

PARA PREVENIR ¡ACTÚA!



Ayuntamiento
de Málaga



PROYECTO SOLIDARIO
POR LA INFANCIA

Contenido

1. TALLER Nº1: BULLYING Y CIBERBULLYING (90 minutos)	3
1.1. Presentación de la entidad (10 minutos)	3
1.2. Bullying (40 minutos).....	4
1.2.1. Presentación del taller (45 minutos)	4
1.2.2. Dinámica: Cortometraje (10 minutos)	6
1.2.3. Dinámica: Mural (20 minutos)	8
1.3. Ciberbullying (35 minutos)	8
1.3.1. Presentación del taller (15 minutos)	8
1.3.2. Dinámica: Cortometraje y reflexión (10 minutos)	10
1.3.3. Dinámica: Mitos sobre el ciberbullying (10 minutos)	10
2. TALLER Nº2: GESTIÓN RESPONSABLE DE TU MARCA EN INTERNET, CIBERSEGURIDAD Y REPUTACIÓN ONLINE (90 minutos).....	13
2.1. Datos personales y cómo protegerlos (15 minutos)	13
2.1.1. ¿Qué son datos personales?	13
2.1.2. Ley de protección de datos (LOPD)	14
2.1.3. Consentimiento de menores.....	15
2.1.4. 10 consejos básicos para proteger tus datos personales en internet.....	15
2.2. Privacidad, identidad digital y reputación en línea (10 minutos)	16
2.2.1. Qué es la privacidad	16
2.2.2. La privacidad de los niños y jóvenes	16
2.2.3. Qué es el sharentig.....	17
2.2.4. Derecho a ser olvidado.....	18
2.2.5. Google	19
2.3. La reputación online: identidad, huella y marca digital (20 minutos)	19
2.3.1. La identidad online.....	20
2.3.2. La huella digital	21
2.3.3. La marca digital.....	22
2.3.4. Recomendaciones y consejos para la creación de una identidad digital positiva	22
2.3.5. ¿Y si mi hijo o hija quiere ser influencer?	23
2.4. Principales riesgos de las TICs y consejos para un uso adecuado (30 minutos)	24
2.4.1. Ciberbullying o ciberacoso.....	24
2.4.2. Grooming.....	25
2.4.3. Sexting.....	26

2.4.4. Phishing	27
2.4.5. Suplantación de Identidad.....	28
2.4.6. Ciberadicción	29
2.4.7. Fake News y bulos	30
2.4.8. Cómo enfrentarse a estos riesgos	31
2.5. Los sistemas de control parental (15 minutos)	32
2.5.1. ¿Cómo funcionan estas herramientas?	32
ANEXO 1: TALLER DE BULLYING Y CIBERBULLYING	34
ANEXO 2: GUÍA PARA EL CONTROL PARENTAL	40

1. TALLER Nº1: BULLYING Y CIBERBULLYING (90 minutos)

1.1. Presentación de la entidad (10 minutos)

Proyecto Solidario (5 minutos)

¿Quiénes somos? Proyecto Solidario es una Organización Internacional de Derechos Humanos que promueve, protege y defiende los Derechos de los niños, niñas y adolescentes (NNA) contribuyendo en la transformación de la realidad y trabajando junto con los Estados y los diversos actores sociales, académicos y económicos en el desarrollo de políticas públicas y programas adaptados a cada contexto que garanticen a los NNA y a sus familias el disfrute y ejercicio pleno de sus Derechos Humanos.

¿Qué hacemos aquí? (5 minutos)

PARA PREVENIR ¡ACTÚA! Es un Proyecto subvencionado por el Ayuntamiento de Málaga. Está dirigido a 125 niños, niñas y adolescentes, y 26 familias y docentes de 2 centros educativos de la provincia de Málaga: IES Nuestra Señora de la Victoria e IES Gibralfaire. Se trata de un Proyecto de carácter educativo para sensibilizar y prevenir sobre el bullying y ciberbullying. Los objetivos de estas charlas son promover medidas de igualdad para el rechazo y eliminación de la violencia sobre la infancia y la adolescencia en contextos educativos de Granada, y reforzar conocimientos y habilidades en niños, niñas y adolescentes para reconocer el acoso y ciberacoso y actuar frente al mismo, a través de las siguientes actividades: Taller de bullying y ciberbullying presencial y un taller online sobre la gestión responsable de tu marca en internet, ciberseguridad y reputación online.

1.2. Bullying (40 minutos)

En el Anexo 1, “Taller de Bullying y Cyberbullying” se puede visualizar la presentación de este taller.

1.2.1. Presentación del taller (45 minutos)

- **¿Qué es el Bullying?**

Según el protocolo de actuación en situaciones de bullying, es una forma de discriminación de unos estudiantes hacia otros por sus características o su forma de vida, orientación sexual, nacionalidad, discapacidad, creencias religiosas, opiniones, etnia, sexo.... Se tiene la intención de hacer daño a otra persona que no es capaz de defenderse a sí misma. Suele ser presenciada por otros observadores o testigos. Puede ser de tipo verbal, física, psicológica, de índole sexual, material o cibernética que vamos a ver un poco más adelante.

Otra de las definiciones es, el acoso escolar y a toda forma de maltrato físico, verbal o psicológico que se produce entre escolares, de forma reiterada y a lo largo del tiempo.

Los casos de bullying revelan un abuso de poder. El acosador logra la intimidación del otro chico, que lo percibe como más fuerte, más allá de si esta fortaleza es real o subjetiva. Poco a poco, el niño acosado comienza a experimentar diversas consecuencias psicológicas ante la situación, teniendo temor de asistir a la escuela, mostrándose retraído ante sus compañeros, etc.

Por lo tanto, es una violación de los derechos de los NNA.

Nunca debe ser aceptado, minimizado o invisibilizado.

- **Perfil del estudiante que hace bullying:**
 - Se burla, es manipulador/a, actitud excluyente.
 - Es posible que haya sido testigo de algún tipo de violencia en el ámbito familiar y educativo, por lo que la violencia es una conducta aprendida y erróneamente percibida como normal.
 - Tiene influencia sobre otras personas, líder, su poder es validado dentro del grupo.
 - Es impulsivo/a y confrontativo/a, no tiene empatía, y no tiene control de sí mismo, ni tolerancia ni frustración.
 - No tiene amigos, sino seguidores/as que le tienen miedo.
 - Promete cosas a sus seguidores/as.

- **El/La estudiante que es víctima:**
 - **Impacto en su salud física:** Trastorno de sueño, de alimentación, problemas digestivos, dolor de cabeza, fatiga...
 - **Consecuencias psicológicas:** nervios, insatisfacción, miedo, soledad, inseguridad, abandono, desconfianza de sí mismo/a.
 - **Impacto en las relaciones familiares y sociales:** poco comunicativo/a, pocos amigos/as.
 - **Consecuencias en la vida escolar:** desmotivación, desinterés, falta de atención en las clases, bajo rendimiento académico, rechazo al colegio.
 - **Conductas extremas:** agresión hacia sí mismo/a, suicidio...

- **Los/as observadores/as o testigos:**

Hay dos tipos de observadores:

- Quien apoya al estudiante que violenta, reconoce y refuerza la acción del agresor/a, incluso lo pueden llegar a aprobar abiertamente. No ven el impacto del daño que se le está haciendo a la víctima.
- El que no hace nada, se siente impotente o tiene miedo a ser la víctima. No hablan ni denunciar por temor.

1.2.2. Dinámica: Cortometraje (10 minutos)

Cortometraje sobre el Bullying en un centro educativo: <https://www.youtube.com/watch?v=91HgatU6zL8> . Al finalizar se realizará una pequeña reflexión y se procederá a dar los siguientes consejos:

- **¿Qué puedo hacer?**

Hay muchas cosas que puedes hacer si estás recibiendo acoso o si conoces a alguien que lo está recibiendo. Puedes:

- Informar a un adulto de confianza. Los adultos que ocupan posiciones de autoridad, como los padres, los profesores o los psicólogos del colegio, suelen poder abordar el bullying sin que el acosador sepa cómo se han enterado del acoso.
- Ignorar al acosador y alejarte. A los acosadores les encanta obtener una reacción por parte de sus víctimas. Si te alejas y los ignoras, les estás enviando el mensaje de que lo que te hacen no te afecta.
- Enderezarte al andar y mantener la cabeza bien alta. Al usar este tipo de mensaje corporal, les transmites la idea de que no eres vulnerable.

- No llegues a las manos. Si recurres a la violencia y te peleas con un acosador tienes más probabilidades de resultar herido y de meterte en problemas. Vence tu enfado de otras maneras, como haciendo ejercicio o escribiendo sobre ello.
- Prueba a hablar con el acosador. Trata de explicarle que su comportamiento es grave y nocivo. Esto puede funcionar bien si te das cuenta de que un miembro de tu grupo se ha empezado a meter o a empezado a hacer de menos a otro miembro del grupo.
- Pon en práctica formas de demostrar la seguridad en ti mismo. Practica formas de responder al acosador verbalmente o con tu comportamiento. Pon en práctica el sentirte bien contigo mismo (aunque al principio lo debas fingir).
- Habla sobre ello. Te puede ayudar el hecho conversar con un orientador escolar, profesor o amigo, o con cualquier persona que te puede dar el apoyo que necesitas. Hablar puede ser una buena forma de expresar los miedos y frustraciones que se te pueden acumular cuando recibes acoso.
- Encuentra a (verdaderos) amigos. Si te han acosado con rumores o chismes maliciosos, explícaselo a tus amigos para que te ayuden a sentirte seguro y confiado. Evita estar solo, sobre todo si te están acosando mucho.
- Da la cara por tus amigos y por otras personas que veas que están recibiendo bullying. Tu comportamiento puede ayudar a la víctima a sentirse apoyada y hasta puede llegar a detener el acoso.
- Únete a los programas de prevención del acoso y de la violencia que se aplican en tu centro de estudios. La mediación entre iguales es otra forma en que se puede abordar el acoso. Si tu centro de estudios carece de este tipo de programas, empieza el tuyo propio.

¿Y si soy yo quien acosa?

Algunas personas acosan a los demás para afrontar su propio estrés, su propia rabia y frustración. Hay acosadores que han sido acosados previamente y ahora quieren mostrar su poder acosando a otras personas.

Si has acosado a alguien:

- Trata de conversar con un adulto de confianza sobre por qué te has convertido en un acosador. Pídele consejos para cambiar.
- Trata de pensar en cómo se siente la persona a quien acosas. Imagínate cómo te sentirías tú si fueras la víctima.

Aunque todos seamos diferentes, es importante tratar a todo el mundo con respeto.

1.2.3. Dinámica: Mural (20 minutos)

Consiste en una actividad grupal, donde realizaran un mural/collage sobre el bullying, con el objetivo de sensibilizar al resto del colegio sobre esta temática.

1.3. Ciberbullying (35 minutos)

1.3.1. Presentación del taller (15 minutos)

- **¿Qué es el ciberbullying?**

Se utiliza para describir cuando un niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otro niño o adolescente, a través de Internet o cualquier medio de comunicación como teléfonos móviles o tablets.

- **Características principales**

- **Intencionalidad.** Lo primero que ocurre en el ciberbullying es que surge una fuerte intención de agresión hacia la víctima.
- **Repetitividad.** Para que sea considerada ciberbullying, la situación debe presentarse más de una vez. El acoso o los ataques por medio de lenguaje inapropiado son continuas por parte del agresor. Por ejemplo, al compartir una fotografía de una persona con algún mensaje negativo y esta tiene muchas visualizaciones, se considera bullying electrónico.
- **Desequilibrio de poder.** Por lo general, la víctima del acoso se encuentra indefensa ante esta situación. Es decir, no tiene el poder de eliminar una foto, video o comentario que se haya difundido en la red en su contra.
- **No existe el contacto físico.** La falta de contacto físico entre el agresor y la víctima impide conocer la reacción de ella ante el acoso. No obstante, no es sinónimo de que la agresión no cause daños en la víctima.
- **Canal abierto.** Como está claro, la característica principal del ciberbullying es que se da en un entorno digital, lo que hace que tenga un mayor alcance, mientras que el bullying suele darse en un espacio más “cerrado”, como en la escuela o un centro educativo.

- **Algunas formas de ciberbullying son:**

- Acoso por mensajería instantánea (WhatsApp, Messenger, Instagram Facebook).
- Robo de contraseñas.
- Publicaciones ofensivas en Blogs, foros, sitios web y redes sociales como Instagram, Facebook, Twitter u otras.
- Encuestas de popularidad para humillar o amedrentar.
- Rumores o suplantación de identidad en redes sociales.

1.3.2. Dinámica: Cortometraje y reflexión (10 minutos)

Se visualizará el siguiente cortometraje y después se realizará una reflexión:

<https://www.youtube.com/watch?v=IPV1fUs3jHw>

- ¿Qué os parece lo ocurrido?
- ¿Creéis que la tecnología: WhatsApp, las redes sociales, ¿son un buen medio para expresar nuestro enfado o rabia hacia otra persona?
- ¿Cómo os sentiríais si empezáis a recibir llamadas, mensajes y publicaciones en las que se os amenaza o insulta continuamente a través de WhatsApp o redes sociales?
- ¿Cómo reaccionarías a una situación así?, ¿qué haríais?
- Y como compañeros de la persona que está sufriendo una situación de acoso ¿cómo os sentiríais?, ¿qué haríais?

1.3.3. Dinámica: Mitos sobre el ciberbullying (10 minutos)

Esta dinámica necesita que los usuarios estén de pie y se puedan mover por el aula. El monitor debe decir una frase sobre el ciberbullying y éstos se colocarán en el lado izquierdo de la clase si están de acuerdo o al lado derecho si piensan que la afirmación es falsa. Se deben justificar las respuestas y el o la responsable de la actividad realizará una explicación sobre las mismas. Si es necesario se aclararán conceptos.

- **El ciberbullying es un delito.** Verdadero, no es una broma ni algo gracioso. Se trata de un delito que puede tener consecuencias legales para quien lo realiza.
- **Si alguien te está molestando o insultando, puedes bloquear al remitente como no deseado y no recibirás más mensajes.** Verdadero, hay que actuar cuanto antes. No se debe aguantar este tipo de conductas. Tanto las redes

sociales como los Chats tienen dispositivos de bloqueo para evitar usuarios molestos.

- **Si el ciberbullying se realiza de forma anónima es imposible saber quién lo realiza.** Falso. Es cierto que en Internet muchas personas utilizan nicks y muchas veces, “inventan” perfiles y características personales falsas. A veces, este anonimato puede favorecer las actitudes agresivas por parte de las personas que se creen anónimas. No obstante, es bastante fácil identificar la dirección desde donde se envían los mensajes. La dirección I.P. de nuestro ordenador es como nuestro DNI. Además, aunque los mensajes se envíen desde ciber-cafés o los ordenadores del instituto, sigue resultando fácil reconocer a la persona que está detrás, puesto que siempre se piden datos reales para utilizar los ordenadores públicos.
- **El ciberbullying termina con el paso del tiempo. Si denuncias será peor.** Falso, es la falta de denuncia la que facilita que el agresor mantenga el acoso. La manera más eficaz de acabar con el ciberbullying es contárselo a alguien que te pueda ayudar. No se trata de una broma pesada de la que el agresor de cansará al cabo de un tiempo.
- **El ciberbullying tiene consecuencias para el agresor y la víctima.** Verdadero. No solo nos referimos a las consecuencias legales de cometer un delito. La víctima puede padecer enfermedades psíquicas y físicas tales como depresión, fobia escolar, ansiedad, trastornos de aprendizaje, cefalea, dolor abdominal, etc. Pero, además, hay estudios que demuestran que el agresor también puede sufrir ansiedad, trastornos de conducta y baja autoestima.
- **Si alguien te insulta o amenaza por Internet, lo mejor que haces es contestarle o borrar los mensajes.** Falso La asociación Protégeles recomienda seguir las siguientes pautas:
 - Pedir ayuda, tanto para ti como para sus compañeros/as.
 - No entrar al juego, o responder ni entrar en discusiones.
 - Guardar siempre las pruebas, hacer pantallazos de los comentarios para poder denunciarlo y aportar pruebas.

- Restringir el máximo de privacidad en redes sociales, para evitar que personas ajenas al círculo de personas de confianza puedan ver fotos o publicaciones que son del ámbito privado.
- No dar información sobre lo que haces o con quien vas. Revisar que hay publicado en Google de ti o en redes sociales, y así conocer si alguien está hablando mal de ti.
- No aceptes perfiles desconocidos en redes sociales.
- En caso de recibir algún insulto en redes sociales, advierte de que tomaras medidas legales y después bloquea al ciberacosador. Reporta la incidencia a los administradores/as.
- Cambiar de forma regular las contraseñas de redes sociales y correos electrónicos.

2. TALLER Nº2: GESTIÓN RESPONSABLE DE TU MARCA EN INTERNET, CIBERSEGURIDAD Y REPUTACIÓN ONLINE (90 minutos)

2.1. Datos personales y cómo protegerlos (15 minutos)

2.1.1. ¿Qué son datos personales?

Cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.

Aunque los datos estén cifrados, o presentados con un seudónimo, si pueden utilizarse para volver a identificar a una persona, siguen siendo datos personales y están protegidos por la ley de protección de datos.

Los datos personales que hayan sido anonimizados, de forma que la persona no sea identificable o deje de serlo, dejarán de considerarse datos personales. Para que los datos se consideren verdaderamente anónimos, la anonimización debe ser irreversible.

Ejemplos de datos personales:

- Nombre y apellidos,
- Domicilio,
- Dirección de correo electrónico, del tipo nombre.apellido@empresa.com,
- Número de documento nacional de identidad,
- Datos de localización (como la función de los datos de localización de un teléfono móvil) (*),

- Dirección de protocolo de internet (IP),
- El identificador de una *cookie* (*),
- El identificador de la publicidad del teléfono,
- Los datos en poder de un hospital o médico, que podrían ser un símbolo que identificara de forma única a una persona.

2.1.2. Ley de protección de datos (LOPD)

Esta Ley tiene como finalidad garantizar la protección y buen tratamiento de datos de carácter personal. Estos datos se dividen en tres niveles atendiendo al nivel de la información que recojamos de nuestros clientes y/o usuarios:

- **Nivel básico:** datos identificativos, como el NIF, N^oSS, nombre, apellidos, dirección, teléfono, firma, imagen, e-mail, nombre de usuario, número de tarjeta, matrícula, etc...
- **Nivel medio:** datos acerca de infracciones administrativas o penales, solvencia o crédito, datos tributarios o de la Seguridad Social, datos de prestación servicios financieros, y datos referentes a la personalidad o comportamiento de las personas, como gustos, costumbres, aficiones etc...
- **Nivel alto:** datos acerca de ideología, religión, creencia, origen racial, salud, vida sexual o violencia de género.

Los principales derechos de las personas bajo el RGPD son:

- Acceso a sus datos
- Corrección de las inexactitudes
- Posibilidad de eliminar información
- Evitar la comercialización directa
- Prevenir la toma de decisiones y perfiles automatizados
- Portabilidad de datos

2.1.3. Consentimiento de menores

La edad en la que pueden consentir el tratamiento de sus datos personales es de 14 años. Es decir, es una posibilidad, no una obligación que consentan los jóvenes de 14 años en adelante. En caso de menores de 14 años, deberán dar su consentimiento sus padres o tutores legales.

La Agencia Española de Protección de Datos está encargada de velar por el cumplimiento de la normativa de protección de datos y controlar su aplicación.

2.1.4. 10 consejos básicos para proteger tus datos personales en internet

1. Piensa qué vas a compartir - en internet se queda todo ¡para siempre! Nunca publiques tus datos personales en internet
2. Considera la privacidad de tus redes sociales. Puedes tener perfiles abiertos a todo el mundo o para que solo tus contactos lo vean.
3. Protege tus dispositivos con contraseñas fuertes - evitar poner datos personales como contraseña
4. Cuidado con las redes wifi abiertas que se pueden quedar con los datos de tus dispositivos
5. Si la información publicada en Internet te perjudica, puedes solicitar su retirada - Derecho al olvido
6. Evita enviar información comprometida como datos bancarios por correo electrónico
7. No almacenar datos comprometidos o contraseñas en lugares muy evidentes
8. Cerrar sesión en todos los dispositivos, sobre todo si son dispositivos de uso público como el ordenador del trabajo, de la biblioteca, etc.
9. No dar información por correo ni por teléfono si no se está 100% seguro de a quién se les dan esos datos
10. Importancia de hablar con niños y jóvenes sobre la seguridad en internet e instalar controles parentales para determinar tiempos y usos de las TICs

2.2. Privacidad, identidad digital y reputación en línea (10 minutos)

2.2.1. Qué es la privacidad

En términos generales, la definición de privacidad digital se entiende como el control que un usuario de internet puede ejercer sobre sus datos, limitando el acceso de otras personas o instituciones a su información privada.

El significado de la privacidad digital ha ido evolucionando con el paso del tiempo. Los requisitos en materia de seguridad y protección de datos privados han ido aumentando con el desarrollo de internet y la era digital.

A ello se unen las nuevas exigencias que introduce el RGPD de aplicación en toda la Unión Europea.

Internet es una herramienta que permite además de otras cosas, la interacción entre dos o más personas. Dicha característica se ve reflejada en sitios como Facebook y Twitter, redes sociales en donde los niños y las personas en general, suelen compartir públicamente los sentimientos, noticias, fotografías, videos, etc.

Si bien esto forma parte de la interacción social normal que se da en la actualidad, es necesario considerar que Internet es un “lugar” abierto al mundo, por lo tanto, cualquier acción que se haga puede tener un impacto global y permanente. Por ejemplo, alguna publicación de la cual una persona pueda arrepentirse (como una fotografía u opinión) no solo podrá ser vista por millones de usuarios, sino que también será prácticamente imposible poder borrarla completamente de la red.

2.2.2. La privacidad de los niños y jóvenes

Al contrario de lo que muchos adultos piensan, los menores sí cuidan su privacidad, pero entendiéndola de una forma diferente: buscan evitar que personas adultas como sus padres y profesores tengan acceso a su información en Internet. Sin

embargo, no dan tanta importancia a las consecuencias de sus actos en Internet y les cuesta pensar en términos de futuro.

Lo mejor es hablar con ellos y formarlos para que sepan establecer qué información quieren mantener al alcance sólo de algunas personas, en un ámbito privado, por su seguridad. Este puede ser más íntimo o amplio, y limitarse a más o a menos personas según nuestras preferencias.

No toda la información que hay sobre nosotros en Internet la hemos publicado conscientemente, también puede tener otras procedencias:

- **Publicación inconsciente.** Información que se puede deducir a partir de una publicación propia.
- **Publicación ajena.** Datos de un usuario publicados en Internet por otras personas.
- **Publicación automática.** Información generada y publicada de forma automática por programas o servicios que los usuarios utilizan (por ejemplo, última hora de conexión, sitios web visitados, geolocalización, versión del navegador utilizado, etc.)

2.2.3. Qué es el sharentig

El "sharenting" -un anglicismo que proviene de share (compartir) y parenting (paternidad)- consiste en documentar las primeras sonrisas, palabras, pasos... y cada una de las anécdotas de los más pequeños en Facebook, Instagram y otras redes sociales.

Y se ha convertido en una práctica tan habitual que el diccionario británico Collins lo incluyó en sus páginas en 2016. Desde entonces, el fenómeno no ha dejado de crecer.

Hasta ahora, no ha existido otra generación de niños con una infancia tan pública. Y es probable que, cuando crezcan, muchos no estén de acuerdo con ello.

Te has planteado ¿Cuánto compartes en internet sobre la vida de tus hijos? ¿Y hasta qué punto quieres ver información sobre la vida de los hijos de los demás en las redes sociales?

<https://www.bbc.com/mundo/noticias-44210074>

2.2.4. Derecho a ser olvidado

A nivel de **usuario**, borrar por completo la huella digital es **prácticamente imposible** porque aunque borremos aquel contenido que ya no queremos que esté en la red, siempre existen registros de este.

El derecho al olvido es la protección legal que le permite preservar su reputación almacenando información que ya no se considera relevante y, por lo tanto, queda obsoleta para los fines del registro.

Dentro de este marco legal, existe la posibilidad de eliminar enlaces dañinos de la web, borrar vídeo de YouTube y limpiar su reputación en línea.

La regulación de la UE 2016/679 ha establecido que:

“La protección de las personas con respecto al procesamiento de datos personales es un derecho fundamental.”

El derecho al olvido puede definirse como la garantía que prevé la no difusión, sin razones particulares, de información que puede constituir un precedente perjudicial para el honor de una persona.

En pocas palabras, el derecho al olvido establece los siguientes puntos fundamentales:

- El gestor de un motor de búsqueda en Internet es responsable del procesamiento de datos personales;
- El gestor está obligado a eliminar los enlaces a ciertas páginas web de la lista de datos personales;
- La ley se aplica si la información es incorrecta, inadecuada, irrelevante o excesiva;
- La solicitud de eliminación debe sopesar los intereses de la persona involucrada y el interés público en acceder a la información.

2.2.5. Google

La autoprotección del derecho al olvido se lleva a cabo descargando directamente de Google un formulario especial al que el motor de búsqueda está obligado, por ley, a otorgar.

El derecho al olvido, aunque está cubierto en el GDPR de 2016, se presenta como un mecanismo difícil de implementar: Google siempre tarda demasiado en analizar las solicitudes de eliminación de información y desindexación.

2.3. La reputación online: identidad, huella y marca digital (20 minutos)

La reputación online es el reflejo del prestigio de una persona, empresa o marca en Internet, creada no solo por la misma, sino también por el resto de las personas que intercambian información y opiniones sobre ella en Internet a través de foros, blogs o redes sociales.

La gestión de la reputación online va desde la recopilación de toda la información relacionada, pasando por su seguimiento, con criterio de si afecta o no negativamente a la reputación e imagen de la persona, empresa o marca, pero, además, de su gestión o control.

La reputación online es un ecosistema complejo que depende de muchísimos elementos... y la mayoría de ellos se escapa a nuestro control. Y sin embargo, de ella puede depender el éxito o fracaso tanto de empresas como de nuestra carrera profesional.

La reputación online es la suma de dos aspectos complementarios:

- Los factores internos, esto es, la información que la propia persona comparte sobre sí misma y las acciones online que lleva a cabo a lo largo del tiempo.
- Los factores externos, es decir, toda la información que aportan otros usuarios

Esto significa que todos los usuarios de internet pueden contribuir a fabricarla aportando sus comentarios y opiniones.

2.3.1. La identidad online

La identidad digital es la versión en internet de la identidad física de una persona. Está compuesta por una gran cantidad de datos que proporcionamos en la red, más allá de nuestro correo electrónico y dirección: incluye nuestras fotos, datos bancarios, preferencias a la hora de comprar, etc.

Además, no es uniforme, porque compartimos distintos atributos en diferentes plataformas. Es decir, no aparecen los mismos datos sobre nosotros en LinkedIn que en Facebook, por ejemplo.

También conocida como identidad 2.0. Se trata de una identidad que engloba todas las acciones que nos identifican en Internet: fotos que publicamos o en las que nos etiquetan, comentarios, likes, retweets, posts y peticiones online que firmamos.

Este tipo de acciones contribuyen a crear una opinión y una reputación que otras personas se forman acerca de nosotros con lo que ven publicado online.

A medida que Internet va creciendo, nuestra identidad digital se ve cada vez más expuesta. Solo observemos la cantidad de actividades que realizamos de forma digital y todos los servicios a los que accedemos con frecuencia: compras, operaciones bancarias, suscripciones, etc. Este avance requiere garantizar la seguridad de nuestra identidad digital y nuestra privacidad.

IDENTIDAD DIGITAL: ¿quiénes somos en la red?

https://www.youtube.com/watch?v=rNmXiYY9iHA&ab_channel=OSIseguridad

2.3.2. La huella digital

Es el rastro que dejamos en Internet. No sólo la que aparece en buscadores, sino cualquier información queda almacenada en bases de datos que construyen nuestra huella digital (DNI electrónico, gestiones de tráfico, información bancaria...). Todo lo que hacemos en Internet deja una huella digital, aunque no se visualice por cualquier persona usuaria.

Por tanto, todas las acciones y omisiones, más la huella digital, construyen tu identidad digital.

2.3.3. La marca digital

Marca personal es todo aquello que somos, hacemos, decimos, y compartimos, así como el valor que somos capaces de generar en los demás. Es la suma de nuestros valores y de cómo somos valorados por el entorno, es el impacto de la huella que dejamos en el camino de nuestra vida personal y profesional.

Son todas aquellas acciones que nos anteceden y nos abren puertas a terceros porque quieren tenernos cerca y contar con nosotros en su vida, entorno y proyectos.

Se puede convertir en una estrategia para posicionar profesionalmente a los jóvenes y puede suponer buenas oportunidades para su futuro.

2.3.4. Recomendaciones y consejos para la creación de una identidad digital positiva

Para ayudar a los niños y niñas y a la juventud a usar las nuevas tecnologías de forma responsable es fundamental hablar con ellos sobre el papel que va a tener la tecnología en la rutina familiar y el modelo de uso que les queremos transmitir.

Enseñar a los menores a crear y mantener una identidad digital positiva en Internet supone mostrarles todas las consecuencias de publicar contenidos que perjudiquen su reputación. Para ello os dejamos los siguientes consejos y recomendaciones:

1. Hablar con ellos y ellas sobre seguridad digital y escuchar sus preocupaciones, opiniones y deseos
2. Plantear la posibilidad de crear una marca personal orientada a conseguir objetivos de trabajo o estudios

3. Los padres, madres y tutores deben actuar como un "modelo a seguir" tanto en línea como fuera de línea
4. Fomentar el uso positivo de las TICS. Por ejemplo, ayudarlos a expresar sus pensamientos e ideas sobre sus hobbies a través de un blog para mejorar sus habilidades de escritura creativa
5. Hacer auditorías de la presencia en línea de los jóvenes para ver cómo se están representando en las redes sociales y los blogs
6. Ayudarles a entender los conceptos de privacidad, huella digital y reputación online y aprender juntos nuevos conceptos
7. Establecer pautas claras sobre "qué hacer y qué no hacer" con sus publicaciones online. Por ejemplo, tener cuidado con las opiniones que se expresan y decir solo lo que se estaría dispuesto a decirle a alguien en persona
8. Entender que el contenido en línea tiene el potencial de volverse viral a la velocidad de la luz y una vez que eso sucede, han perdido el control.
9. Cuidar las imágenes que usan de sí mismos, en cualquier escenario, deberían ser las que les gustaría que un reclutador potencial o un oficial de admisiones vieran
10. Recomendarles que eliminen las etiquetas no deseadas en publicaciones o imágenes inadecuadas.

2.3.5. ¿Y si mi hijo o hija quiere ser influencer?

Es la profesión del momento, ser influencer o Youtuber es el sueño de muchos jóvenes ya que muchos de los personajes públicos que admiran han adquirido fama y mucho dinero de esta forma. Pero hay que tener en cuenta que para llegar a ser exitoso en este ámbito también hay que trabajar duro.

Es necesario tener algún tipo de formación ya sea sobre marketing, comunicación o audiovisuales o sobre aquello de lo que quieran hablar, moda, música, deporte, etc.

- La importancia de ser único y aportar valor a la audiencia que tengan más allá de conseguir likes o seguidores
- Informar sobre los posibles riesgos de exponerse en internet
- Hablar sobre los riesgos del sedentarismo y las adicciones a internet
- Asegurate de que pasan tiempo lejos de la pantalla y con amigos de forma presencial

2.4. Principales riesgos de las TICs y consejos para un uso adecuado (30 minutos)

2.4.1. Cyberbullying o ciberacoso

El cyberbullying o ciberacoso es el acoso de un menor (no un adulto) a otro menor usando las tecnologías: redes sociales, videojuegos online, grupos de whatsapp, etc. Estamos ante un caso de cyberbullying cuando un/una menor atormenta, amenaza, hostiga, humilla o molesta a otros menores usando estos medios.

A diferencia del acoso escolar tradicional, el cyberbullying puede mantenerse durante las 24 horas del día, ya que el acceso a los distintos dispositivos se puede realizar en cualquier momento y desde cualquier lugar, por lo que el perjuicio para la víctima puede ser considerablemente mayor.

Ejemplos de ciberacoso pueden ser:

- Crear un falso perfil en nombre de la víctima en un foro o web para escribir en primera persona cosas vergonzosas.
- Hacer circular falsos rumores sobre malos comportamientos de la víctima para conseguir que otros usuarios también se enfaden.

- Reenviar mensajes amenazantes (email, whatsapp, sms...) suponen formas de apoyo a este tipo de actividades que suponen una amenaza a las víctimas.
- Dar de alta a una persona sin su consentimiento en webs para votarlapersona más fea, menos inteligente, etc.

¿Qué hacer ante una situación de ciberacoso?

- Denunciar la situación
- Ayudar a prevenir e informar de posibles situaciones de acoso
- Informate sobre los protocolos de actuación del colegio o instituto

2.4.2. Grooming

El grooming se produce cuando un adulto trata de engañar a un menor a través de Internet para ganarse su confianza con intención de obtener fotos o vídeos de situaciones sexuales o pornográficas e incluso llegar a chantajearle con ellas. En ocasiones es el paso previo al abuso sexual.

Las consecuencias, además de serias, son graves para el menor y su familia: daños psicológicos en la víctima (depresión, baja autoestima, desconfianza, cambios de humor, bajo rendimiento...), daños a nivel familiar (empeoramiento de las relaciones, chantajes a la propia familia por parte del acosador...).

¿Qué hacer si se observa una situación de Grooming?

Para prevenir, hablar con los niños, niñas y jóvenes sobre:

- No proporcionar fotos e imágenes a desconocidos
- No dar las contraseñas a nadie
- Proteger su privacidad online

Además:

- Valorar si es cierto que tienen material para el chantaje
- No ceder en ningún caso
- Pedir ayuda a los profesionales
- Revisar el equipo e instalar antivirus
- Modificar todas las contraseñas de acceso
- Aumentar las opciones de privacidad en las redes sociales
- Guarda las pruebas del chantaje para poder denunciar

2.4.3. Sexting

El sexting consiste en enviar textos o imágenes insinuantes, eróticas o pornográficas por Internet o por los teléfonos móviles. Es una práctica bastante extendida entre los adolescentes que por iniciativa propia suelen enviar mensajes sexting a sus novios/as como prueba de afecto, a alguien con quien quieren ligar, como broma, etc.

El problema es que ese texto o imagen puede ser utilizada más tarde por el destinatario u otro desconocido para extorsionar o chantajear a la víctima. Esto se conoce con el nombre de sextorsión.

¿Qué hacer para evitar situaciones de extorsión?

- Evitar el envío de fotos comprometidas a otra persona incluso si se confía en ella
- Reflexionar sobre las posibles consecuencias de enviar este tipo de imágenes
- Pedir ayuda a la familia
- Guardar las pruebas del chantaje
- Cortar la comunicación
- Denunciar la situación a la policía

2.4.4. Phishing

El *phishing* es un tipo de estafa que intenta obtener de la víctima sus datos, contraseñas, cuentas bancarias, números de tarjetas de crédito o del documento nacional de identidad, etc. mediante engaños para utilizarlos en el robo de fondos de sus cuentas.

Generalmente se solicitan datos personales haciéndose pasar por una empresa o entidad pública con la excusa de comprobarlos o actualizarlos.

Esta petición de datos se realiza a través de un mensaje de teléfono móvil, una llamada telefónica, una ventana emergente durante la navegación por Internet o bien en un correo electrónico.

¿Cómo identificar los mensajes de phishing?

A menudo, en los emails y mensajes de texto phishing cuentan una historia para engañar y lograr que hagamos clic en un enlace o abramos un archivo adjunto. Los mensajes podrían:

- Decir que se ha detectado alguna actividad sospechosa o intentos de iniciode sesión.
- Afirmar que hay un problema con su cuenta o con su información de pago.
- Decir que debe confirmar algunos datos personales.
- Incluir una factura falsa.
- Pedirle que haga clic en un enlace para hacer un pago.
- Decir que usted es elegible para registrarse para recibir un reembolso delgobierno.
- Ofrecerle un cupón para algo gratis.

Cuatro pasos para protegerse de los ataques de phishing:

1. Proteger el ordenador usando un programa de seguridad. Configure el programa para que se actualice automáticamente de modo que pueda tratar cualquier amenaza de seguridad nueva.
2. Proteger el teléfono móvil configurando la actualización automática del software. Estas actualizaciones podrían ofrecerle una protección crucial contra las amenazas de seguridad.
3. Proteger tus cuentas usando un sistema de autenticación de múltiples factores. Hay algunas cuentas que ofrecen un mayor nivel de seguridad ya que para iniciar la sesión en su cuenta tiene que ingresar dos o más credenciales. Esto se llama autenticación de múltiples factores.
4. Proteger tus datos haciendo copias de seguridad. Haz copias de seguridad y asegúrate de que tus copias de seguridad no estén conectadas con la red de tu casa.

2.4.5. Suplantación de Identidad

La suplantación de la identidad se produce cuando una persona se apropia indebidamente de otra identidad digital y la usa para conseguir información personal, para publicar y desprestigiar, extorsionar o chantajear...

También se produce cuando una persona crea una cuenta o perfil con los datos de otra y se hace pasar por ella actuando en su nombre.

Algunas de las consecuencias de la suplantación de identidad son: mostrar una imagen distorsionada de sí mismo en Internet; ser víctima de burlas, insultos o amenazas, tener un descrédito frente a otros; sufrir una pérdida económica...

¿Qué hacer en caso de suplantación de identidad?

- No comunicar contraseñas a nadie
- Evitar que otros miren al escribir la contraseña en lugares públicos
- Usar contraseñas seguras
- Siempre cerrar la sesión y no almacenar contraseñas
- Pedir ayuda profesional
- Cambiar todas las contraseñas
- Denunciarlo a las autoridades

2.4.6. Ciberadicción

La ciberadicción es un problema de adicción a Internet que se observa en menores y en adultos. Su indicador más significativo es la «conexión compulsiva» que se concreta en la necesidad de tener que conectarse con frecuencia muchas veces al día.

Pero además son indicadores de este problema: la dispersión de la atención, la búsqueda constante de contenidos relacionados con ciertos gustos o adicciones, la creación de distintas identidades, la sustitución de lo real por lo vivido en entornos virtuales, la pérdida de la noción del tiempo, mal humor o nerviosismo cuando no se puede conectar, o dedicar menos horas de sueño y comida.

¿Qué hacer para evitar ciberadicciones?

- Controlar el tiempo de uso de las tecnologías de toda la familia
- Buscar alternativas al uso de internet
- Moderar el uso de videojuegos en línea
- Cuidar las relaciones cara a cara o por otros medios como el teléfono
- Respetar las horas de sueño, comidas, descanso, etc.

2.4.7. Fake News y bulos

Se refieren a cualquier tipo de información imprecisa, descontextualizada o directamente falsa, que alguien difunde de manera intencionada para manipular la opinión o simplemente para obtener algún tipo de beneficio. No es algo nuevo, siempre han existido falsos mitos sobre la alimentación, la salud, etc., solo que a través de Internet se difunden más rápido y pueden llegar a más personas.

Los menores reciben, buscan y comparten información en Internet, en ocasiones sin reflexionar lo suficiente. En consecuencia, pueden acceder a contenidos negativos disfrazados como información real. Esto se conoce como *fake news* y pueden llegar hasta los menores a través de las publicaciones en sus redes sociales con mensajes privados, chats de grupo, vídeos, foros, etc. ya que son sus canales preferidos para recibir información.

Estos contenidos falsos se distinguen teniendo en cuenta su grado de falsedad y engaño deliberado:

- Imprecisos, con escasa calidad informacional, pero que se pueden malinterpretar.
- Descontextualizados o sesgados con intención de influir en la opinión.
- Fabricados intencionalmente con el fin de engañar y manipular.

Las noticias falsas o bulos tienen una serie de características que pueden facilitar su identificación. Enseñar a los menores a cuestionar y contrastar la información que aparece en Internet es fundamental para frenar su difusión y minimizar sus efectos.

La mejor forma de enseñar a los menores a detectar estos contenidos falsos es fomentar el pensamiento crítico y la lectura de contenidos adecuados a su madurez, con el objetivo de que los menores puedan llegar a ser autónomos, diferenciando entre un bulo y una noticia real.

- Comenzar desde edades tempranas. Al acompañarlos en el proceso de aprendizaje digital, es esencial aprovechar oportunidades reales para analizar juntos las posibles noticias falsas que aparezcan en sus redes sociales o en una página web.
- No todo lo que aparece publicado en Internet es cierto. Muchos contenidos se crean para generar algún tipo de beneficio, económico o ideológico. Por tanto, deben aprender a localizar fuentes seguras y fiables de información.
- Acostumbrarse a encontrar y utilizar fuentes de información fiables. En su día a día, por ejemplo, al realizar tareas de clase, pueden incluir citas y referencias en sus trabajos escolares.
- Aprender a valorar diferentes puntos de vista. Fomentar valores sociales positivos como la asertividad, la empatía y la tolerancia, promoviendo el respeto frente a otros colectivos de personas, es clave para que el menor reaccione ante las *fake news* de manera crítica, reflexiva y prudente.
- Practicar la paciencia y evitar la impulsividad. Los bulos crean en el usuario/a la sensación de que es imprescindible compartir la información rápidamente, para así llegar a muchas personas. Por eso es fundamental promover el análisis de la noticia, contrastar los hechos que presenta y verificar las fuentes.

2.4.8. Cómo enfrentarse a estos riesgos

- *Apoyar al menor.* Es fundamental reaccionar con calma y no culparle de la situación, manteniendo la comunicación y la confianza: cuenta con nuestra ayuda y comprensión.
- *Establecer nuevas medidas de seguridad.* Si observamos que existe información privada publicada sin consentimiento, es necesario cambiar las contraseñas de los servicios online utilizados, ya que alguien puede haber accedido a ellos sin permiso.

- *Comunicación.* Si otra persona ha difundido información personal del menor, la primera opción es contactar y hacerle ver que esa información es privada y debería borrarla.
- *Reporte al proveedor de servicios.* Si el paso anterior no es suficiente, se debe contactar con los responsables del servicio donde se ha publicado para que tomen medidas.
- *Denuncia.* Ante una situación de ciberacoso, grooming, o suplantación de identidad, así como problemas derivados de la práctica del sexting, es importante contactar con las Fuerzas y Cuerpos de Seguridad.
- *Buscar ayuda psicológica.* El centro de salud y su centro educativo pueden ofrecer al menor apoyo psicológico y emocional si es necesario.

2.5. Los sistemas de control parental (15 minutos)

Un sistema de control parental es una herramienta que permite a los padres, madres y tutores controlar y/o limitar el contenido a los que sus hijos puedan acceder a internet desde sus dispositivos, ya sean ordenadores, móviles o tabletas.

Existen muchas herramientas de control parental con las que los padres pueden proteger y controlar el acceso a internet, los horarios y sobre todo el contenido al que se exponen sus hijos conocer de una forma cómoda y sencilla, protegiendo de ese modo a sus hijos de las posibles amenazas que estos puedan sufrir en sus diferentes dispositivos móviles.

2.5.1. ¿Cómo funcionan estas herramientas?

El funcionamiento suele ser muy sencillo e intuitivo, se instala la aplicación en el móvil o tableta, y se crea una cuenta en la web con la que se conecta al móvil, con ello ya se puede disfrutar de las ventajas que tienen estas herramientas y de la tranquilidad que ofrecen a sus usuarios.

Las características que pueden tener disponibles este tipo de herramientas son las siguientes:

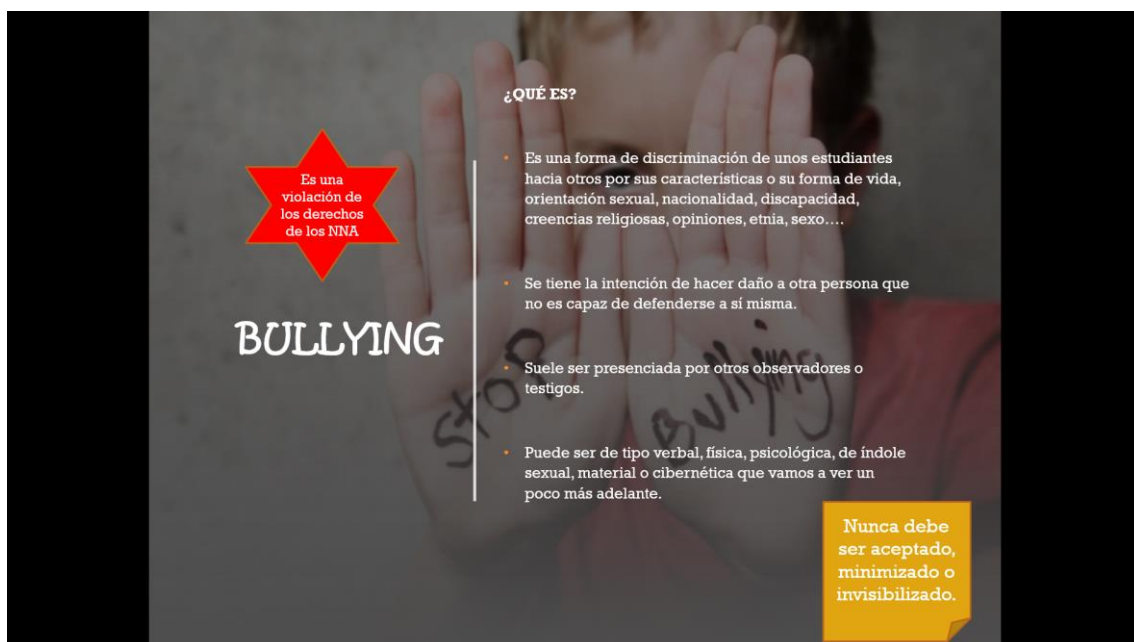
- **Control Web:** El control parental permitirá bloquear sitios web en función de las diferentes categorías que existen, o si lo prefieres puedes poner páginas web concretas las cuales se pueden bloquear.
- **Control de aplicaciones:** De este modo podemos hacer que nuestros hijos no puedan tener acceso a ciertas aplicaciones como por ejemplo programas de mensajería instantánea, aplicaciones de redes sociales, acceso a navegadores web, acceder al Google Play o Apple Store para realizar compras, etc.
- **Bloqueo de llamadas:** Con esta herramienta podrás bloquear los teléfonos a los que no se podrán emitir o recibir llamadas, además de definir el funcionamiento ante llamadas internacionales o números desconocidos.
- **Tiempo de uso:** Con lo que se podrá controlar la cantidad de tiempo de uso que tu hijo pueda tener acceso a las diferentes categorías como por ejemplo juegos o navegadores.
- **Alarmas:** Con esto podrás determinar alarmas para el dispositivo de tu hijo, avisándole de cualquier cosa.
- **Geolocalización:** Te permite conocer la localización en la que está situado tu hijo conociendo donde se encuentra en tiempo real.
- **Botón de Emergencias:** Añade un “Botón del Pánico” al teléfono de tu hijo con el que te envía una alerta de emergencia avisando de una situación excepcional.

Cada plataforma y navegador tiene sus propias funcionalidades para controlar el tipo de contenido y el tiempo que los niños, niñas y jóvenes están frente de la pantalla.

En el Anexo 2 se puede visualizar la Guía para el Control Parental.

ANEXO 1: TALLER DE BULLYING Y CIBERBULLYING

Para abordar el taller de Bullying y Cyberbullying se ha utilizado una presentación en formato Power Point con el siguiente contenido:



ACOSADORA/A



Promete cosas a sus seguidores

Tiene influencia sobre otras personas

Se burla, es manipulador/a

La violencia es una conducta aprendida percibida y como algo normal.

No tiene empatía

No tiene autocontrol

Es impulsivo/a y confrontativo/a

NO+
Bullying

VÍCTIMA



Trastorno del sueño, de la alimentación, dolor de cabeza, ...

Desconfianza en sí mismo

SOLEDAD

Pocos amig@s, poco comunicativo/a

Agresión hacia sí mismo, suicidio...

MIEDO

Inseguridad

NO+
Bullying

OBSERVADORES/AS



Quien apoya al acosador/a, y refuerza su acción, incluso lo pueden llegar a aprobar abiertamente. No ven el impacto del daño que se le está haciendo a la víctima.



El que no hace nada, se siente impotente o tiene miedo a ser la víctima. No hablan ni denunciar por temor.

CIBERBULLYING

¿QUÉ ES?

- Se utiliza para describir cuando un niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otro niño o adolescente, a través de Internet, o cualquier medio de comunicación como teléfonos móviles, ordenadores o tablets.

ALGUNAS FORMAS DE CIBERBULLYING

Acoso por mensajería instantánea

Robo de contraseñas

Publicaciones ofensivas

Encuestas de popularidad para humillar.

Rumores o suplantación de identidad en RR.SS.



Visualizar el video: <https://www.youtube.com/watch?v=91HgatU6zL8>

REFLEXIÓN

- ¿Qué os parece lo ocurrido?
- ¿Cómo reaccionarías a una situación de bullying?, ¿qué haríais?
- ¿Creéis que la tecnología: WhatsApp, las redes sociales, son un buen medio para expresar nuestro enfado o rabia hacia otra persona?
- ¿Cómo os sentiríais si empezáis a recibir llamadas, mensajes y publicaciones en las que se os amenaza o insulta continuamente a través de WhatsApp o redes sociales?
- Como compañeros de la persona que está sufriendo una situación de acoso ¿cómo os sentiríais?, ¿qué haríais?





CONSEJOS

STOP
ciberbullying

- Pedir ayuda, tanto para ti como para sus compañeros/as.
- No entrar al juego, o responder ni entrar en discusiones.
- Guardar siempre las pruebas, hacer pantallazos de los comentarios para poder denunciarlo y aportar pruebas.
- Restringir el máximo de privacidad en redes sociales, para evitar que personas ajenas al círculo de personas de confianza puedan ver fotos o publicaciones que son del ámbito privado.
- No dar información sobre lo que haces o con quien vas. Revisar que hay publicado en Google de ti o en redes sociales, y así conocer si alguien está hablando mal de ti.
- No aceptes perfiles desconocidos en redes sociales.
- En caso de recibir algún insulto en redes sociales, advierte de que tomaras medidas legales y después bloquea al ciberacosador. Reporta la incidencia a los administradores/as.
- Cambiar de forma regular las contraseñas de redes sociales y correos electrónicos.

¡¡MUCHAS GRACIAS A TODOS!!

 @PROY_SOLIDARIO

 @PSOLIDARIO

 PROYECTO SOLIDARIO

www.pontucorazonenlamano.com



ANEXO 2: GUÍA PARA EL CONTROL PARENTAL

A continuación, se muestra una Guía de herramientas de control parental elaborada y promocionada por el Gobierno de España, INCIBE, FordKids, 017, CEAPA, ConCapa, Asociación de Internautas y cofinanciado por la Unión Europea.



GUÍA DE HERRAMIENTAS DE CONTROL PARENTAL

#PantallasMásSeguras

OBJETIVO DE ESTA GUÍA



Esta guía ha sido desarrollada por el Instituto Nacional de Ciberseguridad (INCIBE) a través de Internet Segura for Kids (IS4K), en colaboración con la Confederación Española de Asociaciones de Padres y Madres del Alumnado (CEAPA), la Confederación Católica Nacional de Padres de Familia y padres de Alumnos (CONCAPA) y la Asociación de Internautas.

En esta guía podrás encontrar diferentes herramientas y servicios de configuración de controles parentales para diferentes dispositivos, como son: filtrado de contenidos, control del tiempo, supervisión de actividad, geolocalización y protección de la configuración.

Recuerda que estas herramientas son un complemento en nuestra labor de mediación parental, siempre deben ir acompañadas de actividades digitales en familia que faciliten un clima de comunicación y confianza.

ÍNDICE

2. ¿Qué es un control parental?	Pág. 2
3. Opciones del sistema operativo	Pág. 3
4. Aplicaciones de control parental	Pág. 8
5. Proveedores de contenidos	Pág. 13
6. Opciones de redes sociales	Pág. 18
7. ¿Dónde podemos pedir ayuda?	Pág. 20

LICENCIA DE CONTENIDOS

La presente publicación pertenece al Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-Compartir Igual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y la iniciativa Internet Segura for Kids (IS4K) y sus sitios web: <https://www.incibe.es> y <https://www.is4k.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia:

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES



2. ¿Qué es un control parental?

2/20

Las herramientas de control parental son un apoyo en el aprendizaje digital de los menores, limitando las funciones y el alcance de sus dispositivos cuando se conectan a Internet.

HERRAMIENTAS

Diferentes funciones para cada necesidad



Filtrado de contenidos: mediante diferentes sistemas, bloquea el acceso del menor a ciertos contenidos inapropiados (habitualmente de connotación sexual o violenta).



Control de tiempo: emite alertas o interrumpe la navegación al alcanzar determinada hora o límite de tiempo.



Supervisión de actividad: genera informes con el historial de navegación, búsquedas o reproducción multimedia.



Geolocalización: sigue la posición actual y el recorrido anterior del dispositivo.

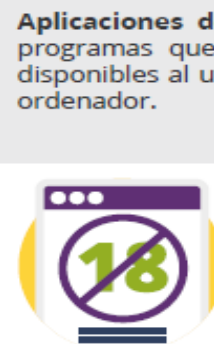


Protección de la configuración: evita modificaciones no deseadas de los ajustes de control parental.

¿Cómo clasificamos las herramientas de control parental en esta guía?



Opciones de sistema operativo: ajustes de control parental presentes en las opciones de configuración de cada dispositivo o servicio. No requieren instalación puesto que están incorporadas en el sistema.



Aplicaciones de control parental: aplicaciones o programas que limitan o controlan las funciones disponibles al utilizar un dispositivo móvil, tableta u ordenador.



Proveedores de contenidos: plataformas de reproducción o búsqueda que ofrecen un conjunto limitado de contenidos apropiados para los menores.





Opciones de redes sociales: ajustes de bienestar digital disponibles en las redes sociales, que limitan o supervisan la actividad en línea del menor.

3. Opciones de sistema operativo

3/20

ANDROID



Dispositivo:  

Opciones configurables de los dispositivos móviles con sistema Android.

FUNCIONES



Control de tiempo: puedes configurar temporizadores para cada aplicación. Cuando el tiempo permitido termine, la aplicación se pausa hasta el día siguiente.



Supervisión: desde el panel de control puedes revisar el tiempo de uso diario, las veces que se ha desbloqueado y las notificaciones que se han recibido.



Protección de la configuración: puedes bloquear esta configuración si utilizas Family Link (ver pág. 8).

EXTRAS



Modo descanso: es posible silenciar la actividad del dispositivo durante un periodo de tiempo establecido.





Modo sin distracciones: permite programar un horario durante el cual las aplicaciones que deseemos se silenciarán o pausarán.



Sincronización con Family Link: puedes realizar ajustes de control parental desde otro dispositivo e impedir que el menor pueda desactivar las opciones establecidas de bienestar digital (ver pág. 8).

TIEMPO DE USO



Dispositivo:   

Herramienta gratuita para dispositivos móviles y ordenadores con sistema macOS e iOS.

FUNCIONES



Filtrado de contenidos: permite restringir las páginas web dirigidas a público adulto, o limitar el acceso solamente a aquellos sitios web que determinemos, así como configurar los ajustes de privacidad.



Control de tiempo: es posible definir durante cuánto tiempo se puede utilizar cada aplicación al día, así como establecer un tiempo de inactividad, un periodo de tiempo durante el cual el ordenador quedará suspendido, exceptuando aquellas aplicaciones a las que demos permiso.



Supervisión: permite llevar un control de tiempo, así como consultar en qué aplicaciones se ha empleado, cuántas notificaciones se han recibido y cuántas veces se ha desbloqueado el dispositivo.



Protección de la configuración: puedes bloquear todos los ajustes con contraseña para que el menor no los pueda modificar sin autorización.

EXTRAS



App Store: puedes impedir que tu hijo/a pueda comprar productos con contenido explícito o restringir todas las compras.



Multidispositivo: existe la posibilidad de utilizar el servicio 'En familia' (accesible en 'Preferencias del sistema') para configurar 'Tiempo de uso' en los dispositivos de los menores.

3. Opciones de sistema operativo

4/20

CONTROL FAMILIAR MICROSOFT



Dispositivo:

Ajustes de control parental que ofrece el sistema operativo Windows.

FUNCIONES

STOP

Filtrado de contenidos: permite restringir programas específicos y controlar tanto los juegos como el tipo de juego a los que el menor podrá acceder. Se puede establecer una clasificación en función de rangos de edad y tipos de contenido. También es posible bloquear sitios web concretos.



Control de tiempo: permite controlar el tiempo que los menores podrán hacer uso del equipo.



Supervisión: recopila informes de la actividad del dispositivo.



3. Opciones de sistema operativo

5/20

SAMSUNG



Dispositivo:

Opciones de control parental en las televisiones *smart TV* de Samsung.

FUNCIONES



Filtrado de contenidos: permite bloquear los programas según la calificación de edad, así como las aplicaciones y programas a los que puede acceder el menor.



Protección de la configuración: los ajustes se bloquean con un código PIN.

EXTRAS



Conectividad con otros dispositivos asociados: posibilidad de utilizar un móvil Samsung vinculado para controlar la televisión a distancia y los ajustes de control parental.



PANASONIC

Panasonic

Dispositivo:

Opciones de control parental en las televisiones *smart TV* de Panasonic.

FUNCIONES



Filtrado de contenidos: permite restringir el acceso a los canales que consideras inadecuados y bloquear las aplicaciones a las que no deben acceder los menores.



Protección de la configuración: los ajustes se bloquean con un código PIN.




3. Opciones de sistema operativo

6/20

LG



Dispositivo: 

Opciones de control parental en las televisiones *smart TV* de LG.

FUNCIONES



Filtrado de contenidos: puedes bloquear manualmente el acceso a aplicaciones y canales que no consideres apropiados para tu hijo/a, así como filtrar los programas según su edad.

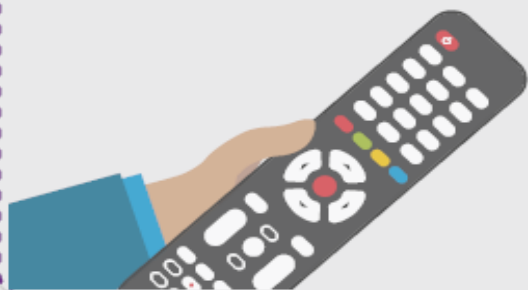


Protección de la configuración: los ajustes se bloquean con un código PIN.

EXTRAS




Bloqueo de entrada a otros dispositivos: puedes restringir el acceso a otros aparatos conectados, como videoconsolas, reproductores o decodificadores.



PLAYSTATION



Dispositivo: 

Opciones de control parental en los modelos de Playstation PS5, PS4, PS3, PS Vita y PSP.

FUNCIONES



Filtrado de contenidos: permite establecer una restricción de edad para los juegos y otros contenidos audiovisuales según el código PEGI. Al conectarse a Internet en Playstation Network, es posible impedir la comunicación con otros usuarios de Playstation y el acceso a contenidos creados por otros jugadores.



Control de tiempo: puedes establecer un horario semanal de tiempo de juego, una duración para cada sesión de juego y/o una hora de finalización.

EXTRAS



Bloqueo de aplicaciones: permite restringir las compras en la tiendas virtual de Playstation creando un límite de gasto mensual.



3. Opciones de sistema operativo

7/20

XBOX



Dispositivo:

Ajustes de control parental en la consola Xbox One.

FUNCIONES

STOP

Filtrado de contenidos: creando un grupo de cuentas familiar administrado por un adulto, permite limitar los juegos a los que puede acceder el menor, las búsquedas web y páginas concretas. También es posible restringir el acceso a aplicaciones y juegos determinados por el administrador familiar, así como limitar las compras en la tienda virtual.



Control de tiempo: permite configurar un recordatorio diario de tiempo, que avisará al menor cuando haya superado el tiempo establecido.



Supervisión: puedes recibir un informe semanal por correo electrónico con un resumen de las sesiones de juego, la duración de las mismas, los juegos y contenidos a los que ha accedido y durante cuánto tiempo.

EXTRAS



Notificaciones: te llegará un aviso para que aceptes o deniegues la solicitud de tu hijo/a cuando quiera acceder a un contenido concreto o realizar una compra.



Control multidispositivo: puedes modificar la configuración a través de la página web de Xbox o desde la propia consola, controlando varias cuentas simultáneamente.

NINTENDO SWITCH



Dispositivo:

Opciones de control parental en la consola.

FUNCIONES

STOP

Filtrado de contenidos: permite restringir aquellos juegos que no son apropiados para nuestro hijo/a, según la clasificación de edades establecida por PEGI. Además, es posible impedir la comunicación con otros usuarios y la publicación de capturas de pantalla en las redes sociales.



Control de tiempo: puedes configurar un horario semanal de tiempo de juego permitido. Cuando la sesión de juego se acerca al tiempo establecido, una alarma avisa a tu hijo/a para que apague la consola. También es posible activar la función 'suspender programa' para que la consola salga del juego de forma automática al terminar el tiempo.



Supervisión: la aplicación elabora un informe de uso diario, indicando los juegos a los que ha accedido y durante cuánto tiempo.

EXTRAS





Control multidispositivo: la aplicación permite supervisar la actividad de varios usuarios desde el dispositivo que actúe como administrador.

4. Aplicaciones de control parental

8/20

FAMILY LINK



Dispositivo:  

Herramienta de Google para dispositivos móviles con sistema Android.

FUNCIONES



Filtrado de contenidos: permite restringir las aplicaciones aprobando o bloqueando las que quiera descargar de Google Play Store.



Control de tiempo: puedes establecer límites de tiempo diarios y configurar una hora de dormir en el dispositivo.



Supervisión: permite consultar cuánto tiempo usa cada aplicación mediante informes de actividad semanales o mensuales.



Geolocalización: permite ver la ubicación del dispositivo móvil de tu hijo/a.



Protección de configuración: permite restringir la modificación de los ajustes de control parental en el sistema Android.



FAMILY TIME



Dispositivo:  

Herramienta de control parental para dispositivos móviles con sistema Android, iOS y Kindle.

FUNCIONES



Filtrado de contenidos: permite restringir las aplicaciones inadecuadas para el menor.



Control de tiempo: puedes establecer un tiempo máximo para cada aplicación o juego.



Supervisión: recopila información sobre las aplicaciones instaladas, contactos, mensajes y navegación. También rastrea los mensajes y llamadas.



Geolocalización: ofrece información sobre la ubicación del dispositivo.

EXTRAS





Notificaciones: alertas automáticas de situaciones peligrosas.

4. Aplicaciones de control parental

9/20

SECUREKIDS



Dispositivo:  

Herramienta para dispositivos móviles con sistema Android.

FUNCIONES



Filtrado de contenidos: permite restringir páginas web de forma individual o por categorías, limitar el uso de los navegadores por tiempo o en su totalidad, instalar la opción de búsqueda segura y controlar el acceso a aplicaciones.



Control de tiempo: puedes establecer alarmas programadas y alarmas instantáneas que se enviarán al dispositivo o bloquear el dispositivo de acuerdo con un horario.



Supervisión: recopila información sobre el uso y las aplicaciones más utilizadas.



Geolocalización: permite localizar el dispositivo y dispone de un botón de alarma, que indicará la posición junto con la captura de una foto.

EXTRAS






Llamadas: puedes bloquear números de teléfonos concretos, así como las que provengan de desconocidos o internacionales.



Control multidispositivo: permite gestionar la actividad de varios menores o dispositivos simultáneamente.

QUSTODIO



Dispositivo:   

Herramienta para dispositivos móviles Android e iOS, y ordenadores Windows.

FUNCIONES



Filtrado de contenidos: permite restringir el acceso a determinadas categorías de sitios web, emitiendo alertas cuando se intenta acceder a páginas web no permitidas.



Control de tiempo: puedes bloquear el dispositivo o una aplicación determinada de acuerdo con un horario.



Supervisión: recopila información sobre el uso y las aplicaciones más utilizadas, así como del tiempo empleado en cada una de ellas.



Geolocalización: opción disponible en versión premium y dispositivos Android.

EXTRAS





Supervisa llamadas y SMS: opción disponible para dispositivos Android.

4. Aplicaciones de control parental

10/20

NORTON FAMILY



Dispositivo:  

Herramienta de control parental
para dispositivos móviles Android e iOS.

FUNCIONES



Filtrado de contenidos: permite limitar los sitios web asignados por categorías, pudiendo establecer listas de páginas permitidas y bloqueadas. También permite restringir el uso del navegador y de otras aplicaciones.



Control de tiempo: permite establecer el número de horas por días, así como su franja horaria.



Supervisión: permite establecer niveles de supervisión, configurar categorías para su bloqueo y sitios web permitidos y restringidos.

EXTRAS





Llamadas: permite el bloqueo o desbloqueo de los números de la agenda, y bloquear llamadas desconocidas o internacionales.



Control multidispositivo: permite gestionar el control desde cualquier otro dispositivo, agregando a la cuenta varios usuarios y dispositivos.

ESET PARENTAL CONTROL



Dispositivo:  

Herramienta de control parental
para dispositivos móviles Android.

FUNCIONES



Filtrado de contenidos: permite filtrar páginas web por categorías, restringiendo determinados tipos de sitios web, recibiendo alertas cuando el menor quiera acceder a una web tipificada como inapropiada. También puedes bloquear el acceso a aplicaciones.



Control de tiempo: permite el uso de aquellas aplicaciones calificadas como juego y diversión durante el número de horas/días especificado.



Supervisión: realiza informes de control web y de uso de aplicaciones.



Geolocalización: opción de seguimiento de localización del dispositivo.

EXTRAS



Notificaciones: es posible configurar alertas personalizadas.





Control remoto del dispositivo: opción de seguimiento de la localización del dispositivo.

4. Aplicaciones de control parental

11/20

SCREEN TIME



Dispositivo:  

Herramienta de control parental para dispositivos móviles Android e iOS.

FUNCIONES



Filtrado de contenidos: permite restringir el acceso a aplicaciones.



Control de tiempo: permite establecer tiempo de uso del dispositivo móvil, tanto del dispositivo en su totalidad como en aplicaciones concretas.



Supervisión: permite controlar el uso que se está haciendo de las aplicaciones permitidas del dispositivo móvil.

EXTRAS




Notificaciones a través del panel de control web puedes configurar las notificaciones que se reciban por email y los informes diarios.



VODAFONE SECURE NET



Dispositivo: 

Servicio de seguridad para clientes de Vodafone.

FUNCIONES



Filtrado de contenidos: permite restringir contenidos por categorías (por ejemplo: redes sociales, violencia, etc.), así como bloqueando sitios web concretos.



Control de tiempo: puedes bloquear el acceso a Internet en los momentos especificados.

EXTRAS





Antivirus y protección web: frente a malware y sitios web maliciosos.

4. Aplicaciones de control parental

12/20

KIDS READY



Dispositivo:  

Servicio de control parental para clientes de Orange.

FUNCIONES



Filtrado de contenidos: permite limitar los contenidos a los que puede acceder el menor, así como impedir el acceso a determinadas aplicaciones que consideremos inadecuadas.



Control de tiempo: se puede establecer un horario en el que se permita el acceso a las aplicaciones.



Supervisión: puedes supervisar las aplicaciones que ha utilizado tu hijo/a, el tiempo que ha empleado en ellas y las páginas web a las que ha accedido (función no disponible en dispositivos iOS).



Geolocalización: puedes saber en tiempo real dónde se encuentra, y también consultar el historial de rutas que ha realizado. Es posible definir zonas y supervisar cuando entra o sale de las mismas.

EXTRAS



Opción de borrado remoto: si tu hijo/a pierde el dispositivo o se lo roban, puedes eliminar el contenido del mismo desde tu móvil.




Control multidispositivo: puedes gestionar varios teléfonos o tabletas desde tu móvil.



Botón de ayuda: en caso de emergencia tu hijo/a puede enviarte una alerta instantánea que incluye la ubicación del dispositivo.

LOCATEGY



Dispositivo:  

Herramienta de control parental para dispositivos móviles.

FUNCIONES



Filtrado de contenidos: permite inhabilitar el uso de aplicaciones, así como el acceso a contenido web no adecuado para el menor.



Control de tiempo: permite establecer un tiempo máximo de uso de dispositivo o en un intervalo horario determinado.



Supervisión: recopila información sobre las aplicaciones instaladas, el contenido web al que ha accedido, además del tiempo de uso.



Geolocalización: que ofrece información sobre la ubicación del menor en tiempo real y permite visualizar las ubicaciones en las que se ha desplazado en los últimos días de uso.

EXTRAS





Bloqueo de aplicaciones: permite bloquear el acceso a determinadas aplicaciones instaladas en el móvil o tableta.



Alertas y notificaciones: permite el envío de notificaciones al adulto en caso de salir de una ubicación determinada o en situaciones de riesgo para el menor.

5. Proveedores de contenidos

MOVISTAR JUNIOR

Dispositivo:  

Aplicación de **entretenimiento multimedia** dirigida a menores de 12 años.



FUNCIONES

STOP

Filtrado de contenidos: permite limitar el acceso a los contenidos asignados al rango de edad elegido (de 0 a 4 años, de 5 a 7 años o de 8 a 12 años).






Control de tiempo: puedes establecer un horario o un límite de tiempo de uso, entre 5 y 180 minutos, tras el cual la aplicación deja de permitir la visualización de contenidos.



Protección de la configuración: permite establecer un código PIN para proteger el acceso a los ajustes de la aplicación frente a modificaciones no deseadas.



YOUTUBE KIDS

Dispositivo:   

Aplicación limitada con **ajustes personalizables** por edad y preferencias.



FUNCIONES

STOP

Filtrado de contenidos: permite adecuar los vídeos que se muestran a la madurez del menor: preescolares (menores de 5 años), niños pequeños (entre 5 y 7 años) y niños mayores (entre 8 y 12 años).



Control de tiempo: puedes establecer un tiempo de visualización, y una vez terminado, la aplicación se bloquea automáticamente.



Protección de la configuración: permite establecer un código PIN o verificar los ajustes resolviendo una operación matemática sencilla.

EXTRAS



Bloqueo de canales: puedes bloquear canales y vídeos que consideres adecuados.



Desactivación de la función 'búsqueda': restringe los canales a los que se puede tener acceso, limitándolo a aquellos verificados por Youtube Kids como adecuados para los menores.



Sincronización con Family Link: ofrece la opción de poder realizar ajustes en el control parental de la aplicación (ver pág. 8).

5. Proveedores de contenidos

NETFLIX



Dispositivo:    

Opciones de control parental disponibles en el servicio de Netflix.

FUNCIONES

STOP

Filtrado de contenidos: limita las series, películas o programas calificados para edades superiores a la establecida en cada perfil, y permite bloquear manualmente aquellos contenidos que consideras inadecuados.



Protección de la configuración: permite establecer un código PIN para proteger el acceso a los ajustes de la aplicación frente a modificaciones no deseadas.

EXTRAS






Perfiles de usuario: puedes establecer diferentes perfiles adaptados a su edad y madurez, donde se almanecerán las preferencias según contenidos que visualicen.



BUSCADOR DE GOOGLE



Dispositivo:   

Opciones disponibles en el buscador de Google.

FUNCIONES

STOP

Filtrado de contenidos: permite filtrar el contenido sexual explícito entre los resultados. Debe complementarse con nuestra supervisión, dado que no impide que el menor pueda acceder directamente a una página web o utilizar otro navegador desde el mismo dispositivo.

EXTRAS



Es necesario **configurar cada navegador y cada cuenta de usuario.**



5. Proveedores de contenidos

15/20

HBO



Dispositivo:    

Opciones de control parental disponibles en el servicio de HBO España.

FUNCIONES

STOP

Filtrado de contenidos: ofrece una sección KIDS con series, películas o documentales aptos para menores. Debe complementarse con nuestra supervisión, ya que no se diferencian los contenidos para los diferentes tramos de edad.



Protección de la configuración: permite establecer un código PIN para proteger el acceso a los ajustes de la aplicación o salir de la sección KIDS.



PRIME VIDEO



Dispositivo:    

Opciones de control parental disponibles en el servicio de Prime Video.

FUNCIONES

STOP

Filtrado de contenidos: permite establecer perfiles infantiles o con restricción por edad que adaptarán las sugerencias de contenido teniendo en cuenta su historial de visualización. El buscador ofrecerá resultados de contenidos calificados para menores de hasta 12 años.



Protección de la configuración: permite establecer un código PIN para proteger el acceso a los ajustes de la plataforma frente a modificaciones no deseadas.



Supervisión: esta herramienta debe complementarse con supervisión parental, dado que se muestran las descargas de contenido de todos los perfiles.

EXTRAS



Bloqueo de aplicaciones: permite restringir las compras en la tienda virtual de Prime Video mediante el PIN de restricción de compras (válido igualmente para la página web y la aplicación para móvil).

5. Proveedores de contenidos

16/20

ORANGE TV

Orange TV

Dispositivo:    

Opciones de control parental disponibles en Orange TV.

FUNCIONES

STOP

Filtrado de contenidos: permite visualizar contenido apto para la edad del menor, así como bloquear el acceso a contenido bajo demanda.



Protección de la configuración: permite establecer un código PIN para proteger el acceso a los ajustes de la plataforma frente a modificaciones no deseadas.



VODAFONE TV KIDS

Vodafone TV

Dispositivo:    

Opciones de control parental disponibles en Vodafone Kids.

FUNCIONES

STOP

Filtrado de contenidos: permite visualizar contenido apto para el menor atendiendo a su rango de edad desde la sección 'Modo Niños'.



Control de tiempo: permite controlar el tiempo de visionado y definir los horarios de acceso a los contenidos idóneos para el menor.



Protección de la configuración: permite establecer un código PIN para proteger el acceso a los ajustes de la aplicación frente a modificaciones no deseadas. Requiere la configuración de un PIN adicional en el decodificador para bloquear contenido no apto para niños.



5. Proveedores de contenidos

17/20

DISNEY+



Dispositivo:

Opciones de control parental disponibles en el servicio de Disney+.

FUNCIONES

STOP

Filtrado de contenidos: limita las series, películas o programas con rango de edad superior al establecido en el perfil de usuario infantil.



Protección de la configuración: permite establecer un código PIN o activar una pregunta de seguridad para proteger el acceso a los ajustes de la aplicación frente a modificaciones no deseadas.

EXTRAS



Perfiles de usuario: puede establecerse un perfil adaptado a una edad o rango concreto que permite reproducir los contenidos aptos para dicho perfil.

MOVISTAR+



Dispositivo:

Opciones de control parental disponibles en el servicio de Movistar +.

FUNCIONES

STOP

Filtrado de contenidos: opción que permite configurar la restricción de los contenidos a los que puede acceder el menor de forma personalizada o acorde a su edad.



Protección de la configuración: : permite establecer un código PIN para proteger el acceso a los ajustes de la aplicación frente a modificaciones no deseadas.



6. Opciones de redes sociales

18/20

YOUTUBE



Dispositivo:    

Opciones de control parental disponibles en los ajustes de la cuenta.

FUNCIONES



Filtrado de contenidos: permite descartar en las búsquedas contenido calificados para adultos, impidiendo a su vez acceder a los comentarios de todos los vídeos que se reproduzcan.



Protección de la configuración: puedes bloquear esta configuración si utilizas Family Link (ver pág. 8).

EXTRAS






Sincronización con Family Link: ofrece la opción de activar el modo restringido de la aplicación desde el dispositivo que actúa como administrador, impidiendo que el menor pueda desactivar las opciones de control establecidas (ver pág. 8).



FACEBOOK



Dispositivo:   

Opciones de bienestar digital disponibles en la aplicación de Facebook.

FUNCIONES



Control de tiempo: puedes configurar un recordatorio diario de tiempo, que avisará al menor cuando haya superado el tiempo establecido.



Supervisión: la aplicación crea un informe diario indicando el tiempo empleado en la red social.



Filtrado de contenidos: es posible configurar que la cuenta sea privada, restringir los comentarios de personas desconocidas (fuera de su lista de contactos) o bloquear comentarios.

EXTRAS



Opciones de privacidad: permite revisar el listado de amistades o configurar las notificaciones que recibirá el menor desde la aplicación.



6. Opciones de redes sociales

19/20

INSTAGRAM



Dispositivo:

Opciones de bienestar digital disponibles en la aplicación de Instagram.

FUNCIONES

STOP

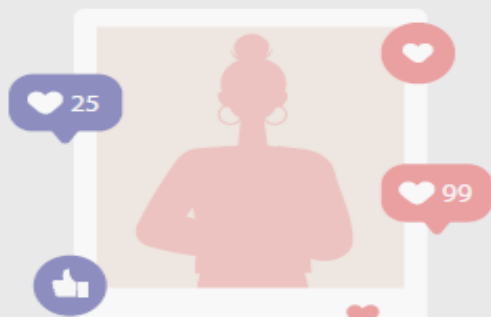
Filtrado de contenidos: es posible configurar la cuenta para que sea privada, restringir los comentarios de personas desconocidas (aquellas que no estén en su lista de contactos) o bloquear aquellos comentarios que contengan palabras concretas.



Control de tiempo: puedes programar un recordatorio diario de tiempo, que indique a tu hijo/a cuándo debe cerrar la aplicación.



Supervisión: la aplicación recoge todos los datos de uso en la red social, como las solicitudes de amistad, los inicios de sesión, el historial de búsqueda o la interacción con otros usuarios.



TIKTOK



Dispositivo:

Opciones de bienestar digital que ofrece la aplicación de TikTok.

FUNCIONES

STOP

Filtrado de contenidos: puedes establecer la cuenta como privada, restringir los comentarios o configurar un filtro que bloqueará aquellos que se consideren ofensivos o que contengan una palabra determinada. Con el modo restringido impide que se sugieran vídeos inadecuados para los menores.



Control de tiempo: permite configurar un periodo de tiempo diario para usar la aplicación.



Encuentra más información sobre estas herramientas en:

<https://www.is4k.es/de-utilidad/herramientas>

7. ¿Dónde podemos pedir ayuda?

20/20

1. Acude al servicio de atención al cliente.

La mayoría de los fabricantes ofrecen apoyo telefónico, chat de soporte o guías de ayuda para configurar las opciones de control parental y mejorar la seguridad del dispositivo.

2. Consulta el catálogo de herramientas.

Encontrarás fichas detalladas de cada herramienta, con enlaces de interés y descripciones paso a paso para configurarlas.

<https://www.is4k.es/de-utilidad/herramientas>

3. Contacta con la Línea de Ayuda en Ciberseguridad de INCIBE: 017.

Siempre que tengas dudas, ponte en contacto con nosotros por teléfono (017), mensajería instantánea en WhatsApp (900 116 117) y Telegram (@INCIBE017) o formulario web a través de:

