Ministerio del Interior y Seguridad Pública

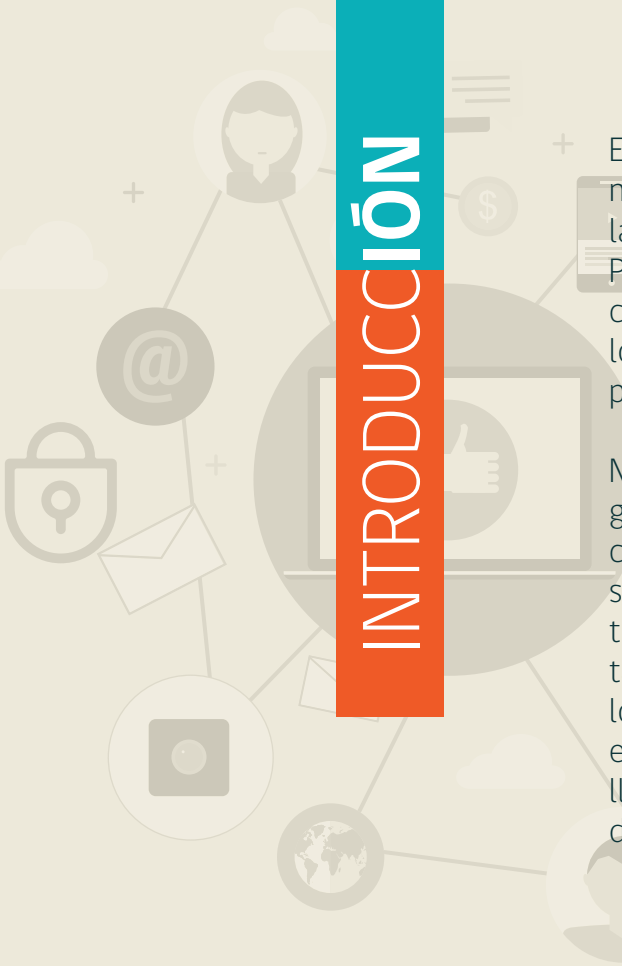
En el Mes de la Ciberseguridad **2021**

Siete grandes ciberriesgos **para Niños, Niñas y Adolescentes**

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

INTRODUCCIÓN



En este nuevo mes de la ciberseguridad, como CSIRT de Gobierno decidimos condensar nuestras principales recomendaciones entregadas a lo largo del año en guías enfocadas en distintos segmentos de la población. Pusimosel foco en los niños, niñas y adolescentes (NNA), un grupo especialmente vulnerable a los engaños por internet, describiendo algunos de los principales riesgos y entregando consejos para que sus madres, padres y tutores puedan enfrentarlos junto a ellos.

No sorprenderá a nadie, menos aún a madres, padres y tutores, el que la gran mayoría de los consejos se relacionan con mantener una relación de confianza y comunicación con los NNA. Este es un requisito para poder saber, aunque sea a grandes rasgos, qué tipo de búsquedas hacen nuestros niños en la red y qué redes sociales y plataformas de juego frecuentan. Y también resulta indispensable crear un ambiente propicio para que los menores nos informen si experimentan los problemas que se delinean en esta guía, ya que son temas que pueden provocar vergüenza y humillación para los menores, especialmente cuando hay involucrado material de carácter sexual y/o burlas de compañeros y falsos amigos.

PRINCIPALES RIESGOS

1.- GROO**MING**

Es la manipulación de un niño, niña o adolescente (NNA) por parte de un adulto, a través de internet, para crear gradualmente lazos emocionales y finalmente acosarlo sexualmente y/o generar pornografía infantil. Si el niño se niega, el adulto procede a chantajearlo (flagelo conocido como sextorsión). Generalmente, para ganarse la confianza del niño, el victimario se hace pasar por otro menor de edad.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

Cómo **enfrentarlo:**

- Explicar a los NNA los riesgos del grooming
- Enseñarles a desconfiar de desconocidos en internet.
- Dejarles claro que nunca deben entregar datos personales o fotos íntimas a nadie.
- Explicarles que deben avisar a sus padres si alguien les pide datos o imágenes personales.

En caso de vivir un **caso de grooming:**

- Los padres deben evitar contactarse con el abusador, nunca acceder a sus chantajes, y denunciarlo ante la Policía de Investigaciones (PDI).

Recomen**daciones:**

- Los padres necesitan mantener una relación de confianza y comunicación con sus hijos, y acordar normas de uso de internet con ellos.
- Pueden decidir de común acuerdo un contrato de uso del internet, con detalles como los horarios y sitios permitidos y que los menores se comprometan a no contactar desconocidos. Un ejemplo es nuestro Acuerdo Parental(1).
- Los menores deben comenzar a utilizar internet bajo supervisión de sus padres. Su uso autónomo debe ser progresivo según su edad y madurez. Cuando son más pequeños pueden usarse controles parentales, como los que delineamos en nuestra Guía de Mediación Parental(2).

(1) https://www.csirt.gob.cl/media/2020/03/Acuerdo-familiar.pdf.pdf
(2) https://www.csirt.gob.cl/media/2020/10/Cibergui%CC%81a-de-mediacio%CC%81n-parental.pdf

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

2.- CYBERBULLING / **CIBERACOSO**

Se trata del tradicional acoso, pero efectuado por medios digitales, lo que posibilita que la intimidación sea realizada en todo momento y lugar, y con un muchísimo mayor alcance y potencial de permanencia. Es importante recordar, asimismo, que cuando se realiza en el contexto escolar, los colegios tienen la responsabilidad legal de adoptar medidas disciplinarias, y de no hacerlo, pueden ser denunciados y recibir multas de hasta 50 UTM.

Cómo **enfrentarlo:**

- Los niños deben tener claro que pueden confiar en padres y profesores para contarles lo que están sufriendo.
- También se debe motivar a los menores a actuar cuando vean a amigos o compañeros ser objeto de acoso.
- Lo mismo para los chicos que abusan de otros, debe hacérseles ver que eso no está bien y deben dejar de hacerlo.

Recomen**daciones:**

- Como en todo problema que afecte a los menores, es indispensable que exista un ambiente de confianza con sus padres para que recurran a ellos cuando sean víctimas de ciberacoso. Es ideal formarles la costumbre de contar a sus padres lo que les sucedió durante el día, tras volver del colegio.

3.- OVER**SHARING**/ COMPARTICIÓN DE EXCESIVOS DATOS PERSONALES

Estemos hablando de niños o adultos, es comùn que en internet publiquemos más información de lo que resulta seguro. Esto es particularmente cuando se trata de NNA, que muchas veces no tienen conciencia de los peligros de dejar en línea fotos o direcciones, que los pueden hacer identificables a potenciales abusadores sexuales, secuestradores o delincuentes.

Cómo **enfrentarlo:**

- Enseñar a los menores que deben publicar lo menos posible, idealmente nunca fotos de ellos mismos y jamás donde viven, donde estudian o donde van a estar en determinado momento. Tampoco difundir de forma pública su número de teléfono.

- Esto mismo debe extenderse a imágenes e información de sus familiares y amigos, especialmente si piensan compartir estos datos sin el consentimiento de sus dueños.

Recomen**daciones:**

- Los padres, además de educar a sus hijos a tener cuidado con lo que publican, deben dejarles claro que todo lo que se publica en internet queda para siempre guardado en algún rincón, que todos pueden verlo, y que si se arrepienten de lo que publicaron seguramente será demasiado tarde.

- También deben aprender las formas de configurar las aplicaciones y dispositivos que usan los menores de forma en que estos recopilen y compartan la menor cantidad de datos personales posible, y asegurarse regularmente de que la configuración de apps y aparatos sigue siendo la más segura.

4.- SEXTING

Se trata de enviar o recibir fotos o videos de connotación sexual de forma voluntaria a través de internet.

Es un problema porque el entregar imágenes sensibles a otros nos expone a chantajes y, especialmente en el caso de los menores de edad, a humillaciones y cyber-bullying. Adultos pueden hacerse pasar por otros menores para intercambiar imágenes y luego chantajear a los NNA a cambio de favores sexuales.

Cómo **enfrentarlo:**

- Nuevamente, la clave es tener conciencia de los riesgos. Recordar a los NNA que una vez algo es compartido en internet, es imposible estar seguro de que haya sido borrado, que hay adultos haciéndose pasar por menores de edad para aprovecharse de ellos y que incluso aunque diga que no las compartirá o que las borrará después de recibirlas, es muy probable que si nos piden fotos de connotación sexual éstas sean guardadas y compartidas por el receptor con sus amigos.

Recomen**daciones:**

- Lo ideal es nunca compartir fotos privadas a través de internet y de hacerlo, evitar que aparezcan en ellas la cara del menor u otros elementos fácilmente identificables, como tatuajes y lunares.

- La confianza es esencial. Para que los niños, niñas y adolescentes tengan confianza de avisarles si han caído en alguna extorsión por sexting, por ejemplo, los padres y tutores deben evitar culpar excesivamente al menor de lo sucedido, y enfocarse en primer lugar en realizar la denuncia ante la PDI.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

5.- COMPRAS EXCESIVAS **ONLINE**

Muchas aplicaciones y juegos exigen u ofrecen la opción de pagar por mejoras o personalizaciones. Y hay niños que aún no saben cómo funciona el dinero, o que pueden comprar sin saber, dejando con abultadas cuentas a sus padres.

Cómo **enfrentarlo:**

- Los NNA deben tener conciencia de que no pueden comprar nada sin hacerlo en presencia y con la aprobación explícita de sus padres.

Recomen**daciones:**

- Si se le va a entregar un dispositivo a un niño para que se conecte a internet, asegurarse antes de que no tenga medios de pago, como tarjetas de crédito, y claves bancarias registradas para facilitar el pago. Lo más seguro es ingresar los datos cada vez.

6.- RETOS VIRALES **PELIGROSOS**

Abundan en las redes sociales distintos desafíos o "challenges", en inglés, que invitan a los seguidores a repetir conductas a veces inocuas, otras peligrosas, como el llamado a consumir cápsulas de detergente que enfermó a varios niños en EE.UU. en 2017.

Cómo **enfrentarlo:**

- Es muy difícil instruir a los NNA para resistir los retos de sus pares, ya sea en el mundo físico o en el digital, ya que el temor a ser excluido es uno de los más fuertes en los menores. Sin embargo, es clave instaurar la importancia de no dejarse arrastrar por conductas peligrosas, y recordar siempre que el verdadero valor de una persona no se mide por sus vistas o likes.

Recomen**daciones:**

- Permitir que los niños y niñas solo accedan a las redes sociales cuando tengan edad y madurez suficiente. Acompañar y vigilar su uso de las redes, si quieren imitar todo lo que aparece se debe poner aún más atención. Mantener la confianza y comunicación y de ser necesario usar aplicaciones de control parental.

7.- CONTENIDO **INAPROPIADO**

Comentarios, textos, fotos o videos que pueden resultar perturbadores para los menores de edad si se encuentran con ellos en internet. Esto debido a múltiples motivos, como corresponder a contenido violento, chocante, sexual o malicioso.

Cómo **enfrentarlo:**

- Los chicos deben saber que en internet se puede ver, casi literalmente, de todo. Y que si se enfrentan a imágenes que los hagan sentir incómodos o asustados pueden contar con sus padres para conversar.

Recomen**daciones:**

- Los controles parentales y aplicaciones para niños son una forma de evitar el acceso a contenido inapropiado por parte de los NNA más pequeños. Entre ellas se cuentan:
  - Google Family Link
  - Kaspersky Safe Kids
  - McAfee Safe Family
  - Surfie

Estos son los siete principales riesgos para los NNA que identificamos en línea, y para que sea más fácil enseñarla tus hijos elaboramos una serie de cuentos didácticos que pueden encontrar aquí:
https://www.csirt.gob.cl/media/2021/08/Master-Rev.-CSIRT-ESPECIAL-AGOSTO-ok.pdf

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CONSEJOS GENERALES QUE TAMBIÉN **DEBEMOS ENTREGAR A NNA**

Hay recomendaciones que todos debemos seguir, no importando la edad, y que debemos asegurarnos que conozcan y sigan nuestros niños:

Usar contraseñas seguras.

Se sugiere que sean de al menos 9 caracteres de largo y usen símbolos, números, mayúsculas y minúsculas.

Una buena idea es usar secuencias de palabras inconexas, por ejemplo, una combinación de "persona", "acción" y "objeto", en combinación con las reglas anteriores.

Nunca entregar nuestras claves a nadie, por mucho que prometa que no se la entregará a nadie más o diga ser un amigo.

Mantener equipos actualizados.

Las actualizaciones parchan vulnerabilidades conocidas en los programas que usamos en computadores y celulares.

Estas actualizaciones deben ser descargadas exclusivamente desde las tiendas oficiales correspondientes a los sistemas operativos de nuestros dispositivos.

Los más pequeños deben ser supervisados en internet, y entregárseles autonomía en su uso según su madurez.

Para los más pequeños existen programas de control parental, que solo les permiten acceder a contenido seguro.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

En el Mes de la Ciberseguridad **2021**

Siete grandes ciberriesgos **para Niños, Niñas y Adolescentes**

Director: Carlos Landeros Cartes

Jefa de contenidos y edición: Katherina Canales Madrid

Colaboradores equipo CSIRT: Ramón Rivera

Diseño y diagramación: Jaime Millán

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile