

DELITOS Y SEGURIDAD EN LA RED

MATERIAL DE APOYO PARA ACTIVIDADES DE FORMACIÓN INTEGRAL Y VALORES (Crear con una aplicación digital: uno de los siguientes organizadores gráficos: Infografía, Mapa mental, mapa conceptual haciendo uso del siguiente material).

Puede complementar este material con el siguiente vídeo que puede ser consultado en:
<https://youtu.be/vQ2CiM0wVwk>

DELITOS Y SEGURIDAD EN LA RED

Presentación:

este material se ha elaborado como un recurso de apoyo a todos los estudiantes para conocer los riesgos, peligros, precauciones y alertas que debemos tener al hacer uso de internet y de las redes sociales. No todas las personas actúan de buena fe frente a un contacto en redes sociales o a través del uso de internet. Siempre debemos tomar nuestras medidas de prevención y de seguridad frente a todas las acciones y actividades que realicemos y lo mejor es estar acompañado o supervisado por un adulto o una persona responsable.

El contenido incorpora riesgos actuales como **grooming, sexting, sextorsión, cyberbullying, phishing, catfishing, robo de identidad, doxxing, deepfakes, estafas, malware, suplantación, manipulación mediante algoritmos e inteligencia artificial**, además de responsabilidades, prevención y ciberseguridad. UNICEF advierte que los riesgos para adolescentes están evolucionando con la inteligencia artificial y que esta tecnología ya puede utilizarse para crear imágenes sexuales falsas y facilitar nuevas formas de explotación.

PROTECCIÓN EN INTERNET Y REDES SOCIALES: GUÍA DE CIBERSEGURIDAD PARA ADOLESCENTES Y MENORES DE EDAD.

PROTECCIÓN EN INTERNET Y REDES SOCIALES

Guía de prevención, responsabilidad y ciberseguridad para adolescentes y menores de edad:

Introducción

Internet es una de las herramientas más importantes de nuestra época. Gracias a Internet podemos estudiar, investigar, comunicarnos con familiares y amigos, escuchar música, ver videos, jugar, aprender nuevas habilidades y conocer personas de diferentes lugares del mundo.

Las redes sociales también forman parte de la vida cotidiana de muchos adolescentes. Aplicaciones y plataformas digitales permiten publicar fotografías, videos, comentarios, historias y mensajes. Sin embargo, Internet no es solamente un lugar para divertirse. También

existen personas que utilizan la tecnología para engañar, acosar, manipular, robar información o cometer delitos.

Por eso, aprender a utilizar Internet de manera segura es tan importante como aprender a cruzar una calle, cuidar nuestras pertenencias o reconocer una situación peligrosa.

Una regla fundamental es:

NO TODO LO QUE APARECE EN INTERNET ES VERDAD, Y NO TODAS LAS PERSONAS QUE CONOCEMOS EN INTERNET SON QUIENES DICEN SER.

Esto no significa que debemos tener miedo de Internet. Significa que debemos aprender a utilizarlo con inteligencia, responsabilidad y precaución.

UNICEF señala que los niños, niñas y adolescentes pueden enfrentarse a riesgos como el ciberacoso, la explotación sexual facilitada por la tecnología, la manipulación comercial, el uso indebido de datos personales y otros peligros relacionados con las nuevas tecnologías.

En Colombia, además, investigaciones recientes muestran que la violencia digital contra adolescentes es un problema real. Un estudio de UNICEF, ECPAT e INTERPOL publicado en 2026 encontró que más de uno de cada cinco niños, niñas y adolescentes encuestados en Colombia fue víctima de explotación o abuso sexual facilitado por la tecnología durante un año.

Por esta razón debemos aprender a proteger nuestra identidad, nuestra información, nuestras fotografías, nuestras cuentas y, sobre todo, nuestra integridad

1. ¿QUÉ SON LOS DELITOS INFORMÁTICOS?

Los delitos informáticos son conductas ilegales que utilizan computadores, tabletas, teléfonos celulares, Internet, redes sociales, videojuegos, aplicaciones u otros medios y dispositivos tecnológicos para causar daño, obtener información, robar dinero, engañar, amenazar, acosar o vulnerar los derechos de otras personas.

Un delito informático puede comenzar con algo aparentemente sencillo.

Por ejemplo:

Un desconocido puede enviar:

“Hola, ¿quieres ser mi amigo?”

Después puede preguntar:

“¿Dónde estudias?”

Luego:

“¿Cuántos años tienes?”

Más adelante:

“¿Vives con tus padres?”

Y finalmente:

“Mándame una fotografía.”

Cada respuesta puede entregar una pequeña parte de nuestra información personal.

El problema aparece cuando una persona utiliza esa información para manipularnos, engañarnos o hacernos daño.

Por eso debemos recordar:

Nuestra información personal tiene valor.

Nuestro nombre, edad, dirección, teléfono, colegio, fotografías, ubicación, contraseñas, documentos, cuentas, amigos y hábitos pueden revelar muchísimo sobre nosotros.

2. GROOMING: CUANDO UN ADULTO INTENTA GANARSE LA CONFIANZA DE UN MENOR

El **grooming** ocurre cuando una persona adulta utiliza Internet para establecer contacto con un niño, niña o adolescente con la intención de manipularlo o explotarlo sexualmente.

El agresor puede utilizar redes sociales, videojuegos, aplicaciones de mensajes, chats u otras plataformas.

Una característica peligrosa es que normalmente no empieza con una amenaza.

Puede comenzar con amabilidad.

El agresor puede decir:

“Eres muy inteligente.”

“Me gusta hablar contigo.”

“Puedes confiar en mí.”

“Yo sí te entiendo.”

“Somos amigos.”

También puede fingir tener una edad parecida a la víctima.

Puede utilizar fotografías de otra persona o inventar una identidad.

Después puede intentar conseguir información privada, fotografías o videos.

En algunos casos intenta convencer al adolescente de mantener la relación en secreto:

“No le cuentes a nadie.”

Esa frase debe ser una señal de alerta.

Si alguien que conocimos en Internet nos pide secretos, fotografías privadas, encuentros personales o conversaciones que nos hacen sentir incómodos, debemos detener la comunicación y contárselo inmediatamente a un adulto de confianza.

UNICEF identifica el grooming como una forma de riesgo y explotación sexual facilitada por tecnologías digitales.

¿Qué hacer?

1. No continuar la conversación.
2. No enviar fotografías íntimas.
3. No aceptar encuentros personales.
4. No entregar dirección o ubicación.
5. Guardar las evidencias disponibles sin volver a interactuar.
6. Bloquear la cuenta.
7. Reportarla en la plataforma.
8. Informar inmediatamente a un adulto de confianza.
9. Si existe una situación grave, realizar la denuncia correspondiente.

Nunca debemos sentir vergüenza por pedir ayuda.

La responsabilidad es del agresor, no de la víctima.

3. SEXTING Y SEXTORSIÓN

El **sexting** consiste en enviar o recibir mensajes, fotografías o videos de contenido sexual mediante dispositivos electrónicos.

Entre adolescentes puede aparecer como una presión:

“Si eres mi amigo, mándame una foto.”

“Si me quieres, demuéstramelo.”

“Solo la voy a mirar yo.”

Pero una vez que una fotografía o video sale de nuestro dispositivo, perdemos el control sobre lo que puede ocurrir con ese archivo.

Puede ser guardado.

Puede ser reenviado.

Puede ser publicado.

Puede ser utilizado para amenazar.

Puede llegar a personas desconocidas.

Una situación todavía más grave es la **sextorsión**.

La sextorsión ocurre cuando alguien utiliza fotografías, videos o información íntima para amenazar a una persona y exigirle algo.

Por ejemplo:

“Si no haces lo que te digo, publicaré la fotografía.”

En ese momento la persona puede sentir miedo.

Pero hay algo muy importante:

No debemos obedecer al extorsionador.

No debemos enviar más fotografías.

No debemos pagar.

No debemos continuar negociando.

Debemos pedir ayuda inmediatamente.

4. CYBERBULLYING O CIBERACOSO

El **cyberbullying** es el acoso realizado mediante tecnologías digitales.

