Ciber Sapiens

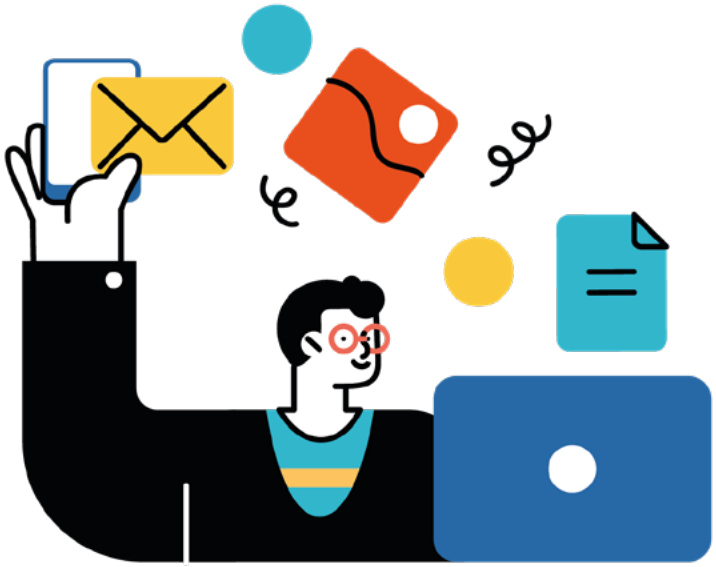
# Guía de recomendaciones

## Riesgos en línea

dirigida a docentes

UNIVERSIDAD EAFIT

ALCALDÍA MAYOR | SECRETARÍA EDUCACIÓN | BOGOTÁ



# Presentación

Este recurso hace parte de la caja de herramientas de CiberSapiens, la estrategia de uso creativo, seguro y responsable de internet de la Secretaría de Educación de Bogotá, que busca la promoción de la seguridad y confianza digital orientada a las comunidades educativas del Distrito.

En un mundo cada vez más conectado, las TIC e internet ofrecen oportunidades invaluables para enriquecer el proceso educativo y empoderar a los estudiantes para enfrentar los desafíos del siglo XXI. Sin embargo, también nos exige ser conscientes de los riesgos y responsabilidades asociados al uso de la tecnología.

Esta guía proporciona recomendaciones y acciones pedagógicas para los docentes que les permitirán abordar el uso seguro de internet a partir del reconocimiento de los riesgos más comunes en línea.

# ¿Cuáles son los riesgos en línea para nuestros estudiantes?

Internet y las tecnologías han abierto un mundo de oportunidades para los niños, niñas y jóvenes, permitiéndoles acceder a una amplia gama de información, entretenimiento y conexiones sociales. Sin embargo, también los ha expuesto a diversos riesgos en línea que requieren atención y comprensión.

Con sus mentes curiosas y ávidas de conocimiento, los estudiantes navegan por Internet para explorar, jugar, estudiar y conectarse con amigos. Pero detrás de este universo virtual se esconden peligros sutiles y amenazantes que pueden afectar profundamente su bienestar físico, emocional y psicológico. Desde el acceso a contenido inapropiado hasta la exposición a ciberacosadores, depredadores en línea y estafadores, la presencia en línea de los niños, niñas y jóvenes puede convertirse en un terreno minado si no se maneja adecuadamente.

Veamos algunos de los riesgos en línea más frecuentes, cómo identificarlos y algunas sugerencias para afrontarlos:

Haz clic en los botones para ampliar la información

- Ciberbullying o ciberacoso
- Grooming
- Sexting
- Phishing
- Ciberdependencia

# Ciberbullying o ciberacoso

## ¿De qué se trata?

Es una forma de acoso virtual, un fenómeno agresivo e intencional que se desarrolla en Internet y las redes sociales. Se dirige hacia individuos vulnerables como nuestros niños, niñas y jóvenes, aquellos que carecen de la capacidad para defenderse o sienten que no pueden hacerlo. El objetivo del ciberacoso es difamar de forma deliberada, repetitiva y hostil a la víctima. Los efectos de este hostigamiento pueden afectar negativamente el rendimiento académico, las relaciones sociales y otras áreas clave del desarrollo psicosocial de nuestros estudiantes.

