CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS
Investigación, Tendencia y Concientización

Vol. Nº 7
Febrero/2021
www.csirt.gob.cl

Convivencia Digital:
Decálogo para que niños y jóvenes estén seguros en redes sociales

Clases online más ciberseguras:
¿Qué debemos considerar ante esta nueva modalidad de estudio?

Cooperación Internacional
Colombia

Tendencias
Los peligros de los retos virtuales y cómo cuidar a nuestros jóvenes

Comunidad Nacionales
Fundación Katy Summer: Apoyo para padres y jóvenes que sufren ciberbullying o acoso

Legal
Ciberbullying, acoso a toda hora y en todo lugar

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

145 8712 7864
096 4321 5541

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

¿Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN Connecting and Protecting

INDICE

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

Director: Carlos Landeros Cartes

Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Carolina Covarrubias
Cristóbal Hammersley
Ramón Rivera

Diseño y diagramación: Jaime Millán

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Los niños y adolescentes son el elemento más preciado de nuestra sociedad. Y también el más expuesto a los riesgos que se pueden encontrar en línea. Porque si bien internet trae un universo de posibilidades a nuestras vidas, son numerosos también los riesgos que involucra, especialmente para los más pequeños, que pueden ver amenazadas incluso sus vidas debido a fenómenos como el grooming, el ciberacoso y algunos peligrosos retos que surgen en las redes sociales.

Es en ese contexto, y ante la inminencia de un regreso a clases que será realizado a distancia, decidimos dedicar el presente número de CiberSucesos a las formas de combatir los peligros que enfrentan niños y adolescentes en la red.

Como tema principal ofrecemos un decálogo de convivencia en las redes sociales, dirigido a los jóvenes, para que sepan qué hacer al enfrentarse al lado oscuro de la interacción digital, como el ciberbullying, la exposición a contenido violento y perturbador, la sextorsión y la violación de su privacidad, con simples consejos para fomentar el autocuidado al interactuar en la red.

En la misma línea, compartimos los pasos a seguir para que los niños tengan la mayor seguridad al conectarse para recibir sus clases de forma virtual, tendencia que continúa desde el año pasado a causa de la pandemia, y que se ha visto posibilitada en muchos casos gracias a los esfuerzos del Gobierno para proveer de computadores y conexión de internet a estudiantes vulnerables a lo largo del país.

Colombia es la nación que comparte su ejemplo en la sección Cooperación Internacional, a través de la experiencia de "En TIC confío", iniciativa destinada a concientizar a los jóvenes para adquirir hábitos saludables en internet, y combatir los delitos que sufren los menores, como la explotación sexual.

En el apartado Comunidad Hacker, los creadores de la Fundación Katy Summer comparten los proyectos e iniciativas que han desarrollado para combatir el ciberacoso a los menores, en honor a su hija, Katy Winter, que murió a causa de este flagelo de la vida online que afecta a niños y adolescentes.

Nuestros expertos de la sección Legal analizan, en esta ocasión, las implicancias judiciales del ciberacoso o ciberbullying, cómo se define y su regulación (o más bien, falta de) en nuestro país. Explican que si bien este delito no está especificado como tal en nuestra legislación, existen instancias a las cuales recurrir en la justicia cuando un niño es víctima, las que se delinean en esta edición.

CONVIVENCIA **DIGITAL**

Decálogo para que niños y jóvenes estén seguros en redes sociales

El uso de las distintas plataformas ha aumentado considerablemente en los últimos años. Utilizada por grandes y chicos, las redes sociales han permitido mantener contacto con amistades o compartir distintas situaciones de la vida de las personas, entre otros beneficios. Sin embargo, algunos jóvenes no ven con tan buenos ojos estos sitios, ya que lamentablemente hay quienes los utilizan para acosarlos o extorsionarlos. Para prevenir estos y otros riesgos, CSIRT entrega 10 consejos con buenas prácticas para convivir de forma más sana en el ciberespacio.

Si en el año 2014, 1.790 millones de personas en el mundo (24%) usaban redes sociales, hoy podemos ver cómo ese número ha crecido exponencialmente según el último informe digital elaborado por We Are Social con Hootsuite que reveló que 4.200 millones de personas utilizan estas plataformas, es decir, un 53,6% de la población mundial.

Y en Chile esta situación no es tan distinta. Hasta enero de 2020, un 79% de la población usaba redes sociales, ya sea niños desde los 8 años hasta adultos mayores. Y si bien tiene innegables bondades, también existen riesgos que muchas personas no ven y que afectan a los jóvenes y niños, debido, en ocasiones, a que se desconocen situaciones riesgosas, falta de acompañamiento por parte de un adulto responsable o temor a contar un hecho que pueda ser vergonzoso.

EL "LADO B" **DE LAS REDES SOCIALES**

Si bien estos sitios se crearon en un inicio con la idea de conectar personas, también se han transformado en una pesadilla para algunos jóvenes y niños, quienes se han convertido en víctimas de delincuentes o de sus mismos pares. Esto, porque a través de estas plataformas existen riesgos como:

1.- **CIBERBULLYING:** Abuso, acoso o humillación constante entre escolares por medio de las redes sociales.

2.- **ACCESO A CONTENIDO INAPROPIADO:** Los sitios a veces muestran contenido que puede ser perturbador para los menores, como comentarios o imágenes maliciosos, agresivos, violentos o sexuales.

3.- **SEXTING:** Consiste en enviar fotos, mensajes o videos con contenido sexual explícito o sugerente.

4.- **SEXTORSIÓN:** Consiste en un chantaje en el que se amenaza a la víctima con la difusión de imágenes, videos o mensajes de contenido sexual propios.

5.- **GROOMING:** Acoso y abuso sexual online que realiza por lo general un adulto, ganándose la confianza del menor para cometer este tipo de actos.

6.- **PÉRDIDA DE PRIVACIDAD:** El hecho de compartir datos personales, imágenes o videos puede llevar a que esa información sea utilizada con fines maliciosos. Una vez que se publica en redes sociales, se pierde el control.


TikTok
in

Sin embargo, a pesar de estas amenazas, de acuerdo al Primer Barómetro del Bienestar Digital, a cargo de Movistar Chile y Fundación Nativo Digital, entregado en septiembre de 2020, y donde la muestra es de 1.046 casos, la generación Z (8 a 18 años) es la que ve con menos preocupación estos temas, siendo parte de la población más vulnerable. Algunos de los resultados de la encuesta sobre asociados a este grupo fueron:

23% Declara haber sido víctima de acoso digital, aumentando a 28% entre jóvenes de 15 y 18 años. Dentro de las causas que lo asocian son racismo (73%); homofobia (63%) y falta de empatía (64%).

