INTERNET SEGURO: enseña a navegar a tus hijos en la Red

SEMINARIOS ONLINE

ÍNDICE

INTRODUCCIÓN

El acceso y uso de Internet es una de las revoluciones que sin duda han cambiado nuestra forma de conocer el mundo, comunicarnos y acceder a la información.

La educación actual se enfrenta al reto del uso de las Nuevas Tecnologías con el problema de las constantes actualizaciones y novedades de su evolución.

Existen muchos aspectos positivos en el uso de las TIC (Tecnologías de la Información y Comunicación) que deben acompañarse de una educación sobre privacidad online y sobre una navegación segura.

La cantidad de información y páginas existentes en la Red hace que sea necesario fomentar la prevención en cuanto a un uso correcto de Internet. A lo que pueden ayudar recursos como programas y recursos de protección para los equipos informáticos.

Además, dentro del ámbito familiar, no podemos olvidar el “diálogo abierto” sobre los contenidos más adecuados en función a la edad de los menores y que sepan distinguir aquellos contenidos o acciones que no son recomendables para ellos.

MÓDULO 1

NATIVOS DIGITALES

1.1. ¿QUIÉNES SON LOS NATIVOS DIGITALES?

Los “Nativos Digitales” son aquellas personas que por haber nacido en pleno big-bag de la era digital, poseen una configuración psicocognitiva diferente.

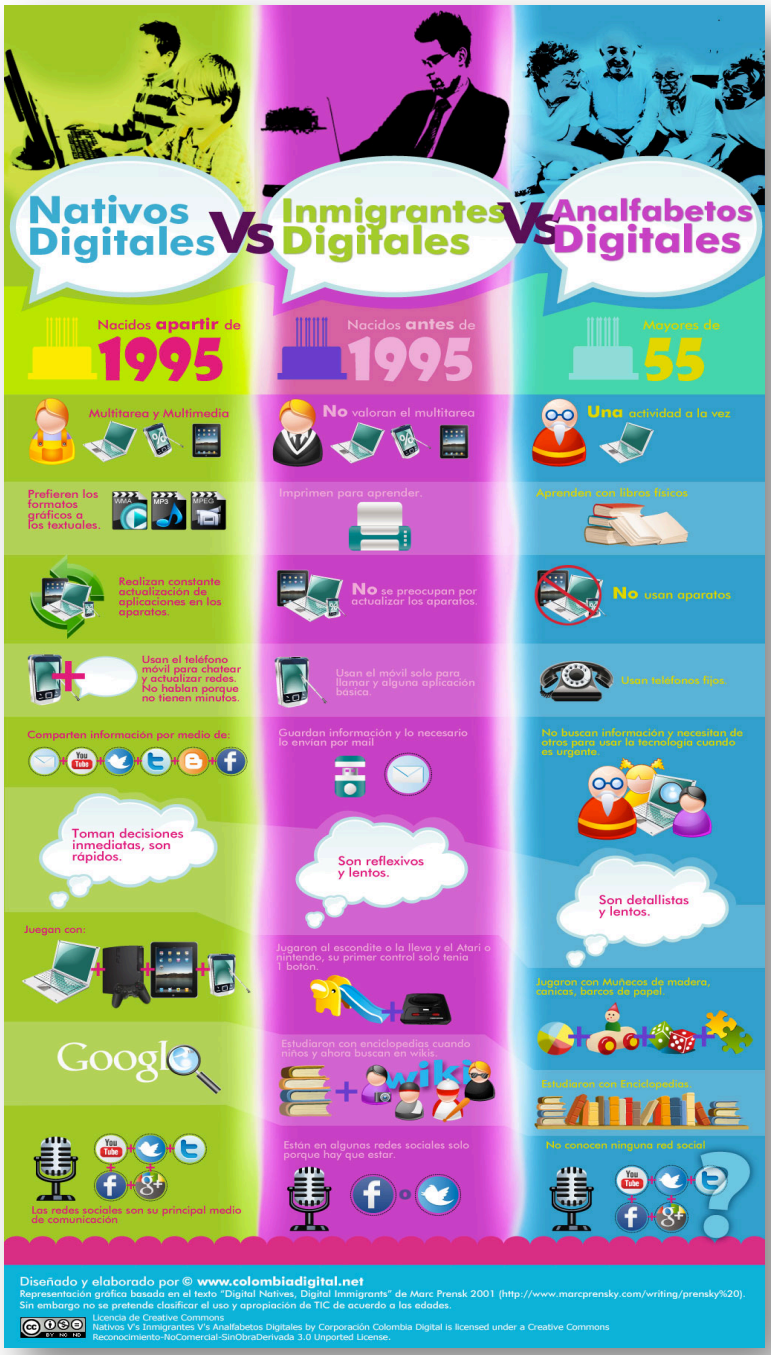
Entre sus habilidades y características podemos encontrar:

- Reciben información de forma rápida.
- Disfrutan los procesos y multitareas paralelos.
- Prefieren los gráficos antes que el texto.
- Defienden los accesos al azar (desde hipertextos).
- Funcionan mejor cuando trabajan en red.
- Prosperan con satisfacción inmediata y bajo recompensas frecuentes.
- Elijen jugar en “serio” en vez de trabajar.
- Se comunican a través de diferentes medios digitales: blogs, foros, redes sociales, etc.
- Utilizan el trabajo colaborativo a través de “comunidades de aprendizaje en Internet”.

Revista “Nativos Digitales”

http://www.protegeles.com/nativos_digitales.asp

1.1. ¿QUIÉNES SON LOS NATIVOS DIGITALES?



