PROTOCOLO

Ambientes Digitales seguros y saludables para niños, niñas y adolescentes

Huellas
Movimiento Juvenil

2021

Metodología para Impulsar Campamentos
y Experiencias Juveniles Cristianas en Modalidad Online
Asociación Civil Huellas, 2021
Primera Edición

Asociación Civil Huellas
Calle Andrés Bello, casa 09, Urb. Los Flores de Catia.
Telf.: 0212 8631650
www.huellas.org.ve

Dirección General
P. Robert Rodríguez, SJ

Coordinador de Adaptaciones Pedagógicas y Recursos Alternativos
Lcdo. Yhitzender Torres

Diseño Gráfico y Diagramación
Jessica Sifontes

Proyecto Financiado por
Asociación Civil Huellas

Editado por
Asociación Civil Huellas
Impreso en Venezuela

INTRODUCCIÓN

La presencia y el uso continuo de las redes sociales es una realidad cotidiana que ha llegado a ocupar un espacio fundamental en la vida de todas las personas sin importar la edad o cualquier otra característica distintiva.

Las redes sociales se convierten en un lugar donde las personas proyectan su identidad y se conectan con otras que comparten sus mismos gustos, ideas e intereses. Los jóvenes son especialmente sensibles a la dinámica de las redes sociales y frente a una realidad que ha llegado para quedarse, el espíritu ignaciano de Huellas nos invita a hacer uso de ellas tanto cuanto nos ayuden a alcanzar el fin que nos hemos planteado: **formar líderes en valores humanos y cristianos.**

Para el **Movimiento Juvenil Huellas**, las redes sociales son una herramienta que nos permite resaltar, cultivar, proyectar y difundir los valores desde los que vivimos, nuestra misión, lo que hacemos y lo que soñamos.

Es importante ser buena noticia en medio de nuestra realidad presencial y digital.

En tal sentido, el siguiente documento es una invitación para todos los jóvenes y adultos implicados en la formación a distancia, mediante redes sociales, aplicaciones móviles y páginas web, a cuidar y proteger la dignidad de los niños, niñas y adolescentes, así como a prevenir los riesgos digitales que vulneran sus derechos.

INTERNET COMO UNA OPORTUNIDAD Y RIESGO

Para los niños las Tecnologías de la Información y Comunicación resultan un recurso importante para el acceso a la información y al aprendizaje. Los hoy llamado **"Nativos Digitales"** utilizan, de forma significativa, las Redes Sociales (RRSS) para comunicarse y conectarse con el mundo, hecho que les ofrece grandes posibilidades para el crecimiento personal, el conocimiento, el compartir y la interacción.

Tanto el internet como las redes sociales pueden ser una herramienta importante para el desarrollo de los Derechos de los niños, niñas y adolescentes, puesto que con un clic pueden acceder a bibliotecas, juegos, canales de comunicación, espacios de expresión, viajes virtuales y museos. Oportunidad que como docentes, padres, representantes y acompañantes debemos potenciar y cuidar constantemente.

Sin embargo, la red también es un espacio de riesgo latente para todos, en especial los niños, niñas y adolescentes por su madurez para identificar riesgos digitales y por consecuencia blindar los espacios virtuales en los que interactúa.

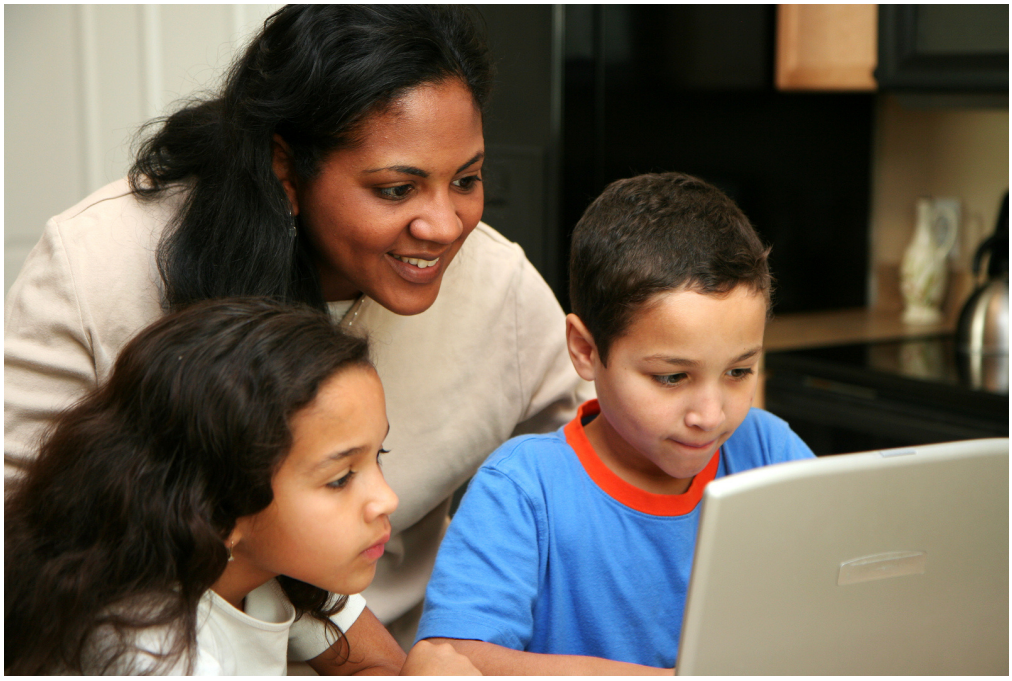
Según el Fondo para las Naciones Unidas para la Infancia (UNICEF) alguno de los elementos que resultan preocupante al momento que los niños, niñas y adolescentes interactúa en la red son:

- Muchos, si no la mayoría de los niños y niñas menores de 13 años, no tienen la madurez necesaria para dar consentimiento informado en cuanto al tratamiento de sus datos personales. En virtud de la Convención de Derechos del Niño, la madurez es progresiva y difiere de unos niños y niñas a otros.

- Los adolescentes, los niños y niñas no comprenden fácilmente qué significa permitir “cookies” o entregar datos personales. Las políticas de privacidad y los términos de servicio son a menudo escritos en un lenguaje difícil y parece que no hay otra opción que entregar los datos personales para poder usar el servicio.

- El uso de técnicas invasivas como solicitudes de fotografías y acceso a cámara web son muy preocupantes porque puede invitar a los niños, niñas y adolescentes a compartir información privada sobre ellos. Los niños y niñas, por su falta de experiencia y madurez, no comprenden las consecuencias que esto puede tener una vez que circulan en la red.

En tal sentido, muchas de las plataformas digitales movilizan e inducen a los niños, niñas y adolescentes a renunciar a sus derechos de protección de datos. El reto entonces, se trata de un acompañamiento sistemático donde los niños, a través de su experiencia y la educación puedan adquirir competencias digitales que les permitan una autonomía en la red. Además, de la disposición de ambientes digitales seguros y saludables por parte de sus padres, profesores y acompañantes.



DEFINICIONES IMPORTANTES[1]

01 Ciberacoso

Es cuando un niño, niña o adolescente es atormentado, amenazado, acosado, humillado o avergonzado **por un adulto** por medio de internet, medios interactivos, tecnologías digitales o teléfonos móviles.

02 Ciberbullying

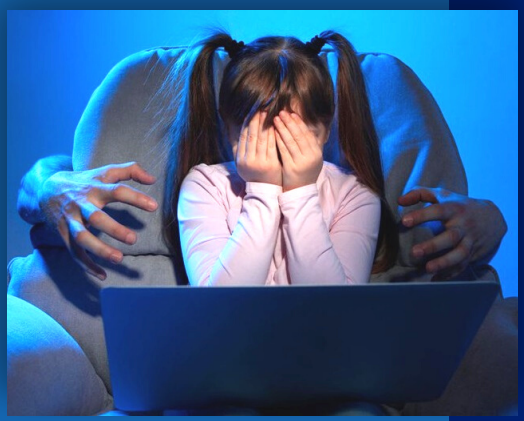
Es cuando un niño, niña o adolescente es atormentado, amenazado, acosado, humillado o avergonzado **por otro niño, niña o adolescente** por medio de internet, medios interactivos, tecnologías digitales o teléfonos móviles.

03 Sexting

(Contracción de sex y texting) es un término que se refiere al envío de contenidos eróticos o pornográficos por medio de teléfonos móviles. Comenzó haciendo referencia al envío de mensajes de texto (o SMS) de naturaleza sexual.

04 Grooming

Conducta de una persona adulta que realiza acciones deliberadas para establecer lazos de amistad con un niño o niña en internet con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del niño o, incluso, como preparación para un encuentro.



1 Fuente: Fondo de las Naciones Unidas para la Infancia (UNICEF)

RIESGOS EN LÍNEA

Las investigaciones actuales clasifican tres categorías de riesgos en línea.[2]

1. Riesgos de contenido: Cuando un niño o niña está expuesto a un contenido no deseado e inapropiado. Esto puede incluir imágenes sexuales, pornográficas y violentas; algunas formas de publicidad; material racista, discriminatorio o de odio; y sitios web que defienden conductas poco saludables o peligrosas, como autolesiones, suicidio y anorexia.

2. Riesgos de contacto: Cuando un niño o niña participa en una comunicación arriesgada, como por ejemplo con un adulto que busca contacto inapropiado o se dirige a un niño o niña para fines sexuales, o con personas que intentan radicalizar a un niño o niña o persuadirlo para que participe en conductas poco saludables o peligrosas.

3. Riesgos de conducta: Cuando un niño o niña se comporta de una manera que contribuye a que se produzca un contenido o contacto de riesgo. Esto puede incluir que los niños y niñas escriban o elaboren materiales que inciten al racismo o al odio contra otros niños y niñas, o publiquen o distribuyan imágenes sexuales, incluido el material que ellos mismos produjeron. En este apartado entra el Ciberbullying, Ciberacoso y el Grooming.

¿QUÉ FORMAS TOMAN ÉSTAS AGRESIONES?

Algunos ejemplos de agresión en línea son:

- Envío o compartir de fotos, videos o datos de contenido sexual.
- El perfil de la víctima es publicado sin autorización en la web para ridiculizar. Conocido como Upload.
- Uso de la identidad (real o falsa) de la víctima para hacer comentarios ofensivos a terceros.
- Compartir contactos (números de celular, direcciones de correo, perfiles de redes) para convertirlos en blanco fácil de Spam y/o acoso.
- Entrar de forma violenta a grupos cerrados para compartir información sensible como pornografía, actos violentos, entre otros.
- Compartir los datos e información personal de las víctimas en plataformas y redes sociales sin su consentimiento.
- Mensajes ofensivos y violentos dentro de grupos cerrados por falta de regulaciones.

Es indispensable que niños, niñas y adolescentes comprendan que tras el perfil de un usuario o siendo usuario de una red social, hay una persona y que, por lo tanto, cualquier acto de agresión, violencia, burla, acoso o discriminación realizado en internet tiene consecuencias en la vida real de la persona afectada.

2 Fuente: Fondo de las Naciones Unidas para la Infancia (UNICEF)

Conversar, intercambiar opiniones, reflexionar y ayudar a la toma de conciencia es una de las mejores maneras de prevenir tanto que realicen como que sean víctimas de situaciones de acoso o discriminación.

¿QUÉ HACER PARA MANTENER AMBIENTES DIGITALES SEGUROS Y SANOS PARA LOS NIÑOS, NIÑAS Y ADOLESCENTES?

La responsabilidad de los padres, representantes, profesores y acompañantes es prevenir, cuidar y proteger la dignidad de los niños, niñas y adolescentes, tanto en la presencialidad como en la vida digital. Entonces, la invitación es a planificar, desarrollar y clausurar los espacios de formación digital teniendo como criterio fundamental la seguridad y bienestar digital.

ANTES DE IR AL AMBIENTE DIGITAL

A. Investiga la plataforma en donde se intercambiará la información con los menores de edad. Asegura que ofrezca la posibilidad:

- Cifrar datos de extremo a extremo, es decir, que los datos compartidos mediante la plataforma solo podrán ser, en el mejor de los casos, decodificados por el emisor, el receptor y la empresa que ofrece el servicio.[3]

- Privacidad, la plataforma debe ofrecerte la posibilidad de crear espacios privados, asegurados con contraseñas. De igual forma, asegura no compartir el enlace por vías públicas, lo recomendable es no compartir enlaces, sino ingresar a los participantes de forma manual, de este modo aseguras que no entrarán terceros desconocidos. En el caso de compartir el enlace, hazlo en grupos privados haciendo la observación de no hacerlo público.

- Bloqueo de acciones, si la plataforma te ofrece la posibilidad de bloquear acciones determinadas en los usuarios será de suma importancia, puesto que podrás, durante la sesión formativa, mitigar acciones que se puedan salir de control. Por ejemplo, no permitir que compartan fotografías, audios o vídeos a personas en concreto o simplemente evitar que se puedan capturar pantallas.

B. Registra previamente a los participantes:

Lo ideal es desarrollar sesiones privadas solo con usuarios invitados, así que lo recomendable es realizar inscripciones donde obtengas los datos necesarios de los invitados. Esto te permitirá invitarlos de forma privada al grupo dentro de la plataforma y evitar que entren desconocidos. Importante, solo solicita información necesaria de modo a que no comprometas información que no es útil.

