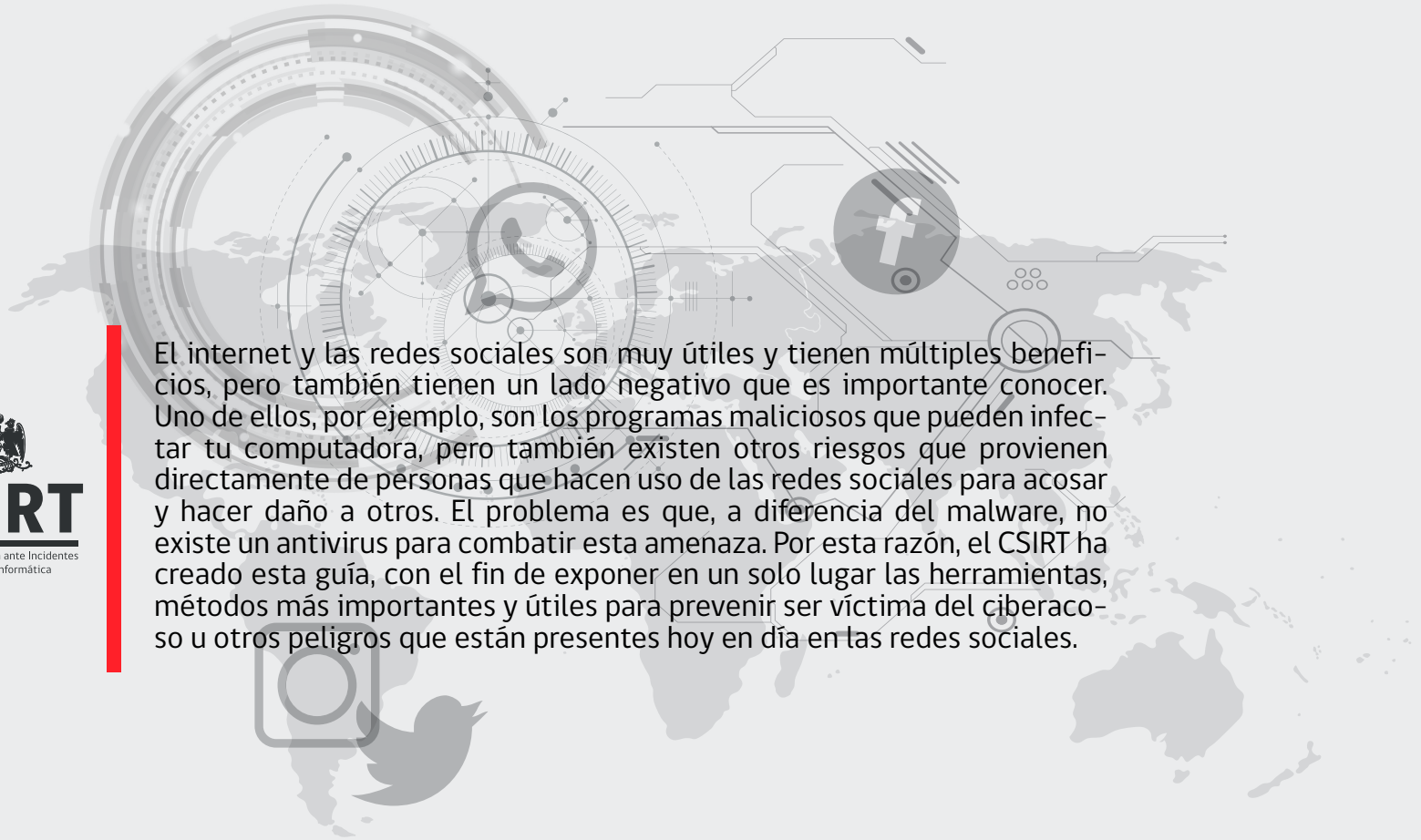
CSIRT
Equipo de Respuesta ante Incidentes
de Seguridad Informática

MEDIDAS PREVENTIVAS A CONDUCTAS ABUSIVAS EN RRSS.



