

# Guía de recomendaciones

## Riesgos en línea de nuestros niños, niñas y jóvenes



dirigida a familias y cuidadores





## 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 invaluableles 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 para las familias y cuidadores que les permitirán abordar el uso seguro de internet a partir del reconocimiento de los riesgos más comunes en línea.





 Haz clic en los botones para ampliar la información

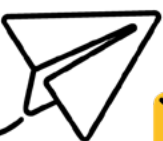
**01 CIBERACOSO**

**02 GROOMING**

**03 SEXTING**

**04 PHISHING**

**05 CIBERDEPENDENCIA**





# Las cinco W del internet

01

## ¿Qué es el Internet?

Imaginemos que el internet es como un gran espacio en el que todas las computadoras del mundo pueden hablar entre sí. Es como un lugar gigante donde la información viaja como correos electrónicos o mensajes.

02

## ¿Cómo funciona?

Pensemos en el internet como un camino de cables invisibles. Cuando enviamos fotos, mensajes o buscamos información, estos viajan por esos cables como si fueran paquetes pequeños, y luego se ensamblan para que podamos ver lo que queremos en nuestros computadores, celulares, tabletas, otros.

03

## ¿Quiénes lo usan?

Casi todos pueden usar el internet si tienen un celular, una tableta o un computador. Niños, niñas y jóvenes de todo el mundo utilizan el internet para aprender, conectarse con amigos, jugar, descubrir cosas nuevas y explorar un mundo lleno de posibilidades en línea.



04

### ¿Para qué se usa?

Usamos el internet de manera segura y responsable para aprender sobre diversos temas, explorar nuevas ideas y pasiones, conectar con amigos y familiares, compartir nuestras creaciones, acceder a recursos educativos en línea o descubrir formas emocionantes de crecimiento personal y social en un entorno digital.

### ¿Por qué es importante?

El internet es como una gran biblioteca que está siempre abierta. Abre un mundo de oportunidades creativas a niños, niñas y jóvenes para que exploren sus intereses, se expresen a través de la creación de contenido único, aprendan de forma interactiva, y se conecten con personas de todo el mundo. Fomenta la creatividad y el desarrollo personal, preparándolos para un futuro lleno de posibilidades y contribuyendo a su crecimiento en una sociedad cada vez más conectada.

05

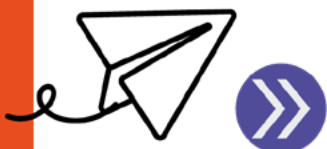


# ¿Cuáles son los riesgos más comunes a los que los niños, niñas y jóvenes están expuestos mientras navegan en línea?

Internet nos brinda un sinnúmero de oportunidades para facilitar muchas de las actividades cotidianas y contribuir a nuestro desarrollo personal. Desde la educación en línea hasta la comunicación global instantánea, el acceso a información y la posibilidad de conectarnos con personas de todo el mundo han revolucionado la forma en que interactuamos en el entorno digital.

A medida que nuestros horizontes digitales se expanden, también aumenta la exposición a amenazas en línea. Desde el ciberacoso hasta el robo de identidad y el acceso no autorizado a datos personales, la era digital ha introducido una serie de desafíos que deben abordarse con precaución. Somos responsables al educarnos sobre estos riesgos y tomar medidas para proteger nuestra seguridad y la de nuestros niños, niñas y jóvenes.

Conoce algunos de los cinco riesgos a los cuales nos exponemos diariamente al navegar por internet:





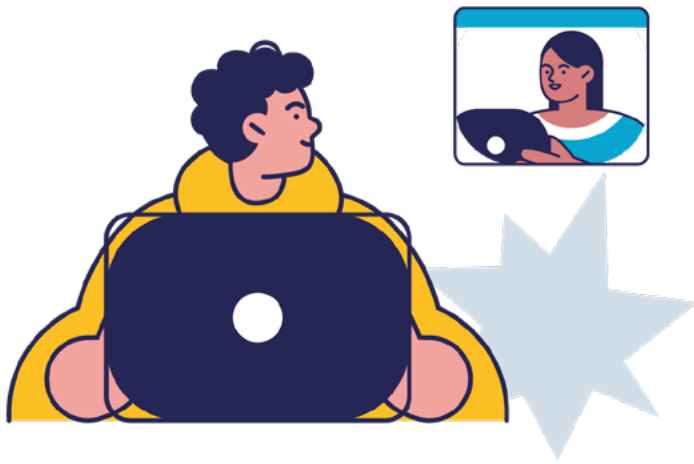
## Ciberbullying o Ciberacoso

Consiste en usar Internet, mensajes de texto u otras tecnologías para hacer daño a otra persona. Puede incluir asuntos como decir cosas malas sobre alguien en línea, amenazarlo o enviar mensajes crueles. Es como el acoso que ocurre en persona, pero sucede en línea.

Para comprender mejor el ciberacoso, te invitamos a ver este video que muestra cómo este tipo de comportamiento puede difundirse rápidamente a través de las plataformas digitales, teniendo un impacto negativo en la reputación y la autoestima de la víctima.



<https://www.youtube.com/watch?v=PNFiYVsost4>



## Grooming

Ocurre cuando un adulto trata de ganarse la confianza de un niño, niña o joven a través de internet para hacerle daño. Pueden fingir ser amigos y luego pedir imágenes, videos u otro contenido de carácter sexual o intentar encontrarse en persona.

Es importante estar atento a las señales que podrían indicar que alguien está intentando el grooming, tales como:

**Contacto excesivo:** La persona intenta comunicarse de manera excesiva, buscando ganar la confianza del niño o adolescente.

**Secretismo:** Solicita mantener el contacto en secreto, evitando que los padres o cuidadores se enteren.

**Búsqueda de información personal:** El delincuente pregunta sobre la vida personal, actividades y amigos del niño.

**Regalos y Favores:** Ofrece regalos, dinero o favores para establecer un vínculo emocional.





**Interés sexual prematuro:** Introduce conversaciones o comentarios de contenido sexual.

**Uso de halagos:** Elogia constantemente al niño, niña o joven, manipulando su autoestima.

**Fotos y videos:** Pide imágenes o videos personales, utilizando la intimidad para ejercer control.

**Aislamiento social:** Trata de aislar al menor de sus amigos y familiares.

**Intimidación o amenazas:** Utiliza amenazas o manipulación emocional para mantener el contacto.

Es importante estar consciente de estas señales y mantener una comunicación abierta con los niños, niñas y jóvenes para que se sientan seguros compartiendo cualquier experiencia que les cause incomodidad.

Para ampliar la información sobre casos de grooming te invitamos a ver la serie web "Somos CiberSapiens"



[https://www.youtube.com/playlist?list=PL3jXkGijvcErSLqa40GOi\\_bbEGfpQo9Nx](https://www.youtube.com/playlist?list=PL3jXkGijvcErSLqa40GOi_bbEGfpQo9Nx)





## Sexting

Se refiere al acto de grabarse en video o tomarse fotos con contenido de naturaleza sexual, erótica o pornográfica, para luego enviar dichos videos o imágenes a una persona a través de un dispositivo electrónico como un teléfono móvil, computador u otro medio similar.

Veamos un caso de sexting es cuando...

Carlos, un joven de 17 años, descubrió que su exnovia había compartido fotos íntimas de él sin su permiso en las redes sociales y las había enviado a algunos de sus amigos. Carlos se sintió traicionado y avergonzado, ya que nunca había dado su consentimiento para compartir esas imágenes personales.

Las fotos comenzaron a circular entre sus compañeros de clase, y Carlos se convirtió en el centro de burlas y comentarios despectivos. Se sintió invadido en su privacidad y angustiado por las repercusiones que esta difusión no consensuada tenía en su vida diaria y su autoestima.





Cuatro consejos para hablar sobre sexting con nuestros niños, niñas y jóvenes:

**01.**

Habla de sexting, de manera directa y franca. Es importante que los menos no se sientan culpables y que sepan que merecen estar protegidos.

**02.**

Prioriza fortalecer los vínculos en la familia, donde se fomente la empatía, la asertividad, la resiliencia y la expresión emocional. Evita las actitudes autoritarias o sobreprotectoras.

**03.**

El acto de 'sexting' podría ser una manifestación de la represión sexual que los adolescentes experimentan debido a la estigmatización que los adultos a veces imponen sobre la sexualidad. En este sentido, es importante que fomentes una educación sexual desde casa.

**04.**

La cuestión no es prohibir a los niños, niñas y jóvenes el uso de teléfonos celulares o cámaras, sino ayudarles a comprender las implicaciones de realizar 'sexting', incluso con personas en las que confían.

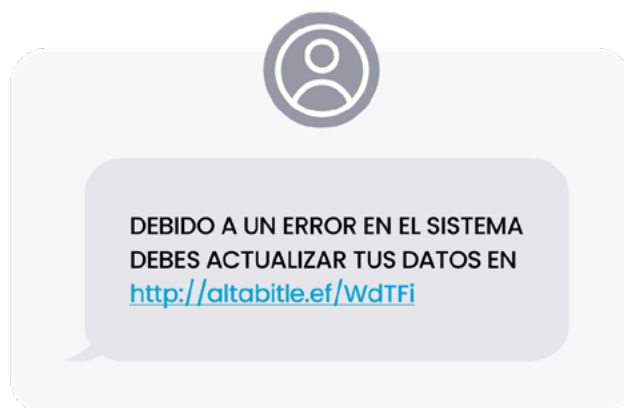






## Phishing

**¿Alguna vez has recibido un mensaje de texto como este?**



Una de las formas de engaño más comunes es el phishing. En este tipo de engaño, se envían mensajes a través de correo electrónico, mensajes de texto o aplicaciones de mensajería, solicitando a la víctima que haga clic en un enlace o descargue un archivo. El propósito es dirigir a las personas a una página web falsa en Internet, donde podrían perder información personal, bancaria o comercial. Los delincuentes se hacen pasar por instituciones u otras empresas de confianza para lograr que las personas realicen acciones que beneficien a los estafadores.

### **¿Cómo identificar un caso de phishing?**

Podría tratarse de un mensaje de un estafador cuando:

- Indica que ha sido detectada alguna actividad sospechosa en su cuenta, aunque esta afirmación carece de veracidad.

- Asevera que existe un problema con su información de pago, cuando en realidad no hay ningún inconveniente.
- Solicita que verifique datos personales o financieros, a pesar de que dicha acción no es necesaria.
- Adjunta una factura desconocida y falsa con la intención de generar confusión.
- Insiste en que haga clic en un enlace para realizar un pago, mientras que dicho enlace contiene software malicioso.
- Afirma que tiene derecho a inscribirse para recibir un reembolso del gobierno, pero en realidad se trata de una estafa.
- Ofrece un cupón que supuestamente le permite obtener algo de manera gratuita, aunque esta promesa carece de fundamento.





# Ciberdependencia

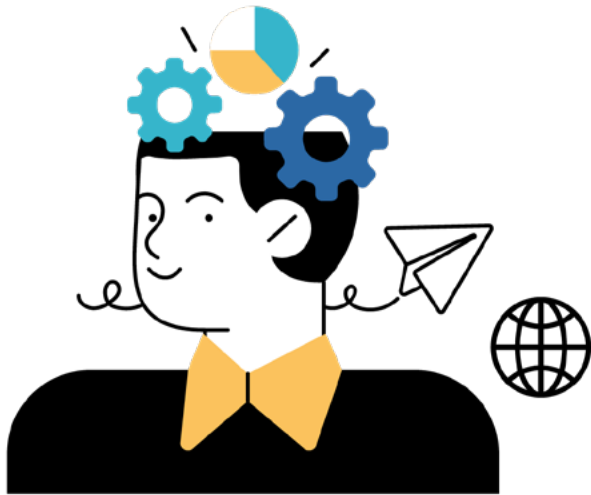
La ciberdependencia se manifiesta cuando una persona desarrolla una excesiva dependencia de dispositivos digitales e Internet. Este comportamiento lleva a dedicar un tiempo desproporcionado a la interacción con estos dispositivos, y a sufrir dificultades al intentar reducir su uso, incluso cuando esto impacta negativamente en sus responsabilidades y relaciones en el mundo real. En ocasiones, los individuos afectados pueden experimentar síntomas de temor, ansiedad o angustia cuando se encuentran "desconectados", llegando incluso a descuidar aspectos esenciales de su vida como la alimentación y el descanso.