3. ¿Qué debo saber sobre el cifrado?: https://ssd.eff.org/es/module/%C2%BFqu%C3%A9-es-el-cifrado

C. Diseña normas de Netiqueta: Es un conjunto de reglas que regulan el[4] comportamiento de los usuarios para comunicarse en la red, en pocas palabras es la etiqueta del ciberespacio. Diséñalas pensando en los destinatarios, las normas comunes de comunicación y resaltando la mística de la organización.

D. Asignar un nombre adecuado a la sala, que respete tu privacidad y la de las personas participantes. Además, que solo muestre la información necesaria.

Ejemplo adecuado:
Encuentro de Voluntarios 2020.
Ejemplo no adecuado:
Reunión sobre con _X tema_ con _X miembro_ para X actividad.

E. Añadir contraseña a la llamada o al grupo de ser posible. Dicha contraseña no debe ser pública, compártela en privado.

F. En videollamadas habilita la sala de espera y **verificar la identidad de las personas** antes de autorizarlas a la llamada. También configura que las personas eliminadas no puedan volver a unirse a la llamada.

G. Considera **deshabilitar la opción de compartir archivos** para los participantes, de esta forma puedes evitar que posibles infiltrados compartan información no deseada.

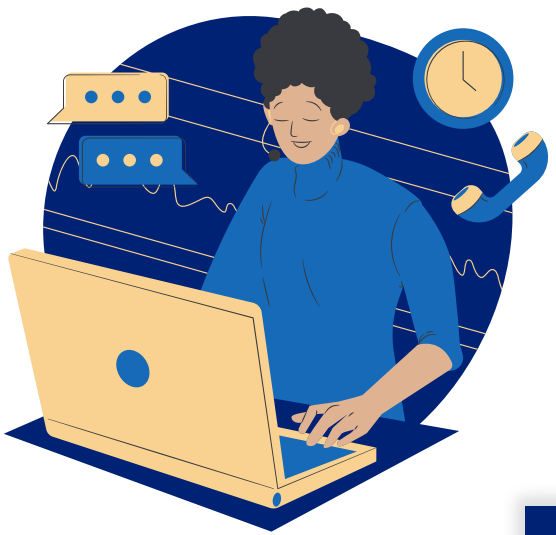
DURANTE EL DESARROLLO DEL ESPACIO EN EL AMBIENTE DIGITAL

- Conéctate siempre desde la página oficial de la plataforma que presta el servicio de videollamadas, grupo o foro. Cuida que estés conectado desde una red privada (casa o trabajo), nunca desde una red pública.

- Conéctate siempre desde equipos de confianza, bien sea propios o de familiares o amigos muy cercanos. Si se trata de un equipo prestado, asegura eliminar la información al cerrar el espacio.

- Asegura que todas las personas que ingresen al ambiente tengan su identificación y que se encuentren en tu lista de invitados. Ten cuidado con desconocidos, si es el caso consulta su identidad por privado.

- Comparte las normas de Netiqueta. Insiste en su uso durante toda la actividad.



4. https://blog.continental.edu.pe/uc-virtual/la-netiqueta-y-sus-10-reglas- 4 basicas/

- Solo solicita información necesaria, cuida información sensible como: números de celulares, direcciones, perfiles de redes sociales, información de bancos, número de cedulas de identidad o pasaporte.

- Cuida que al momento de compartir información multimedia como vídeos o fotos no se evidencie información innecesaria: direcciones, lugares públicos reconocidos, entre otros. Así como información sensible: desnudos, símbolos obscenos, frases violentas.

- Promueve el uso de fondos virtuales, tanto para quien lidera el espacio como[5] para los participantes. De esta forma estarás cuidando no dar información del ambiente físico próximo.

- Cuida la ortografía, el uso de palabras violentas o de ejemplos que puedan ser interpretados de forma incorrecta. No compartas información sensible que pueda vulnerar a los participantes.

- Cuida el tiempo de conexión, recuerda mantener sesiones abiertas por no más de 2 horas reloj. Planifica tu tiempo y se puntual. Igualmente, planifica actividades que necesiten de desconexión por parte del participante, como por ejemplo: dibujar, pintar, buscar objetos, es decir, actividades fuera del dispositivo electrónico.

- Si deseas grabar la llamada asegúrate de consultarlo con los participantes. Al finalizar cuida la grabación está segura.

AL CERRAR TU AMBIENTE DIGITAL

A. Asegúrate de ser el último en salir de la sala, así evitas que los participantes se queden conectado durante más tiempo y ocurran imprevistos en el ambiente diseñado por ti o la organización.

B. Al momento de compartir información multimedia (vídeos, imágenes, textos), asegúrate de que no contengan información personal de los participantes (números de celulares, direcciones, correos, nombres de perfil e información sensible (frases violentas, gestos obscenos, desnudos).

C. Solo guarda la información necesaria. Elimina textos, vídeos, fotos, mensajes, entre otros datos que no te serán útiles. En el caso de guardar información necesaria para fines de testimonios guárdala de forma segura y solo has uso de ello para tal fin.

D. Elimina el grupo o la sala de videollamadas, así aseguras que cualquier información compartida no será posible recuperarla.

5. Fondos virtuales: https://support.zoom.us/hc/en-us/articles/210707503-Virtual-Background

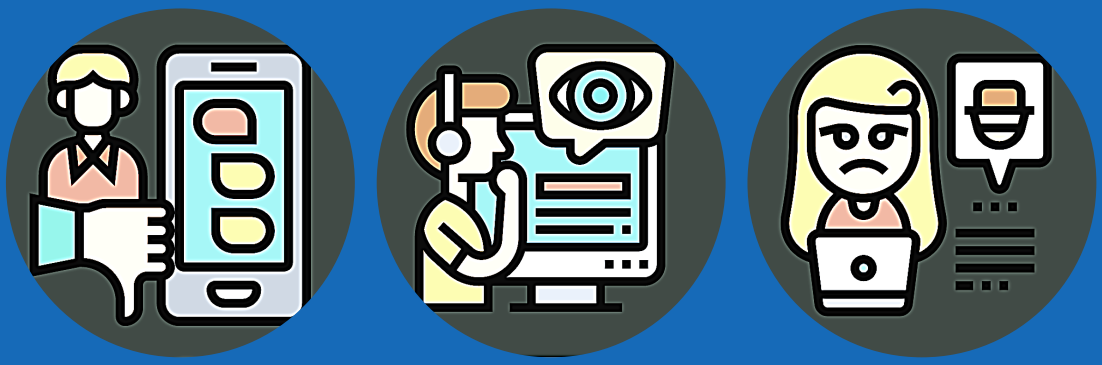
ACCIONES INMEDIATAS

1. Identifica a la persona visitante no deseada.

2. Expulsa a la persona de la llamada.

3. Bloquear la reunión, si no estaba bloqueada para evitar que haya intentos de ingresar nuevamente.

4. Reportar a la plataforma. En las opciones de seguridad está la opción para reportar, también puedes enviar un correo electrónico a la atención de la plataforma. Recuerda que, por la seguridad de otros participantes, la acción inmediata es expulsar a la persona de la llamada y después reportar a la plataforma. El contacto de la persona quedará en tu lista de participantes..



ACCIONES SECUNDARIAS

1. Atiende a las víctimas. Acompaña y dialoga.

2. Si trata de un victimario conocido, es decir, no anónimo deberás denunciar ante organismos competentes. Es crucial tener información real de la persona antes de proceder.

3. Registra los hechos en forma de actas. Así tendrás un soporte para presentar a las autoridades competentes.

4. Evita normalizar estas acciones como parte de las interacciones digitales. Para combatir la violencia. Visibiliza este tipo de agresiones. Contar tu historia en primera persona es un paso hacia el combate en contra de las violencias digitales; así como compartir recomendaciones para protegernos y proteger a niños, niñas y adolescentes.

NOTA: La Asociación Civil Huellas se suscribe a todos los acuerdos, procedimientos y normas de convivencia establecidos en los Colegios Fe y Alegría, Centros Educativos de la Compañía de Jesús (ACSI), parroquias y comunidades eclesiales donde funciona el Programa Grupo Juvenil, siempre y cuando estos no contravengan las leyes y normativas vigentes en la legislación venezolana para la protección de la integridad de la persona humana, especialmente la de los niños, niñas y adolescentes.

REFERENCIAS

- (UNICEF), F. d. (2019). NIÑOS, NIÑAS y ADOLESCENTES EN LÍNEA (Riesgos en las redes y herramientas para protegerse). Retrieved from http://www.codajic.org/sites/ www.codajic.org/files/guia(2).pdf
- Aguilar, P. (2020, Julio). Protege.LA. Retrieved from Comunicaciones seguras en Zoom (o herramientas similares): https://protege.la/comunicaciones-seguras-en-zoom/
- Hernández, O. (2020, Mayo). SEGURIDAD DIGITAL: Conceptos y Herramientas Básicas. Retrieved from https://conexo.org/conceptos-y-herramientas-basicas
- Huellas, A. C. (2016). Lineamientos del Programa Grupo Juvenil. Caracas