## ¿Sabías qué?

**El 90% de los niños, niñas y jóvenes nunca informan a sus padres, cuidadores o docentes de haber sufrido ciberacoso.**

Juvonen, J., & Gross, E.F. (2008). Extending the school grounds? Bullying experiences in cyberspace. The Journal of School Health. 78, 9, 496-505

Cuando nos enfrentamos a una situación de ciberacoso, es esencial abordarla desde la responsabilidad y la empatía. Aquí tienes algunas recomendaciones para que puedas hacer frente a esta problemática:

**Observa y escucha:**
Presta atención a los comportamientos y comentarios que puedan indicar ciberacoso por parte de un estudiante. Escucha a los demás estudiantes si mencionan situaciones que revelen el ciberacoso.

**Comunica:**
Informa a los familiares o cuidadores del estudiante acosador y del estudiante afectado sobre la situación. Trabaja en conjunto con ellos para encontrar una solución adecuada.

**Recopila evidencia**
Si es posible, guarda evidencia del ciberacoso, como capturas de pantalla o registros de mensajes. Esto puede ser útil para demostrar el problema y tomar medidas.

**Promueve un ambiente seguro:**
Fomenta un ambiente de respeto y empatía ya sea en el aula, en las clases virtuales y demás espacios de socialización de los estudiantes. Habla con ellos sobre la importancia del respeto y el uso creativo,

**Acompaña:**
Habla con el estudiante que está llevando a cabo el ciberacoso y explícale las consecuencias de sus acciones. Anima a que se responsabilice de sus comportamientos.

**Educa:**
Realiza actividades educativas sobre el ciberacoso y sus consecuencias, propicia que tus estudiantes reflexionen sobre la importancia del respeto y la empatía en línea.

# Grooming

**¿De qué se trata?**

Se trata de una situación en la que un adulto establece una conexión maliciosa con un niño, niña o joven a través de dispositivos digitales e Internet, con intenciones sexuales. El agresor utiliza tácticas de manipulación y engaño para ganarse la amistad y confianza del menor, con el objetivo de obtener imágenes íntimas o mantener encuentros sexuales.

El acosador (también llamado groomer), actúa de manera sutil y sigilosa en Internet, con el propósito de obtener el control de la relación y explotar sexualmente al joven. Utiliza tácticas como el envío de mensajes, imágenes y regalos.

En este *juego de sombras*, es crucial estar alerta y empoderar a nuestros estudiantes para que reconozcan las artimañas de los manipuladores digitales.

## ¿Cómo se desarrolla el grooming?

1. **Vínculo inicial:**
El adulto establece un vínculo afectivo con el menor y obtiene gradualmente su información personal y de contacto.

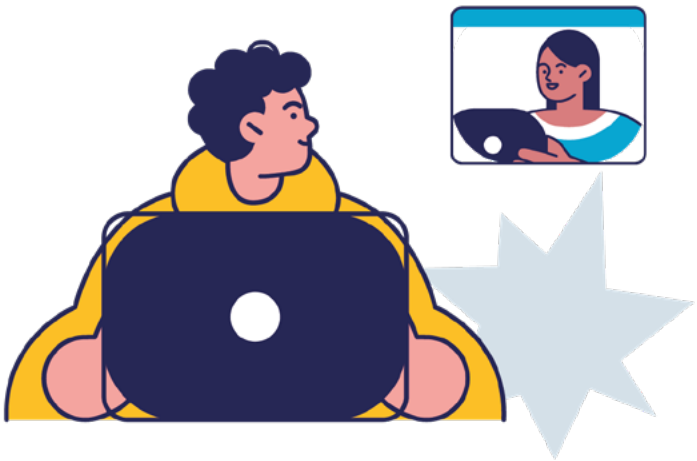
2. **Persuasión:**
El abusador convence al menor para que se desnude o realice actos sexuales mediante seducción amistosa, adulación, envío de regalos, etc.

3. **Activación:**
Cuando la víctima confía en el abusador, se vuelve más explícito en sus intenciones, enviando material pornográfico o preguntando sobre sus experiencias y preferencias sexuales.

4. **Contacto y manipulación:**
Finalmente, el adulto propone al menor que se conozcan personalmente, pero si este se niega, el abusador puede recurrir al acoso o al chantaje. Este proceso puede extenderse desde minutos hasta algunos días, varios meses e incluso años.

Si quieres conocer más sobre el grooming te invitamos a ver la serie web “Somos CiberSapiens”

https://www.youtube.com/playlist?list=PL3jXkGIjvcErSLqa40GOi_bbEGfpQo9Nx



# Sexting

## ¿De qué se trata?

Consiste en el envío, la recepción o el reenvío de mensajes, imágenes o videos sexualmente explícitos a través de medios electrónicos, como redes sociales o aplicaciones de mensajería instantánea, y es un comportamiento cada vez más frecuente entre jóvenes. La palabra es un acrónico en inglés formado por las palabras “*sex*” (sexo) y “*texting*” (escribir mensajes).

Las investigaciones apuntan a tres tipos diferentes de sexting:

**Sexting consensuado:**
Los participantes intercambian mensajes íntimos de forma consciente y sin chantajes ni presión. Se establecen acuerdos claros sobre lo que están dispuestos a compartir. Los expertos sostienen que esta práctica fomenta la exploración de la identidad sexual y fortalece la conexión emocional entre los involucrados.

**Sexting no consensuado:**
El envío, recepción o reenvío se hace sin el consentimiento de quien lo produjo.

En este contexto, los niños, niñas y jóvenes pueden enfrentar situaciones de acoso, chantaje o vergüenza, y consecuencias graves en su bienestar emocional y social.

**Sexting presionado:**
Es el producto de la presión ejercida por un amigo, familiar, compañero o conocido.

El sexting presionado ocurre cuando la persona se siente obligada, manipulada o coaccionada para enviar contenido sexualmente explícito.

**¡Ojo, profe!**

En cada caso es importante educar y sensibilizar a los estudiantes sobre los riesgos del *sexting*, enfocándose especialmente en las situaciones no consensuadas y en aquellas en las que existe presión. Además, se debe fomentar una comunicación abierta y un ambiente seguro para que los niños, niñas y jóvenes compartan sus preocupaciones.

## Phishing

**¿De qué se trata?**

Es el intento fraudulento de obtener información confidencial como nombres de usuario, contraseñas y detalles de cuentas bancarias o tarjetas de crédito, haciéndose pasar por una fuente confiable.

Después de que la víctima cae en la trampa, el método de phishing desencadena una red de sitios web fraudulentos que han sido diseñados para imitar la fuente genuina y lograr que las personas introduzcan sus datos personales en lo que aparenta ser una transacción legítima.

Si bien su arma predilecta es el correo electrónico, el phishing no se limita a este medio. Puede esconderse en mensajes de texto, llamadas telefónicas o incluso acechar en redes sociales.

**Colombia registró en 2022 más de 54.000 denuncias por delitos cibernéticos, superando ampliamente la cifra de 2021, cuando se documentaron 11.223. Los casos más comunes son a través de computadoras, tabletas y teléfonos celulares.**

Álvarez C. (13 de enero de 2023). Colombia registró un crecimiento de ataques informáticos en el último año. Voz de América. https://www.vozdeamerica.com/a/colombia-registro-crecimiento-ataques-informaticos-ultimo-ano-/6916577.html

## ¿Cómo reconocer y evitar casos de *phishing*?

Existen varias señales que pueden ayudarnos a detectar si estamos frente a un intento de *phishing*:

1. La presencia de subdominios, URLs mal escritas o sospechosas.

2. El uso de direcciones de correo electrónico públicas, como Gmail, Hotmail o similares, en lugar de direcciones corporativas (con el dominio de la empresa).

3. Los mensajes suelen presentar una apariencia urgente y, en ocasiones, intimidante. Utilizan frases como "tu cuenta ha caducado", "tus servicios podrían bloquearse si no pagas".

4. Solicitan verificar información personal, como datos bancarios o contraseñas.

5. Los mensajes contienen errores de ortografía o están mal redactados.

6. Los logos e imágenes parecen desproporcionados o no coinciden con los colores habituales de la empresa.

7. Los estilos del correo electrónico son incoherentes o no coinciden con los habituales.

Reconocer y evitar casos de phishing en tu institución educativa es fundamental para proteger la información personal y sensible de los estudiantes, maestros, directivos docentes, familiares y cuidadores. Aquí tienes algunos consejos para identificar y prevenir el phishing:

**Educar a la comunidad educativa es fundamental,** ya que la concienciación desempeña un papel crucial en la prevención del phishing. Se pueden llevar a cabo sesiones de capacitación y sensibilización para enseñar a los miembros de la comunidad a identificar correos electrónicos, mensajes y enlaces sospechosos.

**Mantén el software actualizado**, asegúrate de que todos los dispositivos y software utilizados en la institución educativa estén actualizados con las últimas actualizaciones de seguridad para protegerse contra vulnerabilidades conocidas.

**Utiliza software de seguridad**, es importante instalar y mantener actualizado un software antivirus y antimalware en todos los dispositivos utilizados en la institución educativa.

**Reporta posibles casos de phishing**, establece un proceso para que los miembros de la comunidad educativa puedan reportar correos electrónicos o mensajes sospechosos. Cuanto más rápido se identifiquen los intentos de phishing, más fácil será tomar medidas para protegerse.

## Ciberdependencia

### ¿De qué se trata?

También conocida como adicción a la tecnología, la ciberdependencia es una condición en la cual perdemos el control sobre el uso racional de dispositivos digitales e Internet. Es como si quedáramos hipnotizados por la magia del ciberespacio, dedicando horas interminables a deslizarnos por redes sociales, sumergirnos en aplicaciones y devorar contenido digital compulsivamente. Esta adicción abarca el uso excesivo de computadoras, teléfonos móviles, tabletas, consolas de videojuegos y otros dispositivos conectados a Internet.

Los niños, niñas y jóvenes atrapados en la ciberdependencia pueden experimentar un impacto negativo en su rutina diaria, lo que repercute en sus relaciones con amigos, compañeros y familiares, su rendimiento escolar y su bienestar tanto emocional como físico.

# Actividad

## ¡Vamos a jugar!

**¿Has presentado alguna de estas conductas en un momento de tu vida?**

**A continuación, te presentamos el termómetro de la ciberdependencia. Cada vez que reconozcas una de estas conductas en tu vida cotidiana, pinta un espacio del termómetro de la ciberdependencia, esto te dará un panorama de qué tan dependiente eres de los dispositivos digitales y el internet.**

**Phubbing:** entendido como la unión de las palabras *phone* (teléfono) y *snubbing* (despreciar), hace referencia a la conducta de ignorar a las personas que están a nuestro lado por estar pendientes de los dispositivos digitales.

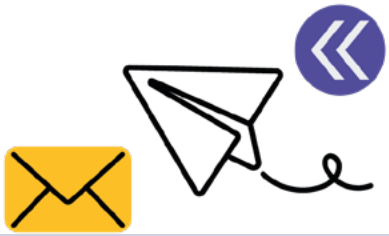
**Textofrenia:** es la ansiedad que siente una persona por recibir mensajes de texto o a través de aplicaciones móviles.

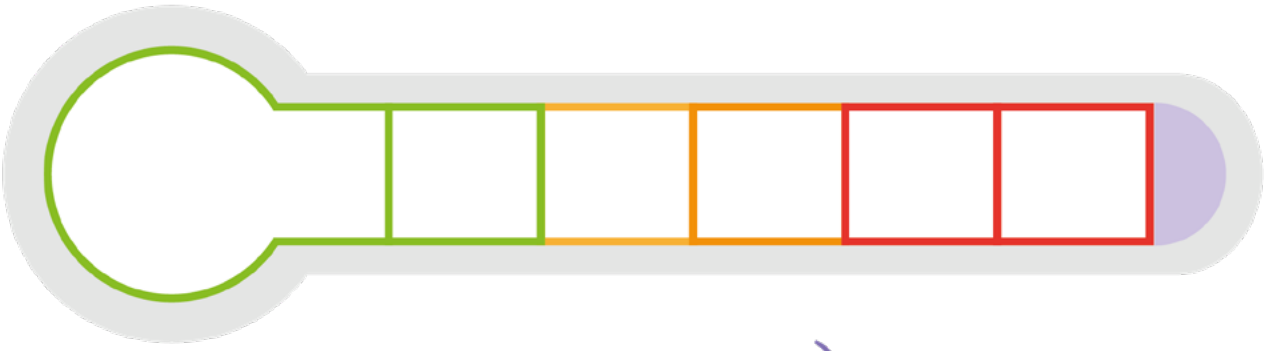
**Nomofobia:** hace referencia al temor excesivo de no tener a mano un dispositivo electrónico o de quedarse sin acceso a internet.

**Vamping:** es la unión de las palabras vampire (vampire) y texting (envío de mensajes) y corresponde a un comportamiento en el cual la persona usa los dispositivos electrónicos hasta altas horas de la noche.

**Taxiedad:** hace referencia a la sensación de ansiedad que surge cuando no se obtiene una respuesta inmediata después de enviar un mensaje de texto o a través de aplicaciones móviles.

**Síndrome mensaje múltiple:** es una conducta y sentimiento de angustia, que consiste en la necesidad de sentirse incluido socialmente a través de grupos o chats de mensajería instantánea.





**Sugerencias metodológicas:**

Introducción y explicación: Antes de comenzar la actividad, es importante explicar en qué consisten las diferentes conductas de ciberdependencia, como el phubbing, la nomofobia, etc. Asegúrate de que los estudiantes comprendan claramente cada concepto.

Entrega el termómetro: proporciona a cada estudiante una hoja con un termómetro en blanco, también puedes hacer que los estudiantes dibujen su propio termómetro.

Autoevaluación: Pide a los participantes que se autoevalúen y marquen cuántas de estas conductas reconocen en su vida cotidiana.

Discusión en grupo: Después de completar la actividad puedes fomentar una discusión en grupo. Pregunta a tus estudiantes cómo se sienten con respecto a sus resultados, si están sorprendidos por alguna de sus conductas, y si desean cambiar algo en su relación con la tecnología.

## Acciones pedagógicas de prevención para docentes

A continuación, tienes una serie de acciones pedagógicas que pueden ayudarte a prevenir problemas relacionados con el uso de la tecnología en tus estudiantes. Estas acciones siguen el protocolo propuesto por el Ministerio de Educación (2020)[1].

Promover el conocimiento y manejo de los riesgos relacionados con el uso de las TIC, siendo un ejemplo que seguir para los estudiantes.

Motivar a los estudiantes a adoptar una actitud positiva y valiente frente a los riesgos, en lugar de temerles sin tomar medidas para protegerse.

Estimular la identificación de posibles riesgos y amenazas digitales que los estudiantes pueden enfrentar al explorar, generar o compartir información en sus asignaturas y actividades.

Ampliar la información de los estudiantes sobre los riesgos asociados al uso de la tecnología digital mediante el análisis de casos, videos, películas, noticias y contenido presente en las redes.

Analizar con los estudiantes las razones que convierten ciertas situaciones en riesgos o amenazas para su bienestar personal o colectivo, fomentando el pensamiento crítico, tanto en situaciones de la vida real como en ejemplos audiovisuales.

Ayudar a los estudiantes a reflexionar sobre sus motivaciones, emociones, creencias y expectativas personales que los llevan a involucrarse en riesgos digitales.

Explorar junto a los estudiantes su responsabilidad personal en diferentes situaciones de riesgo digital, al exponerse innecesariamente, participar activamente o no buscar ayuda o información relevante.

Destacar la responsabilidad de los estudiantes en cuanto a las consecuencias que sus acciones digitales puedan tener sobre otras personas, conocidas o desconocidas.

Hacer hincapié en el papel que juegan los estudiantes en situaciones de ciberacoso, al comentar, aprobar, etiquetar, postear o compartir contenido ofensivo sobre otros.

Indagar si los estudiantes están al tanto de las posibles consecuencias personales, institucionales y legales de participar en situaciones en línea que vulneren el derecho a la intimidad, la honra y el buen nombre de otras personas.

Verificar con los estudiantes su conocimiento acerca de los protocolos y procedimientos institucionales para enfrentar situaciones de ciberacoso y delitos tecnológicos, mediante ejercicios simulados.

Evaluar las habilidades técnicas y socioemocionales de los estudiantes para manejar los riesgos asociados con el uso de tecnología digital, a través de situaciones simuladas en las que puedan estar involucrados.

Desarrollar junto a los estudiantes un listado de recursos y necesidades de información y formación en competencias que el grupo requiere para fortalecerse frente a los riesgos en el uso de las TIC.

Colaborar con los estudiantes en la creación de planes de acción personalizados para fortalecerse ante los riesgos digitales, considerando sus propios recursos y los de la institución.

Identificar con los estudiantes cuándo es necesario buscar apoyo de expertos tecnológicos aliados para fortalecer sus estrategias de protección y gestionar esta ayuda con la institución.

Estimular la generación de propuestas para involucrar a padres, estudiantes y docentes en el fortalecimiento frente a los riesgos asociados con la ciber tecnología.

Facilitar que los estudiantes desarrollen su propio conjunto de herramientas para enfrentar las ciberamenazas.

Motivar a los estudiantes a crear material digital que pueda ser utilizado para alertar y fortalecer a la comunidad educativa en relación con los riesgos digitales.

# Actividad
## de reflexión

**Tómate un momento para reflexionar y responde las siguientes preguntas:**

**¿Has tenido algún estudiante que haya experimentado alguno de estos riesgos en tu institución educativa? En caso afirmativo, ¿cómo manejaste la situación?**

**¿Cuáles crees que son las posibles consecuencias que puede traer alguno de estos riesgos en Internet para los estudiantes involucrados?**

¿Qué estrategias y medidas preventivas consideras efectivas para abordar y prevenir estos riesgos en Internet?

# Canales de atención

**Conoce los canales de atención a los que puedes acudir para reportar situaciones de riesgo y delitos informáticos.**

**CAI virtual de la policía**

Puedes comunicarte para solicitar apoyo o presentar una denuncia relacionada con delitos de ciberseguridad.

CaiVirtual

@CaiVirtual

Cai Virtual

+57 3202948647

www.caivirtual.policia.gov.co

Comunícate

**Te protejo**

**Comunícate para reportar una situación que afecta a niños, niñas y/o jóvenes.**

www.teprotejo.org

Comunícate

Ciber Sapiens

UNIVERSIDAD EAFIT

ALCALDÍA MAYOR | SECRETARÍA EDUCACIÓN | BOGOTÁ