquiridos por los creadores de obras literarias y artísticas de cualquier tipo que enmarcan libros, pinturas, tesis, monografías, software, entre otros, que son protegidos y reconocidos. Hace referencia a la invención de algo con la facultad que la comunidad pueda utilizarla ya sea con fines públicos o privados, tal como sucede con las vacunas, atribuyendo los derechos a quien la desarrolló, se atribuye a los signos, imágenes y publicidades de una empresa la cual representa de manera única y original sus productos y servicios, hoy en día es donde más existe plagio debido a los medios digitales.

Son modelos bidimensionales o tridimensionales que sirven de prototipos para nuevos productos o modificaciones de los mismos, tales como teléfonos, inmobiliario, electrodomésticos, entre otros. Es un derecho que se ha facultado como un símbolo para productos de origen específico, ya sea para sus cualidades o bondades del mismo, tales como el vino, el queso, especias, las cuales presentan condiciones especiales llamadas “sui generis” que consisten en las condiciones de protección compartidas en diferentes países para evitar conflictos entre los mismos; es la protección a la información de cada empresa y su información no puede ser divulgada ni compartida, su uso es netamente interno para el funcionamiento de la empresa y se hace con el fin de una libre competencia y uso comercial.

4. 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 aceptan términos y condiciones sin leer previamente, como en un ciberataque realizado por un pirata informático o los tan mencionados hackers.

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, la cual 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, porque la información es muy susceptible a que sea usada por terceros para sus propios fines, los cuales son delictivos, esto hace que la privacidad sea un blanco 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:

- **Oversharing**

  Es la sobreexposición en redes, es decir, que se publica todo tipo de información personal, lo que se hace, dónde y con quién se está, sobre todo en usuarios digitales nuevos que no logran dimensionar el alcance que tienen sus publicaciones, es una práctica muy negativa y se termina por entregarle la responsabilidad a la tecnología de lo malo que pueda pasar, sin darse cuenta de que simplemente radica en cómo se utiliza la tecnología de una forma arriesgada y desacertada.

- **Secuestro de información**

  Es una de las amenazas más típicas a la privacidad de la información, los ciberdelincuentes han desarrollado códigos maliciosos (malware) que tienen como objetivo robar la información personal o empresarial, encriptando los datos para después solicitar dádivas económicas de la propia información. Esta es una práctica muy común en países latinoamericanos, este tipo de infecciones llega al usuario con correos engañosos disfrazados con archivos que normalmente se conoce, pero lo que hacen es apoderarse de la información y esta deje de ser legible.

- **Protocolos inseguros**

  Así como tienes seguridad en tu casa para el ingreso con la llave, en el mundo digital es muy parecido, se llaman protocolos y muchas veces no se usan los más seguros, esto hace que sea muy fácil el ingreso a tus datos y puedan terminar en manos de terceros malintencionados.

- **Códigos maliciosos**

  Se debe tener mucho cuidado con toda la información digital que se recibe de terceros o remitentes sospechosos, porque suelen enviar archivos que contienen órdenes específicas para vulnerar la información. Estos artefactos de software tienen la tarea específica de averiguar contraseñas, monitorear tu actividad digital para robar información y que esta sea de dominio público, transgrediendo tu integridad para el secuestro o uso malintencionado de los datos.

- **Mal uso de la tecnología**

  La saturación de información, el analfabetismo tecnológico y las desviaciones psicopáticas son algunas de las características propias del mal

uso de recursos informáticos; las brechas generacionales desde los nativos tecnológicos hasta los que tuvieron que sufrir esta transición digital han hecho que la privacidad se vea afectada por no poder usar bien la tecnología, debes tener en cuenta que la era digital es un hecho y hay que estar preparados para que la información no caiga en manos de terceros.

- **Datos en manos de terceros**

  Todos los datos que compartes en Internet están sujetos a ser vulnerados, debido a que los servicios que se usan cotidianamente solicitan gran cantidad de información y estos son compartidos entre proveedores para hacerte llegar productos y servicios según tus preferencias, aunque esto tiene connotación legal, los datos reposan en sitios que no cumplen con las políticas de privacidad y es allí cuando tu información sensible puede ser pública afectando tu seguridad, es por ello que cada vez que te solicitan los datos personales verifica fuentes y así no te arrepientas de lo que se comparte.

- **Robo o pérdida de dispositivos**

  Una de las amenazas más latentes a la pérdida de los datos y afectación a tu privacidad, es la pérdida de información personal contenida en los dispositivos. Es habitual pensar que por ser dispositivos que solo tú manejas nunca los proteges, pero la delincuencia que, está a la orden del día, no solo puede afectar económicamente, sino psicológicamente, porque las prácticas del mal uso de la tecnología son muy comunes, es por ello que es mejor tener copias en nube y protegidas con contraseña, sincronizadas de manera segura.

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:

a) Configura los buzones de correo electrónico con confirmaciones de lectura.
b) Encripta los mensajes, existen programas y aplicaciones que logran que estos sean leídos solo por los destinatarios requeridos.
c) Almacena la información de forma que solo tú puedas acceder para que atacantes no puedan acceder a ellos.
d) Usa conexiones seguras y verifica que los navegadores sean de confianza.
e) Escribe directamente las URL o las direcciones electrónicas, evita al máximo apoyarte en los buscadores.
f) Realiza copias de seguridad encriptadas de manera que solo tú puedas acceder a la información de manera segura, tanto en los dispositivos físicos como en servicios de nube.
g) Define permisos de nivel medio o superior al aceptar cookies en la navegación, que no se aceptan de terceros creando listas de excepciones, incluso navegar de forma anónima.
h) Ten cuidado con la información que se publica en redes sociales, analiza y verifica qué se puede o no publicar.
i) Ten cuidado a la hora de crear contraseñas, no uses la misma para todas las plataformas y evita fechas de nacimiento, o datos que son fáciles de adquirir por los atacantes.
j) Protege los dispositivos con los cuales accedes a la red, estos son el medio por el cual pueden ingresar a tu información y vulnerar tu privacidad.

5. 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 socioemocional 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, porque 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:

- **Ciberbullying**

  Se caracteriza por presentarse generalmente entre menores de edad de manera intencional y reiterada por medio de insultos y amenazas.

- **Sextorsión**

  Se caracteriza, principalmente, por la extorsión con intenciones de carácter sexual hacia la víctima amenazando con exponer contenido sexual de ella.

- **Grooming**

  Es el acoso que realiza un adulto hacia un menor de edad con intenciones sexuales. Generalmente el mayor de edad se hace pasar por menor de edad para empatizar con la víctima y así ganar su confianza.

- **Ciberviolencia de género**

  Se presenta por una persona o grupo de personas hacia otra u otros del sexo opuesto, en el que se ejerce violencia a través de insultos, acoso, control, ataques, chantaje.

- **Sexting**

  Consiste en el envío de imágenes de índole sexual entre dos personas, generalmente de manera consensuada.

El ciberbullying tiene diferentes características las cuales permite ser consciente 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:

- **Hostigamiento**

  Envío de fotografías, imágenes, memes tratando de denigrar a las víctimas.
- **Exclusión**

  Bloqueo de páginas o accesos a sitios, foros, bloqueos de chat o plataformas digitales.
- **Manipulación**

  Uso de información sensible, ingreso a perfiles digitales que perjudiquen la reputación digital de la víctima.

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:

- **Agresores**

  Usuario que pretende humillar o denigrar a una persona usando medios digitales y plataformas electrónicas.

- **Víctimas**

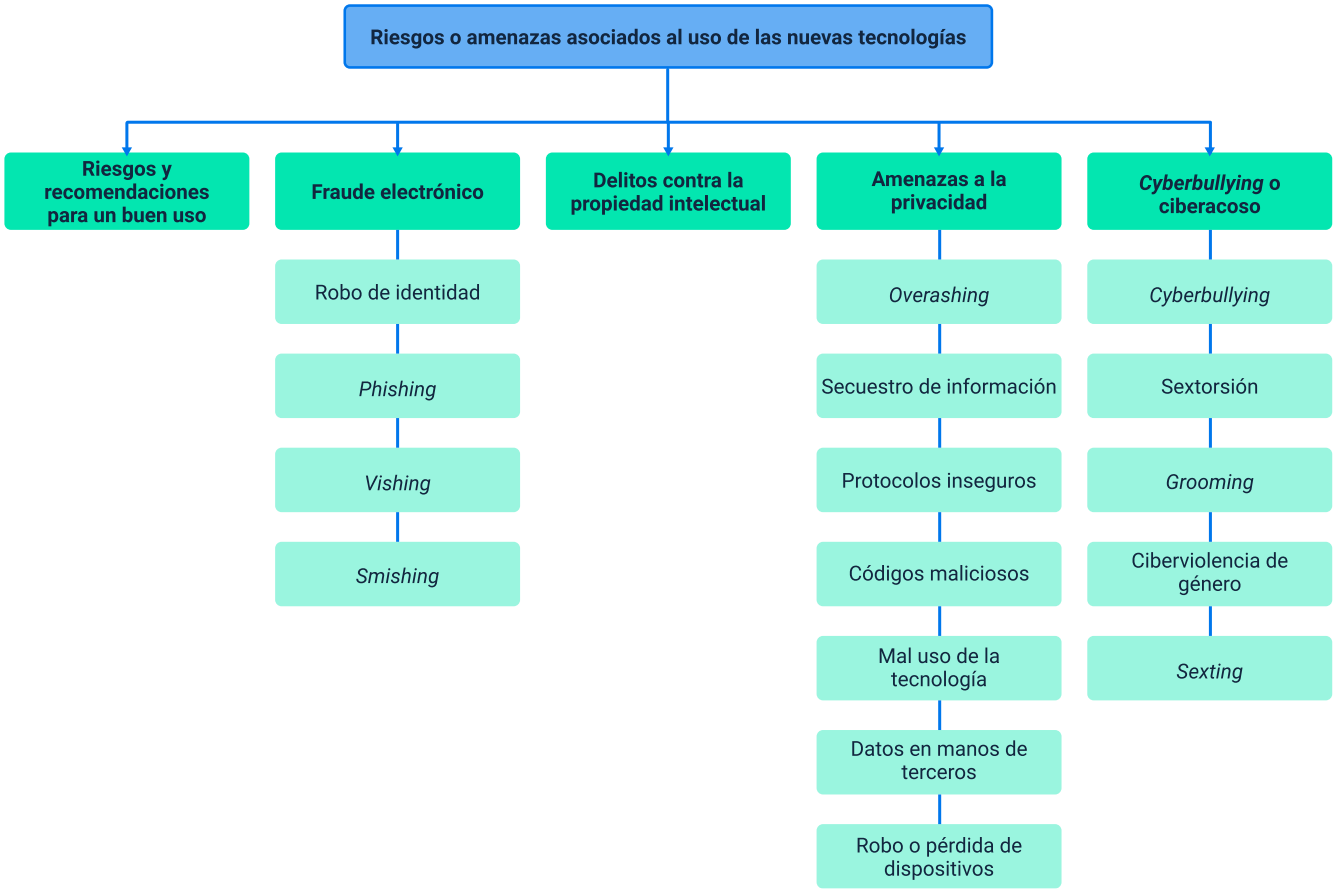
  Usuario que recibe las humillaciones, discriminaciones o comentarios lascivos por parte de personas que atacan directamente en sus post o publicaciones.

- **Espectadores**

  Son las personas que miran las humillaciones y agresiones que han hecho a las víctimas, aunque es un ente pasivo, hace parte de la cadena del ciberacoso y muchas veces se intimidan frente al acosador o agresor apoyando directa o indirectamente la agresión.

Síntesis

A continuación, se presenta a manera de síntesis, un esquema que articula los elementos principales abordados en el desarrollo del componente formativo. o.



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Riesgos o amenazas asociados al uso de las nuevas tecnologías	Cartilla de Seguridad para Internet. (s.f.). Navegar es necesario, ¡Arriesgarse NO!	Página web	https://cartilla.cert.br/
Fraude electrónico	Sánchez, G. (2012). Delitos en Internet: clases de fraudes y estafas y las medidas para prevenirlos. Boletín de Información, 324, pp. 67-88.	Artículo	https://dialnet.unirioja.es/descarga/articulo/4198948.pdf
Ciberbullying o ciberacoso	Molina, M., Furnari, A. & Hagelstrom, I. (2017). Guía de sensibilización sobre Convivencia Digital.	PDF	https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf
Ciberbullying o ciberacoso	Ministerio de Justicia y Derechos Humanos – Presidencia de la Nación. (2014). Cyberbullying - Guía práctica para adultos.	PDF	http://www.edusalta.gov.ar/index.php/docman/secretaria-de-planeamiento-educativo/buenas-practicas-de-convivencia-institucional/2728-cyberbullying-guia-practica-para-adultos/file
Ciberbullying o ciberacoso	Flores, J. y Casal, M. (2008). CiberBullying. Guía rápida para la prevención del acoso.	PDF	https://www.ararteko.eus/RecursosWeb/DOCUMENTOS/1/1_1218_3.pdf

Glosario

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: es el tratamiento que se debe brindar a la información sensible que se comparte en Internet. Esta información debe protegerse, a través de configuraciones y canales que permitan preservar la integridad de los datos que la constituyen.

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 estos (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.

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

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

Créditos

Nombre	Cargo	Centro de Formación y Regional
Milady Tatiana Villamil Castellanos	Responsable del Ecosistema	Dirección General
Olga Constanza Bermúdez Jaimes	Responsable de Línea de Producción	Centro de Servicios de Salud - Regional Antioquia
Pedro Javier Lozada Villota	Experto Temático	Centro de Teleinformática y Producción Industrial - Regional Cauca
Paula Andrea Taborda Ortiz	Diseñador Instruccional	Centro de Diseño y Metrología - Regional Distrito Capital
Rafael Neftalí Lizcano Reyes	Asesor Metodológico y Pedagógico	Centro Industrial del Diseño y la Manufactura - Regional Santander
Ana Catalina Córdoba Sus	Evaluadora Instruccional	Centro de Servicios de Salud - Regional Antioquia
Juan Daniel Polanco Muñoz	Diseñador de Contenidos Digitales	Centro de Servicios de Salud - Regional Antioquia
Jorge Armando Villamizar Moreno	Diseño Web	Centro Industrial del Diseño y la Manufactura - Regional Santander
Luis Jesús Pérez Madariaga	Desarrollador Fullstack	Centro de Servicios de Salud - Regional Antioquia
Edgar Mauricio Cortés García	Actividad Didáctica	Centro de Servicios de Salud - Regional Antioquia
Luis Fabian Robles Méndez	Desarrollo Front-end	Centro Industrial del Diseño y la Manufactura - Regional Santander
Andrés Mauricio Santaella Ochoa	Soporte Front-end	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Centro de Formación y Regional
Daniela Muñoz Bedoya	Animador y Productor Multimedia	Centro de Servicios de Salud - Regional Antioquia
Andrés Felipe Guevara Ariza	Locución	Centro de Servicios de Salud - Regional Antioquia
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro de Servicios de Salud - Regional Antioquia
Margarita Marcela Medrano Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro de Servicios de Salud - Regional Antioquia
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro de Servicios de Salud - Regional Antioquia