78% Considera internet como un "lugar seguro".

74% Confía que sus datos se encuentran seguros en internet. Esta cifra aumenta a un 87% entre los menores de 8 y 14 años.

34% Mantiene perfiles y cuentas públicas en sus redes sociales, aumentando a un 42% entre los adolescentes de 15 y 18 años.

33% Ha tenido que cerrar sus cuentas por agresiones en internet.

DECÁLOGO DE **CONVIVENCIA DIGITAL**

Con el objetivo de promover buenas prácticas y cuidar a nuestros jóvenes de estos peligros, es importante que los padres guíen a sus hijos en su vida digital. Por esto, CSIRT entrega los siguientes consejos:

1. Conversa con tus hijos sobre sus gustos, riesgos, cómo cuidarse, qué hacer si tienen un problema y entrégales confianza para que puedan pedir ayuda.

2. Promueve buenos hábitos con los menores sobre cómo quieren ser tratados en redes sociales y motívalos a compartir contenido y realizar comentarios positivos.

3. Cuidado con las publicaciones, ya que pueden entregar información sensible como su ubicación, datos personales, etc., lo que puede ser usado para crear estafas o para humillarlos.

4. Respeto. Antes de publicar, se debe pedir autorización a quien se pueda ver afectado, ya sea una imagen o comentario.

5. No aceptar a desconocidos. Aunque sea muy atractivo para tus hijos tener muchos seguidores, no todos tienen buenas intenciones o no son quienes dicen ser. Explícales los riesgos.

6. No todas las plataformas sirven para todas las edades. Infórmate para evitar que los menores accedan a contenido inapropiado o sean contactados por desconocidos.

7. Una contraseña segura puede proteger la información de tus hijos. Ayúdalos a crear una diferente para cada red social, nunca con información personal y que jamás la compartan con sus parejas o amigos.

8. Un perfil privado evita que desconocidos accedan a los contenidos y usen la información o imágenes con fines maliciosos.

9. Guía a los menores para que compartan contenido con precaución, sobre todo si es privado. Una vez que se suba la información, nunca se sabe dónde termina.

10. Las redes sociales tienen la opción de bloquear y denunciar a quienes publican comentarios o contenido molestos. Enséñales a utilizarlas para disminuir situaciones de acoso. Se recomienda contar con respaldo de todas las agresiones para denunciar a las entidades correspondientes.

¡OJO CON EL **SHARENTING!**

Si estamos educando a nuestros a nuestros niños, también tengamos precaución con la propia exposición que nosotros hacemos de ellos en Redes Sociales, ya que es muy usual que compartamos fotos de nuestros hijos, sobrinos, nietos de una manera inocente y no consideramos la privacidad o las posibles consecuencias futuras, ya que estamos dejando en el ciberespacio una huella de ellos.
Sharenting es el término en ingles que surge de la unión del verbo To Share (Compartir) y Parenting (crianza), y se usa para definir un nuevo fenómeno en el que mamás y papás publican muchos contenidos (fotos, audios, videos) de sus hijos en sus redes sociales sin ninguna consideración de seguridad y privacidad

CIBERBULLYING Y CENTROS EDUCACIONALES

Una de las consecuencias que tiene el ciberbullying es el alcance que tiene, ya que si un joven sufre de bullying en el colegio probablemente esta situación continúa en sus redes sociales. Por lo tanto, la víctima está siendo constantemente atacada, lo que sin duda debe llegar a su fin e informar en el centro educacional que corresponda.

Chile cuenta con la Ley 20.536 sobre Violencia Escolar y el 2011 se creó la figura del encargado de convivencia, el cual es el "responsable de la implementación de un Plan de Gestión de la Convivencia, con sus respectivos protocolos y medidas pedagógicas que determinen el Consejo Escolar o el Comité de Convivencia Escolar para enfrentar las situaciones de violencia". Teniendo esto presente, es importante que los padres o adultos a cargo de los niños acudan a ellos ante una situación de acoso y/o ciberbullying para que se puedan tomar las medidas necesarias.

SI TU HIJO(A) SUFRE
DE CIBERBULLYING
RECOMENDAMOS:

1. Recolectar las pruebas que demuestren que el menor es víctima de acoso.

2. Acudir al encargado de convivencia escolar, informar de lo sucedido, entregar la información y pedir ayuda para evitar que continúen los ataques.

3. Entregar apoyo y contención a la víctima.

4. Se aconseja ir donde un especialista para que evalúe el estado psicológico del menor y entregarle las herramientas que le permitan superar este tipo de situaciones.

En caso de ser víctima de ciberbullying

DENUNCIA

Unidad de Cibercrimen de la PDI

22708 0658

CLASES ONLINE **MÁS CIBERSEGURAS:**

¿Qué debemos considerar ante esta nueva modalidad de estudio?

Pronto llega marzo y ante la incertidumbre de cómo realmente se realizarán las clases durante el 2021, tanto el Ministerio de Educación como algunos centros educacionales ya han fijado sus formas de trabajo. Y si bien nada es 100% seguro, las clases en línea se mantienen siendo una opción, ya sea en mayor o menor medida, en colegios y universidades.

Desde hace más de 10 años que existen en Chile y en el mundo los colegios virtuales, una modalidad poco conocida y que consiste en instituciones que funcionan a través de Internet. ¿Y quién iba a decir que el 2020 se iba a caracterizar por masificar esta manera de hacer clases?

El año marcado por la pandemia, logró que un 60,5% de los colegios adoptara plataformas de educación remota o aulas virtuales; un 27,4% incorporó sistemas de videoconferencias y un 11,6% utilizó las redes sociales, según datos obtenidos por el estudio "Radiografía Digital de los Colegios en Pandemia", realizado por VTR a 984 directores de colegios municipales y particulares subvencionados de todas las regiones de nuestro país entre agosto y septiembre de 2020.

Y ahora, para el 2021 la modalidad de estudio es un poco incierta. Si bien se espera poder retornar a las clases presenciales, los resultados de este mismo estudio indican que 7 de cada 10 colegios continuarán usando plataformas de videoconferencia tras volver al colegio de forma física. Una situación similar vivirán las universidades, quienes aseguraron que sólo el 9% de los programas volverá a la normalidad.

Ante esto, es importante informarse sobre las brechas de seguridad que podrían tener las distintas plataformas de clases o videoconferencia, por eso a continuación, haremos un breve recorrido de las sistemas online más utilizados el año 2020.

GOOGLE **CLASSROOM**

Esta herramienta creada exclusivamente para el mundo educativo nació el año 2014. En octubre de 2019 ya contaba con 40 millones de usuarios en más 230 países y desde principios de marzo de 2020 duplicó los usuarios diarios a 100 millones.

En Chile, de acuerdo al estudio presentado por VTR, un 60,5% de los encuestados aseguró haber adoptado plataformas de educación remota o aulas virtuales como Google Classrom, una herramienta gratuita, fácil de manejar y que permite que los profesores envíen tareas y se comuniquen con los alumnos.

Para acceder a las opciones que ofrece esta plataforma, los estudiantes deben tener una cuenta de Google, el cual actuará como identificador. Por lo tanto, profesores y los alumnos deben tener su Gmail.

RIESGOS Y **RECOMENDACIONES:**

¿QUÉ **HACER?**

Al ser una aplicación educativa, Google cuenta con políticas de privacidad más estrictas, las que prohíben hacer seguimiento y recopilar datos de los niños y niñas, excepto lo necesario con fines educativos. Sin embargo, si se activan algunas herramientas de Classroom, como por ejemplo YouTube, es posible obtener información.

1. Por lo general, los correos electrónicos de Classroom son entregados por el centro educativo, por lo tanto si quieres acceder a los ajustes de privacidad conversa con la entidad para ver qué información puedes controlar para tener una cuenta más segura.

2. Si quieres saber qué datos compartes, revisa la opción “Datos y Personalización”, donde encontrarás información sobre contraseñas, direcciones, datos de navegación, entre otros.

3. Asegúrate que tus hijos siempre utilicen las cuentas entregadas por los centros educacionales para acceder a clases, de lo contrario Google rastreará su comportamiento al navegar por Internet.

4. Cuidado con los correos electrónicos. Los niños pueden enviar y recibir un e-mail, por lo tanto asegúrate de conocer quiénes son sus compañeros y profesores para saber con quién interactúa y así confirmar que no reciba mensajes ofensivos o falsos.

5. En caso de que los niños usen un correo personal, asegúrate de configurar la privacidad de sus cuentas y datos de navegación.

MICROSOFT **TEAMS**

El año 2017 se lanzó Microsoft 365 que integra Microsoft Teams. Dos años después de su creación, la plataforma registraba 19 millones de usuarios de forma semanal. Al llegar la pandemia, Teams educativo fue utilizado por más de 183.000 instituciones y la herramienta contó con más de 75 millones de usuarios activos diarios, llegando incluso a conectar más de 200 millones de participantes en un solo día.

Para los alumnos que utilizan Teams sus cuentas escolares de Office 365 deben ser administradas por el centro educacional que corresponda. En cuanto a la privacidad de los datos, Microsoft asegura tener un real compromiso, por lo que aseguran en su sitio web “nunca usamos los datos de tu Teams para mostrarte anuncios, no monitorizamos la atención de los participantes o el uso de multitarea durante las reuniones de Teams, tus datos se eliminan después de la rescisión o el vencimiento de tu suscripción y tomamos medidas firmes para garantizar que el acceso a tus datos sea restringido y definimos cuidadosamente los requisitos para responder a las solicitudes de datos por parte de los gobiernos”, entre otros.

Sin embargo, una importante falla de seguridad detectada el 2020 en Microsoft Teams y que ya se encuentra corregida, fue la exposición del robo de datos personales, al compartir imágenes animadas en formato GIF a través del chat. Una vez que la persona la recibía y era visualizada, corría el riesgo de un ataque de ransomware, ser víctima de robo o de eliminación de datos.

CONSEJOS PARA UNA MEJOR **PROTECCIÓN AL UTILIZAR ESTA PLATAFORMA**

1. Utilizar siempre la última versión de Teams. En caso de conectarse a través de un dispositivo móvil, es importante además contar las actualizaciones de las aplicaciones de App Store o Google Play.

2. Un usuario puede ingresar desde dos dispositivos diferentes a la misma cuenta, por eso es fundamental contar con contraseñas robustas y seguras, para evitar que terceras personas ingresen a la cuenta. Además, nunca se deben compartir las contraseñas.

3. Revisar las opciones de privacidad y asegurarse de estar entregando la información que realmente se necesita.

ZOOM

Un 27,4% de los centros educacionales, según el estudio “Radiografía Digital de los Colegios en Pandemia,” incorporó en su forma de trabajo plataformas de videoconferencia. En este sentido, dentro de las más utilizadas fueron Zoom y Google Meet.

La herramienta Zoom se hizo muy popular con la llegada de la crisis sanitaria. Según el reporte de la compañía la cifra de participantes a reuniones pasó de 10 millones en diciembre de 2019 a 300 millones en abril de 2020. Sin embargo, este incremento de usuarios también dejó en evidencia importantes brechas de seguridad, como por ejemplo la falta de cifrado en las videollamadas; el descuido en su app que permitía a Facebook conocer los datos privados de los usuarios y el famoso “Zoombombing” (irrupción indeseada y perturbadora de un externo a la videoconferencia).

Y si bien Zoom ha actualizado su plataforma para entregar mayor protección, de igual manera tanto los profesores como los padres y alumnos deben mejorar los niveles de seguridad con el que utilizan la plataforma. Algunos sencillos consejos son:

1. Mantener actualizada la última versión de Zoom y utilizar la versión del navegador web, más que la app.
2. Nunca compartir el número de identificación o contraseña de la reunión con desconocidos y/o en redes sociales.
3. Las clases deben ser configuradas en modo privado.
4. Las contraseñas deben ser seguras para cada participante.
5. Habilitar la opción de notificar al anfitrión cuando alguien se quiera unir a la clase.

INICIATIVAS DEL **MINISTERIO DE EDUCACIÓN**

Durante el 2020, el MINEDUC promovió diversas iniciativas para apoyar a los colegios tanto públicos como privados que realizaron sus clases de forma virtual. Algunas de ellas fueron:

- Sitio web aprendoenlínea.mineduc.cl: Se habilitó esta plataforma para los alumnos de educación básica y media.
- "Aprendiendo a leer con Bartolo": Software gratuito dirigido a niños y niñas de 1er y 3er básico para apoyar la lectura y escritura desde la casa.
- Alianza MINEDUC con el Ministerio de Transportes y Telecomunicaciones y Asociación de Telefonía Móvil (ATELMO), con el objetivo de que los estudiantes pudieran navegar de firma gratuita.
- Distribución de SIM Cards: Junto con WOM se entregaron 3.500 chips a estudiantes prioritarios del país por tres meses.
- Entrega de computadores: Más de 122 mil computadores fueron entregados a niños y niñas de 7° básico de establecimientos públicos y particulares subvencionados más vulnerables del sistema educativo.
- Convenio con Google Classroom y Microsoft Teams.

UNA CLAVE SEGURA DEBE TENER:

1. Extensión mínima de 9 caracteres.
2. Mezclar letras mayúsculas, minúsculas, números y símbolos.
3. Frases fáciles de recordar como pedazos de canciones.

UNA CONTRASEÑA NO SE DEBE CREAR CON:

1. Datos personales como Rut, direcciones, teléfonos, etc.
2. Nombres de familiares.

EJEMPLO CONTRASEÑA SEGURA:

Con la letra de una canción y alternando mayúsculas y minúsculas:

- MICancionFavoriTa
- A la letra le podemos agregar símbolos: MI.Cancion(FavoriTa)
- Reemplazar y/o agregar letras por números: MI.C4ncion(Favor7Ta)

EL EJEMPLO DE COLOMBIA PARA COMBATIR LAS AMENAZAS **DIGITALES QUE APUNTAN A LOS JÓVENES**

“En TIC confío” se llama la iniciativa del Gobierno de Colombia para promover entre los menores de edad de ese país buenos hábitos de interacción con el mundo digital y la tolerancia cero ante la explotación sexual de niños y adolescentes.

El programa En TIC confío, del Estado Colombiano, nace hace justo una década, como un proyecto del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, con el fin de ayudar a la sociedad a interactuar de manera responsable con las tecnologías, aprovechando sus oportunidades sin dejar de vista la seguridad, junto con promover la convivencia digital y poniendo énfasis enla cero tolerancia ante el material de explotación sexual de niñas, niños y adolescentes.

Actualmente y en el contexto de la pandemia, En TIC confío se ha dedicado también a realizar la difusión de consejos para reducir la transmisión del virus, como lavado frecuente de manos y de pantallas, como, asimismo, mensajes de concienciación de los jóvenes para identificar ejemplos de información falsa sobre la epidemia propagadas por redes sociales, lo que se ha calificado como “desinfodemia”.

ALCANCE NACIONAL Y CHARLAS **DISEÑADAS PARA JÓVENES**

Las principales formas en que En TIC confío busca cumplir con sus objetivos son a través de la entrega a la ciudadanía de herramientas para enfrentar los riesgos del uso de la tecnología, y la comunicación de buenas prácticas.

Esto lo realiza a través tanto de internet, con su sitio web y sus cuentas en las principales redes sociales, mediante charlas, usualmente llevadas a cabo de forma presencial, aunque dado el contexto sanitario actual lo están haciendo través de videoconferencias.

Las charlas son gratuitas y están dirigidas a los jóvenes mayores de 12 años, siendo disponibles a lo largo y ancho de toda Colombia gracias a los embajadores que representan a En TIC confío en los 32 departamentos del país. A través de su página web (enticconfio.gov.co) las instituciones educacionales y empresas pueden pedir recibir una de estas charlas, de forma gratuita.

Para lograr el mayor efecto en niñas, niños y adolescentes, En TIC confío desarrolló una charla tipo especialmente diseñada, lúdica, gratuita y con enfoque de género, que es la que sus embajadores tradicionalmente replican en cada departamento como parte de su evangelización en buenas prácticas y contra los riesgos del mundo online, y que en el presente momento se imparten a través de plataformas de videoconferencia.

Esta charla creada por En TIC confío está hecha de forma de tener un mayor impacto en niñas, niños y adolescentes desde 12 años y sus padres, madres y cuidadores.

Las campañas digitales igualmente son diseñadas para llamar la atención de los jóvenes. Usan ilustraciones y videos cortos, presentados algunas veces por adolescentes, tal como los chicos a los que buscan llegar, donde les hablan de igual a igual, a través de las redes sociales más populares.

Dentro del material disponible en línea, existen cursos cortos virtuales para conocer los principales riesgos del internet y cómo evitarlos. Asimismo, En TIC confío colabora estrechamente con otras campañas del MinTIC tendientes a mejorar la relación de los ciudadanos con la tecnología y aprovechar su enorme potencial, como Transformación Digital Naranja, ConVerTIC, la actual campaña para facilitar la implementación del Teletrabajo en Colombia y #ConvivenciaDigital.

Este último, #ConvivenciaDigital, es programa que busca dar a conocer entre la ciudadanía los protocolos que permiten una correcta interacción de las personas con la comunidad digital, para promover comportamientos de respeto, y que toda interacción y comunicación en los escenarios digitales se realice bajo la máxima de "trata a los demás como quieres ser tratado".

TOLERANCIA **CERO**

Pero más allá de la importante labor de concientización para el mejor uso del internet en el día a día, En TIC confío pone énfasis en educar a los menores para la prevención del grooming, el ciberacoso, la ciberdependencia, el sexting y la difusión de material de explotación sexual de niñas, niños y adolescentes. Estas están claramente entre las más graves amenazas que encuentran los jóvenes en su interacción con el mundo digital, debido al enorme impacto, muchas veces irreparable, que tienen sobre las vidas de niños y adolescentes.

En este contexto, es clave el trabajo y la difusión que hacen en su web del programa Te Protego (teprotejo.org), portal colombiano de denuncia online y confidencial de delitos contra menores de 18 años, como pornografía infantil y ciberacoso.

LOS PELIGROS DE LOS RETOS VIRTUALES Y **CÓMO CUIDAR A NUESTROS JÓVENES**

Tal como en otros aspectos de la vida de niños y adolescentes, en el ámbito tecnológico es clave que los padres mantengan un buen nivel de comunicación con los hijos, para poder notar cuanto antes cualquier comportamiento extraño.
En todo caso, y si bien es imposible mantener un control total sobre lo que los niños puedan consumir a través de las redes sociales, es bueno saber que muchos de los supuestos retos mortales son magnificados por los medios y en realidad son noticias falsas o corresponden a casos aislados.