CSIRT
Equipo de Respuesta ante Incidentes
de Seguridad Informática

El internet y las redes sociales son muy útiles y tienen múltiples beneficios, pero también tienen un lado negativo que es importante conocer. Uno de ellos, por ejemplo, son los programas maliciosos que pueden infectar tu computadora, pero también existen otros riesgos que provienen directamente de personas que hacen uso de las redes sociales para acosar y hacer daño a otros. El problema es que, a diferencia del malware, no existe un antivirus para combatir esta amenaza. Por esta razón, el CSIRT ha creado esta guía, con el fin de exponer en un solo lugar las herramientas, métodos más importantes y útiles para prevenir ser víctima del ciberacoso u otros peligros que están presentes hoy en día en las redes sociales.

a. Configuración de privacidad en **RRSS**

La primera medida preventiva ante conductas abusivas es tener una adecuada configuración de privacidad en cada una de las redes sociales en las que tienes un perfil, con el objetivo de proteger tu información. Algunas de las medidas básicas que debes tener en consideración en las redes sociales para tener una mejor privacidad en tus cuentas son:

Facebook:

1. Configura tu cuenta como privada.
2. Utiliza una contraseña de al menos 10 caracteres que contenga letras mayúsculas y minúsculas, número y algún símbolo.
3. Si quieres aún mayor seguridad, activa desde tu cuenta la verificación de dos pasos. Si roban tu contraseña para ingresar se les solicitará una segunda clave configurada por ti.
4. Evita proporcionar información personal en la red social o, en caso de hacerlo, mantenla oculta para que tus amigos o contactos no accedan a ella. Algunos de los datos que no debes entregar son:

   a.– Número telefónico
   b.– Correo electrónico
   c.– La comuna o dirección donde vives
   d.– Lugar de estudios
   e.– Orientación sexual

5. No enlaces tu cuenta con la de tus familiares ni tampoco des a conocer ningún tipo de vínculo familiar.
6. Configura desde tu cuenta una alerta por si alguien intenta conectarse a ella desde un dispositivo no reconocido.
7. Configura tu cuenta para que, si alguien postea o publica algo sobre ti, te llegue una notificación para que apruebes si quieres que ese posteo se publique.
8. No aceptes a desconocidos por ninguna razón. Ojo que en las redes no todos son quienes dicen ser.
9. No entregues información que normalmente no entregarías a un desconocido.
10. Revisa si te encuentras compartiendo tu ubicación en Facebook, para esto confirma si se encuentra activada la función "Amigos cerca" en tu app de Facebook y en tu celular, más detalles en el siguiente enlace https://es-la.facebook.com/help/337244676357509. Para desactivar los servicios de ubicación de las RRSS revisa el siguiente enlace https://es-la.facebook.com/help/275925085769221?helpref=faq_content

WhatsApp:

1. No incluyas información personal en tu estado.
2. Cambia los ajustes para que nadie o solo tus contactos puedan ver tu última hora de conexión.
3. Configura los ajustes para que nadie o solo tus contactos puedan ver tu estado.
4. Cambia tu configuración para que nadie o solo tus contactos puedan ver tu foto de perfil.
5. Desactiva las confirmaciones de lectura.

Instagram:

1. Configurar la cuenta de Instagram como privada.
2. Utiliza una contraseña de al menos 10 caracteres que contenga letras mayúsculas y minúsculas, números y algún símbolo.
3. Si quieres aún mayor seguridad, activa desde tu cuenta la verificación de dos pasos. Si roban tu contraseña para ingresar se les solicitará una segunda clave configurada por ti.
4. Nunca publiques:

   a.– Número telefónico
   b.– Correo electrónico
   c.– La comuna o dirección donde vives
   d.– Lugares que sueles frecuentar
   e.– Lugar de estudios
   f.– Orientación sexual

5. Configura filtros en comentarios que podrían ser ofensivos.
6. Revisa si estás compartiendo tu ubicación con Instagram, puedes desactivar los servicios de ubicación desde Android o IPhone para las RRSS, el paso a paso en el siguiente enlace https://es-la.facebook.com/help/instagram/171821142968851?helpref=related

Twitter:

1. Piensa en un nombre de usuario que no sea tu nombre completo (nombre y apellido) o incluso puedes utilizar uno que no sea real.
2. Utiliza una contraseña de al menos 10 caracteres que contenga letras mayúsculas y minúsculas, número y algún símbolo.
3. Si quieres aún mayor seguridad, activa desde tu cuenta la verificación de dos pasos. Si roban tu contraseña para ingresar se les solicitará una segunda clave configurada por ti.
4. Haz que tus tweets sean privados en la configuración de twitter para que solo quienes te sigan puedan verlos. Para ello dirígete a la sección: Privacidad y seguridad - Audiencia y etiquetas.
5. En la misma sección anterior puedes evitar que otras personas te etiqueten en sus fotos, solo tú podrás etiquetarte.
6. Decide quién puede encontrarte desactivando la opción de que quienes tengan tú correo o tú teléfono puedan hacerlo.
7. Solo permite que te puedan enviar mensajes directos tus contactos en la configuración de mensajes directos.
8. En la misma sección, desactiva las confirmaciones de lectura en los mensajes privados.
9. Revisa que aplicaciones tienen acceso a tú cuenta y desvincula aquellas que ya no necesites o aquellas que tengan permisos excesivos en la sección de "Aplicaciones y sesiones".

Para obtener más información sobre cómo configurar tu cuenta como privada, cada red social cuenta con un espacio para explicar los pasos:
Para esto, puedes visitar:

Facebook: https://www.facebook.com/help/325807937506242
WhatsApp: https://faq.whatsapp.com/general/security-and-privacy/staying-safe-on-whatsapp
Instagram: https://help.instagram.com/196883487377501/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Managing%20Your%20Account
Twitter: https://help.twitter.com/es/safety-and-security#ads-and-data-privacy

b.

Denuncia y bloquea. Aquí te enseñamos como:

Una segunda medida que te permitirá estar más seguro en redes sociales ante conductas abusivas como el ciberbullying es denunciar aquellas cuentas desde donde provienen las agresiones. Pueden ser perfiles de personas conocidas o casos de suplantación de identidad. En ambas situaciones, el CSIRT recomienda denunciar y bloquear dichas cuentas.

1. Si no sabes cómo hacerlo, puedes acceder al "Procedimiento para denunciar suplantación de identidad en redes sociales" que el CSIRT pone a tu disposición en el siguiente enlace: https://www.csirt.gob.cl/recomendaciones/procedimito-pra-dnunciar-suplantacion-de-identidad-en-redes-sociales/

2. También ponemos a tú disposición la guía paso a paso para "denunciar el abuso digital" ya sea ante la propia red social o ante las autoridades de justicia en el siguiente enlace: https://www.csirt.gob.cl/recomendaciones/ciberguia-acoso-digital/

Las redes sociales también disponen de sitios con consejos y apoyo en casos de bullying. Para más información puedes visitar:

Bullying Facebook: https://es-la.facebook.com/safety/bullying
Bullying WhatsApp: https://faq.whatsapp.com/general/security-and-privacy/staying-safe-on-whatsapp
Bullying Instagram: https://about.instagram.com/es-la/community/anti-bullying
Bullying Twitter: https://help.twitter.com/es/safety-and-security/cyber-bullying-and-online-abuse
Bullying Steam: https://support.steampowered.com/kb_article.php?ref=7597-KZNM-3716

C.

La importancia de tu correo electrónico

En general, todas las redes sociales piden un correo electrónico para poder crear una cuenta, por lo que nuestro correo electrónico es prácticamente nuestra llave a todas ellas, y por eso es utilizado por acosadores, suplantadores de identidad y otras personas para tomar el control de tus redes sociales y así causarte daño o extorsionarte.

A través del correo electrónico puedes:

1. Recibir notificaciones de los cambios en las políticas de uso y privacidad.
2. Recuperar y reestablecer contraseñas.

Recomendaciones:

a.– Utiliza siempre claves seguras y robustas:

- Que tu clave tenga al menos una extensión de 10 caracteres.
- Utilizar letras mayúsculas y minúsculas, números y caracteres especiales (puntos y símbolos).
- Para que sea más fácil recordarlas, utiliza frases de una canción, cita, película o pasaje de un libro.
- Utiliza secuencias de palabras inconexas (con reglas de mayúscula/minúscula incluida).
- Utiliza tres palabras bajo la secuencia "persona", "acción" y "objeto" (con reglas de mayúscula y minúscula incluida).

b.– Configura el doble factor de autenticación, si roban tu contraseña para ingresar se les solicitará una segunda clave configurada por ti.

c.– Registra tus cuentas de correo electrónico en un sitio que notifique filtración de datos para cambiar la o las contraseñas de las cuentas vulneradas oportunamente.

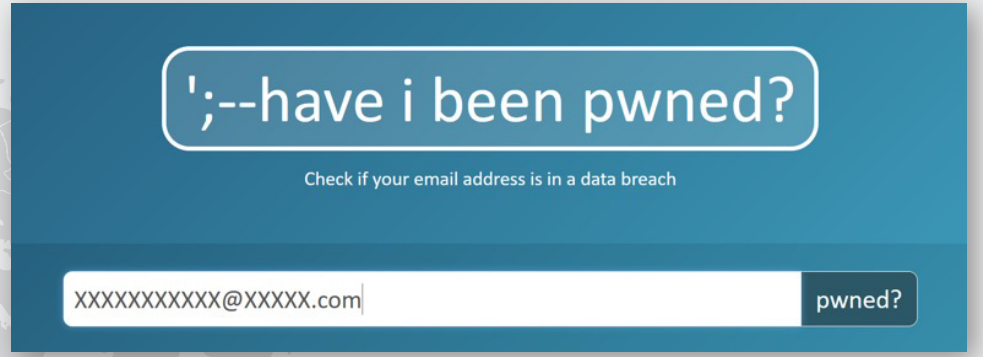
d.

Herramientas para saber si tu información fue expuesta en una filtración de datos

Existen ciertas plataformas que permiten tener una mayor noción y control sobre la información que de nosotros circula en internet, así como también si alguna de nuestras cuentas fue vulnerada.

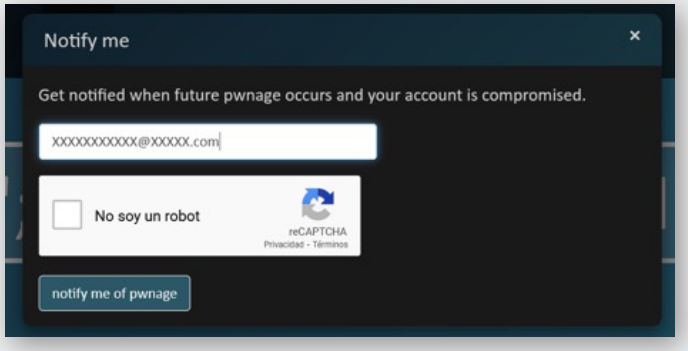
1 Haveibeenpwned: https://haveibeenpwned.com/

Aquí puedes ingresar las cuentas de correo electrónico que quieras revisar y verificar si alguna cuenta o aplicación relacionada fue vulnerada.



Si tu dirección de correo electrónico aparece en alguna filtración de datos conocida, te recomendamos cambiar la contraseña tanto del correo como de las cuentas a las que esté asociado.

Para enterarte automáticamente de las filtraciones de datos en que tu cuenta de correo podría estar comprometida así como de servicios relacionados, puedes registrar tu cuenta y solicitar recibir una notificación cada vez que se detecte una filtración en esa misma página web.



❷ **Firefox monitor**:

Incluye consejos sobre qué hacer en caso de ser víctima de una filtración. Para revisar tu cuenta y recibir notificaciones de filtraciones de datos accede a https://monitor.firefox.com/ y sigue los pasos.

Estas herramientas permiten tener una mayor noción y control sobre nuestra información personal que puede haber sido expuesta, la que entre otras cosas podría utilizarse para causarnos algún tipo de daño.

e.

Herramienta para saber qué sabe internet de ti

¿Cómo puedes hacer frente a situaciones que no conoces? Es imposible, es por ello que para evitar ser víctima de conductas como el bullying o situaciones como el ciberacoso y otras, es importante saber qué información existe sobre nosotros en internet y cómo podría ser utilizada para perjudicarnos. Con esto, puedes adoptar las medidas que sean necesarias para sacar de circulación o limitar el acceso a información que podría ser comprometedora, así como enterarte de quienes están hablando o publicando cosas sobre ti.

❶ Google dorks:

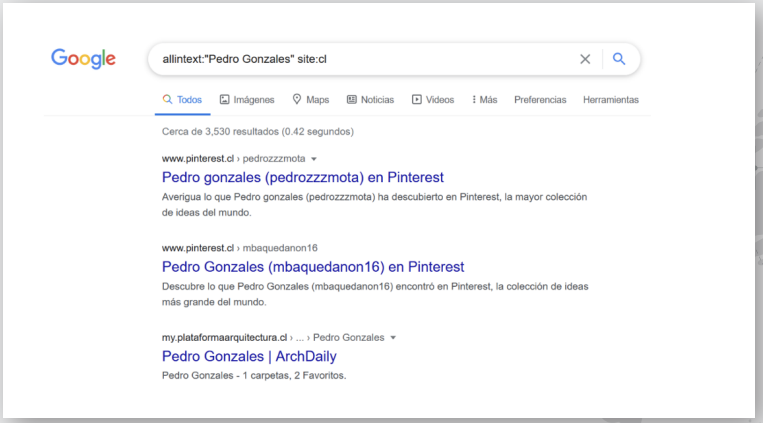
Permite, de una manera fácil y rápida, hacer un levantamiento de lo que internet sabe de nosotros, mediante ciertos comandos de palabras que buscan en Google información muy específica sobre algo o alguien en particular.
Estos comandos son:

- **intext =** te permite buscar ciertas palabras en el contenido de un sitio.
- **allintext =** busca todas las palabras mencionadas en el contenido del sitio.
- **site =** permite filtrar las búsquedas en sitios cl, com, org, o hasta en páginas como por ejemplo facebook.com, gob.cl.
- **filetype =** permite elegir qué tipo de archivo buscar (pdf, xlsx, docx).

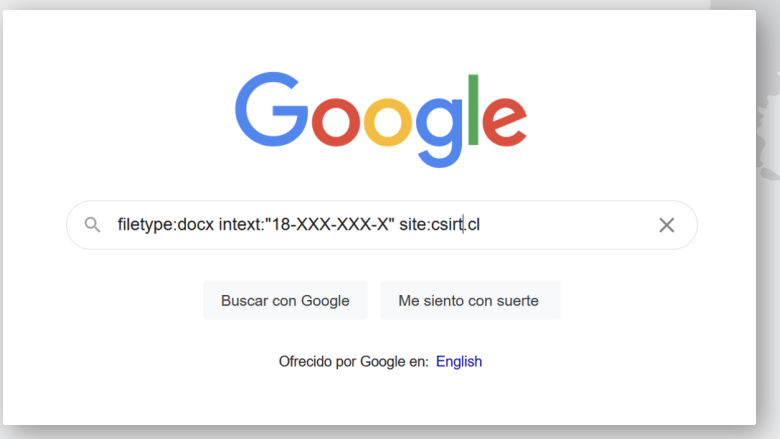
Aquí tienes un ejemplo de cómo funciona:

Para buscar información sobre "Pedro Gonzales" en sitios chilenos, nos dirigimos a Google y escribimos lo siguiente:

A continuación, se desplegará en el buscador toda la información existente en sitios chilenos sobre “Pedro Gonzales”:



Por otro lado, si quieres saber si tu Rut está disponible en archivos Word en una página específica, la operación sería la siguiente:



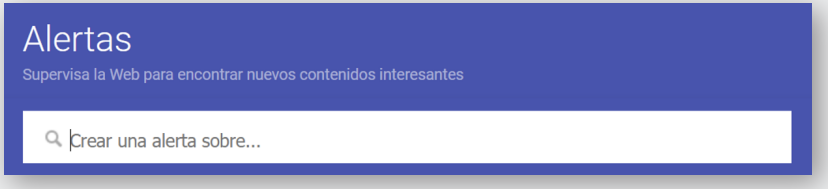
f.

Herramientas para enterarte en tiempo real si están hablando sobre ti

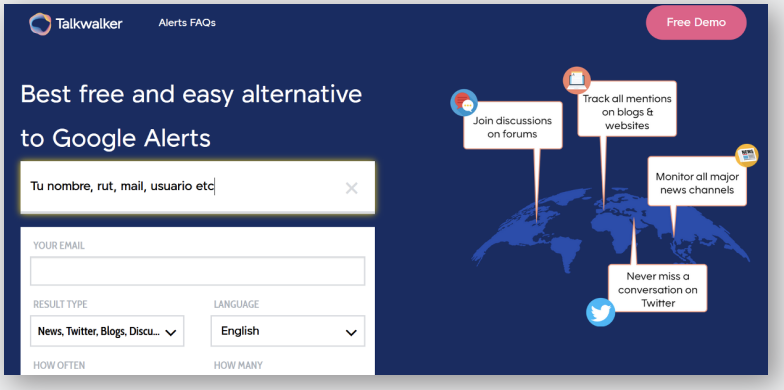
Para esto, existe un sistema muy parecido a Google dorks pero que puedes programar para que siga todas tus menciones en internet o de toda la información que sea relevante. En este caso puedes programar la plataforma para que solo te alerte si sale la información sobre tu persona.

La idea es crear alertas con datos personales, datos que sean únicos para identificarte a ti, como tu rut, nombre, correos electrónicos, nombres de usuario que utilices en otras plataformas, Etc., para que estas herramientas te notifiquen si hablaron o están compartiendo información sobre ti.
Dos excelentes plataformas para hacer esto son:

1. **Google alerts:** Accede con tu cuenta Google en el siguiente link: https://www.google.com/alerts y añade todas las alertas que quieras recibir desde el recuadro que se muestra en la imagen.
   Para más información de cómo crear alertas, accede a: https://support.google.com/websearch/answer/4815696?hl=en



2. **Talkwalker:** Ingresa al siguiente link https://www.talkwalker.com/alerts y agrega todas las alertas que quieras recibir desde el recuadro que se muestra en la imagen y agrega tu correo electrónico.



8.

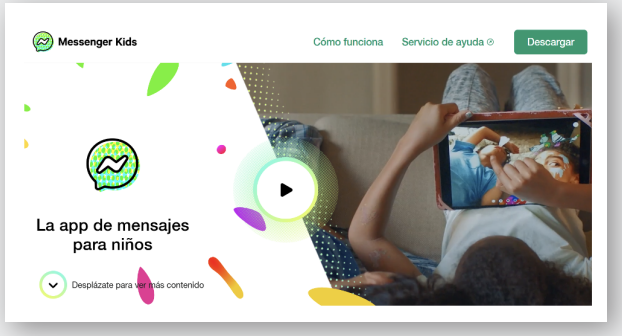
Herramientas para proteger a los más pequeños de conductas abusivas en apps de mensajería

Un grupo muy importante que debemos cuidar y proteger en Internet y en las redes sociales son los niños, navegar por internet e ingresar a las distintas apps puede ser muy atractivo para ellos, sin importar su edad. Pero es importante que los padres conozcan qué hacen los menores o con quiénes conversan, de manera que tengan una vida virtual saludable.

Es por ello que se han diseñado herramientas de control parental, las cuales permiten tener un registro de las actividades que realizan los menores en los dispositivos móviles o plataformas de streaming. Sirve de apoyo para los padres, pero no reemplaza el hecho de que los adultos deban acompañar a los menores. Algunas de éstas son:

1. **Safetonet:** Es una de las mejores herramientas que existen para saber si tu hijo es víctima de conductas abusivas en internet y en su interacción con los demás sin invadir su privacidad. Mediante el uso de inteligencia artificial notifica a los padres en caso de que su hijo esté siendo hostigador u hostigado a través de internet. La aplicación aún no está disponible en español.

2. **Messenger kids:** Es la versión de Facebook Messenger especialmente creada para niños. La gracia de esta app es que los padres pueden controlar la lista de contactos de sus hijos, el tiempo que la pueden utilizar, ver las conversaciones, entre otros. Una ventaja importante que la diferencia de otras aplicaciones es que permite comunicación con Facebook Messenger en su versión estándar, pero solo con contactos aprobados, por lo que no obliga a los cercanos a tener que hacer uso de una app a la cual no están acostumbrados para poder comunicarse con los más pequeños. Puedes descargarla en el siguiente link: https://messengerkids.com/



3. **Family Link:** Es una App, que permite establecer normas básicas para guiar a niños y adolescentes mientras aprenden, juegan y descubren cosas online con sus dispositivos digitales.

4. **Kaspersky Safe Kids:** Es una Apps que permite bloquear el acceso a sitios web inapropiados, controlar el tiempo que los niños pasan frente a la pantalla, localizar y monitorear la batería de los dispositivos.

5. **McAfee Safe Family:** Es una App que ofrece protección al bloquear ciertos sitios web y aplicaciones, administrar el tiempo frente a la pantalla e incluso rastrear la ubicación de los más pequeños.

6. **Surfie:** Es una App que ofrece protección contra posibles peligros de Facebook, la Mensajería Instantánea y los programas de chat, con especial atención en las amenazas de ciberbullying y la evasión de protección.

Si quieres saber más sobre la mediación parental, te invitamos a revisar "la guía de mediación parental del CSIRT", en la cual se entregan una serie de consejos para lograr que los menores hagan un uso seguro y responsable de internet.

Guía completa disponible en el siguiente enlace:

https://www.csirt.gob.cl/recomendaciones/ciberguia-de-mediacion-parental/

MEDIDAS PREVENTIVAS A CONDUCTAS ABUSIVAS EN RRSS.

Director: Carlos Landeros Cartes

Jefa de contenidos y edición: Katherina Canales Madrid

Colaboradores equipo CSIRT: Cristobal Hammersley

Diseño y diagramación: Jaime Millán

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

Teatinos 92 piso 6
Santiago, Chile