Buenas prácticas para uso adecuado de servicios de Internet

CIRION TECHNOLOGIES ECUADOR S.A. al ser un proveedor de Servicios de Valor Agregado de Internet, a continuación emite recomendaciones para usuarios a manera de guía para un uso adecuado y beneficioso del servicio de Internet.

Así, las recomendaciones que se manifiestan son las siguientes:

Sobre su cuenta de Internet:

- El usuario principal del servicio de Internet que paga y administra el contrato del servicio en mención debe procurar un manejo adecuado de los usuarios (hijos, conyugue, usuarios empresariales, etc.) mediante controles parentales o políticas de seguridad para el acceso a estos servicios.
- El usuario que haga uso del servicio de Internet puede efectuar pruebas de capacidad contratada conectando su computadora directo al dispositivo de red del proveedor sin equipos intermedios y hacer pruebas de envío y recepción de información.

Uso de claves:

- El uso de claves para servicios de Internet debe manejarse de manera secreta. No se la debe mencionar ni escribir para evitar divulgación de dicha información, y a su vez evitar correos que solicitan información sensible (número de tarjeta o número de cuentas, etc.) ya que pueden ser correos falsos que utilizan tácticas de ingeniería social para obtener información y realizar fraudes.
- La clave del usuarios (password) debe de ser conocido solo por el usuario que es dueño de la cuenta de correo, que incluyan mínimo 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales, esto es por su seguridad.
- Se recomienda cambiar la clave periódicamente, de preferencia cada 3 meses.

Sobre el uso del correo electrónico:

- Evite renviar correos masivos, los cuales son diseñados para generar SPAM lo cual congestiona la red de internet, además que es una forma para obtener direcciones de correos, que luego son utilizadas para enviar propaganda publicitaria que no se ha solicitado. Si considera conveniente renviar un correo masivo, sugerimos primero verificar la fuente o validar si dicho correo no es un engaño (Hoax), para lo cual puede consultar en su buscador de internet la palabra HOAX y parte del texto recibido en el correo con lo cual se enterará si dicho correo ha sido generado para engañar al público.
- No responder ningún correo por confiable que este parezca ante la solicitud de su clave. Las empresas que tienen un manejo responsable de la información, no solicita las claves por correo.
- Es conveniente usar de forma adecuada la dirección de correo electrónico evitando informar o publicar la dirección y clave en páginas web, dado que esto se presta para la copia de listas de correo electrónico para distribución de propaganda y correo no deseado (SPAM).
- En el caso de que se publique información en Internet, tenga cuidado de que estas publicaciones no tengan efectos ilícitos o dolosos. Esto a fin de preservar una adecuada conducta con la información publicada.

Sobre las redes sociales:

- Cuando acceda a una sesión de chat (chat room), nunca se deben de escribir número de tarjetas de crédito, contraseñas o información personal que pueda ser utilizada por terceros para hacer mal uso de ella.
- Tener siempre la certeza de a quien se acepta como supuesto amigo o contacto en las conocidas redes sociales. Se recuerda que estos contactos pueden tener puerta abierta a que conozcan toda la información que se publica en el portal personal, incluidas fotos familiares, amigos, información personal, actividades diarias, entre otros.
- Se recomienda que la publicación de información personal sea la mínima posible y el manejo de la privacidad sea configurado para que su información no esté abierta o se preste para el uso doloso o nocivo.
- La pérdida de la privacidad se produce cuando se proporciona, a través de Internet, información sobre la vida personal del usuario, o imagen personal, esto para poder entrar en determinados espacios comunes o para la utilización "gratuita" de servicios. Muchas páginas solicitan datos personales para un uso fraudulento de los mismos. Para evitar esto, se recomienda no usar siempre el mismo nombre de usuario y contraseña en todos los servicios que utilice (si se desea conservar una misma contraseña, se le puede ir agregando algún número a la misma para que sea distinta según distintos servicios que se usen en Internet). No proporcionar, por principio, datos personales como nombre, dirección, número de cédula, número de teléfono o fotografías/vídeos suyas o de su familia.

El Internet y el entorno familiar:

- En el caso de entornos familiares. Los padres de familia deben animar a sus hijos a dialogar sobre los contenidos desplegados en Internet y sobretodo acerca del contenido que sea desagradable para el uso de Internet. Procure mantener momentos adecuados para la reflexión de la información publicada en Internet y de los efectos que esta puede causar si no se tiene la precaución y cuidado del caso.
- Se recomienda a los padres de familia aprender sobre computación y sobre conceptos de web tales como los "wikis", los blogs, las redes sociales, los podcast, con la finalidad de conocer el mundo cibernético en el que están sus hijos y ser sus guías y orientadores.
- Para los padres de familia, se recomienda que tengan esquemas de control parental básico para que hijos y usuarios de la red del hogar eviten el acceso a páginas de contenido nocivo o falso. Así también, para el uso de sistemas de conversación (chats), se recomienda que los padres de familia tengan conocimiento de dichos sistemas y orienten a sus hijos respecto del uso y riesgos que existen.

El Internet y el entorno empresarial:

- En entornos empresariales, las políticas de uso de Internet se deben normar a fin de que la información que el usuario final tenga prevención en el uso de Internet y se establezca una política de cambio periódico de claves.
- Nunca deje el computador prendido con sesiones activas de banco o de compras en Internet. Para esto procure usar protectores de pantalla con clave.

Otros temas generales:

- Para el uso de compras por Internet, tener la prevención de que la publicidad colocada en dichas páginas no siempre tiene resultados beneficiosos ni necesarios para el usuario que accede a dicho contenido. Por otra parte, procure manejar sistemas de pago seguro y tenga sus tarjetas de crédito debidamente controladas. Consulte con su entidad de servicios bancarios para el uso adecuado y recomendaciones de seguridad de la tarjeta de crédito para compras en Internet.
- El “PISHING” es un método para el intento de adquirir fraudulentamente información de una persona, como la identidad y código secreto de una tarjeta electrónica o del acceso a los datos bancarios. Actúa a través de la recepción de un correo electrónico en el que en nombre de una entidad bancaria, se pide al usuario esta información. El mensaje suele imitar con mucha exactitud la imagen y textos habituales de la entidad bancaria o comercial. Para evitar caer en este tipo de fraudes, haga caso omiso de dichos correos y NO proporcione nunca información sobre su cuenta bancaria, su identidad o el código de acceso. Informe a su entidad bancaria o comercial de la recepción de cualquier correo sospechoso.
- En el caso de servicios de Telefonía IP por Internet, se debe leer las condiciones de servicio que se prestan por dicho servicio. A su vez, tener la precaución de usar usuarios con claves seguras y sistemas de control para evitar los fraudes de tipo telefónico.

RECOMENDACIONES PARA CONFIGURACIÓN DEL CONTROL PARENTAL

1. INTRODUCCIÓN

La Internet y las redes sociales se han convertido en herramientas que brindan oportunidades para el aprendizaje, desarrollo académico y socialización de la niñez y adolescencia; sin embargo, también presentan riesgos y amenazas a los que están expuestos los niños, niñas y adolescentes.

Hacer de la Internet un espacio seguro está en nuestras manos, acompañémosles mientras navegan en la red.

Para prevenir, es necesario conocer los riesgos, por ello a continuación se explica algunos de los peligros, por los que, los niños, niñas y adolescentes podrían ser víctimas de ataques cibernéticos:

Ciberacoso o Ciberbullying

Consiste en la publicación de textos, imágenes, videos y/o audios que son difundidos a través de medios electrónicos, como mensajería instantánea, redes sociales, juegos en línea, y son utilizadas para agredir y/o humillar a alguien.

Grooming

Es la acción deliberada en la cual, una persona adulta contacta a un niño, niña o adolescente, a través de medios electrónicos, con el objetivo de ganar su confianza y finalmente obtener video o fotos con carácter sexual.

Sexting

Se refiere al envío de fotografías y/o videos producidos por uno mismo con connotación sexual a otra(s) persona(s) a través de distintos servicios de mensajería, y usualmente son enviadas a través de dispositivos móviles. Dicho material puede derivar en su publicación, por ejemplo, en un sitio web, o ser viralizada sin el consentimiento de la persona. En algunos casos el atacante extorsiona a la víctima para obtener

más material de connotación sexual, derivándose en la práctica de Sextorsión.

A fin de proteger a los niños, niñas y adolescentes de los peligros cibernéticos antes descritos, sitios inseguros y contenidos inadecuados, a los cuales estén expuestos en internet, se pueden utilizar filtros y herramientas de control parental.

¿Qué es el Control Parental?

El control parental es una herramienta que busca monitorear, restringir o bloquear el acceso de niños, niñas y adolescentes a sitios web, cuyo contenido sea inapropiado o ponga en riesgo su integridad. También permite establecer un tiempo límite para el uso de dispositivos como computadoras, TV, smartphones, tablets, y cualquier otro equipo que tenga acceso a una red WiFi.

Por ejemplo, si estás en redes sociales como Facebook, Twitter o Instagram y se observa que alguna publicación no es apta para que un niño, niña o adolescente la vea, puedes reportarla y el contenido desaparecerá de la línea de tiempo.

Se recomienda el uso de control parental para niños, niñas y adolescentes entre 4 y 18 años, debido a que los niños comienzan su aprendizaje digital en la escuela y hogares a temprana edad, lo que implica una mayor exposición al internet conforme crecen, aumentando uso de dispositivos móviles o redes sociales.

2. ¿PARA QUE SIRVE EL CONTROL PARENTAL?

Entre los principales beneficios del control parental tenemos:

1. Evitar que los niños, niñas y adolescentes sean contactados o se comuniquen con personas desconocidas y prevenir casos de grooming, ciberacoso, sexting, sextorsión, entre otros.

2. Evitar el acceso de los niños, niñas y adolescentes a sitios web con contenido no adecuado, como, por ejemplo: sitios con contenido para personas adultas (pornografía), que fomenten la discriminación, la violencia o hábitos autodestructivos.

3. Limitar el tiempo de uso y horarios que los niños, niñas y adolescentes utilicen aplicaciones en sus dispositivos móviles y establecer horarios para su uso.

4. Controlar la descarga de las aplicaciones que quieran instalar los niños, niñas y adolescentes en sus dispositivos móviles.

5. Evitar que se realicen compras en línea no deseadas.

6. Activar la geolocalización de los dispositivos para que los padres y madres, puedan conocer, en tiempo real, la ubicación del niño, niña o adolecente.

7. Conexión remota al dispositivo electrónico de los niños, niñas y adolescentes por parte de los padres, madres o tutores, para conocer que están haciendo y ofrecer asistencia remota en la solución de eventos en su dispositivo.

3. TIPOS DE CONTROL PARENTAL

Existen varias herramientas para el control parental, depende del alcance y funciones que se quiera.

Las herramientas de control parental agrupan principalmente en dos grupos:

- **Herramientas de monitorización**: Llevan un registro de las páginas visitadas y tiempo de navegación, pero no prohíben ni filtran el acceso a páginas web con contenido inapropiado.

- **Filtros de contenidos**: Bloquean y restringen el acceso a páginas web cuya dirección contenga un determinado patrón o el propio contenido de la página web tenga determinadas palabras. También permiten bloquear el acceso a ciertos servicios de Internet como chats.

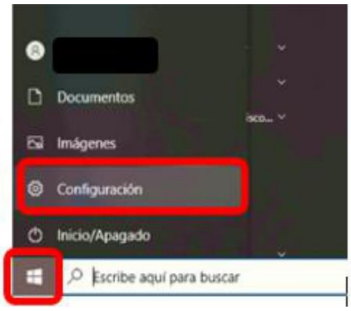
Existen varias herramientas y diferentes tipos de configuraciones para activar los controles parentales, en este documento se detallará los controles en Sistemas Windows y YouTube. A lo largo del año la Agencia de Regulación y Control de las Telecomunicaciones elaborará más guías con la configuración de controles parentales adicionales.

4. CONFIGURACIÓN DE CONTROLES PARENTALES

4.1 En sistemas Windows 10

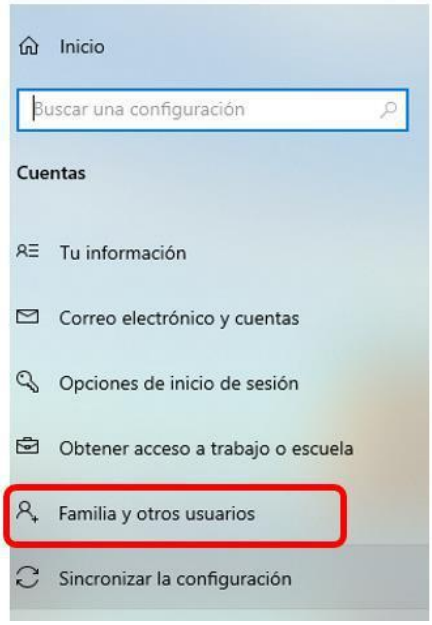
A continuación, explicaremos cómo configurar controles parentales en computadores con sistema operativo Windows 10:

a. Dar click en el botón **Inicio** y seleccionar **Configuración**.

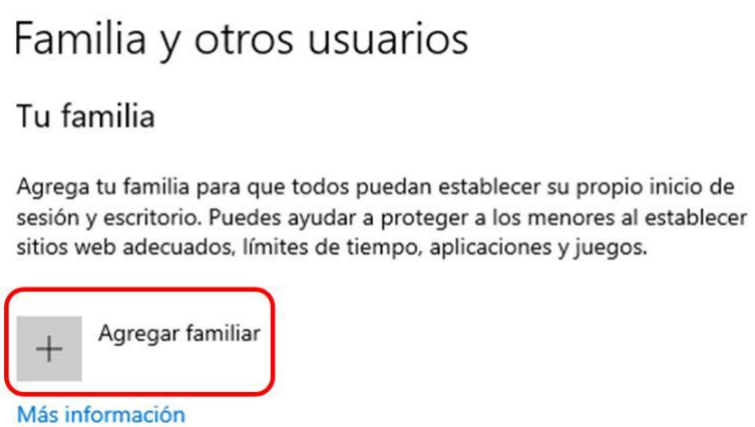


b. Seleccionar la opción **Cuentas**

c. Seleccionar **Familia y otros usuarios**

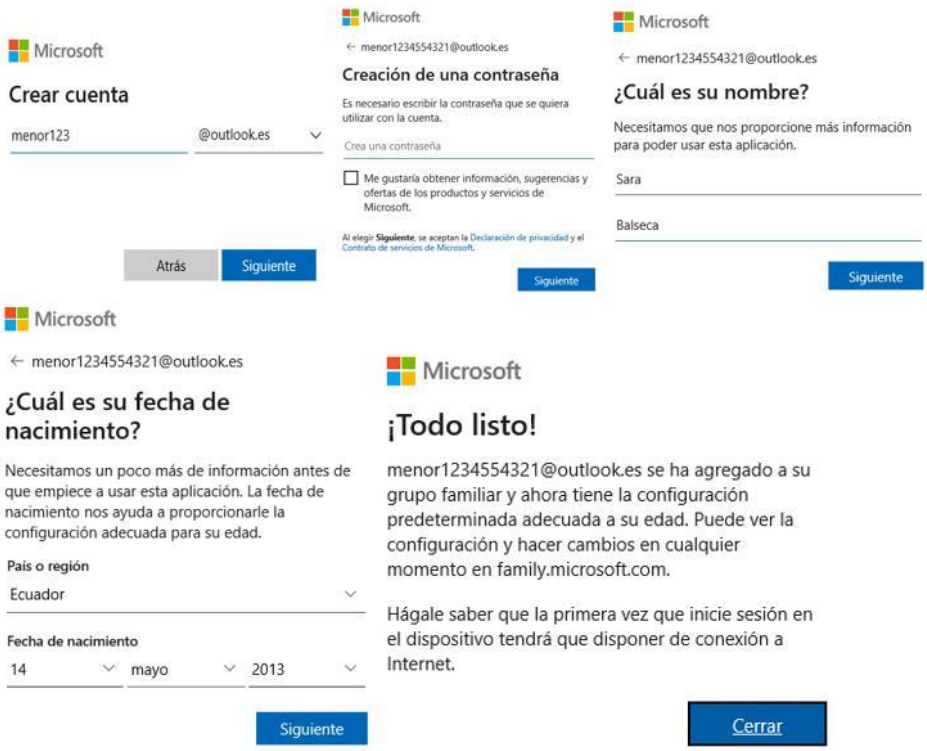


d. Seleccionar la opción **Agregar Familiar**.



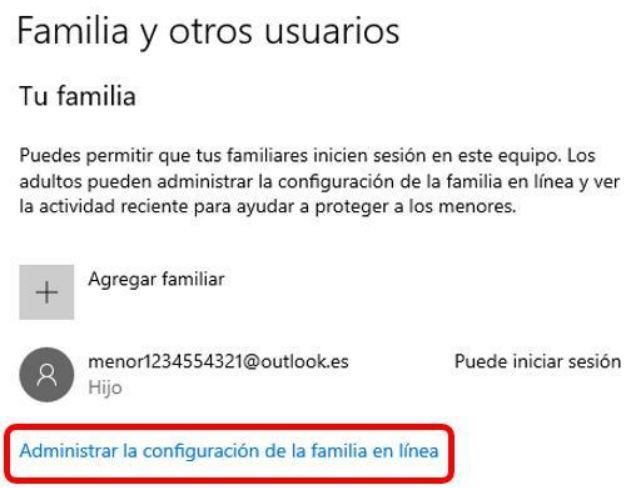
e. Automáticamente se abre una ventana en la cual se deberá seleccionará "**Crear para un menor**"

f. A continuación, solicitará la creación de un correo electrónico para los niños, niñas y adolescentes, configuración de contraseña y fecha de nacimiento. Una vez ingresada esta información aparecerá un mensaje de confirmación. Dar click en **Cerrar**.

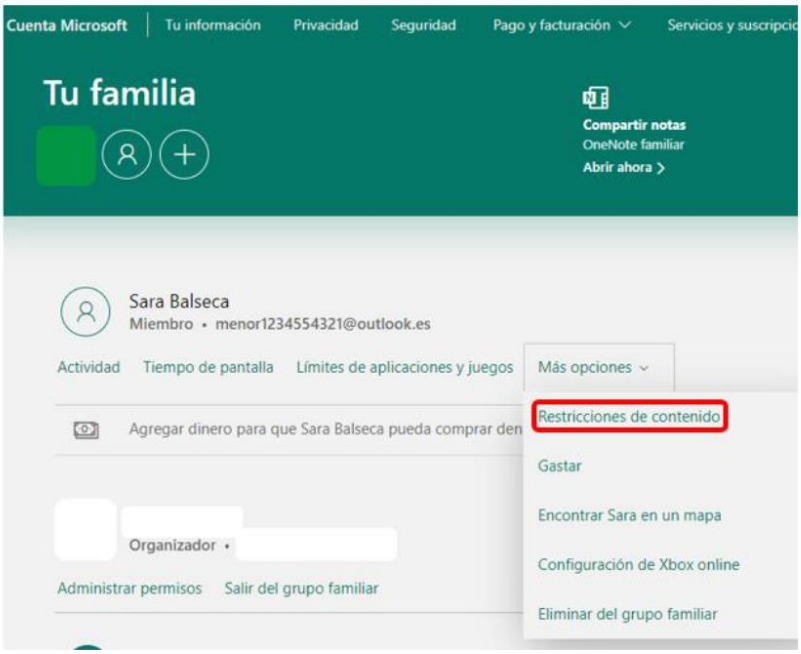


g. En su correo electrónico recibirá una notificación de la creación de la cuenta de los niños, niñas y adolescentes.

h. Regresará a la pantalla **Familia y otros usuarios**, y aparecerá la cuenta de los niños, niñas y adolescentes que creamos. Dar click sobre la opción **Administrar la configuración de la familia en línea**.



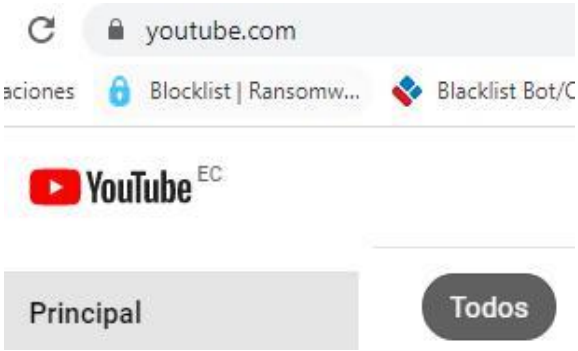
i. En el explorador se abrirá una pantalla para la administración de controles parentales. Debajo del nombre del niño, niña o adolescente aparecerán varias opciones, como por ejemplo Restricciones de contenido.



j. También existen otras configuraciones como: Límites de aplicaciones y juego, tiempo de pantalla encendida, restricciones en compras, opción para ver la actividad del niño, niña o adolecente.

4.2 Configuración de control parental en YouTube en el computador

a. Ir a la página www.youtube.com



b. Registrar su usuario y contraseña en la opción de **Acceder**.

c. Una vez que se ha accedido a YouTube con su usuario, ir a su perfil (junto a la campana de alertas) y seleccionar la opción **Modo restringido**.

d. Activar la opción de **Modo restringido**.

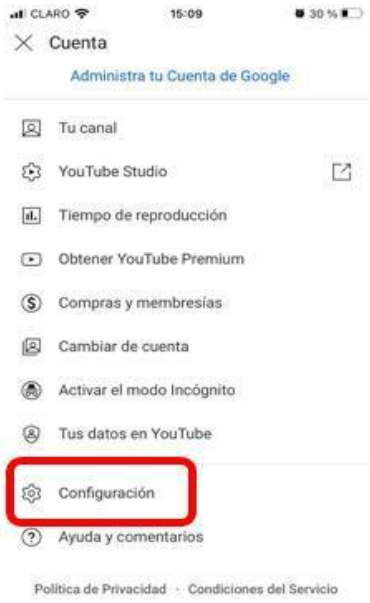
e. Salir de la cuenta de YouTube.

f. Repetir este procedimiento para otros navegadores que estén a disposición del niño, niña o adolescente, ya que este control parental solo estará operativo desde el navegador en el que habilita el modo restringido de la aplicación YouTube.

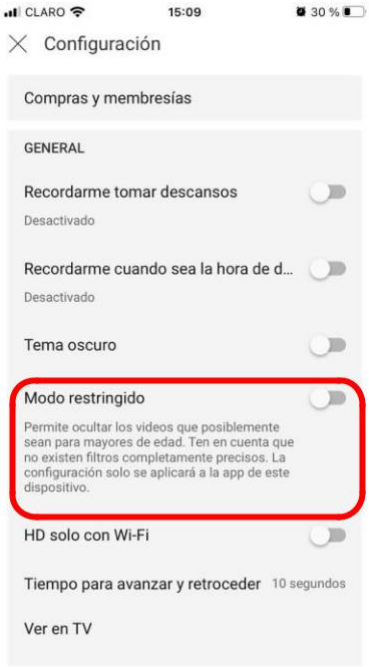
4.3 Configuración de control parental en YouTube en dispositivos móviles

a. Abrir la aplicación de YouTube en el dispositivo móvil.

b. Ingresar al perfil, ubicado en la esquina superior derecha de la ventana para para desplegar el menú de opciones y seleccionar **Configuración**.



c. En la configuración, activar el **Modo restringido**.



d. Salir de la cuenta de YouTube.

5. RECOMENDACIONES ADICIONALES

El control parental es una herramienta útil para ayudar a minimizar los riesgos que pueden enfrentar las niñas, niños y adolescentes en la Internet, pero no son 100% efectivos. Es realmente importante enseñarles habilidades como el pensamiento crítico y la capacidad de recuperación, para que sepan qué hacer si se enfrentan a un riesgo. Aliéntelos siempre a hablar con usted o una persona de su confianza sobre cualquier cosa que les moleste en línea.

A continuación, otras recomendaciones:

1. Comprobar que el dispositivo del niño, niña o adolescente tenga instalado un antivirus, actualizadas las aplicaciones, programas y sistema operativo.
2. Cubrir o apagar las cámaras web cuando no se estén utilizando.
3. La cuenta de usuario que el niño, la niña o adolescente utiliza no debe tener nunca privilegios de administrador.
4. Enseñar al niño, niña o adolescente sobre los peligros y amenazas que pueden encontrar en la red y de cómo pueden evitarlos.
5. Advertir al niño, niña o adolescente sobre los riesgos de compartir fotografías, número de teléfono o cualquier información personal o de su familia.
6. Conversar con los niños, la niñas o adolescentes a fin de que alerten ante alguna interacción incómoda o que ponga en riesgo su integridad.
7. Prevenirles sobre los delitos que se comenten a través de la Internet, sobre todo de la suplantación de identidades para que estén alertas el momento que reciben solicitudes de amistad.
8. Para mayor información consultar en: https://internetsegura.gob.ec/

[illegible]

- INTECO. Recuperado el 16 de marzo de 2021. Obtenido de http://www.edu.xunta.gal/centros/ceipjoaquinrodriguez/system/files/Control+parental+uso+Internet.pdf.
- Adeva, R. (31 de marzo de 2019). adsl zone. Recuperado el 11 de marzo de 2021. Obtenido de https://www.adslzone.net/windows-10/control-parental/.
- MICROSOFT. Recuperado el 10 de marzo de 2021. Obtenido de https://answers.microsoft.com/es-es/windows/forum/windows_10-security-winpc/informaci%C3%B3n-importante-control-parental-en/d116cbbc-3225-4226-b043-0130d3e31c1d.
- GCF AprendeLibre. Recuperado el 11 de marzo de 2021. Obtenido de https://edu.gcfglobal.org/es/seguridad-en-internet/control-parental-en-youtube/1/.

- UNICEF (25 de abril de 2020). Recuperado el 12 de marzo de 2021. Obtenido de https://www.unicef.org/uruguay/historias/como-mantener-tu-hijo-salvo-mientras-navega-en-internet-durante-el-brote-de-covid-19.
- Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires (2019). Violencia contra la mujer en el entorno digital. Derechos, conceptos y recomendaciones. Recuperado el 19 de marzo de 2021. Obtenido de http://cpdp.defensoria.org.ar/wp-content/uploads/sites/5/2019/03/Violencia-contra-la-mujerCuadernillo.pdf.
- INCIBE. Recuperando el 26 de marzo de 2021. Obtenido de https://www.incibe.es/aprendeciberseguridad/grooming.
- INCIBE. Recuperando el 26 de marzo de 2021. Obtenido de https://www.incibe.es/aprendeciberseguridad/sexting.