## **¿Cómo podemos prevenir la ciberdependencia en nuestros niños, niñas y jóvenes?**

- Desde temprana edad, debemos establecer límites claros sobre cuánto tiempo pueden pasar nuestros niños, niñas y jóvenes frente a dispositivos digitales. Es posible crear horarios que incluyan actividades físicas, interacción social y aprendizaje fuera de las pantallas.
- Demostrar con nuestro propio comportamiento que también limitamos el tiempo en línea y tenemos actividades fuera de las pantallas. Los menores aprenderán de nosotros.

- Hablar con nuestros hijos sobre los pros y contras de la tecnología. Les explicamos los posibles riesgos de un uso excesivo, como la ciberdependencia, y estamos abiertos a escuchar sus inquietudes.
- También es posible crear reglas específicas sobre el uso de dispositivos electrónicos, como evitarlos durante las comidas o antes de dormir. Además, todos en la familia debemos comprender y seguir estas reglas.
- Animar a nuestros hijos a participar en actividades extracurriculares, deportes, arte y otras opciones fuera de las pantallas.
- Es importante crear espacios compartidos donde la familia pueda disfrutar de actividades y conversaciones juntos.
- Finalmente, es importante mantener abiertas las líneas de comunicación para que nuestros niños, niñas y jóvenes se sientan cómodos compartiendo con nosotros sobre sus experiencias en línea. Si surgen problemas, podemos estar allí para guiarlos y resolver situaciones complicadas.





## Actividad

A continuación, encontrarás una serie de preguntas relacionadas con los diferentes riesgos en línea sobre los que hemos hablado.

Acomoda el nombre que más se ajuste a cada definición.

Ciberbullying o  
Ciberacoso

Grooming

Sexting

Phishing

Ciberdependencia

\_\_\_\_\_ es cuando los estafadores hacen trampa para conseguir datos personales, como contraseñas o tarjetas de crédito.

\_\_\_\_\_ es cuando un adulto finge ser amigo de un niño, niña o joven en línea para luego hacerle daño, como abusar sexualmente de ellos o explotarlos de manera emocional o física.

\_\_\_\_\_ es cuando alguien pasa mucho tiempo en línea, afectando su vida diaria y relaciones personales.

\_\_\_\_\_ es cuando alguien lastima emocionalmente a otros en línea, usando mensajes crueles o compartiendo información que puede avergonzar.

\_\_\_\_\_ es cuando se comparten fotos o mensajes sexuales en línea, lo que puede tener consecuencias serias.





# Alertas digitales

## Reconoce señales de peligro en niños, niñas y jóvenes en el mundo digital

Es importante estar atentos a las señales que podrían indicar que un niño, niña o adolescente está enfrentando un riesgo digital. Identifica estas 5 señales de alerta que podrían indicar que algo no está bien en su experiencia en línea:



Cambios notables en la cantidad de tiempo que pasa usando dispositivos.



El niño reacciona emocionalmente (se enoja, se disgusta o se pone triste) ante lo que ve en su dispositivo.



Ha ajustado la privacidad de sus cuentas en redes sociales o ha creado nuevas cuentas.



Empieza a evitar situaciones sociales, incluso aquellas que solía disfrutar.



Muestra signos de aislamiento o tristeza, o pierde el interés en actividades y relaciones.





ICBF (13 de mayo de 2020). Señales de alerta que indican que un niño, niña o adolescente está siendo víctima de un riesgo digital. ICBF.

<https://www.icbf.gov.co/mis-manos-te-enseñan/señales-de-alerta-que-indican-que-un-niño-niña-o-adolescente-está-siendo>



Nota: Es importante recordar que estas señales de alerta no siempre indican que un niño, niña o joven está siendo víctima de un riesgo digital, pero pueden ser indicios de que algo no está bien. Si observas cualquiera de estas señales o tienes preocupaciones, es fundamental hablar de manera abierta y comprensiva, y buscar la ayuda adecuada si es necesario.





