

SEGURIDAD DIGITAL EN CONSERVATORIOS: MANUAL DE AYUDA PARA MADRES/PADRES Y FAMILIAS

1.- Privacidad y seguridad en Internet (Introducción)

Los cambios provocados por la incorporación de las TIC en los procesos enseñanza-aprendizaje y de comunicación requieren que desde los centros educativos se diseñen acciones que velen por la seguridad de sus usuarios. El objetivo de este documento es servir de soporte a las familias en el uso de los recursos que proporciona la red, en las acciones administrativas, académicas y didácticas específicas en el contexto escolar del Conservatorio Profesional de Música de León.

La situación provocada por la irrupción de la pandemia (COVID19) y las directrices emitidas desde las administraciones en los procesos de gestión y comunicación con los ciudadanos han acelerado la incorporación de recursos tecnológicos que obligan a los usuarios a un proceso de adaptación constante y complejo, no exento de ciertos desequilibrios, que con frecuencia generan situaciones de estrés, malestar e inseguridad, en especial en colectivos y personas donde la brecha digital es más patente.

Las acciones aquí descritas se dirigen al aprovechamiento de los recursos disponibles en el Conservatorio Profesional de Música de León, en el Área de Programas Educativos – Integración de las TIC y en el Portal de Educación con la finalidad de ayudar a los usuarios madres, padres y familias de nuestra comunidad educativa en el uso seguro de internet en las actuaciones concernientes a los procesos educativos de nuestro centro.

El sector de madres, padres y familias es un colectivo que abarca un amplio espectro de usuarios en lo que habilidades digitales se refiere. El esfuerzo realizado por el personal de la administración y la secretaría del centro en la atención a las familias, la información sobre los recursos digitales disponibles en la web del centro, así como la labor realizada por el profesorado, en especial los tutores, han conseguido que estos usuarios, con carácter general, resuelvan todas aquellas actuaciones relacionados con la gestión de la matriculación, el uso de las credenciales de las plataformas Centrosnet y el Portal de Educación de los usuarios Alumnos y los procesos de información académico-institucional relevantes. Queda pendiente la normalización de uso de estos recursos a través de los propios perfiles de familias (madres/padres/tutores) en herramientas tan fundamentales como las Aulas Virtuales y la utilización preferente de los canales de comunicación proporcionados por el Portal de Educación. También resulta ineludible realizar una labor de concienciación en lo que se refiere al uso de imágenes, grabaciones y videograbaciones en los diferentes contextos y actividades del aprendizaje musical, fomentando el uso de recursos seguros, informando sobre las condiciones de seguridad y privacidad que deben darse en cada situación, favoreciendo un uso razonado y razonable de los recursos digitales e

incidiendo en las conductas que se deben evitar. A la espera de una dotación adecuada de recursos digitales para este colectivo en el nuevo edificio, el equipo directivo, el personal docente y el personal de administración y servicios, ejercerán las medidas expuestas en este plan, con el ánimo de superar las barreras impuestas por la brecha digital allí donde proceda, siendo conocedores de las implicaciones educativas que este hecho genera en los objetivos de aprendizaje de nuestro proyecto educativo. Este documento complementa la información contenida en el Documento de Bienvenida a Familias disponible en el siguiente enlace: http://conservatorioleon.centros.educa.jcyl.es/sitio/upload/BIENVENIDA_CPRM_US_LEON_familias_1.pdf

2.- Uso saludable de Internet

Seguridad y buenas prácticas

El marco educativo y social actual favorece la normalización del uso de Internet y los recursos digitales como herramientas para los procesos de aprendizaje, implementando la realización de una gran cantidad de tareas y actividades en los entornos digitales, espacios no exentos de ciertos peligros que padres, madres, tutores y educadores debemos conocer y prevenir. Para ello, nos debemos servir de todos aquellos recursos que desde las administraciones educativas y desde los centros educativos, se ponen a nuestra disposición para prevenir situaciones no deseadas e incluso delictivas con consecuencias gravemente perjudiciales para el desarrollo formativo y personal de nuestros alumnos. A continuación, exponemos una serie de recomendaciones con carácter general que pueden ayudarnos en esta nada fácil tarea de protección que como familias debemos asumir:

No dar información personal bajo ningún concepto a contactos poco conocidos o desconocidos, en cualquier plataforma como redes sociales, juegos en línea, foros, etc. Nunca se deben facilitar datos suyos, de su familia o amigos, además de cuidar con especial atención el envío o difusión en medios electrónicos de imágenes o vídeos personales y familiares.

Utilizar diferentes cuentas de correo electrónico. De esta forma los alumnos menores podrán tener un e-mail personal con el que operen normalmente para temas escolares y un segundo correo con el que puedan registrarse en otras plataformas. También es recomendable la supervisión de la difusión o envío de las direcciones de correo personales de los alumnos a usuarios desconocidos. En relación a esto último, es necesario educar a nuestros jóvenes en el respeto al uso de los datos personales de los demás, insistiendo en que deben evitar facilitar o difundir los datos de otros en los entornos digitales, si no se cuenta con los permisos correspondientes.

Rechazar correos spam o los que contengan archivos de descarga. Descargar archivos sin conocer su procedencia puede comprometer la seguridad de los dispositivos introduciendo virus o incluso rastreando información en los equipos.



Mantener la confianza familiar. Ganarse la confianza de nuestros jóvenes es fundamental para que nos expliquen sus actividades en Internet y las relaciones que establecen en la red para minimizar riesgos.

Fomentar el espíritu crítico en los menores. Es importante aprender a filtrar y contrastar la información que se encuentra en la red, no considerando y todo lo recibido como bueno. Conviene insistir en que el engaño y la manipulación de emociones son recursos habituales de la ciberdelincuencia.

Cuidar la imagen en Internet. A veces no tenemos en cuenta el alcance real de Internet y subimos imágenes comprometidas, sin ser conscientes de la cantidad de personas que las están viendo.

En las enseñanzas musicales debemos tener en cuenta que de manera habitual, trabajamos con grabaciones de audio y vídeo, tanto dentro del ámbito de aula como en las actividades extraescolares y complementarias, para lo cual, en el momento de la matriculación, se solicita a los alumnos/as y a sus padres o tutores legales cuando son menores de 16 años una autorización específica de uso de imágenes y voz para la difusión de actividades del centro. Para este último supuesto, la difusión de imágenes/vídeo/voz en las actividades extraescolares en la web y redes sociales del centro, recordamos que dicha autorización puede revocarse siempre que los interesados lo consideren oportuno y así lo soliciten por escrito en la secretaría del centro. Por esta situación tan específica, creemos necesario recordar las siguientes pautas sobre la realización de videograbaciones y materiales audiovisuales dentro de nuestro ámbito escolar:

En el contexto del aula: La utilización de videograbaciones para uso didáctico y docente es un recurso didáctico que no se puede prohibir, por lo que para el intercambio de estos materiales entre usuarios es altamente recomendable utilizar exclusivamente las aplicaciones que pone a disposición la Consejería de Educación a sus usuarios -esto es, Microsoft Teams o Microsoft Stream- o bien optar por el uso de dispositivos físicos tipo memoria USB, debiendo ser custodiado manteniendo las precauciones de seguridad, al igual que cualquier otro tipo de documentación académica. Deben evitarse otros medios como WhatsApp o aplicaciones de mensajería que no garanticen las condiciones de privacidad. La difusión de estos materiales para otros fines, como publicación de artículos de diferente tipos o difusión en canales como blogs, sitios web donde compartir vídeos o redes sociales está prohibido si no se tiene el correspondiente permiso de los interesados alumnos y/o padres/tutores donde proceda.

En el contexto de las actividades extraescolares o de aquellas otras en las que participen otros miembros de nuestra comunidad educativa: como ya se ha señalado en el momento de la matriculación, se solicitará el correspondiente permiso para la difusión de las actividades del conservatorio en la web del centro y en las redes sociales que tenemos activas (Facebook, Youtube, Twitter e Instagram), pudiendo revocarse dicha autorización en cualquier momento del curso, situación que deberá comunicarse por escrito en la secretaría del centro. Al igual que en el supuesto anterior, si estos materiales se utilizasen para otros fines, se deberá contar con una autorización específica,



que se solicitará por los profesores responsables o el equipo directivo. En este contexto, conviene recordar a los usuarios madres/padres/tutores legales y a los alumnos, que pueden realizar cualquier videograbación de estos actos para uso privado y personal siempre y cuando no implique a otros usuarios, no estando permitida la difusión de estos materiales (WhatsApp, Youtube, etc.) si no se cuenta con el conocimiento y consentimiento de los implicados en la actividad.

Procedimientos académicos y administrativos con el centro educativo: Recordamos a nuestros usuarios que en la web institucional pueden encontrar información actualizada sobre cómo activar los diferentes perfiles Madres/Padres y Alumnos, tanto en la plataforma Centrosnet como en el Portal de Educación. La activación del perfil Madres/Padres del Portal de Educación da acceso a las aulas virtuales Moodle. Cuando un/a docente habilite un aula o curso virtual, informará de la activación de este recurso a los sus alumnos y correspondientes familias, quedando esta situación reflejada en la programación didáctica correspondiente. De la misma forma, a los usuarios Madres/Padres de alumnos menores de edad, recomendamos que tengan acceso a las credenciales de las plataformas Educacyl y Centrosnet de sus hijos, ya que se pueden habilitar procedimientos administrativos de recogida de información o tramitación de gestiones, que solamente pueden hacerse a través de las aplicaciones informáticas que habilita la Consejería de Educación para tal fin (Formularios Forms, por ejemplo). Como en el resto de las administraciones educativas, todos los procedimientos administrativos de nuestro centro educativo pueden realizarse mediante los procesos de firma y certificado digital, sin perjuicio de seguir atendiendo estas acciones mediante la atención presencial. En referencia a las acciones educativas, docentes y didácticas que desarrollan nuestros profesores y tutores, cada curso académico se organizará un plan de contingencia específico cuyo resumen se publicará de manera permanente en la página de inicio de nuestra web. Dada la importancia que tiene la utilización de los certificados y firmas digitales en el ámbito de la comunicación y las gestiones con la administración, ofrecemos aquí un vídeo explicativo sobre cómo obtener el certificado digital: https://youtu.be/z_g4EBizgik

Finalmente, en lo que concierne a este punto, remitimos a algunos enlaces sobre seguridad digital que facilitan el conocimiento y la formación de los usuarios de nuestra comunidad educativa en relación a este aspecto tan vital de nuestra vida académica y personal:

Seguridad digital en el Portal de Educación:
<https://www.educa.jcyl.es/plandeseguridad/es/materiales/material-multimedia/videos-corta-duracion-informacion-difusion-promocion-uso-se>

Protección de datos de carácter personal en centros educativos:
https://www.educa.jcyl.es/es/lopd_guia_centros

Plan de Seguridad digital elaborado por el Área de Programas Educativos de la dirección Provincial de Educación de León:
<https://www.educa.jcyl.es/dpleon/es/area-programas-educativos-p/seguridad-confianza-digital>



Talleres para familias, elaborado por el Área de Programas Educativos de la dirección Provincial de Educación de León:
<https://www.educa.jcyl.es/dpleon/es/area-programas-educativos-p/seguridad-confianza-digital/talleres-familias>

INCIBE: Actividades para menores, padres y educadores:
<https://www.is4k.es>

3.- Plan estratégico educativo de seguridad y privacidad en la red.

Riesgos y propuestas antes incidentes

La realidad del uso de las tecnologías ha provocado la emergencia de varias amenazas y peligros a los que nos vemos expuestos los usuarios en la cotidianidad de nuestras actividades. Teniendo en cuenta que nuestra prioridad es proteger la privacidad y seguridad propias y de nuestros jóvenes, conviene alertar sobre algunos de estos riesgos:

Uso abusivo y adicción: Situación que produce una dependencia o uso excesivo provocando un aislamiento social frente a la familia o los compañeros, así como una disminución en la concentración y rendimiento académico del alumno.

Acceso a contenidos inapropiados: De carácter sexual, violento, racista o sexista, cuestiones estéticas (anorexia, bulimia, conductas de riesgo, etc.) contenido que vulnera el desarrollo emocional y personal de los menores.

Ciberacoso o cyberbullying: Ser acosado, insultado o amenazado por niños (cyberbullying pasivo). Acusar, insultar o amenazar a niños (cyberbullying activo) ser insultado por adultos, citas con desconocidos.

Acoso sexual: Ser objeto de acoso sexual.

Amenazas a la privacidad: Facilitar datos personales, difundir imágenes del alumno sin conocimiento, que el alumno grabe y difunda imágenes inapropiadas.

Amenazas técnicas: Virus, programas maliciosos, intrusión en cuentas de servicio web.

Para conocer con un poco más sobre las problemáticas aquí definidas, recomendamos el visionado de los siguientes materiales multimedia:
<https://www.educa.jcyl.es/plandeseguridad/es/materiales/material-multimedia/videos-corta-duracion-informacion-difusion-promocion-uso-se>

Para el uso correcto de los dispositivos electrónicos que utilizamos en el entorno familiar hay una serie de medidas o propuestas que los padres y educadores debemos tener en cuenta:

- Conocer Internet y saber cómo funciona.
- Establecer una comunicación abierta con los hijos, hablar sobre aspectos y conductas de la seguridad digital como un elemento más de nuestra convivencia personal y social.



- Educar en la auto-protección de la imagen personal y del derecho de la privacidad.
- Controlar la actividad de nuestros jóvenes en la red y en los dispositivos tecnológicos.
- Advertir de los riesgos y peligros potenciales que supone el uso indiscriminado de la tecnología en especial como forma exclusiva de ocio. Poner en conocimiento de nuestros hijos de las consecuencias del uso irresponsable de los recursos tecnológicos e Internet.
- Favorecer los espacios y los períodos de desconexión digital dentro del propio ámbito familiar.
- Concienciar a nuestros hijos y alumnos de que las conductas inapropiadas en el contexto digital tienen las mismas consecuencias legales que si se realizaran en el contexto de la vida real, insistiendo que nuestras acciones en el terreno tecnológico dejan una huella digital, con todas las implicaciones que ello conlleva para nosotros mismos y nuestro entorno más cercano.
- Mantenerse informado a través de páginas divulgativas solventes sobre ciberseguridad y uso seguro de Internet
- Utilizar programas de protección y control parental y realizar una supervisión de la información que de los mismos se deriva. Mantener actualizados los programas antivirus
- Limitar el acceso a carpetas y documentación que no atañe al alumno/a para la realización de su trabajo.
- Aplicar filtros en la navegación web. Impedir el acceso a redes externas que no sean necesarias para el desarrollo de su trabajo.
- Poner en conocimiento y denunciar cualquier abuso o indicio de conducta delictiva que se observe en el contexto virtual a quien corresponda según el caso (responsables de centros educativos, policía, etc.).
- Tomar conciencia de las consecuencias de compartir imágenes y datos personales en la web, en aplicaciones de mensajería y en redes sociales. Evitar compartir datos de cualquier tipo en espacios web no protegidos.
- Evitar compartir datos e imágenes de terceros, si no se tiene la correspondiente autorización.

En atención a esto consideramos necesario resaltar la formación de usuarios a través de los programas diseñados por administraciones educativas e instituciones como el INCIBE o Castilla y León Digital, que nos permitirán mejorar nuestra competencia digital:

- Talleres para familias DPE León Área de Programas Educativos:
<https://www.educa.jcyl.es/dpleon/es/area-programas-educativos-p/seguridad-confianza-digital/talleres-familias>

- CYL Digital: <https://www.cyldigital.es>
- INCIBE: Actividades para menores, padres y educadores: <https://www.is4k.es>.
- Canal Telegram de Alertas INCIBE al que uno puede suscribirse que ofrece información constante y actualizada sobre los diferentes riesgos emergentes en lo que a privacidad y seguridad digital se refiere.
- Oficina de Seguridad del internauta: <https://www.osi.es/es>
- Hijos digitales: <https://www.hijosdigitales.es/es/>
- Pantallas amigas: <https://www.pantallasamigas.net>
- Cuida TIC Salud Castilla y León - Proyecto Labyros: <https://www.somospacientes.com/noticias/asociaciones/tecnologia-como-fomentar-un-uso-adecuado-y-seguro-entre-los-menores/>

En el anexo final de este documento presentamos algunas infografías educativas con licencias Creative Commons elaboradas por estos agentes y dirigidas especialmente a las familias.

Protección de las infraestructuras y dispositivos personales

Técnicas eficientes

Además de lo descrito en los puntos anteriores pasamos a exponer algunas pautas y recursos que pueden ser de gran utilidad para proteger nuestros dispositivos.

- Mantener nuestros conocimientos y habilidades actualizados a través de páginas recomendadas en el epígrafe anterior.
- Proteger nuestros dispositivos con programas o aplicaciones antivirus: Kaspersky, Norton, McAfee, etc.
- Instalar en los dispositivos que utilicen nuestros hijos programas de control parental como Qustodio, Kaspersky Safe Kids, MmGuardian, Norton Family Premier, etc.
- Evitar el uso de redes wifi públicas, en especial para actividades personales delicadas.
- Utilizar contraseñas seguras para acceder a nuestras aplicaciones que combinen una serie de unos 8-12 caracteres aleatorios de letras mayúsculas, minúsculas, números y otros caracteres alfanuméricos y cambiarlas periódicamente.
- Realizar regularmente copias de seguridad de nuestra información relevante.
- Impedir que terceros accedan a nuestros dispositivos electrónicos.
- Solicitar ayuda a soportes acreditados ante situaciones delictivas y de abuso.



- Cumplir indicaciones y seguir las recomendaciones del profesorado, tutores, personal de administración en relación al uso de dispositivos y recursos electrónicos en el entorno escolar que corresponda.
- Participar de las encuestas de funcionamiento que se proponen desde el centro.
- Conocer y mantener el contacto con los representantes de los sectores padres/madres, alumnos del Consejo Escolar y con el AMPA del centro.

Ante una posible situación de abuso o acoso

Recordamos que en nuestro *Proyecto Educativo* y en nuestro *Plan TIC* de centro disponibles a través de nuestra web institucional: <http://conservatorioleon.centros.educa.jcyl.es/sitio/>, figuran los principios educativos del uso de las TIC y otros recursos tecnológicos con las finalidades didácticas propias de nuestro particular contexto escolar; y que dentro del apartado *Disciplina Escolar* del *Reglamento de Régimen Interno* se establece la tipología de conductas contrarias a la convivencia relacionadas con el uso inadecuado de las herramientas y recursos TIC, con sus correspondientes sanciones. No obstante y teniendo en cuenta el alcance que de este tipo de acciones se puede derivar, recordamos que ante cualquiera de las situaciones de abuso, acoso o agresión virtual que se detecten en nuestro entorno educativo siempre se debe informar a los responsables del centro (profesores, tutores y equipo directivo), además de hacer uso de los recursos que ofrece la administración educativa, el INCIBE e incluso los servicios de ciberseguridad de la policía cuando la situación lo requiera, evitando la cronificación de situaciones perniciosas para el desarrollo personal de nuestros hijos y alumnos.

ANEXO: INFOGRAFÍAS INFORMATIVAS DE SEGURIDAD DIGITAL PARA FAMILIAS

LA SEGURIDAD DE TUS HIJ@S EN LA RED

Explica a tu hijo/a que una contraseña jamás debe compartirse

Enseñale a comunicarse de forma segura y respetuosa

Conoce los servicios de Internet que suele usar tu hijo/a y dale a conocer nuevos sitios

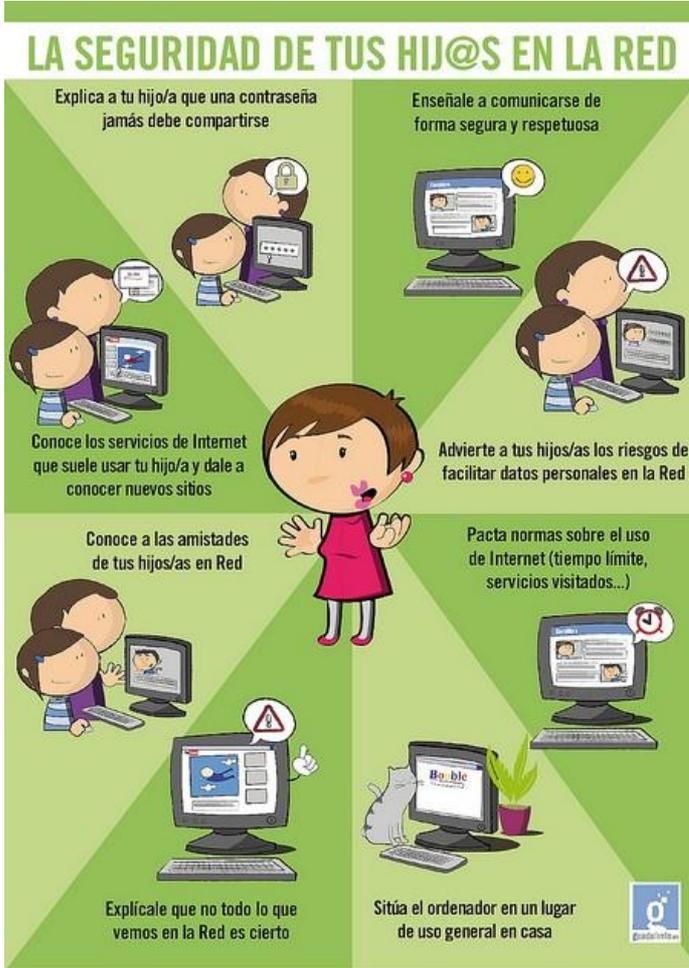
Advierte a tus hijos/as los riesgos de facilitar datos personales en la Red

Conoce a las amistades de tus hijos/as en Red

Pacta normas sobre el uso de Internet (tiempo límite, servicios visitados...)

Explícale que no todo lo que vemos en la Red es cierto

Sitúa el ordenador en un lugar de uso general en casa



DECÁLOGO: USO DE LAS IMÁGENES EN LA RED



- Cuida las imágenes que publicas, dan más información de lo que imaginas.
- Tus hijos/as tienen derecho a su intimidad. Su difusión puede significar un delito.
- Pide permiso antes de etiquetar a otras personas en las imágenes de las redes sociales.
- No solo ve las fotos tu familia, hay mucha gente en las redes observando. Cuidado.
- Tapa las webcam, pueden ser activadas remotamente aunque estén apagadas.
- Recuerda que pierdes el control de tus imágenes cuando las subes a la red.
- Publica lo que no te importaría que vieran tus padres.
- Una imagen erótica es siempre comprometida. No la envíes.
- Las empresas buscan información sobre ti en las redes sociales.
- Recuerda que las redes sociales son una ventana abierta a tu intimidad. Presévala.

GRUPO DE TRABAJO DE TIC DEL COPCYL
WWW.COPCYL.ES



TU AYUDA EN CIBERSEGURIDAD







Cuida tu privacidad



¿Tienes una cuenta de Google?

- ✓ Aprende a configurar tu cuenta
- ✓ Realiza búsquedas de forma segura
- ✓ Sácale el mejor partido al Asistente de Google



https://files.incibe.es/is4k/is4k_guia_controles_parentales.pdf



LÍNEA DE AYUDA

LÍNEA DE REPORTE



CIBERSEGURIDAD PARA FAMILIAS





FAMILIA CIBERSEGURA #CiberCOVID19

MEDIACIÓN PARENTAL

- Prepárate para guiarle**
 - ✓ Conoce el **entorno** y sus **motivaciones**.
 - ✓ Comunicación, **acompañamiento** y supervisión.
 - ✓ Eres su **ejemplo** a seguir.
- Prepara su entorno TIC**
 - ✓ **Reglas y límites** ajustados a su madurez.
 - ✓ Apóyate en herramientas de **control parental**.
 - ✓ **Contenidos positivos** y de calidad.
- Prepárale para el mundo digital**
 - ✓ Desarrollo de una **identidad digital** positiva.
 - ✓ **Protección de datos**, evitar virus y fraudes.
 - ✓ **Pensamiento crítico** ante noticias falsas.
 - ✓ **Relaciones** respetuosas y saludables.
 - ✓ **Uso equilibrado** de las TIC.

www.is4k.es/ciberCOVID19

<https://www.is4k.es/sites/default/files/contenidos/materiales/Campanas/c11-covid19/is4k-competencias-digitales.pdf>

FAMILIA CIBERSEGURA

EDÚCALE PARA SER UN BUEN CIUDADANO DIGITAL

- Frena el ciberacoso**
 - ✓ **No utilices** Internet para **atacar o herir** a los demás.
 - ✓ **Ponte en el lugar** de la otra persona.
 - ✓ **Respetar** su identidad digital.
 - ✓ **Actúa** ante situaciones de acoso.
- No alimentes al trol**
 - ✓ **Expresa tu opinión** con respeto.
 - ✓ **No respondas** a mensajes de odio.
 - ✓ **Evita reaccionar** de forma impulsiva.
 - ✓ **Reporta las conductas** inadecuadas.

www.is4k.es/ciberCOVID19

FAMILIA CIBERSEGURA #CiberCOVID19

FOMENTANDO EL PENSAMIENTO CRÍTICO EN FAMILIA

¡Pequeñas prácticas en familia para **promover la reflexión en Internet!**



Utilizar dispositivos, aplicaciones y juegos **con sentido común.**
 Buscar **contenidos positivos** y de calidad.
 Identificar **información fiable** y aprender a gestionarla.
 Reaccionar de forma **responsable** ante bulos y noticias falsas.
 Analizar las **estrategias publicitarias** en Internet.

www.is4k.es/ciberCOVID19






SEIS PASOS PARA LA DEESCALADA DIGITAL EN FAMILIA



- 1 Obsérvate**
Identifica qué cosas haces con el móvil, las redes sociales o los videojuegos que antes del confinamiento no hacías
- 2 Conoce bien tus nuevas rutinas**
Trata de saber cuándo, cómo y hasta dónde las has incorporado
- 3 Establece tus objetivos**
Fija de forma realista pero ambiciosa la nueva situación deseada tras el proceso de desescalada
- 4 Ayúdate de una estrategia**
Cambia costumbres, pon en práctica trucos que te alejan de la pantalla, mide los avances...
- 5 Comparte tu propósito**
Haz participe a tu entorno de tu voluntad en cambiar ciertos hábitos y pídeles colaboración y comprensión
- 6 Revisa tu plan**
Periódicamente mide los avances, identifica y cambia lo que no va bien, reajusta las metas y prémiate por los logros

www.desescaladadigital.com

© 2020 PantallasAmigas



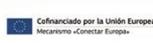
<https://youtu.be/pNEP9sSL1i0>

CÁMARAS RESPONSABLES PERMITIDAS

FAMILIARES Y AMIGOS QUE ACUDÍS AL CENTRO ESCOLAR:

- Fotografía solo a tus familiares y amigos (y mejor fuera del centro).** Si quieres incluir a los demás, mejor una foto de grupo.
- No compartas imágenes en las que se vean a otras personas, adultas o menores. Para difundirlas necesitas su permiso expreso.**
- Conoce y respeta las normas.** Pregunta en qué momento puedes hacer fotos.
- Si alguien te pide que borres una foto en la que aparece, hazlo y respeta su decisión.**

¿TIENES DUDAS?
900 116 117
Línea de ayuda en ciberseguridad incibe_





ACUERDO PADRES-HIJOS PARA EL USO DEL TELÉFONO MÓVIL



- 1 Un teléfono es una gran responsabilidad. Te regalamos uno porque confiamos en ti. ¿A que tus papás son geniales?
- 2 Quizá algún día revisemos juntos tu teléfono. Prometo no fisionear en tus llamadas y mensajes pero podré revisar su configuración y su estado de seguridad y vulnerabilidad, así como las aplicaciones instaladas siempre que lo considere necesario. Tú estarás delante y de este modo aprenderemos juntos.
- 3 Si suena, cógelo. Di "hola". Sé educado/a. Coge siempre, siempre, la llamada de mamá o papá.
- 4 No debe interferir en tus deberes o en tus horas de sueño. Podrás utilizarlo en cualquier momento, pero siempre deberás gestionarlo correctamente tus tiempos. No permitas que influya negativamente en tu rendimiento escolar, en tus horas de sueño o en cualquier otra actividad.
- 5 Mantén el teléfono en buen estado de "salud". Y con ello me refiero a varias cosas: no instales aplicaciones de orígenes no oficiales, no modifiques su seguridad con cambios que lo vuelven peligroso (jailbreak, root), mantenimiento debidamente actualizado y utiliza algún antivirus.
- 6 Instalaremos filtros parentales, pero lo haremos juntos y siempre de común acuerdo. Te ayudarán a protegerte de zonas de Internet a las que no debes acceder porque son peligrosas. También configuraremos juntos lo necesario para rastrearlo o borrarlo en caso de pérdida.
- 7 Sigue escrupulosamente las normas del colegio. Nunca utilices el teléfono en horario escolar, a menos que esté expresamente permitido por el profesor/a o tutor/a para realizar alguna actividad. Durante tu tiempo de descanso, recuerda lo importante que es relacionarse con los demás y no aislarse socialmente, conversa y habla con la gente y con tus amigos en persona.
- 8 No uses el teléfono para mentir, hacer tonterías o engañar a otro ser humano. No te involucres en conversaciones que sean dañinas para los demás. Sé un buen amigo.
- 9 No envíes mensajes, correos electrónicos o digas nada a través del teléfono que no dirías en persona o en voz alta y en presencia de tus padres. Autocensurate.
- 10 Las redes sociales. Facebook, Twitter, Instagram y otras plataformas online tienen un mínimo de edad legal de 14 años y no puedes utilizarlas hasta cumplir esa edad. Si aún así logras hacerle con alguna cuenta, prométe que no aceptarás nunca una amistad con personas desconocidas y que nos consultarás cualquier duda o situación que te resulte sospechosa o extraña.

- 11 Nada de guarraditas. No envíes ni recibas imágenes de partes íntimas tuyas ni de otras personas. No te rías. Algún día estarás tentado/a de hacerlo a pesar de tu gran inteligencia. Es arriesgado y puede arruinar tu vida de adolescente, joven y adulto. El ciberespacio es más poderoso que tú y es imposible hacer que algo de esa magnitud desaparezca, incluyendo una mala reputación.
- 12 Silencialo cuando te encuentres en lugares públicos. Especialmente en restaurantes, en el cine o mientras hablas con otro ser humano. No eres una persona maleducada, no dejes que el teléfono te cambie.
- 13 Si tienes cualquier problema, duda o te ves acosado por alguien a través de Internet, debes contárnoslo rápidamente, de este modo encontraremos una solución cuanto antes y juntos, nosotros no te refiriemos. No hacerlo solo aumentará el problema.
- 14 No compartas fotografías con información personal. Piensa que las imágenes pueden dar más información de la que parece. Evita publicar fotos y videos que permitan identificar lugares donde sueles estar, como tu casa, el colegio u otros lugares que frecuentas. Personas con malas intenciones podrían aprovechar esa información para hacerte daño a ti, a tus amigos o a tu familia.
- 15 No vivas para el teléfono. Es una gran herramienta y te puede ser útil e incluso imprescindible en muchas ocasiones. Pero utilízalo con sentido común y no dejes que absorba todo tu tiempo. En el mundo hay muchas cosas que ver y experimentar y ahora tienes la suerte de poder hacerlo junto a tu teléfono.
- 16 Tienes el mayor acceso a la música que ha existido jamás, aprovéchate de ello. Escucha lo que te guste, pero no olvides investigar otros campos, como la música clásica o de otras épocas más recientes. Amplía tus horizontes. Pregúnta.
- 17 Puedes utilizar juegos, pero sin abusar. Juega a juegos interesantes, que te hagan pensar, que te hagan razonar No te limites a juegos monótonos y adictivos que están de moda y que poco o nada aportan a tu imaginación. No te olvides de experimentar.
- 18 Meterás la pata. Te quitaré el teléfono. Nos sentaremos y hablaremos sobre ello. Te enfadarás conmigo y contigo mismo. Nos volveremos a sentar a hablar sobre ello. Tú y yo estamos aprendiendo sin cesar. Estamos de tu parte. Estamos juntos en esto.



He leído detenidamente este manual de uso/acuerdo con los padres y entiendo todas las responsabilidades que conlleva, no solo las ventajas. Al firmarlo, las asumo y me comprometo a cumplirlas.

Fecha _____ de _____ de _____

Nombre hijo@ _____

Firma

Padre/Madre _____

Firma