Puede ocurrir mediante:

- Redes sociales.
- Mensajes.
- Grupos de chat.
- Videojuegos.
- Foros.
- Comentarios.
- Videos.
- Fotografías.

Puede incluir insultos, amenazas, burlas, rumores, humillaciones, publicación de fotografías sin autorización o creación de cuentas falsas para molestar a alguien.

Por ejemplo, varios estudiantes pueden crear un grupo para burlarse continuamente de un compañero.

También pueden publicar una fotografía y escribir comentarios ofensivos.

Eso no es simplemente “una broma” si está causando daño y se realiza de manera repetida.

UNICEF explica que el ciberacoso puede incluir la difusión de mentiras, fotografías vergonzosas, mensajes ofensivos o amenazas, y que deja una huella digital que puede servir como evidencia.

¿Qué hacer ante el cyberbullying?

NO responder con más agresiones.

Debemos:

- Mantener la calma.
- Guardar evidencias.
- Tomar capturas de pantalla cuando sea necesario.
- Bloquear al agresor.
- Reportar la cuenta.
- Informar a padres, acudientes o profesores.
- Solicitar ayuda institucional.

Y existe otra regla:

Si vemos que están acosando a otra persona, tampoco debemos participar.

Compartir una publicación ofensiva también puede aumentar el daño.

5. PHISHING: EL ENGAÑO PARA ROBAR INFORMACIÓN

El término correcto es **phishing**.

El phishing es una técnica utilizada para engañar a una persona con el objetivo de obtener información privada.

Puede llegar mediante:

- Correo electrónico.
- Mensajes de texto.
- Redes sociales.
- WhatsApp.
- Videojuegos.
- Páginas web falsas.

El mensaje puede decir:

“Tu cuenta será cerrada.”

“Ganaste un premio.”

“Haz clic para reclamar.”

“Tu contraseña debe ser actualizada.”

“Tenemos una fotografía tuya.”

“Confirma tus datos.”

El mensaje intenta provocar una reacción rápida.

Por eso debemos aplicar una regla:

¡PIENSA ANTES DE HACER CLIC!

No debemos ingresar contraseñas desde enlaces sospechosos.

No debemos descargar archivos desconocidos.

No debemos entregar códigos de verificación.

No debemos proporcionar información personal a desconocidos.

Si tenemos dudas, debemos consultar directamente a un adulto o ingresar al sitio oficial escribiendo nosotros mismos la dirección conocida.

6. CATFISHING: IDENTIDADES FALSAS

El **catfishing** ocurre cuando una persona crea una identidad falsa en Internet para engañar a otra.

Puede utilizar:

- Nombre falso.
- Fotografía de otra persona.
- Edad falsa.
- Lugar de residencia falso.
- Información inventada.

Por ejemplo, alguien puede decir:

“Tengo 13 años y vivo en tu ciudad.”

Pero realmente puede ser una persona completamente diferente.

Por eso una fotografía de perfil **no demuestra quién está detrás de una cuenta**.

Nunca debemos confiar solamente en una imagen o en lo que alguien dice sobre sí mismo.

7. ROBO DE IDENTIDAD Y SUPLANTACIÓN

El robo de identidad ocurre cuando alguien utiliza información de otra persona para hacerse pasar por ella.

Puede intentar utilizar:

- Nombre.
- Fotografías.
- Número telefónico.
- Correo electrónico.
- Cuentas.
- Información familiar.
- Documentos.
- Datos personales.

Un delincuente puede crear una cuenta utilizando la fotografía y el nombre de otra persona.

Después puede escribir a sus amigos.

Por eso debemos revisar periódicamente nuestras cuentas y avisar si aparece un perfil falso utilizando nuestra identidad.

Para proteger nuestra identidad:

No publiques información innecesaria.

No muestres documentos.

No publiques boletos, tarjetas, direcciones o información privada.

No compartas códigos de acceso.

Utiliza contraseñas diferentes para diferentes cuentas.

8. DOXXING: CUANDO PUBLICAN INFORMACIÓN PRIVADA

El **doxxing** consiste en divulgar públicamente información privada de una persona sin su autorización, especialmente cuando se utiliza para intimidarla, acosarla o ponerla en riesgo.

Puede incluir:

- Dirección.
- Teléfono.
- Lugar de estudio.
- Ubicación.
- Información familiar.
- Fotografías privadas.

Por eso debemos tener cuidado con las fotografías.

Una fotografía puede mostrar más información de la que pensamos.

Por ejemplo:

Si publicamos una fotografía frente a nuestra casa, puede aparecer la dirección.

Si mostramos el uniforme, alguien puede identificar nuestro colegio.

Si mostramos una pantalla, pueden aparecer datos privados.

Debemos aprender a observar el fondo de nuestras fotografías antes de publicarlas.

9. DEEPPAKES E INTELIGENCIA ARTIFICIAL

La inteligencia artificial puede ser muy útil.

Puede ayudarnos a estudiar, crear imágenes, traducir textos, resolver problemas y aprender.

Pero también puede ser utilizada de manera incorrecta.

Los **deepfakes** son contenidos manipulados o generados mediante tecnología que pueden hacer parecer que una persona dijo o hizo algo que realmente nunca ocurrió.

Una fotografía puede ser modificada.

Una voz puede ser imitada.

Un rostro puede ser colocado en otra imagen.

Un video puede ser manipulado.

Esto genera nuevos riesgos.

UNICEF ha advertido que la inteligencia artificial está aumentando los riesgos para niños y adolescentes y que también puede utilizarse para crear imágenes sexuales falsas de menores.

Por eso:

No debemos creer automáticamente todo lo que vemos.

Antes de compartir una imagen o video debemos preguntarnos:

¿Quién lo publicó?

¿De dónde salió?

¿Existe otra fuente que confirme la información?

¿Podría estar manipulado?

¿La publicación intenta provocar miedo, rabia o sorpresa?

Pensar antes de compartir es una forma de ciberseguridad.

10. ESTAFAS EN INTERNET

Los delincuentes también utilizan Internet para intentar obtener dinero.

Algunas estafas ofrecen:

- Premios falsos.
- Regalos.
- Videojuegos gratuitos.

- Monedas virtuales.
- Becas falsas.
- Concursos falsos.
- Empleos falsos.
- Productos demasiado baratos.
- Supuestas inversiones.

Una señal de peligro es cuando alguien promete algo extraordinario a cambio de información, dinero o acceso a una cuenta.

Por ejemplo:

“Ganaste un teléfono. Solo debes pagar el envío.”

Debemos detenernos.

Preguntar.

Verificar.

Consultar.

11. MALWARE Y ARCHIVOS PELIGROSOS

El **malware** es software malicioso creado para causar daño, robar información o realizar acciones no autorizadas.

Puede llegar mediante:

- Aplicaciones falsas.
- Archivos desconocidos.
- Enlaces.
- Programas piratas.
- Juegos modificados.
- Archivos enviados por desconocidos.

Por eso debemos descargar aplicaciones desde fuentes confiables y mantener actualizado nuestro dispositivo.

Nunca debemos instalar programas simplemente porque alguien diga:

“No pasa nada, es totalmente seguro.”

12. ¿QUÉ ES UN ALGORITMO?

Un **algoritmo** es un conjunto de instrucciones ordenadas que permite solucionar un problema o realizar una tarea.

Por ejemplo, una receta de cocina puede verse como un algoritmo:

1. Conseguir ingredientes.
2. Mezclarlos.
3. Cocinarlos.
4. Servirlos.

Los computadores también utilizan algoritmos.

Las redes sociales utilizan algoritmos para decidir qué contenido mostrarnos.

Por ejemplo, si vemos muchos videos sobre fútbol, una plataforma puede interpretar que nos interesa el fútbol y comenzar a mostrarnos más videos relacionados.

Los algoritmos pueden estudiar diferentes señales:

- Lo que vemos.
- Lo que buscamos.
- Lo que compartimos.
- Lo que comentamos.
- Cuánto tiempo observamos un video.
- Las cuentas que seguimos.
- Nuestra interacción con determinadas publicaciones.

Esto puede resultar útil, pero también significa que debemos cuidar la información que proporcionamos.

UNICEF advierte que los sistemas de inteligencia artificial y recomendación pueden influir en las experiencias digitales de los niños y adolescentes.

13. ¿UTILIZAN LOS DELINCIENTES ALGORITMOS?

Los delincuentes pueden utilizar herramientas tecnológicas y automatizadas para intentar identificar posibles víctimas, enviar grandes cantidades de mensajes, crear cuentas falsas, analizar información pública o producir contenidos engañosos.

No necesitamos aprender a realizar esas actividades.

Lo importante es conocer el riesgo para poder protegernos.

Por ejemplo, si una persona publica diariamente:

“Estoy solo en casa.”

“Mis padres salieron.”

“Estoy de vacaciones.”

“Este es mi colegio.”

“Esta es mi ruta.”

“Esta es mi casa.”

Toda esa información puede permitir que alguien construya un perfil sobre sus hábitos.

Por eso una buena regla es:

NO PUBLIQUE INFORMACIÓN QUE UN DESCONOCIDO PODRÍA UTILIZAR PARA LOCALIZARTE O MANIPULARTE.

14. LA HUELLA DIGITAL

Todo lo que hacemos en Internet puede dejar una **huella digital**.

Una publicación puede ser descargada.

Una fotografía puede ser guardada.

Un comentario puede ser capturado.

Un video puede ser compartido.

Aunque eliminemos algo, otra persona puede haberlo guardado previamente.

Por eso debemos preguntarnos antes de publicar:

¿Me sentiría tranquilo si esta publicación fuera vista por mi familia, mis profesores o mis compañeros?

Si la respuesta es no, probablemente no debemos publicarla.

15. RESPONSABILIDADES COMO USUARIOS DE INTERNET

Tener acceso a Internet también significa tener responsabilidades.

Debemos:

1. Respetar a otras personas.
2. No insultar.

3. No amenazar.
4. No difundir rumores.
5. No publicar fotografías de otras personas sin permiso.
6. No crear perfiles falsos para hacer daño.
7. No compartir información privada.
8. No participar en cyberbullying.
9. Reportar contenidos peligrosos.
10. Pedir ayuda cuando algo nos haga sentir incómodos.

La tecnología no elimina las reglas básicas de convivencia.

Detrás de cada cuenta hay una persona.

16. DECÁLOGO PARA PROTEGERSE EN INTERNET

1. PROTEGE TUS CONTRASEÑAS

Utiliza contraseñas fuertes y diferentes.

No las compartas con amigos.

Una contraseña es personal.

2. ACTIVA LA AUTENTICACIÓN EN DOS PASOS

Cuando sea posible, activa la verificación en dos pasos.

Así, aunque alguien descubra tu contraseña, tendrá una barrera adicional.

3. NO COMPARTAS INFORMACIÓN PERSONAL

Evita publicar dirección, teléfono, ubicación, colegio, horarios o información familiar.

4. NO ACEPTES A CUALQUIERA

No todas las solicitudes de amistad corresponden a personas reales o confiables.

5. PIENSA ANTES DE PUBLICAR

Pregúntate:

¿Esto podría causarme problemas después?

6. NO ENVÍES FOTOGRAFÍAS ÍNTIMAS

Especialmente si alguien te presiona, amenaza o promete guardar el secreto.

7. NO HABLES A SOLAS CON DESCONOCIDOS SOBRE TEMAS PRIVADOS

Si alguien comienza a hacer preguntas incómodas, termina la conversación.

8. BLOQUEA Y REPORTA

Las redes sociales tienen herramientas para bloquear y reportar cuentas.

Utilízalas.

9. CUÉNTALE A UN ADULTO

Si ocurre algo extraño, no permanezcas solo con el problema.

Habla con tus padres, acudiente, profesor, orientador u otro adulto de confianza.

10. NO TENGAS MIEDO DE PEDIR AYUDA

Pedir ayuda no significa ser débil.

Pedir ayuda es una forma inteligente de protegerse.

17. LISTA DE CIBERSEGURIDAD PARA ADOLESCENTES

Antes de utilizar una red social, revisa:

CONTRASEÑAS

- ☐ Tengo una contraseña segura.
- ☐ No la comparto.
- ☐ No utilizo la misma contraseña para todo.

PRIVACIDAD

- ☐ Mi cuenta tiene configuraciones de privacidad adecuadas.
- ☐ No publico mi dirección.
- ☐ No publico mi número telefónico.
- ☐ No publico mi ubicación en tiempo real.
- ☐ No muestro información de mi colegio.

CONTACTOS

- ☐ Conozco a las personas que acepto.
- ☐ No confío automáticamente en desconocidos.
- ☐ No acepto invitaciones sospechosas.

PUBLICACIONES

- ☐ Pienso antes de publicar.
- ☐ Reviso las fotografías.
- ☐ No publico información privada.
- ☐ No publico contenido que pueda perjudicar a otra persona.

SEGURIDAD

- ☐ Mantengo actualizado mi dispositivo.
- ☐ Instalo aplicaciones desde fuentes confiables.
- ☐ No abro enlaces sospechosos.
- ☐ No descargo archivos desconocidos.
- ☐ Tengo activada la verificación en dos pasos cuando está disponible.

18. ¿QUÉ HACER SI YA CAÍ EN UNA SITUACIÓN PELIGROSA?

Lo más importante es:

NO ENTRAR EN PÁNICO.

Si alguien te está amenazando:

No respondas con amenazas.

No intentes enfrentarte físicamente.

No envíes más información.

No envíes más fotografías.

No pagues si existe una extorsión.

Guarda las evidencias disponibles.

Bloquea y reporta cuando sea apropiado.

Cuéntaselo inmediatamente a un adulto de confianza.

Recuerda:

El miedo hace que algunas personas permanezcan calladas.

Pero hablar permite recibir ayuda.

En Colombia existen mecanismos para reportar situaciones que afectan a niños, niñas y adolescentes. UNICEF Colombia señala, entre otras rutas, Te Protejo, CAI Virtual, la Línea 141 del ICBF y otras autoridades competentes, dependiendo de la situación.

19. SI ALGUIEN TE DICE: “NO SE LO CUENTES A NADIE”

Esta frase merece especial atención.

Un amigo puede pedirte guardar un secreto sobre una sorpresa de cumpleaños.

Eso es diferente.

Pero si un desconocido o cualquier persona te dice:

“No le cuentes a tus padres.”

“Borra esta conversación.”

“Si dices algo, tendrás problemas.”

“Esto queda entre nosotros.”

“No confíes en los adultos.”

Debemos desconfiar.

Los adultos responsables y las personas que realmente quieren protegerte no necesitan manipuarte mediante amenazas o secretos peligrosos.

20. INTERNET NO ES EL ENEMIGO

Es importante entender algo:

Internet no es malo.

Internet es una herramienta.

Puede utilizarse para estudiar, crear, comunicarnos, aprender, investigar y divertirnos.

El problema aparece cuando una persona utiliza la tecnología para hacer daño.

Por eso no se trata de abandonar Internet.

Se trata de aprender a utilizarlo correctamente.

Debemos desarrollar tres capacidades:

PENSAMIENTO CRÍTICO

No creer todo lo que vemos.

RESPONSABILIDAD

Pensar en las consecuencias de nuestras acciones.

SEGURIDAD

Proteger nuestra información y pedir ayuda ante situaciones peligrosas.

21. LAS CINCO PREGUNTAS ANTES DE HACER CLIC

Antes de abrir un enlace, podemos hacernos cinco preguntas:

- 1. ¿Quién me lo envió?**
- 2. ¿Conozco realmente a esa persona?**
- 3. ¿Por qué me está pidiendo esta información?**
- 4. ¿El mensaje intenta asustarme o presionarme?**
- 5. ¿Puedo verificarlo por otra fuente?**

Si algo parece extraño:

DETENTE.

PIENSA.

VERIFICA.

PIDE AYUDA.

22. EL SEMÁFORO DE LA SEGURIDAD DIGITAL

Una forma fácil de recordar las reglas es utilizar un semáforo.

☐ **VERDE: PUEDO HACERLO**

- Estudiar.
- Investigar.
- Hablar con personas conocidas.
- Utilizar aplicaciones seguras.
- Aprender.
- Crear contenido positivo.
- Reportar situaciones peligrosas.

☐ **AMARILLO: DEBO TENER CUIDADO**

- Solicitudes de amistad de desconocidos.
- Enlaces extraños.
- Premios inesperados.
- Mensajes que solicitan información.
- Perfiles nuevos.
- Fotografías que contienen información personal.
- Personas que hacen demasiadas preguntas.

☒ **ROJO: DEBO DETENERME Y PEDIR AYUDA**

- Amenazas.
- Extorsión.
- Grooming.
- Solicitudes de fotografías íntimas.
- Chantaje.
- Acoso.
- Suplantación de identidad.
- Amenazas de publicar información privada.
- Contenido sexual dirigido a menores.
- Personas que quieren encontrarse a solas con nosotros.

23. MI COMPROMISO COMO CIUDADANO DIGITAL

Ser ciudadano digital significa utilizar la tecnología respetando nuestros derechos y los derechos de los demás.

Mi compromiso debe ser:

Yo protegeré mis datos.

Yo cuidaré mis contraseñas.

Yo pensaré antes de publicar.

Yo respetaré a los demás.

Yo no participaré en cyberbullying.

Yo no compartiré fotografías privadas de otras personas.

Yo verificaré la información antes de compartirla.

Yo no aceptaré automáticamente a desconocidos.

Yo pediré ayuda cuando algo me haga sentir incómodo o amenazado.

Yo utilizaré Internet para aprender, crear, comunicarme y crecer de manera segura.

24. CONCLUSIÓN

Internet es una herramienta extraordinaria, pero debemos utilizarla con inteligencia.

Los delincuentes pueden utilizar redes sociales, videojuegos, aplicaciones, correos electrónicos y herramientas de inteligencia artificial para intentar engañar a las personas.

Algunos riesgos son el grooming, sexting problemático, sextorsión, cyberbullying, phishing, catfishing, robo de identidad, suplantación, doxxing, estafas, malware, deepfakes y diferentes formas de manipulación digital.

Sin embargo, conocer estos riesgos nos hace más fuertes.

La mejor protección no consiste únicamente en instalar un programa antivirus.

La verdadera ciberseguridad comienza con nuestras decisiones.

Una persona que piensa antes de hacer clic.

Una persona que protege sus contraseñas.

Una persona que no publica información privada.

Una persona que no confía automáticamente en desconocidos.

Una persona que sabe bloquear y reportar.

Una persona que pide ayuda.

Esa persona está utilizando Internet de manera inteligente.

Debemos recordar que **no somos culpables cuando una persona intenta engañarnos o hacernos daño**. Lo correcto es pedir ayuda.

UNICEF recomienda mantener una comunicación abierta, establecer hábitos seguros, utilizar configuraciones de privacidad, bloquear y reportar situaciones dañinas y acudir a adultos y autoridades cuando sea necesario.

Por eso, la frase más importante de toda esta guía es:

“PIENSA ANTES DE PUBLICAR, PIENSA ANTES DE HACER CLIC Y PIDE AYUDA CUANDO ALGO NO ESTÉ BIEN.”

La tecnología puede ser una gran herramienta para nuestro futuro.

Aprendamos a utilizarla de manera responsable, segura, respetuosa e inteligente.

DECÁLOGO FINAL DE CIBERSEGURIDAD

- 1. NO COMPARTAS TUS CONTRASEÑAS.**
- 2. NO PUBLIQUES INFORMACIÓN PERSONAL INNECESARIA.**
- 3. NO ACEPTES A DESCONOCIDOS SIN PENSAR.**
- 4. NO ENVÍES FOTOGRAFÍAS ÍNTIMAS.**
- 5. NO HAGAS CLIC EN ENLACES SOSPECHOSOS.**
- 6. NO CREAS TODO LO QUE VES EN INTERNET.**
- 7. NO PARTICIPES EN CYBERBULLYING.**

- 8. BLOQUEA Y REPORTA A QUIEN TE AMENACE O ACOSA.**
- 9. CUÉNTALE A UN ADULTO DE CONFIANZA CUANDO ALGO TE PREOCUPE.**
- 10. RECUERDA: TU SEGURIDAD Y TU DIGNIDAD SON MÁS IMPORTANTES QUE CUALQUIER “LIKE”, SEGUIDOR, VIDEO O MENSAJE.**