GUÍA DE USO SEGURO Y RESPONSABLE DE LAS TIC

CRA EL PINAR
CURSO 23-24

ÍNDICE

1. PRINCIPIOS SOBRE EL BUEN USO DE LAS TIC

El buen uso de las Tecnologías de la Información y Comunicación (TIC) es fundamental para aprovechar sus beneficios mientras se minimizan los riesgos y desafíos asociados, y por ello, debemos indicar a nuestros hijos/as, familiares y alumnos/as cuáles son estos peligros.

Entre los principios fundamentales cabría destacar:

- **Ética digital:** Respetando la privacidad de otros/as, evitando el acoso en línea y siendo consciente de las consecuencias de tus acciones en entornos digitales.
- **Respeto a la privacidad:** Protegiendo la información personal y respetando la de los demás.
- **Seguridad en línea:** Manteniendo protegidos tus dispositivos y cuentas mediante contraseñas robustas y actualizaciones regulares de software.
- **Responsabilidad digital:** Siendo consciente de tú impacto en línea. Piensa antes de publicar cualquier contenido.
- **Alfabetización digital:** Desarrollando habilidades digitales para comprender y utilizar eficazmente las TIC, por ejemplo, buscando información, utilizando herramientas digitales o evaluando la fiabilidad de las fuentes, siempre de forma segura.
- **Uso equilibrado:** Manteniendo un equilibrio saludable entre el tiempo en línea y fura de línea, evitando la dependencia excesiva.
- **Colaboración y participación:** Fomentando la participación de manera constructiva y utilizando las TIC como herramienta para aprender y compartir conocimientos.

Además, creemos conveniente destacar más principios de manera más concreta con los destinatarios de dicha guía.

1.1 ALUMNADO

a) Cuidar su correcta posición corporal al usar cualquiera de estos dispositivos.

b) Ser prudentes y no concertar encuentros con personas que no conocen y que les proponen quedar a solas.
c) Tener respeto a otros usuarios, evitando las burlas, difamaciones, humillaciones y agresiones.
d) No suplantar la identidad de nadie en la red.
e) No compartir datos personales en chats, redes sociales o por email (imágenes, datos, perfiles, números de teléfono...).
f) No publicar información de otra persona sin consentimiento.
g) Saber que tienen el deber de pedir ayuda a una persona mayor cuando algo no les guste o lo consideren peligroso para chicos o chicas de su edad, incluso si no les afecta personalmente.

1.2 FAMILIA

Es muy importante la contribución de las familias en los siguientes principios:

a) Estar al día en todo lo relativo a internet y nuevas tecnologías, ya que cuanta más información mejor se podrá atender a los menores.
b) Acordar unas normas de uso claras, estableciendo y haciendo cumplir un horario.
c) Crear un espíritu crítico sobre la información que aparece en la red y explicarles que no todas las web tienen la misma credibilidad.
d) Enseñar a utilizar motores de búsqueda y contrastar varias fuentes sobre un mismo campo, evitando el “corta y pega”.
e) Fomentar el diálogo sobre hábitos de utilización de las TIC y sus riesgos. Es importante que el menor sienta que cuando le suceda algo extraño o le incomode, puede decírselo a sus padres sin sentirse culpable.
f) Utilizar filtros de control de acceso a la red y programas de control parental, con los que se evitará que los menores accedan a páginas de contenido inapropiado.
g) Tener el ordenador en una zona de uso común, ya que facilitará tanto la supervisión del tiempo de utilización como las situaciones que puedan resultar incómodas para el menor.

h) Cuidar la postura respecto al ordenador, siguiendo pautas como mantener la espalda recta, acostumbrar al menos a levantar la vista de la pantalla cada 15 o 20 minutos y situándole a una distancia mínima del monitor/pantalla del doble de la diagonal de la pantalla.
i) Enseñarles en qué consiste la privacidad, que los datos personales son información sensible y que pueden ser utilizados en su contra.
j) Explicarles que detrás de cada apodo hay una persona y que siempre hay que ser educado.

1.3 PROFESIONALES DE LA ENSEÑANZA

a) Controlar el tiempo que se conectan a internet en clase.
b) Fomentar la utilización de una posición correcta para el cuerpo frente al ordenador, siguiendo pautas cómo mantener la espalda recta y reposada la zona lumbar, acostumbrar al menos a levantar la vista de la pantalla cada 15 o 20 minutos y situándole a una distancia mínima del monitor/pantalla del doble de la diagonal de la pantalla.
c) Fomentar el respeto a otros usuarios, evitando las burlas, difamaciones y agresiones.
d) Enseñar a navegar por internet de forma segura, accediendo solo a contenidos aptos para su edad.
e) Crear un espíritu crítico sobre la información que aparece en la red y explicarles que no todas las web tienen la misma credibilidad.
f) Enseñar a utilizar motores de búsqueda y contrastar varias fuentes sobre un mismo campo, evitando el “corta y pega”.
g) Advertir del derecho a la privacidad de la información personal del alumnado y a que no sea difundida sin su consentimiento por la red. Hay que tener cuidado con los datos que se comparten tanto en chat, redes sociales o por email (imágenes, datos, perfiles, números de teléfonos.), leyendo atentamente las condiciones de las páginas a las que nos suscribimos.
h) De la misma manera, explicar que no se puede publicar información de otra persona sin su consentimiento.

2. RIESGOS EN EL USO DE LAS TIC

1. Problemas Psicológicos y Académicos:

El uso excesivo de las Tecnologías de la información y la comunicación (TIC) puede llevar a problemas psicológicos como ansiedad, estrés y falta de concentración. En el ámbito académico, la distracción constante puede afectar el rendimiento y el tiempo dedicado al estudio.

2. Problemas Sociales:

Las TIC pueden contribuir a la desconexión social, generando problemas de comunicación interpersonal. Además, la exposición a contenidos negativos en línea puede afectar las relaciones interpersonales.

3. Problemas para la Salud Física:

El uso prolongado de dispositivos electrónicos puede ocasionar problemas físicos, como fatiga visual, dolores musculares y trastornos del sueño. Además, el sedentarismo relacionado con el uso de las TIC puede contribuir a problemas de salud a largo plazo.

4. Consejos Generales para Evitar Problemas:

- ⇨ Establecer límites de tiempo: Definir periodos específicos para el uso de dispositivos y redes.
- ⇨ Fomentar el equilibrio: Promover actividades fuera de las TIC para mantener un estilo de vida saludable.
- ⇨ Educación digital: Capacitar sobre el uso responsable y seguro de las TIC.
- ⇨ Monitoreo parental: Supervisar el acceso de los niños a las TIC para garantizar un entorno seguro.
- ⇨ Descansos regulares: Incorporar pausas durante el uso prolongado de dispositivos para prevenir problemas físicos.

La adopción consciente y equilibrada de las TIC es esencial para mitigar estos riesgos y aprovechar sus beneficios de manera saludable y productiva.

3. OTROS PROBLEMAS: CIBERDELITOS

En este apartado se aborda un listado de problemas que quizás sean los que más preocupación despiertan entre los docentes y entre los padres.

3.1 VIOLACIÓN DEL DERECHO A LA IMAGEN E INTIMIDAD. PRIVACIDAD

Este problema es de vital importancia, ya que el desconocimiento del derecho a la privacidad es la base de otras situaciones mucho más graves.

Todo el mundo tiene derecho a la protección de sus datos personales, así como tenemos el deber de respetar la privacidad de otros. No por ser menor se está eximido de estas responsabilidades y no por desconocer las leyes, se puede incumplirlas.

Nadie puede pedir a un menor sus datos personales sin el consentimiento de sus padres si el menor no tiene todavía los 14 años. Solo los mayores de 14 años pueden autorizar el tratamiento de sus datos de carácter personal.

Los peligros de la violación de la privacidad son, entre otros, (algunos de ellos serán tratados en apartados posteriores), los siguientes:

- Ciberacoso o ciberbullying
- Sexting
- Acoso sexual o grooming
- Estafa
- Acceso a cuentas de correo, perfiles de redes sociales, etc.
- Spam, Malware o programas maliciosos que se instalan en el equipo y recogen datos de forma opaca
- Etiquetado de fotos en redes sociales para comprometer o perjudicar a la víctima
- Suplantación de la identidad en redes sociales
- Distribuir, sin querer y/o sin saberlo, imágenes o vídeos de pornografía Infantil.

¿Cómo prevenirlo?

Consejos para menores:

- Ser muy cuidadosos al compartir datos personales propios o ajenos, muy especialmente las imágenes.
- Internet no significa anonimato.
- Utilizar contraseñas seguras.
- Es mejor usar un nick o seudónimo que el nombre propio en entornos que no sean absolutamente seguros.
- Nunca se deben revelar datos personales, como dirección, DNI, teléfono, números de cuentas bancarias, etc., a desconocidos, o en situaciones de comunicación que no hagan imprescindible su conocimiento por la otra persona.
- En el uso de dispositivos móviles, revisar los permisos de las aplicaciones.

Consejos para padres y educadores:

- Hacerles ver a los menores que si revelan datos personales y ceden imágenes o vídeos personales a desconocidos tienen mayor probabilidad de ser víctimas de ciberacoso, acoso sexual, suplantación de identidad, etc.
- Advertirles de no compartir contraseñas con nadie.
- Ayudarles en la medida de lo posible en el uso de la seguridad en redes sociales, foros, etc.
- Hacerles reflexionar a la hora de publicar sobre quién verá su información.
- Hacerles ver la importancia de su reputación y comportamiento en la red y las consecuencias que de ello se pueden derivar de cara al futuro personal y profesional.
- Asesorarles sobre los riesgos de la instalación en los dispositivos móviles de aplicaciones que demanden permisos no coherentes con la utilidad para la que han sido creadas.

- Vigilar si se producen cambios de comportamiento en los menores, si experimentan síntomas físicos inusuales (molestias, dolores…), rechazo repentino a estar con amigos o asistir al centro escolar, o una bajada repentina del rendimiento escolar, por si estuviese relacionada con situaciones de acoso.

¿Qué hacer si se producen problemas? Un caso especial: las redes sociales

Una red social en internet no es más que una plataforma o portal web a través del cual sus usuarios se mantienen en contacto y comparten intereses, opiniones, multimedia, etc. Los usuarios, al darse de alta, pueden personalizar y administrar su perfil.

Existen muchas redes sociales, entre las más populares se encuentran:

- Facebook
- Twitter
- Instagram
- Snapchat

Un criterio para agrupar las redes sociales podría ser el interés que el usuario persigue una vez es miembro:

- **Interrelación en general:** Facebook, Twitter, Google+, HiS.
- **Interés profesional:** Linkedin
- **Interés por una actividad particular:** Pinterest, Flickr, YouTube, etc.

Las redes sociales pueden ofrecer una serie de ventajas a los usuarios:

- Potencian la comunicación de los participantes con su entorno y, por tanto, las relaciones personales.
- Son un lugar de intercambio de opiniones y de intereses.
- Fomentan la colaboración entre los miembros de una comunidad, ya sea con el fin de ayudar o de elaborar trabajos de forma colaborativa.
- Promueven el uso de herramientas tecnológicas.
- Son una fuente de información continua y actualizada.

Pero también su uso conlleva riesgos:

- Riesgo de difundir datos personales y privados.
- Los menores son vulnerables a sufrir ciberdelitos, al aceptar en su comunidad a usuarios que no conocen personalmente.
- Muchas de las acciones personales que el usuario va seleccionando quedan registradas y almacenadas durante mucho tiempo.
- Fomentan comunidades de conocidos y amigos virtuales que están totalmente desconectadas con el mundo real.

Muchas de las redes actualmente más usadas poseen una política para impedir el registro de usuarios demasiado jóvenes, como consecuencia de la normativa internacional COPPA, han añadido un lugar donde informar sobre abuso dentro de la red, botones o funcionalidades destinadas a denunciar abusos y falsedades, o han hecho más fácil la configuración de la privacidad dentro del perfil del usuario.

En cualquier caso, la responsabilidad final del uso de la red social recae **en el mismo usuario**, o, en el caso de un menor, en sus padres, quienes deben velar por la seguridad y privacidad de sus hijos cuando acceden a ellas, los datos que deben proporcionar y las cláusulas que aceptan al realizar el registro.

3.2 CIBERBULLYING

¿Qué es?

Se trata del acoso (insultos, chantaje, humillación, vejaciones…) entre iguales, mediante el uso de las nuevas tecnologías.

El acoso escolar ha existido desde siempre, pero con las nuevas tecnologías se abre una nueva vía para que los acosadores actúen. Esta situación ocurre por la desinformación de los propios menores sobre la repercusión de realizar este tipo de actos a través de la red, pero también por la inacción de quienes contemplan estas acciones sin denunciarlas. No es lo mismo insultar en el patio del colegio que hacerlo a través de la red; la difusión es mayor y las repercusiones también, ya que se extienden en el espacio y en el tiempo.

Para considerar el ciberbullying como tal se deben tener en cuenta estos aspectos:

1. Se desarrolla entre iguales, de un menor o de un grupo de menores a otro. Nunca de un adulto a un niño.

2. Tiene lugar en un entorno TIC.

3. No es un hecho aislado, sino que es reiterado y mantenido en el tiempo.

4. Se basa en la difamación de la víctima, sobre la que se vierten falsas acusaciones o informaciones vejatorias y difamatorias, que persiguen excluirla de sus grupos sociales por la vía del rechazo o de la vergüenza.

5. Con frecuencia, los acosadores implican a terceros, inicialmente pasivos, para que participen del hostigamiento.

6. No es de índole sexual ya que, en ese caso, se considera grooming.

El ciberbullying da pie al anonimato, sensación que, efectivamente, proporciona internet, pero hay que advertir que siempre se puede detectar desde qué equipo informático y lugar se lleva a cabo una determinada actividad.

¿Cómo reconocerlo?

• Descubrir un perfil falso, que la víctima no ha creado (a veces aparece incluso con su foto) a su nombre, en el que se vierten datos personales y aspectos falsos sobre la misma.

• Recibir amenazas, insultos a través de SMS, correos electrónicos, mensajería multiplataforma (WhatsApp, Line, etc.) de forma reiterada.

• Usurpar fotografías comprometidas de la víctima (reales o realizadas mediante montaje), datos personales y distribuirlos por la red avergonzándola.

• Apropiarse de datos de acceso a chats, foros, correo electrónico, mensajería multiplataforma, etc. y usarlos de manera indiscriminada, ver- tiendo mensajes ofensivos, etc., para hacer creer que la víctima es la responsable de toda esa actividad.

¿Se puede prevenir?

En el caso de los menores:

• Usar un nick o seudónimo que sea conocido por sus amigos más cercanos y familiares, evitando difundir sus datos personales reales.

• Configurar adecuadamente el grado de privacidad de los perfiles sociales, de modo que la información personal no pueda ser conocida por personas ajenas al círculo más próximo.

• Ser prudentes en la aceptación de invitaciones o peticiones de amistad en las redes sociales.

• Tener especial cuidado con las imágenes, vídeos que se vayan a publicar en plataformas o redes sociales, ya sean propias o de otras personas, consultando y solicitando consentimiento, previa publicación de las mismas, a las personas afectadas. Evitar siempre enviar esos archivos multimedia a personas desconocidas.

• Evitar en la medida de lo posible la difusión de datos personales reales.

• No responder a las provocaciones.

• No establecer ningún tipo de relación virtual con personas a las que no se conoce personalmente.

• Comunicar de inmediato a padres o a educadores que se está siendo víctima de amenaza, chantaje, coacción, insultos, injurias o calumnias. En el caso de los padres:

• Establecer normas sobre el uso de ordenadores y dispositivos móviles y acceso a internet.

• Colocar el ordenador en zonas comunes del hogar, con el fin de conocer el tiempo de uso de los mismos, su actividad en la web.

• Establecer una comunicación con el menor e instruirle acerca de los peligros que supone la difusión de imágenes y datos personales en la red, así como de las consecuencias que conllevan conductas poco adecuadas y agresivas hacia otras personas.

• Mantener una supervisión periódica de los dispositivos y cuentas de servicios que usa el menor para conocer su actividad: sitios web que visita, historial de búsqueda, etc.

En el caso de los profesionales de la enseñanza:

• Incluir actividades relacionadas con la prevención y detección del ciberbullying en el Plan de Acción Tutorial y en el Plan de Convivencia del Centro acerca del buen uso y el mal uso de internet, ordenadores y dispositivos móviles.

• Reflexión sobre los riesgos de internet, ordenadores y dispositivos móviles.

• Tomar conciencia de qué es el ciberbullying y sus consecuencias.

• Análisis del rol del observador pasivo que ve lo que ocurre y no actúa.

• Fomentar la reflexión entre el alumnado de las diferencias entre chivar y denunciar.

. Realizar dinámicas que permitan reconocer los distintos roles que participan en un caso de ciberbullying (víctima, acosador, observador…).

• Establecer protocolos de actuación que favorezcan la detección del ciberacoso y estandaricen las acciones que, ante un caso, deban realizar los distintos estamentos del centro educativo.

¿Qué hacer?

Para menores:

• Contar de inmediato a los padres el caso y, si se ha venido desarrollando en el ámbito del centro educativo, al tutor.

• No borrar ningún rastro del acoso recibido, ya que es una prueba del mismo.

Para profesionales de la enseñanza:

Si el ciberacoso procede del entorno escolar:

• Informar al equipo directivo, al orientador y al tutor para aplicar el apoyo necesario al alumno, tanto si es víctima, acosador u observador.

• Aplicar los protocolos de actuación que el centro pudiese tener para estos casos.

• Recurrir a organizaciones especializadas en acoso escolar.

• Informar a los padres de todos los menores implicados en el suceso, así como proporcionar información a la víctima y a su familia sobre las diferentes posibilidades de que disponen para denunciar.

Para las familias/ tutores:

En este caso, las familias pueden encontrarse con que su hijo ha sido víctima, agresor u observador. En cualquier caso:

• Se debe escuchar al menor y dejar que exponga cuanto desee sobre el asunto.

• Comprobar que se trata de una situación real y no es producto de su imaginación. En ningún caso arrojar dudas injustificadas sobre la situación relatada por el menor.

• Intentar aplicar alguna estrategia para detener el daño que pueda estar recibiendo u originando el menor.

• Si el hecho se ha producido en el ámbito escolar, ponerse en contacto con el tutor del menor y solicitar información y una intervención por parte del centro.

• Denunciar ante las autoridades.

3.3 GROOMING

¿Qué es?

Bajo el nombre de grooming se incluye toda actividad llevada a cabo por cualquier usuario adulto que intenta contactar con menores con fines sexuales como conseguir imágenes del menor desnudo o realizando actos sexuales o incluso puede perseguir establecer un contacto directo con finalidad sexual con el menor.

Al principio, el acosador contactará con la víctima haciéndose pasar por otra persona, entablando entonces una relación más estrecha con ella, hasta que llega a convencerla para realizar fotografías comprometidas. Entonces se inicia una fase cruel de chantaje donde el menor es amenazado con difundir las imágenes (sextorsión) si no cumple los caprichos del acosador, quien en casos extremos puede exigir una cita con el menor.

¿Se puede prevenir?

Recomendaciones para evitar esta situación

Para el menor:

- Usar perfiles privados en redes sociales.
- No aceptar invitaciones, contactos o comunicaciones de personas que no conozca personalmente.
- No revelar datos personales íntimos ni mostrar imágenes o vídeos propios o de amigos en webs o plataformas públicas.
- No aceptar mensajes de contenido pornográfico o sexual.
- En ningún caso posar para fotos o grabaciones de vídeo de contenido sexual, o de tono comprometido, incluso si tienen como destino amigos
- En el caso de ser víctima de grooming, no aceptar el chantaje ni eliminar las pruebas.

Para la familia:

- Hablar abiertamente del tema con el menor, explicándole en qué consiste el acoso sexual.
- Advertirles de los peligros de hacer públicos sus perfiles en redes sociales, datos personales o imágenes y vídeos comprometidos.
- Hacerles ver que la webcam no es imprescindible y que, en caso de usarla, lo hagan con prudencia.
- Insistir en la idea de que en la red no se debe hacer nada que no se haría en la vida real.
- Aconsejarles sobre el riesgo de aceptar amistades que no conocen en persona.
- Estar atentos sobre la actividad del menor en la red:

  → Si pasa muchas horas y si lo hace por la noche.

  → Si se encuentran archivos multimedia pornográficos en su ordenador.

  → Si el menor se comporta de forma extraña, se aísla, no sale ya con sus amigos, presenta síntomas físicos de difícil explicación o sufre una brusca alteración de su rendimiento escolar.
- No borrar nunca las pruebas del delito.

¿Qué hacer?

Para los menores:

- Ante los primeros síntomas de acoso, pedir ayuda a los padres explicando todo lo sufrido.

Para los padres o educadores:

- Comprobar que lo que cuenta el menor es cierto, para lo que es necesario recabar toda la información posible, analizando qué actividad ha desarrollado el acosador y cuál es constitutiva de delito y demostrable.
- Recopilar todas las pruebas de la actividad del acosador: mensajes, multimedia...
- Denunciar el caso.

3.4 SEXTING

¿Qué es?

Consiste en el envío de imágenes y vídeos pornográficos de menores, tomadas por ellos mismos, a través de teléfonos móviles.

¿Cómo prevenirlo?

Consejos para menores:

- No enviar multimedia de contenido pornográfico propio o de otra persona a través del móvil es la mejor manera de prevenir. Una vez enviado, ese material se vuelve incontrolable, ya que es imposible prever cómo pueden circular esas imágenes o vídeos y a quién pueden llegar.
- Si se recibe multimedia de pornografía infantil, debe comunicárselo a un adulto y borrarse inmediatamente
- No distribuir nunca multimedia de nadie sin su consentimiento, ya que la imagen de una persona es un dato personal cuyo uso está protegido por la Ley.
- Nunca confiar en la seguridad de las redes sociales ni en redes wifi públicas, ya que pueden ser atacadas por hackers y acceder a los datos, imágenes y vídeos personales.

Consejos para padres y educadores:

- Insistir a los menores en la necesidad y la importancia de la privacidad.
- Hablar abiertamente sobre el tema, incluso antes de que éste aparezca, y explicarles a los menores los riesgos del sexting.
- Generar en el menor la confianza suficiente para que, en caso de que sea víctima o testigo de un caso de sexting, sepa que debe dirigirse y recurrir a un adulto.
- Observar conductas anormales en el menor, como tiempo excesivo en el empleo del móvil, hacerlo encerrado en su habitación, facturas del móvil de cuantía mayor de lo normal, alejamiento de sus actividades y amigos habituales, etc.

¿Qué hacer?

- Si se es menor de edad, o si un hijo o alumno está sufriendo una situación de sexting, es obligatorio denunciarla, por ser un delito.

3.5 PHISHING

¿Qué es?

Consiste en el envío de correos electrónicos masivos que suplantan la identidad de bancos o empresas de internet, solicitando la actualización de los datos personales al usuario (contraseñas, número de la tarjeta de crédito, etc.) a través de una página de la empresa en cuestión que parece totalmente real y auténtica. Cuando el usuario introduce los datos en dicha página, éstos son captados o pescados por la red de ciberdelincuentes.

¿Cómo prevenirlo? Consejos para menores:

• No se debe responder a ningún correo que pida datos personales.

• Nunca hacer clic en enlaces sospechosos que recibamos en el correo electrónico.

• Antes de introducir contraseñas en páginas web, comprobar que son las reales

Consejos para padres y educadores:

• Nunca se debe enviar información personal o financiera por correo electrónico.

• Tener cuidado con los archivos adjuntos que se reciben a través del correo electrónico, así como con su descarga, ya que pueden ser maliciosos.

• Nunca hacer clic en enlaces sospechosos que recibamos en el correo electrónico.

• Desconfiar de correos que parecen provenir de compañías, empresas, etc., con las que el usuario mantiene relación y en los que se avisa o advierte de que se va a cancelar una cuenta bancaria, un servicio, etc., si el usuario no responde.

• Hay que tener cuidado igualmente con aquellos correos que envían teléfonos a los que llamar para facilitar la información.

• Eliminar los correos electrónicos de empresas que soliciten o pidan la actualización de la información personal (contraseñas, cuenta bancaria, números de tarjeta de crédito, etc.). Los bancos, compañías, etc., nunca van a operar de esa manera ni van a solicitar esos datos por correo electrónico.

¿Qué hacer?

• Se pueden enviar los mensajes recibidos a la empresa u organización suplantada para que esté en su conocimiento.

• Denunciar el caso

3.6 VIRUS, MALWARE, SPYWARE..

¿Qué es?

Son virus, gusanos o troyanos; es decir, programas cuyo objetivo es alterar el funcionamiento del equipo que infectan, sin que el usuario lo note y lo consienta. Actúan bien robando información personal y sensible del usuario, usando el equipo para, desde él, cometer otros actos delictivos, o bien eliminando datos del equipo, o encriptándolos y solicitándole al usuario dinero a cambio de recuperarlos.

Los dispositivos que, potencialmente, pueden verse afectados son:

- Ordenadores personales y servidores
- Móviles
- Tablets
- Videoconsolas

¿Qué hacer?

Lo mejor es instalar un programa antivirus para asegurar una protección en tiempo real contra la instalación no deseada de cualquier tipo de programa malicioso. Paralelamente, el programa antivirus detecta y elimina todo programa que esté alterando el funcionamiento del equipo, escaneando todos los archivos del sistema operativo, los programas instalados y la memoria. Para que el antivirus sea efectivo y eficiente debe mantenerse actualizado continuamente.

4. ENLACES DE INTERÉS

Webs más importantes

- https://notecalles.educarex.es/
- https://emtic.educarex.es/seguridad
- Grupo de delitos telemáticos de la Guardia Civil https://www.gdt.guardiacivil.es/webgdt/home_alerta.php
- Denunciar el delito informático en la Guardia Civil https://www.gdt.guardiacivil.es/webgdt/pinformar.php

Webs generalistas

- Alerta en Línea http://www.alertaenlinea.gov/
- Grupo de delitos telemáticos. Guardia Civil https://www.gdt.guardiacivil.es/webgdt/home_alerta.php
- Guía de buenas prácticas TIC para las familias http://www.educa.jcyl.es/educacyl/cm/gallery/web-guia/index.html
- Ins@fe http://www.saferinternet.org/
- Kontuzdatos http://www.avpd.euskadi.net/s04-kontuzdt/es/
- Oficina de seguridad del internauta http://www.osi.es/
- Privacidad en internet http://privacidad-internet.blogspot.com.es/

Webs de temas concretos

- Ciberacoso y ciberbullying https://ciberacoso.wordpress.com/
- Denuncia online http://www.denuncia-online.org/
- Instituto nacional de ciberseguridad https://www.incibe.es/
- Phishing http://www.consumer.es/phishing