Recientemente se conoció la muerte de Antonella, una niña de 10 años en Sicilia, supuestamente por seguir un desafío viral en TikTok donde usuarios llamaban a otros a asfixiarse hasta el desmayo y compartir el video. Este es solo uno de los tantos casos de "challenges" que se popularizan con rapidez todos los días por las distintas redes sociales.
Si bien la mayoría de las veces estos retos llaman a realizar acciones inofensivas, como bailar, en ocasiones se han conocido casos de personajes que motivan a sus seguidores a conductas peligrosas, como cuando en 2018 se viralizó el consumo de un modelo de cápsulas de detergente que, según se popularizó en internet, tenían la apariencia de dulces, y que terminó con varios menores envenenados.

También se habla mucho de retos que directamente llamarían a los menores a seguir desafíos que acaban en autolesiones o suicidio, aunque la evidencia en estos casos no suele ser tan concreta, como en el caso de la niña en Italia o del que se dio a conocer como "reto de la ballena azul" hace 4 años, el del "Momo" en 2018 o el "skull cracker challenge" en 2020.
Este tipo de desafíos, se supone, plantea al niño hacer tareas en un comienzo simples y sin riesgo, para ir escalando a labores cada vez más complejas y peligrosas. El caso del "challenge" de la ballena azul, por ejemplo, habría incluido realizarse una herida cortante con forma de aquel cetáceo, para culminar en el suicidio. Afortunadamente, según la BBC, no está claro que el reto haya existido, por cuanto las autoridades no han confirmado la relación de ningún suicidio con mensajes o imágenes de ballenas en foros o redes sociales.

Como sea, es esencial que el niño sienta que puede confiar en sus padres y comunicarles lo que encuentra en internet, con tal de conversar frecuentemente sobre las apps y páginas que más visita. Y por lo mismo, antes de que los menores se enfrenten a internet, es importante que como adultos responsables les hagamos entender cuáles son los riesgos de la red, y las cosas que deben tener claras al enfrentarse a un dispositivo.

LOS PRINCIPALES **PELIGROS SON**

1. **Incitación a realizar actos violentos, autolesiones o cometer suicidio:** Los niños deben saber que este tipo de contenido existe, y que, si se enfrentan a él, pueden confiar en sus padres para denunciarlo. Deben tener claro que no serán reprendidos por eso, para que no sigan consumiendo contenido peligroso debido a que no se atreven a contarle a sus adultos responsables por miedo a un castigo.

2. **Acoso o bullying:** Otra forma de violencia a los que se ven expuestos los menores es al matonaje virtual, muchas veces una continuación de actitudes que ya sufren en sus colegios. Nuevamente, la comunicación es fundamental para romper las conductas de abuso reiterado, que se ven facilitadas cuando las víctimas se sienten solas y vulnerables.

3. **Grooming y solicitudes de pornografía infantil:** Insistir en que no deben subir ni compartir nunca fotos sugerentes, con poca ropa, o que les avergonzaría que otras personas pudieran llegar a ver.

EN TÉRMINOS GENERALES, ES NECESARIO CREAR CONCIENCIA EN LOS NIÑOS Y ADOLESCENTES SOBRE:

1. Internet es para siempre: Es imposible asegurarnos de que una información desaparezca una vez que ha sido compartida en línea, y los niños deben tenerlo claro.

2. Nadie es 100% anónimo: Deben interactuar con internet como si su identidad fuera conocida, aunque lo hagan de forma anónima. Por un lado, es posible que las personas en internet descubran su identidad, aunque no la difundan, y por otro, el pensarnos anónimos nos hace, en general, comportarnos de forma menos considerada por los demás y sin tener en cuenta las consecuencias de lo que compartimos.

3. No todo lo que ven en internet es real: Otro consejo que también debemos recordar los adultos es que lo que se ve en la red es verdad, y deben confiar en que, ante cualquier duda, pueden conversar con sus padres.

ALTERNATIVAS DE CONTROL PARENTAL **ESPECIALMENTE PARA LOS NIÑOS**

Los sistemas operativos de los teléfonos Apple y Android cuentan con opciones para reducir el tiempo que se pasa frente a la pantalla. También hay aplicaciones específicas para limitar los sitios que los niños pueden visitar en internet, como Google Family Link, Surfie, McAfee Safe Family y Kaspersky Safe Kids. Algunos además incluyen seguimiento de la ubicación del smartphone de los menores, y alertas a los padres en el caso de que aparezcan contenidos no deseados en sus dispositivos.

FUNDACIÓN KATY SUMMER:

APOYO PARA PADRES Y JÓVENES QUE SUFREN CIBERBULLYINGO ACOSO

El acoso es un enemigo que en muchos casos es silencioso y puede tener resulta dos fatales para las familias Por esto, como una manera de apoyar, prevenir, sen sibilizar y desarrollar herramientas útiles para este fin, el 2018 nació esta funda ción. Te invitamos a conocer los proyectos e iniciativas que desarrollan para evitar que más jóvenes sean víctimas de acoso.

KATY SUMMER Fundación

Evanyely Zamorano y Emanuel Pacheco son los creado- res de la Fundación Katy Summer. El nombre de esta or- ganización es en honor a su hija Katy Summer, una ado- lescente de 16 años que fue víctima de ciberbullying y de sus letales efectos. En diciembre del año 2018, for- maron esta entidad, con la finalidad de crear conciencia y contribuir a que tanto padres como jóvenes entre 15 y 29 años sepan cómo enfrentar una situación de este tipo, mediante distintas iniciativas.

“Uno de los fenómenos que explican el ciberbullying o acoso, desde nuestro punto de vista, es que las personas no son conscientes de que sus comentarios agreden o hacen daño, sino que por el contrario son divertidos y no se dan cuenta de los efectos que pueden tener”, asegura Emanuel.

Por esto, para lograr sus objetivos, durante estos dos años de vida, la fundación ha trabajado en conjunto con comunidades escolares, entidades públicas, privadas y otras organizaciones sociales en la prevención del suici- dio adolescente, acompañando a niños, niñas y jóvenes y/o sus familias que están sufriendo los resultados del acoso escolar.

Gracias a la convicción de sus fundadores y a su firme propósito de disminuir el acoso entre los jóvenes, la fundación ha trabajado arduamente para llegar con conversatorios, campañas masivas, charlas, seminarios, entre otras iniciativas a más de 90.000 personas. Algunas de las actividades realizadas son:

"HAY PALABRAS QUE MATAN": En noviembre de 2018, en conjunto con este Ministerio, lanzaron esta campaña masiva para detectar ciberacoso en las redes sociales, como Facebook, Instagram y Twitter.

DOCUMENTAL "NO MÁS BULLYING": Difundido en todos los colegios municipales y subvencionados del país, en marzo de 2019 entregaron un documental sobre la vida de Katy, producido por La Ventana Chile con el apoyo de Ripley y Canal 13, y que tuvo como fin alfabetizar a los padres en redes sociales y orientarlos en cómo mantener un canal de comunicación con sus hijos.

CAMPAÑA "GOODBYE CIBERBULLYING": Para Lollapalooza del año 2019 y el Festival Convive produjeron y lanzaron la última canción de Katy Summer con archivos de audio y video de toda su vida. La campaña llegó a 250 millones de personas en Latinoamérica, salió finalista en Cannes y obtuvo mejor idea país en El Ojo de Iberoamérica.

CHARLA "YO ELIJO SALVAR": En noviembre de 2019, la fundación llevó a cabo su primera charla enfocada en la prevención del acoso y suicidio juvenil, llegando a más de 80.000 personas.

CONGRESO CHILE: En marzo de 2019, los creadores de la fundación participaron en comisiones de educación de la Cámara y del Senado por la Ley de Ciberbullying y Ciberacoso.

SEMINARIO "YO ELIJO VIVIR SIN CIBERBULLYING": Esta actividad, dirigida a padres e hijos, se desarrolló junto con la Municipalidad de Las Condes, con la finalidad de promover conversatorios sobre las experiencias digitales en familia en octubre de 2019.

CAPACITACIÓN SERVICIO NACIONAL DE LA MUJER Y EQUIDAD DE GÉNERO: Para prevenir situaciones de ciberviolencia contra la mujer, en febrero de este año comenzaron una capacitación dirigida a funcionarios y funcionarias de este servicio a nivel nacional para que aprendan a identificar este tipo de ataque.

Gracias a estas instancias, hoy es posible contar con más espacios de conversación y visibilizar aún más un problema país que requiere de una intervención por parte de todos los actores involucrados: padres, adultos responsables, centros educacionales y gobierno.

PASOS **A SEGUIR**

La fundación no descansa y este año ya está planificando nuevas campañas y capacitaciones enfocadas en la ciberviolencia de género, debido a que cerca de un 73% de quienes sufren acoso en línea son mujeres a nivel mundial

Así también, dentro de los proyectos para este año, los fundadores de Katy Summer aseguran: "Después de un 2020 intenso para los centros educacionales, este 2021 queremos trabajar más con las áreas de convivencia escolar, considerando que este año probablemente también será diferente. Además, estamos desarrollando una aplicación con inteligencia artificial para detectar proactivamente comportamientos depresivos o identificar situaciones de acoso en redes sociales".

El apoyo que puedan brindar los padres, madres y/o sus cuidadores/as a sus hijos e hijas es muy importante, por eso es fundamental que "los adultos aprendan y conozcan qué les gusta a sus hijos e hijas, cómo viven en las redes sociales, a quienes siguen y por qué, y cómo se pueden acercar al mundo de las y los jóvenes", explica Emanuel. Y en base a esto, el 2021 la fundación continuará realizando charlas de sensibilización en empresas y universidades, para así llegar a este público que debe saber qué está pasando en la actualidad con los jóvenes.

Por otra parte, y para contribuir en materia legislativa, Evanyely y Emanuel participan en conversaciones sobre los proyectos y legislaciones actuales, de manera de "considerar a los medios digitales como un canal más para que las leyes que hoy protegen en el mundo físico se traspase al digital", aseguran.

RECOMEN**DACIONES**
para padres

Evanyely enfatiza que para avanzar en este tema “nos falta como adultos reconocer nuestra ignorancia. Nos tenemos que poner la mano en el corazón y reconocer que por ignorantes no identificamos, no vemos, criticamos, minimizamos, comparamos cuando éramos chicos y no somos capaces de informarnos, reconocer y aprender, y por culpa de esto estamos perdiendo niños, niñas y jóvenes, y cortando relaciones importantes, ya que les demostramos que no pueden contar con nosotros”.

Es por esto, que los creadores de la fundación recomiendan a los padres y madres acercarse a sus hijos e hijas, generando espacios de conversación con ellos, con confianza y sin prohibiciones, de manera que les permitan conocer sus gustos e intereses y saber cómo se de sarrollan en este nuevo ambiente tecnológico.

KATY SUMMER
Fundación

RECOMEN**DACIONES**
Para Jovenes

Por su parte, para los jóvenes el consejo más importante es denunciar. “Si no se atreven a hacerlo con los padres o en su centro educacional, al menos deben recurrir a una fundación como nosotros o a entidades que les permitan hablar sobre lo que les está pasando. No están solos ni solas, hay quienes estamos disponibles para guiarlos y conversar. Lo mejor es buscar ayuda, nunca quedarse callados, ignorar lo que está pasando o desconectarse de las redes sociales, debido a que todo trae consecuencias y es importante abordarlo de manera integral y correcta”.

La Fundación Katy Summer cuenta con instancias de conversación y contención para quienes lo necesiten. Para ello, puedes escribir al correo **redes@fsummer.org** o informarte más en su sitio **web fsummer.org**
También los puedes seguir en Instagram: **fsummercl**

Legal

CIBERBULLYING

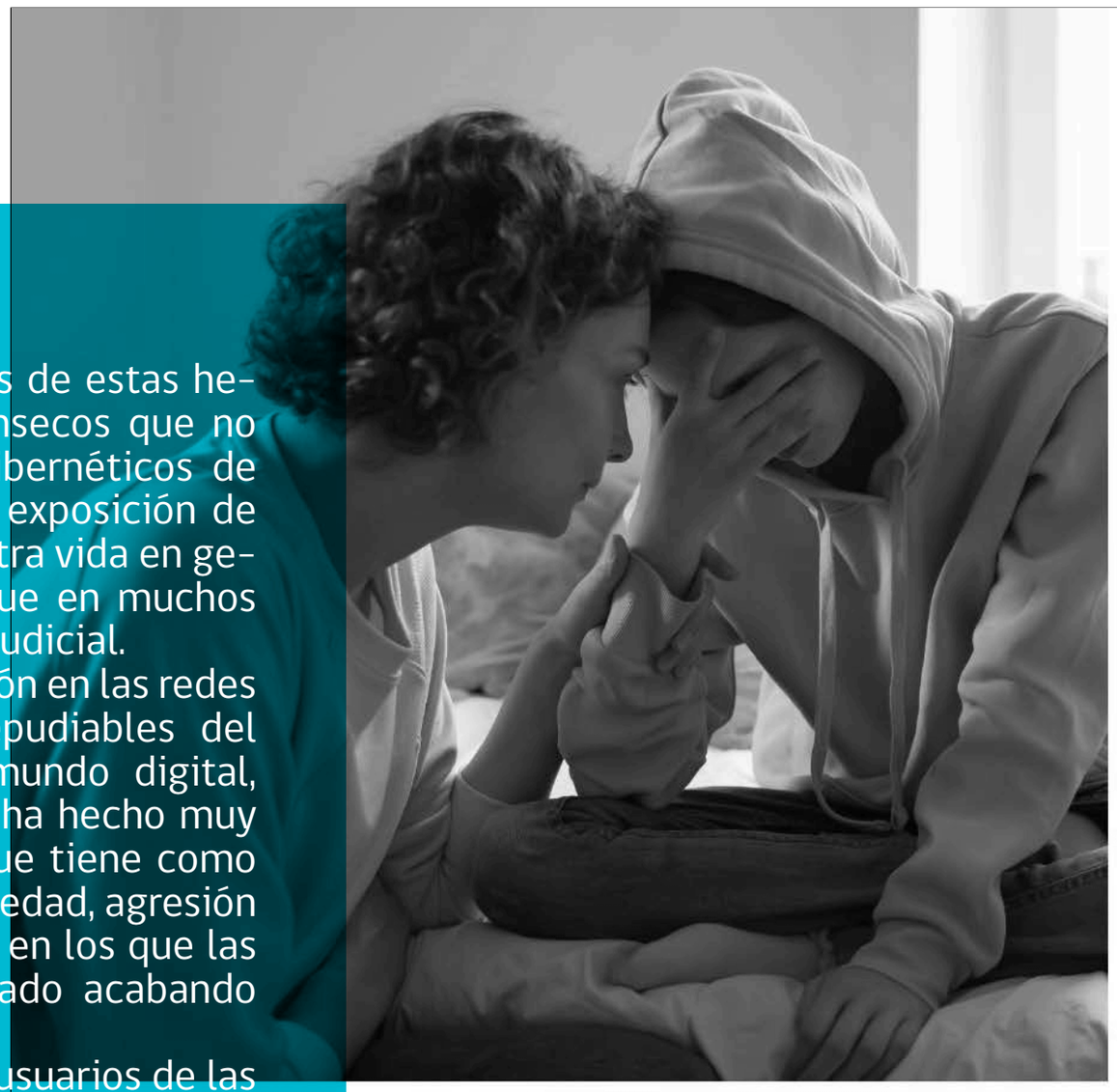
ACOSO A TODA HORA Y EN TODO LUGAR

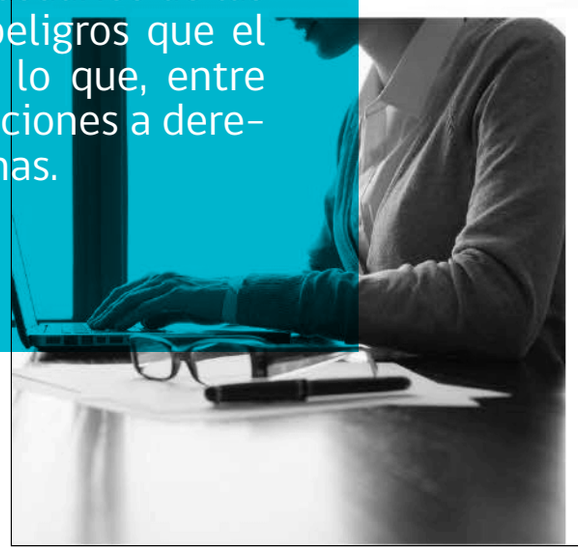
Con la creación del internet y las nuevas capacidades para procesar datos, hemos estado viviendo durante las últimas décadas una revolución constante en el surgimiento de nuevos dispositivos electrónicos y servicios, los que haciendo uso del internet, han cambiado para siempre la forma en que nos comunicamos e interactuamos con los demás. Aplicaciones tales como WhatsApp, Facebook, Tik Tok, Tinder y Snapchat han abierto la posibilidad de acabar con las barreras de la distancia, permitiéndonos estar más cerca en todo momento de aquellos que físicamente están más lejos.

A pesar de las ventajas evidentes de estas herramientas, existen riesgos intrínsecos que no podemos desconocer. Riesgos cibernéticos de diversa índole, como una mayor exposición de nuestros datos personales y nuestra vida en general en espacios digitales, lo que en muchos casos puede llegar a ser muy perjudicial.

Esta exposición y mayor interacción en las redes ha generado que conductas repudiables del mundo físico se trasladen al mundo digital, como el Ciberbullying, el que se ha hecho muy común en las redes sociales y que tiene como principales autores a menores de edad, agresión que ha llegado a casos extremos en los que las víctimas del mismo han terminado acabando con su vida.

Por esto, es fundamental que los usuarios de las redes sociales comprendan los peligros que el mal uso de éstas puede causar, lo que, entre otros, podría generar graves violaciones a derechos fundamentales de las personas.





¿QUÉ ES EL **CIBERBULLYING?**

Según el Centro de Investigación de la OEA, el ciberbullying es el "daño intencional y repetido infligido mediante el uso de computadoras, teléfonos celulares y otros dispositivos electrónicos". Por otro lado, la agencia Española de Protección de datos lo define como "una intimidación que tiene lugar a través de dispositivos digitales como teléfonos celulares, computadoras y tablets". De dichas definiciones se deprende que el ciberbullying considera todas las comunicaciones realizadas a través de internet, ya sea mediante mensajería instantánea, posts, correo electrónico o juegos en línea.

Así el ciberbullying no es más que una forma no convencional del bullying o acoso, en que por el medio en que se realiza, la posibilidad del anonimato y de ser efectuarlo en cualquier momento y lugar, es en general mucho más agresiva que su formato original.

REGULACIÓN DEL **CIBERBULLYING EN CHILE**

En Chile no existe una regulación expresa que sancione el ciberbullying como tampoco una definición. En ese sentido, la única ley que constituye un avance sobre la materia es la Ley N° 20.536 de Violencia Escolar del año 2011, la que introdujo una definición de convivencia escolar y de acoso escolar. Destacando que esta ley, al definir acoso escolar también consideró que la agresión u hostigamiento efectuado por medios tecnológicos podía ser constitutivo de un acoso escolar. Sin embargo, no definió expresamente acoso cibernético o ciberbullying. Por otro lado, las sanciones contempladas en dicha ley para quien realice el acoso o ciberbullying son eminentemente disciplinarias y deben ser aplicadas por el establecimiento educacional, las que podrían incluir desde una medida pedagógica hasta la cancelación de la matrícula en los casos de mayor gravedad. Finalmente, y solo en caso de que las autoridades del establecimiento educacional no apliquen las medidas correctivas o disciplinarias que su reglamento defina para estos casos, pueden llegar a ser sancionadas con multas de hasta 50 UTM.

Desde el año de entrada en vigencia de la referida ley, tanto las víctimas del bullying y sobre todo del ciberbullying han aumentado considerablemente en nuestro país, es por ello que al día de hoy existen dos proyectos de ley en tramitación en el congreso y que tienen por objeto, entre otros, modificar el decreto con fuerza de Ley N° 2 de 2010 a fin de que se incluya una definición de ciberbullying, aumentar la pena aplicable al establecimiento educacional aumentándolas de 50 a 200 UTM, como también ampliar la legitimación activa de quienes pueden iniciar acciones civiles o penales en contra de los responsables de las conductas que atenten gravemente la buena convivencia escolar.

HERRAMIENTAS JURÍDICAS **CONTRA EL CIBERBULLYING**

Junto a la respectiva denuncia ante la institución educacional que corresponda para que ella adopte las medidas disciplinarias a las que hace referencia la Ley 20.536, existe una variedad de recursos legales para hacer frente a este tipo de situaciones, los cuales también aplican para los casos de bullying.

ACCIÓN CONSTITUCIONAL DE PROTECCIÓN:

Una de las primeras medidas a adoptar, podría ser la interposición de una medida legal de protección fundada en el artículo N°1 de la Constitución incisos primero, segundo y cuarto en razón de que los niños y adolescentes deben estar resguardados y se les debe garantizar que puedan ejercer sus derechos, así como desplegar libremente su personalidad, sin ser víctimas de violencia, discriminaciones u otros actos que nieguen o desprecien su dignidad. En ese sentido también el artículo N°19 numerales 1° que consagra "El derecho a la vida y a la integridad física y psíquica de la persona", 2° "La igualdad ante la ley", 9° "El derecho a la protección de la salud", 10° "El derecho a la educación".

Es por ello que, respecto a algunos de estos derechos constitucionales, en caso de que sean vulnerados, el afectado o un tercero a su nombre, como sus padres o el propio establecimiento educacional, podrían interponer una acción de protección ante la Corte de Apelaciones respectiva, para por ejemplo evitar o poner término a la difusión de mensajes, posts, videos y fotografías humillantes en redes sociales.

MEDIDA DE PROTECCIÓN ANTE TRIBUNALES DE FAMILIA:

Esta es otra herramienta legal a la cual se puede recurrir para que los tribunales establezcan una medida de protección en favor del afectado. Pueden ser sujetos activos tanto el afectado, sus padres, el colegio o un tercero.

Ello en virtud de que los tribunales de familia son competentes para conocer todos los asuntos que tengan relación con niños, niñas o adolescentes gravemente vulnerados o amenazados en sus derechos de los cuales se requiera adoptar alguna medida de protección. Un aspecto que destacar es que el requerimiento presentado no necesita cumplir formalidad alguna, bastando con la sola petición de protección para dar por iniciado el procedimiento.

DENUNCIA O QUERELLA ANTE AUTORIDADES COMPETENTES:

Hay casos de ciberbullying que son constitutivos de delito, los que deben ser denunciados ya sea al Ministerio Público, a las policías o tribunales con competencia penal. En este sentido, es de suma relevancia tener a la vista lo dispuesto en el artículo 175 del Código Procesal Penal que dispone que los directores, inspectores y profesores de establecimientos educacionales están obligados a denunciar los delitos que afectaren a los alumnos o que sucedan en el establecimiento, denuncia que deben efectuar dentro de 24 horas desde el momento que tomaron conocimiento del hecho.

También se debe tener en consideración lo establecido en la ley de responsabilidad penal adolescente que señala que "se aplicará a quienes al momento en que se hubiere dado principio de ejecución del delito sean mayores de catorce y menores de dieciocho años, los que, para los efectos de esta ley, se consideran adolescentes".

En consecuencia, los menores que se encuentren dentro de ese rango de edad son responsables ante la ley penal por los hechos que cometan, como podrían serlo las injurias proferidas respecto de otra persona.

ACCIONES CIVILES POR PERJUICIOS:

En términos generales cuando una persona causa un daño a otra, surge entre ellas una obligación en que la víctima pasa a ser acreedor y el causante del daño el deudor.

En este punto se debe distinguir entre la responsabilidad contractual y extracontractual.
La responsabilidad contractual se origina por el incumplimiento doloso o culposo de una obligación contraída mediante un contrato, la que acarrea perjuicios. Esto supone, por lo tanto, la existencia de un vínculo jurídico previo de carácter contractual entre las partes.

Es en ese sentido, en virtud del contrato de prestación de servicios educacionales que existe entre el alumno y la institución de enseñanza, y que impone a esta última un deber de vigilancia sobre la conducta de los estudiantes y una obligación de proteger a los mismos, la institución podría ser obligada a indemnizar los perjuicios derivados de bullying o ciberbullying por el incumplimiento de la obligación contractual de cuidado.

Por otro lado, y sin perjuicio de lo anterior, también podría existir responsabilidad extracontractual, entendiendo por tal aquella en que no existe un contrato ni un vínculo jurídico entre el autor del daño y la víctima. En este caso y, a diferencia de la responsabilidad contractual en que se incumple dolosa o culpablemente una obligación derivada de un contrato, aquí el daño proviene de la comisión de un delito o cuasidelito civil, esto es, de un hecho ilícito cometido con intensión de dañar que causa daño o de un hecho ilícito culpable, cometido sin intención de dañar que causa daño.

En nuestro ordenamiento jurídico existen varias disposiciones que hacen responsables extracontractualmente a los padres por los daños que han cometido sus hijos. Esto se conoce como responsabilidad por hecho ajeno y una de sus máximas expresiones se encuentra consagrada en los artículos 2320 y 2321 del Código Civil.

Así, por ejemplo, la víctima del ciberbullying podría dirigirse en contra de los padres del agresor, para obtener indemnizaciones por perjuicios, Ejemplo:
como los gastos en tratamientos psicológicos.
Como se puede ver, en Chile aún queda mucho camino por recorrer para hacer frente al ciberbullying tanto desde el punto de vista legislativo como el relativo a campañas de concientización y de educación que generen un impacto positivo en la sociedad y en la convivencia de nuestros niños.

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

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

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS

+(562) 2486 3850

registra un incidente

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl