

ABC de los riesgos y violencias digitales

en el marco del Decreto 769 de 2026
(Entornos Digitales Sanos y Seguros para Niños, Niñas y Adolescentes)

Internet abre oportunidades para aprender, crear y conectarse con el mundo. Por eso, la mejor herramienta de protección es contar con información, acompañamiento y hábitos que promuevan un uso seguro y responsable de la tecnología.



¿QUÉ SON LOS RIESGOS EN LÍNEA?

Son situaciones que pueden afectar la seguridad, la privacidad, la salud o los derechos de niñas, niños y adolescentes cuando utilizan internet, redes sociales, videojuegos, aplicaciones y dispositivos digitales.

¿POR QUÉ EXISTEN ESTOS RIESGOS?

Porque la vida de niñas, niños y adolescentes también ocurre en entornos digitales. Allí estudian, juegan, crean contenido, hacen amigos y acceden a información, pero también pueden encontrarse con personas o contenidos que representen una amenaza.

¿QUÉ ES UNA VIOLENCIA DIGITAL?

Es el daño que ocurre cuando un riesgo se materializa. Puede presentarse mediante agresiones, amenazas, engaños, difusión de información privada, explotación o cualquier acción que afecte el bienestar de una persona a través de medios digitales.



¿CÓMO SE GENERA EL RIESGO?

Los expertos lo explican con una fórmula sencilla:

Amenaza + vulnerabilidad + exposición = riesgo

Por ejemplo, una cuenta falsa (amenaza), sumada a la falta de acompañamiento adulto (vulnerabilidad) y al contacto frecuente por redes sociales (exposición), puede generar una situación de riesgo.

¿CUÁLES SON LAS VIOLENCIAS DIGITALES MÁS FRECUENTES?

Ciberacoso: insultos, burlas, humillaciones o persecuciones a través de redes sociales, chats o plataformas digitales.

Suplantación de identidad: cuando alguien utiliza fotografías o información personal para hacerse pasar por otra persona.

Explotación y abuso sexual en línea: situaciones en las que una persona busca manipular o vulnerar a niñas, niños o adolescentes mediante internet.

Captación digital: estrategias utilizadas para ganar la confianza de menores de edad con fines de explotación, engaño o reclutamiento.

Vulneración de datos personales: publicación o uso indebido de información privada como fotografías, ubicación, números telefónicos o rutinas diarias.

¿CUÁLES SON LAS SEÑALES DE ALERTA?

- Cambios repentinos de comportamiento.
- Aislamiento o miedo al usar dispositivos.
- Mensajes insistentes de desconocidos.
- Solicitudes de fotografías, videos o datos personales.
- Uso excesivo de plataformas digitales sin supervisión.
- Episodios de ansiedad, tristeza o estrés relacionados con internet.

¿CÓMO PUEDEN PROTEGERSE LAS FAMILIAS?

- Conversar frecuentemente sobre el uso de internet.
- Configurar opciones de privacidad y seguridad.
- Establecer acuerdos de uso según la edad.
- Enseñar a bloquear y reportar contenidos o usuarios.
- Verificar la información antes de compartirla.
- Promover la confianza para que niñas, niños y adolescentes pidan ayuda cuando algo les incomode.



DECRETO DE ENTORNOS DIGITALES SANOS Y SEGUROS

¿QUÉ BUSCA EL DECRETO DE ENTORNOS DIGITALES SANOS Y SEGUROS?

Promover una cultura de prevención y cuidado que permita reducir los riesgos en línea mediante educación, protección de datos, diseño seguro de plataformas, rutas de atención y acciones coordinadas entre familias, instituciones educativas, empresas y entidades del Estado.



TIC