Ver infografía a tamaño completo: https://alfredovela.files.wordpress.com/2012/04/nativosdigitales.jpg

MÓDULO 2

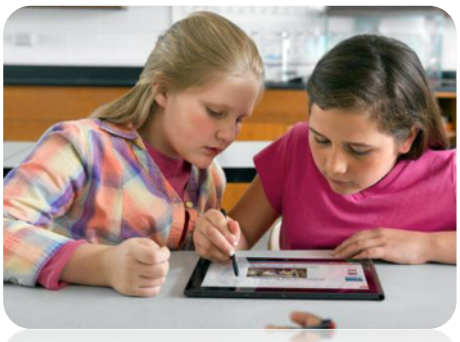
BENEFICIOS Y PELIGROS DE LAS NUEVAS TECNOLOGÍAS E INTERNET

1.1. BENEFICIOS DE LAS NUEVAS TECNOLOGÍAS PARA MENORES

Son muchos los beneficios que los menores pueden obtener de las Nuevas Tecnologías.

1. **Ayudan a la socialización**.
Los menores disponen de múltiples recursos online para poder comunicarse con amigos, hacer nuevas amistades y también mantenerse en contacto con su familia.

2. **Facilitan el acceso a la información**.
A un solo clic pueden acceder a un montón de contenidos que luego pueden utilizar en su centro educativo y también compartir en familia.



3. **Fomentan el "aprendizaje interactivo".**
Hoy en día, los menores son los protagonistas de su propio aprendizaje. Algo que les motiva y les ayuda para continuar aprendiendo.

4. **Ponen a disposición de los menores recursos educativos.**
Además del contenidos que pueden ver en los Centros Educativos, las Nuevas Tecnologías ofrecen a los menores multitud de recursos online. Estas herramientas permiten compartir también momentos en familia utilizándolos.

1.2. PRINCIPALES AMENAZAS EN INTERNET

Unos buenos hábitos de prevención supondrán una parte fundamental del uso de Internet en familia así como conocer la terminología y características de las amenazas que pueden producirse en Internet.

De esta forma, los padres y tutores serán capaces de identificar posibles problemas que se puedan producir e intervenir en caso de que sea necesario.

A continuación explicaremos las principales amenazas que pueden sufrir los menores por el uso de las nuevas tecnologías e internet:

GROOMING

Ocurre cuando un adulto intenta establecer una relación emocional con algún menor a través de Internet, a través de chat, foros y otros medios haciéndose pasar por otra persona.

CIBERBUYING

Se produce cuando menores de su entorno acosan al menor a través de chantaje psicológico utilizando Internet y las Redes Sociales como medio.

SEXTING

Afecta más a chicas que a chicos. El acosador se hace pasar por otra persona hasta que gana la confianza del menor. Así consigue acceder a sus imágenes o a que muestre su webcam y luego para luego chantajearlas.

1.2. PRINCIPALES AMENAZAS EN INTERNET

PHISING

Consiste en la “suplantación de identidad”.
Con ello, la persona que lo realiza puede hacerse pasar por el menor en las redes sociales y en Internet publicando en su nombre.

FÍSICOS

Si los menores comparten información en sus redes sociales como imágenes “geolocalizadas” pueden exponerse a que algún acosador les encuentren en los lugares que frecuentan.

OTROS

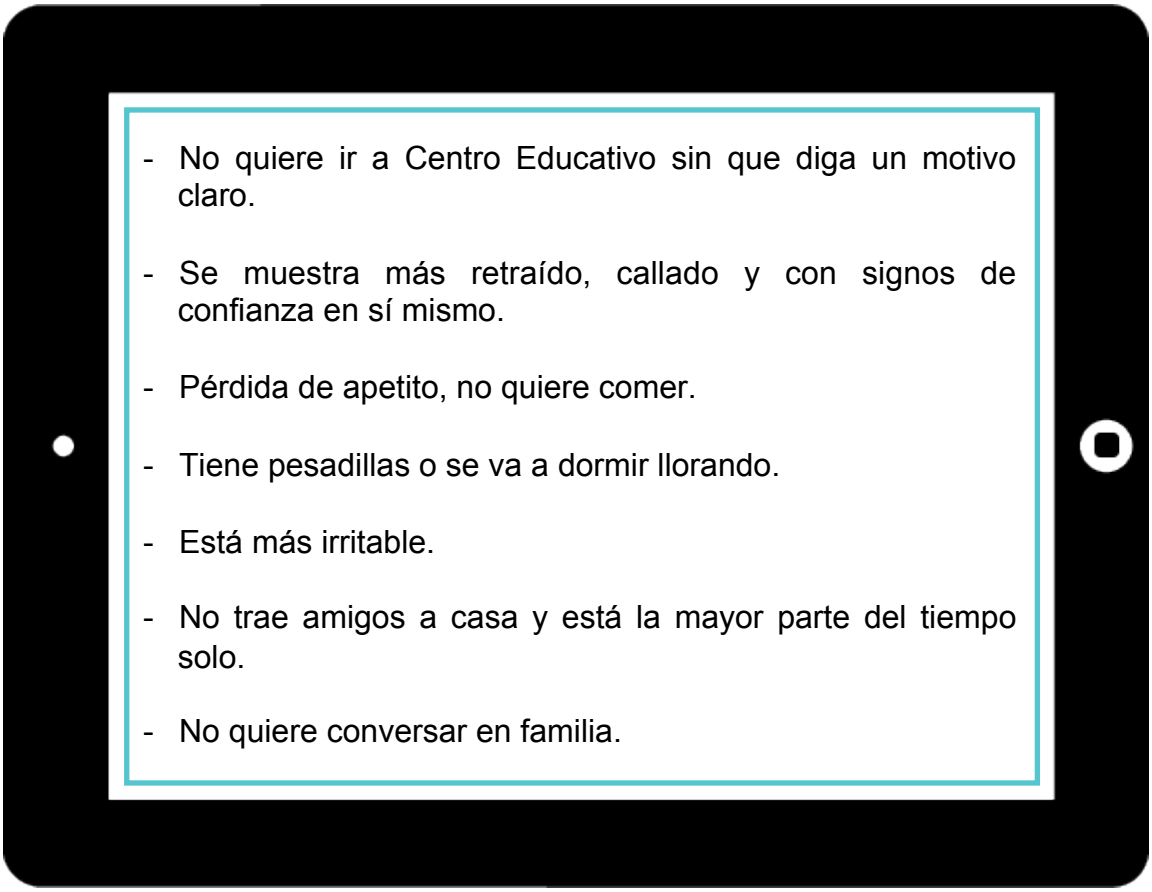
Contenidos que pueden influir en los menores de forma negativa: violencia, pornografía, muestra de forma positiva el caer en enfermedades como la bulimia o la anorexia.

1.2. CONSEJOS PARA PROTEGER A NUESTROS HIJOS

Cada padre, madre o tutor conoce la forma en la que sus hijos expresan la angustia, que es por lo general la clave con la que se aparece un cambio de actitud en la conducta.

No hay un signo único que indique que el menor está siendo acosado, pero los signos que se indican a continuación pueden darnos algunas pistas sobre si está sufriendo alguno de los peligros antes comentados.

Sobre todos deberemos estar alerta si se producen notables cambios de conducta en los siguientes aspectos.



1.1. MEDIDAS QUE PODEMOS ADOPTAR EN EL HOGAR

A continuación destacamos algunas medidas que, como familias, podremos poner en práctica en el hogar para proteger y prevenir alguno de los peligros antes mencionados.

- Es importante que haya una comunicación fluida entre los miembros de la familia. Hacer preguntas cotidianas sobre lo que ha hecho el menor durante el día nos permite conocer información sobre sus sentimientos, estado anímico y relaciones con sus amigos.

No debemos conformarnos con respuestas cortas a las preguntas que les hagamos, es necesario intentar que las preguntas sean propicias para que el menor no responda con un sí o no.

- Una "escucha activa" de los sentimientos de los menores, su tono de voz, prestar atención a expresiones faciales y gestos pueden darnos muchas pistas de cómo se encuentran.

- Si el menor recibe mensajes insultantes a través, por ejemplo del teléfono móvil podemos seguir las siguientes pautas de actuación:

• Aconsejad al menor que no abra los mensajes enviados por acosadores o desconocidos.

• No responder a los mensajes o sólo responder una vez de forma breve indicando que se desea que se termine el acoso.

1.1. QÚE HACER Y A QUÉ EDAD

De 4 a 12 años

- Acompañarles mientras utilizan el ordenador. Así podremos guiarles y ver qué contenidos les interesan.

- Conocer las claves de acceso. Ayudarles a la hora de elegir claves y contraseñas de acceso seguras (combinación de letras y números, mayúsculas y minúsculas. Cambiarlas cada cierto tiempo y no compartirlas con amigos.

- Enseñarles que no deben descargar nada sin permiso. Algunos archivos pueden llevar un nombre que no corresponda con lo que contiene.

- Definir las condiciones de uso.

De 13 a 18 años

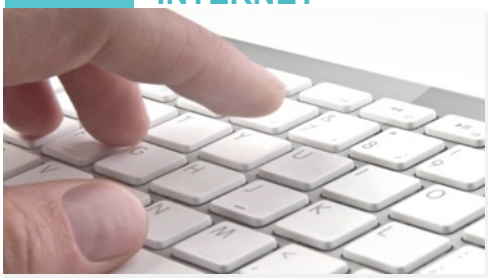
- Conocer los remitentes para no tener que leer los correos. Los adolescentes son muy celosos de su privacidad, por lo que podemos llegar al acuerdo de que los padres conozcamos las direcciones pero no leer el contenido del correo. Así, si vemos una dirección desconocida, podremos preguntar al menor.

- Estar alerta si se citan con algún desconocido. Insistirles en que no vayan solos y que sea en lugares públicos con más gente. Y enseñarles ejemplos de que en Internet no todo es lo que parece.

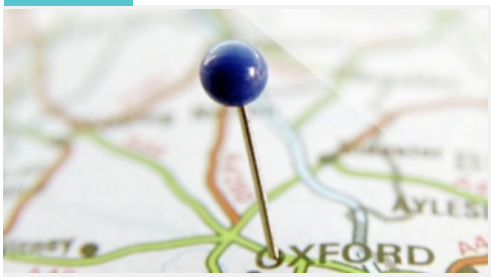
- Enseñarles a tener un comportamiento responsable, respetuoso y ético en Internet. Al estar en Internet, pueden pensar que lo que hacen se quedará impune y en ocasiones actúan de forma más agresiva que en la vida real. Por eso es recomendable explicarles qué es el ciberacoso y que algo que hace daño a otras personas no es divertido.

- Asegurarse de que consultan antes de realizar cualquier transacción en línea. El comercio electrónico es cada vez más común en juegos en línea, etc; por ello no es necesario prohibirles que compren en Internet, pero sí el hacerlo de forma segura y a través de medios de pago autorizados.

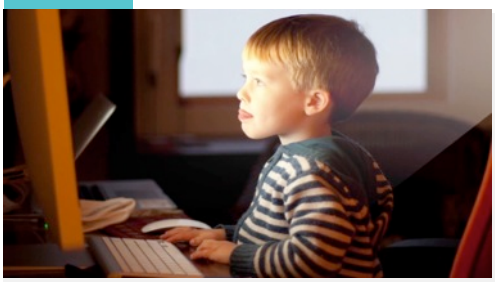
1 PENSAR BIEN LA INFORMACIÓN QUE PUBLICAMOS EN INTERNET



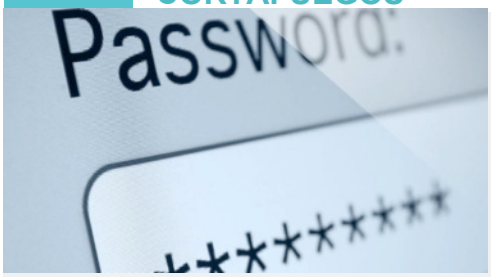
2 CUIDADO CON COMPARTIR LAS LOCALIZACIONES



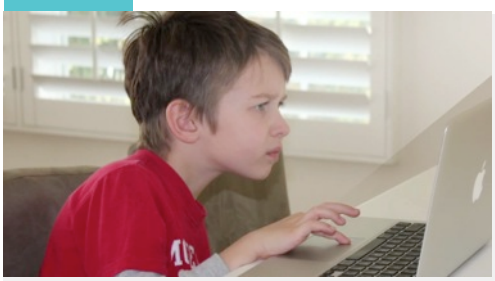
3 ORDENADOR SITUADO EN LUGAR COMÚN DEL HOGAR



4 CONTRASEÑAS SEGURAS Y EQUIPOS CON ANTIVIRUS Y CORTAFUEGOS

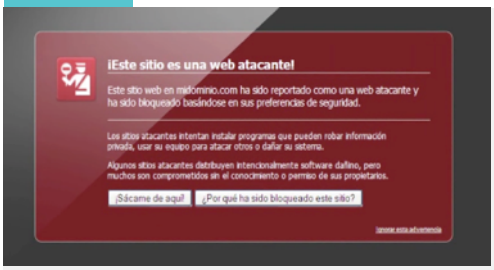


5 USAR SISTEMAS DE CONTROL PARENTAL

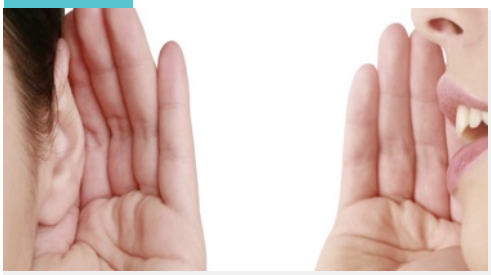


6 VIGILAR LOS JUEGOS, CONSOLAS Y DISPOSITIVOS DEL MENOR

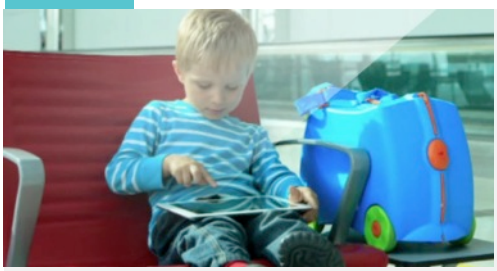
7 CUIDADO CON PÁGINAS, ENLACES Y DESCARGAS SOSPECHOSAS



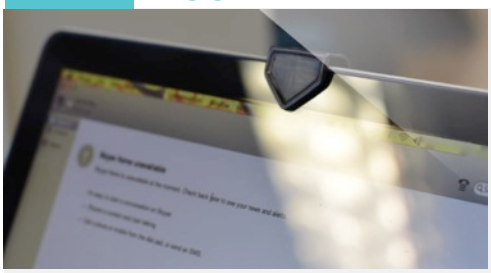
8 NO COMPARTIR LAS CONTRASEÑAS



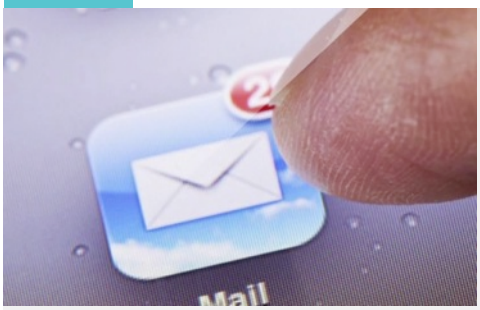
9 EN WIFIS ABIERTAS NO COMPARTIR DATOS PERSONALES



10 TAPAR LA WEBCAM DE LOS EQUIPOS INFORMÁTICOS DEL HOGAR



11 TENER DOS CUENTAS DE CORREO ELECTRÓNICO



Los expertos recomiendan que el menor tenga dos cuentas de correo diferentes: una para cosas importantes (como las tareas escolares, que será compartida con amigos y familiares) y otra con un "Nick" o seudónimo inventado, sin datos personales como la edad para usarla en redes sociales, chat, etc.

ACTIVIDAD PARA HACER EN FAMILIA EN FAMILIA

La web navegacionsegura.es es un recurso educativo que podemos realizar en familia.

Se presenta como un divertido juego como el popular TRIVIAL en el que podremos conocer más sobre seguridad en Internet y comprobar lo que los menores conocen.

De una forma divertida podremos ver lo que saben o no los menores sobre contenidos como: virus, troyanos y gusanos, spyware, ciberbullyng y grooming.

ACTIVIDAD PARA HACER EN FAMILIA EN FAMILIA

OSI Oficina de Seguridad del Internauta

- La web de la Oficina de Seguridad del Internauta en la página http://www.osi.es/es/node/3388/take pone a nuestra disposición un test sobre conceptos a tener en cuenta sobre Seguridad en Internet.
- A través de las diferentes preguntas que componen dicho test podremos poner a prueba nuestros conocimientos y saber más sobre las precauciones que debemos tener en la Red y en el uso de nuestros equipos informáticos.
- Una interesante actividad para hacer en familia para que todos los miembros estemos al tanto de las últimas novedades sobre seguridad online.

MÓDULO 3

PROBLEMAS QUE LOS MENORES PUEDEN ENCONTRAR EN LA RED

2.1. ENLACES QUE CONTENGAN VIRUS Y ARCHIVOS DAÑINOS

Los enlaces acortados están de moda y su uso es cada vez más frecuente, ya que pueden resultar más prácticos en dispositivos móviles y a nivel estético quedan mejor que un enlace que ocupe dos líneas.

Pero estos enlaces pueden dirigir a páginas para descargar algún archivo que contenga virus u otro tipo de archivos dañinos.

Para evitar este tipo de problemas, además de tener un antivirus instalado y actualizado en nuestros equipos informáticos, podemos ayudarnos de ciertas páginas que analicen tanto las URL´s como archivos descargados antes de abrirlos.

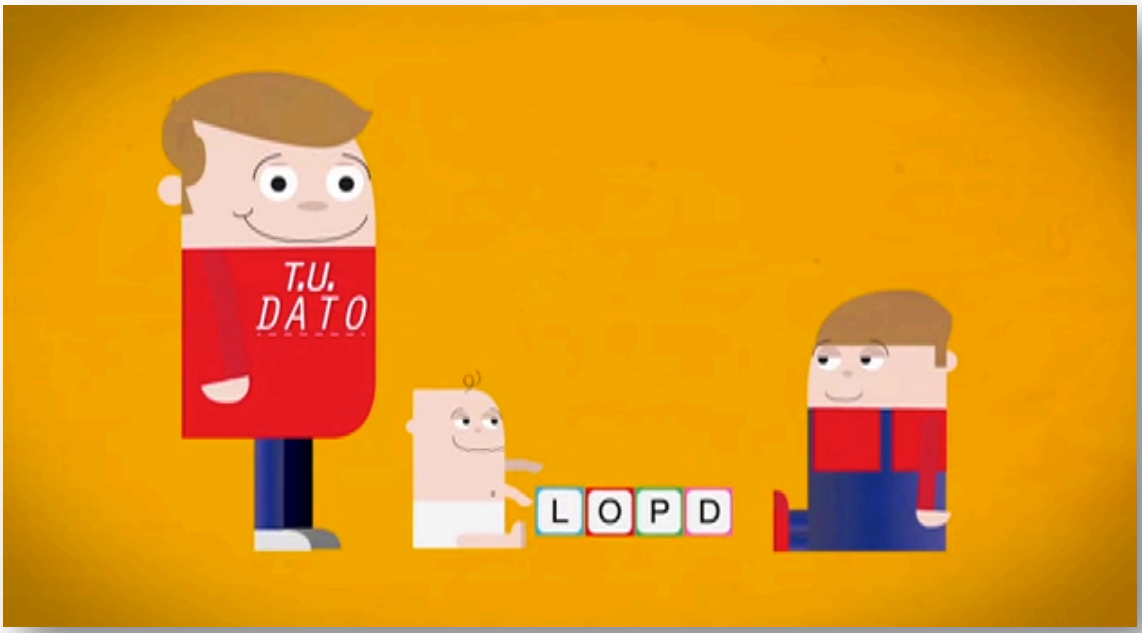
https://www.virustotal.com/es/

2.1. PRIVACIDAD DEL MENOR

Es fundamental hablar en familia sobre los datos que son importante mantener de forma privada y mentalizar al menor de los que tienen especial relevancia sin que puedan ser compartidos sin la autorización de los padres.

También es fundamental que si el menor posee una web, blog o similar, que esté informado del respeto de los datos personales de otros usuarios y del uso de imágenes y elementos que pueden contener derechos de propiedad intelectual y podría tener consecuencias importantes.

En la actualidad, la privacidad está protegida por la Ley de Protección de Datos, que si no se respeta, puede tener consecuencias legales.



https://www.youtube.com/watch?v=lRozhQS6kN8

2.1. CONFIANZA EN LA RED

Al haber nacido en la era de Internet, muchas veces creen que todo lo que se publica en ella en cierto. Por ello, hay que explicarles que es necesario que tengan sean críticos con lo que ven y escuchan en la Red y que verifiquen la información en fuentes fiables.

En cuanto problemas que los menores puedan encontrar en Internet, ha surgido el “malvertising”, que es una técnica que se utiliza para infectar los equipos. El nombre de esta práctica viene de las palabras "malicious advertising" (publicidad maliciosa) y lo que hace es esconder malware para infectar nuestros dispositivos en los espacios de publicidad de otras páginas webs.

Deriva de su antecesor, el “adware”, que es cualquier programa que automáticamente va mostrando publicidad al usuario durante su instalación y/o durante su uso y con ello genera beneficios a sus creadores.

Habitualmente se instalan sin que el usuario lo sepa dado que, aunque no es nada recomendable, en más de una ocasión optamos por la instalación "SIGUIENTE-SIGUIENTE-SIGUIENTE".

2.1. CONTENIDO INAPROPIADO

Además del contenido sexual que se puede encontrar en Internet, también proliferan páginas de contenido violento, xenófobo y de otro tipo que aún no pueden llegar a comprender por no estar adaptado a su edad.

Por ello, podemos ayudarnos de ciertos recursos para que los menores naveguen sin que estos contenidos les puedan afectar.

Entre ellos, podemos utilizar buscadores especialmente diseñados para los menores como: http://buscadorinfantil.com/

2.1. CONTENIDO INAPROPIADO

Otro recurso que tenemos disponible es el de configurar la seguridad del navegador.

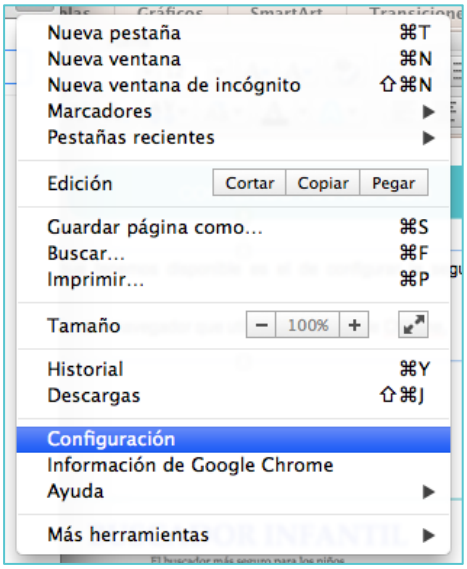
Así, por ejemplo, si el navegador que utilizamos es Google Chrome, podremos configurar algunas opciones avanzadas para proteger el equipo con ciertas medidas.

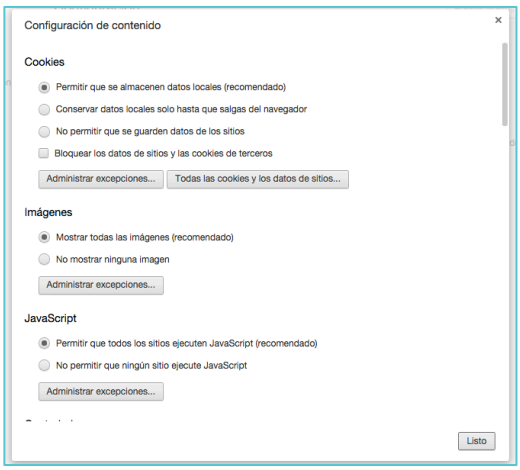
- Para acceder a estas opciones nos dirigimos a la "Configuración" del navegador situado en la parte superior derecha en el menú.

- Accedemos al enlace de la opción de "mostrar la configuración avanzada.

- En la opción "Privacidad" podremos habilitar funciones como la protección contra phising y software malicioso.

- En la opción de "Configuración de contenido" podremos retringir ciertas descargas o contenido que se muestre en la navegación del equipo.





2.1. CONTENIDO INAPROPIADO

También podemos configurar el tipo de vídeos que aparezcan en YouTube. De esta forma, los menores podrán navegar por esta web pero sin temor a que aparezcan vídeos de contenido inapropiado.

- Para configurar la seguridad en YouTube, nos dirigimos a la parte inferior de la página y pulsamos sobre el apartado “Seguridad”.

- Para configurar la seguridad en YouTube, nos dirigimos a la parte inferior de la página y pulsamos sobre el apartado “Seguridad”.

- Si lo activamos y guardamos, todos los vídeos de contenido considerado inapropiado para menores no se mostrarán.

2.1. CONTENIDO INAPROPIADO

La Ley se va adaptando a los diferentes usos de Internet aunque a veces no va en sincronización con el ritmo de los cambios tecnológicos.

A día de hoy, podemos destacar en cuanto a cuestiones que afectan a los menores, las leyes más importantes son:

- La Ley de Protección de Datos. Regula, entre muchas otras cosas, el uso que se hace de las imágenes, datos personales o vídeos en la Red. Y estipula fuertes multas en el caso de que se invada la privacidad de una persona.

- La Ley de Propiedad Intelectual. Indica que los programas de ordenador (aplicaciones y juegos) pirateados son delito e impone fuertes multas por ello. El “software pirateado” son aquellos programas no gratuitos que se utilizan sin haber pagado licencia o habiéndose saltado la protección que tengan.

2.1. USO DEL CORREO ELECTRÓNICO

Para darse de alta o registrarse en cualquier lugar de Internet, es necesario tener un correo electrónico. Y aunque para los menores, su uso no está entre sus usos preferidos en Internet, es recomendable que adquieran una serie de hábitos de seguridad sobre la utilización de esta tecnología que les puede acompañar durante muchos años.

Entre las acciones recomendables están:

- Que tengan dos cuentas de correo electrónico. Una para sus familiares, colegio y amigos y otra para registrarse en foros, redes sociales o juegos en línea.

- Que no contesten a correos electrónicos de personas desconocidas.

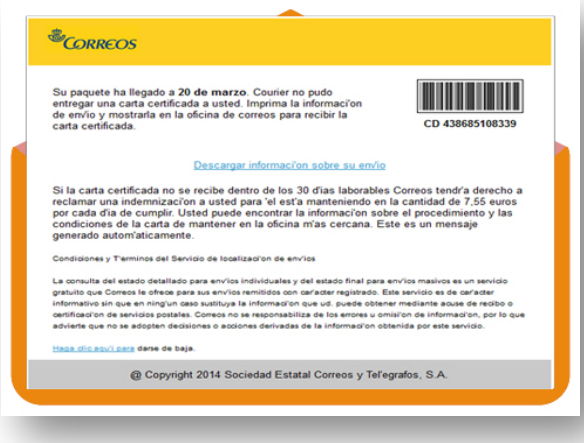
- Eliminar correos sospechosos que pueden tratarse de engaños, e incluso contener un virus.

- Explicarles que en Internet circulan una gran cantidad de bulos.

- No descargar archivos adjuntos si no están seguros de quién escribe el mensaje.

- Pasar el antivirus antes de abrir cualquier archivo descargado.

Como ejemplo de un correo que en la actualidad está causando infección en equipos informáticos es el que aparentemente nos llega del organismo de “Correos” como si nos hubiera llegado un paquete a una de sus oficinas y nos requieren ciertos datos.


CORREOS

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 438685108339

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Condiciones y T'erminos del Servicio de localizaci'on de env'ios

La consulta del estado detallado para env'ios individuales y del estado final para env'ios masivos es un servicio gratuito que Correos le ofrece para sus env'ios remitidos con car'acter registrado. Este servicio es de car'acter informativo sin que en ning'un caso sustituya la informaci'on que ud. puede obtener mediante acuse de recibo o certificaci'on de servicios postales. Correos no se responsabiliza de los errores u omisi'on de informaci'on, por lo que advierte que no se adopten decisiones o acciones derivadas de la informaci'on obtenida por este servicio.

Haga clic aqu'i para darse de baja.

@ Copyright 2014 Sociedad Estatal Correos y Tel'egrafos, S.A.

2.1. JUEGOS ONLINE

Internet ha hecho que los juegos online formen parten de la diversión de los menores. Pueden jugar con otros usuarios de todo el mundo.

Muchos de estos juegos disponen de un chat para que los jugadores se comuniquen de forma rápida.

Es importante que el software que está instalado en el ordenador para jugar en línea esté actualizado con los últimos “parches de seguridad” y que no se instalen parches que no sean oficiales por si pueden tratarse de virus.

https://www.osi.es/es/actualidad/blog/2015/01/12/game-over-asi-de-facil-te-pueden-robar-tu-cuenta-al-jugar-online

MÓDULO 4

IDENTIDAD DIGITAL

2.1. IMPORTANCIA DE LA IDENTIDAD DIGITAL

Internet ha hecho que los juegos online formen parten de la diversión de los menores. Pueden jugar con otros usuarios de todo el mundo.

Muchos de estos juegos disponen de un chat para que los jugadores se comuniquen de forma rápida.

https://www.osi.es/es/actualidad/blog/2015/01/12/game-over-asi-de-facil-te-pueden-robar-tu-cuenta-al-jugar-online

Es importante que el software que está instalado en el ordenador para jugar en línea esté actualizado con los últimos "parches de seguridad" y que no se instalen parches que no sean oficiales por si pueden tratarse de virus.

https://pipl.com/

http://www.yasni.com/

https://www.google.es/alerts

"Derecho al olvido" Tribunal de Justicia de la Unión Europea.
Solicitar a Google:
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=es

Saber dónde aparece la foto de un menor en Google. Subir imagen.

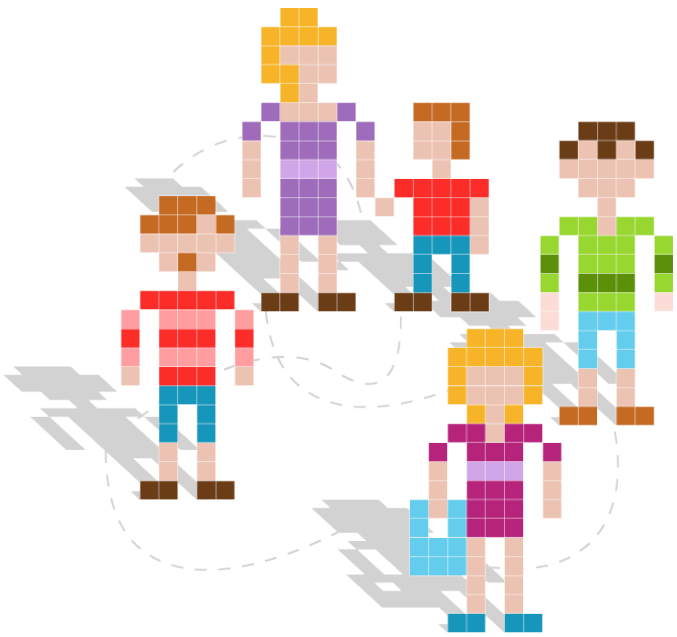
5.1. IDENTIDAD DIGITAL Y SU IMPORTANCIA EN EL MUNDO ONLINE

Cuando navegamos por Internet, todos dejamos un rastro de información acerca de nosotros mismos, las páginas que visitamos, nuestros gustos, opiniones y que forman parte de nuestra “Identidad Digital”.

Es fundamental informar y debatir con los menores el “yo” virtual que cada día se va construyendo en la Red. Con todo lo que supone, tanto en este momento de su vida como en el futuro próximo cuando, por ejemplo, deseen incorporarse al mundo laboral.

Los adolescentes deben ser conscientes de que una de las técnicas que utilizan las empresas a la hora de elegir entre varios candidatos para un puesto de trabajo, es buscar información sobre ellos en Internet. Y toda la información que hemos ido publicando a través de diferentes medios online puede ser encontrada: comentarios, fotos, etc.

Por todo ello, es importante que sean precavidos sobre la información que comparten en Internet, ya que pueden traerles consecuencias tanto a corto y como a largo plazo.

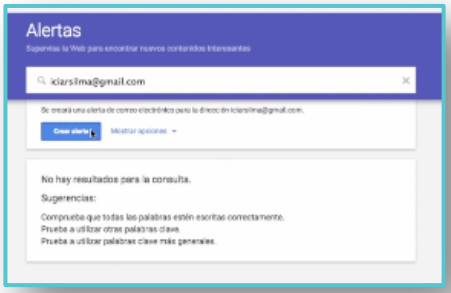


5.1. IDENTIDAD DIGITAL Y SU IMPORTANCIA EN EL MUNDO ONLINE

Como ejercicio práctico con los menores, podemos ver varias herramientas online con ellos para que comprendan la importancia de su "Identidad Digital" así como lo que se muestra en "Internet" sobre ello.

- El buscador "yasni" posee un apartado para encontrar información acerca de una persona. En la opción indicada como "¿Qué sabe la red acerca de…?" el menor podrá poner su nombre y pulsar en el botón "Saber". Al hacerlo, comenzará la búsqueda de los a datos y aparecerá toda la información y webs donde aparece.

- Alertas de Google sobre correo electrónico y datos personales. Si el menor dispone de una cuenta de Google, podremos administrar las alertas personales desde la dirección web https://www.google.es/alerts. Activando la opción "Presencia en Internet", cada vez que Google detecte que se menciona nuestro correo y datos personales que tenemos configurados en nuestra cuenta, nos enviará un aviso por email para que estemos informados de ello.



Con estas prácticas que podemos hacer junto con el menor, conocerá de una forma rápida la información sobre la identidad digital que los demás pueden conocer de él en Internet y la "reputación online" que se está construyendo y que afectará a su vida.

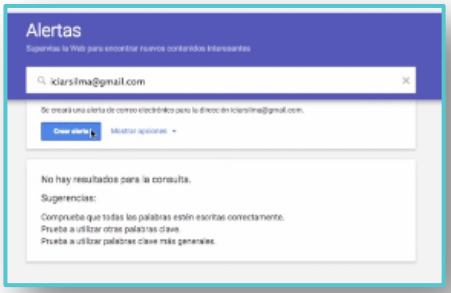
Está en nuestra mano como adultos recordarles que "En Internet todo queda" aunque piensen que haya borrado la información siempre puede pasar que no se haya hecho esa eliminación completa o que antes de borrarla otras personas la hayan compartido.

5.1. IDENTIDAD DIGITAL Y SU IMPORTANCIA EN EL MUNDO ONLINE

Como ejercicio práctico con los menores, podemos ver varias herramientas online con ellos para que comprendan la importancia de su "Identidad Digital" así como lo que se muestra en "Internet" sobre ello.

- El buscador "yasni" posee un apartado para encontrar información acerca de una persona. En la opción indicada como "¿Qué sabe la red acerca de…?" el menor podrá poner su nombre y pulsar en el botón "Saber". Al hacerlo, comenzará la búsqueda de los a datos y aparecerá toda la información y webs donde aparece.

- Alertas de Google sobre correo electrónico y datos personales. Si el menor dispone de una cuenta de Google, podremos administrar las alertas personales desde la dirección web https://www.google.es/alerts. Activando la opción "Presencia en Internet", cada vez que Google detecte que se menciona nuestro correo y datos personales que tenemos configurados en nuestra cuenta, nos enviará un aviso por email para que estemos informados de ello.



Con estas prácticas que podemos hacer junto con el menor, conocerá de una forma rápida la información sobre la identidad digital que los demás pueden conocer de él en Internet y la "reputación online" que se está construyendo y que afectará a su vida.

Está en nuestra mano como adultos recordarles que "En Internet todo queda" aunque piensen que haya borrado la información siempre puede pasar que no se haya hecho esa eliminación completa o que antes de borrarla otras personas la hayan compartido.

5.2. “NETETIQUETA” O “NORMAS DE ETIQUETA EN LA RED”

Es recomendable que los menores conozcan las normas de uso aconsejables y lo que los expertos denominan “Netetiqueta”, que consiste en seguir las normas correctas de uso en Redes Sociales.

Entre estas normas destacaremos las siguientes para comentar con los menores y que las conozcan y respeten:

- Pide permiso antes de “etiquetar” fotografías de otras personas.

- Utiliza las etiquetas de manera positiva, no para insultar, ya que esto puede dañar a otras personas.
- Expresa tu opinión pero sin burlas, ya que incluso podría ir contra la Ley.
- Si algo no te apetece hacer di que “NO”.

- Evita que te denuncien como spam, por hacer un comentario incorrecto.
- Respeta la privacidad e intimidad de otras personas y la tuya propia.
- Usa recursos disponibles para expresarte mejor como: emoticones, símbolos, dibujos, etc. Así evitarás malentendidos.

Con estos consejos conseguiremos que el menor actúe con prudencia y respeto en las redes sociales en las que participa.

MÓDULO 5

CONEXIONES SIEMPRE SEGURAS

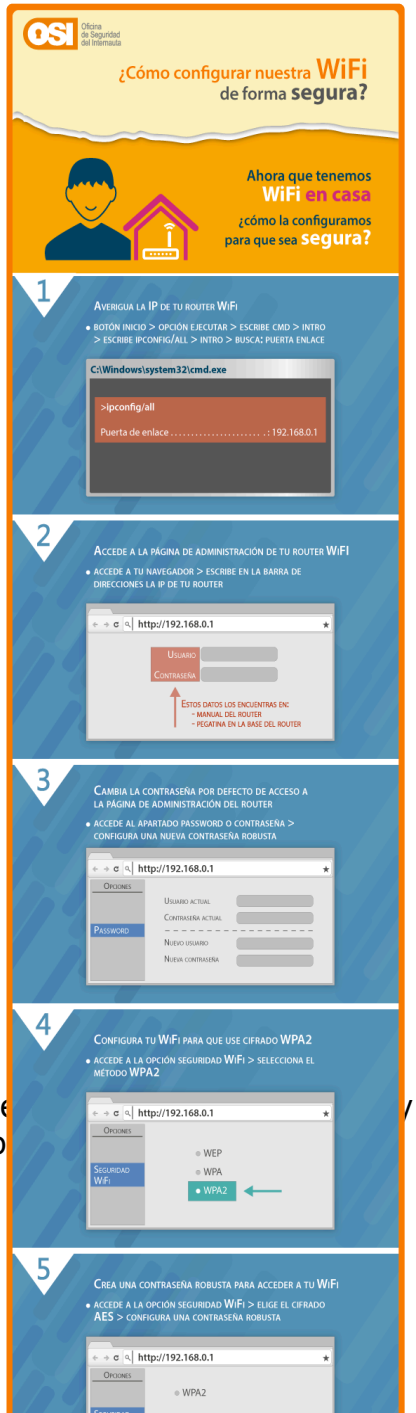
5.2.

WIFIS SEGURAS

Es recomendable que los menores conozcan las normas de uso aconsejables y lo que los expertos denominan “Netetiqueta”, que consiste en seguir las normas correctas de uso en Redes Sociales.

Entre estas normas destacaremos las siguientes para comentar con los menores y que las conozcan y respeten:

- Pide permiso antes de “etiquetar” fotografías de otras personas.
- Utiliza las etiquetas de manera positiva, no para insultar, ya que esto puede dañar a otras personas.
- Expresa tu opinión pero sin burlas, ya que incluso podría ir contra la Ley.
- Si algo no te apetece hacer di que “NO”.
- Evita que te denuncien como spam, por hacer un comentario incorrecto.
- Respeta la privacidad e intimidad de otras personas y la tuya propia.
- Usa recursos disponibles para expresarte mejor como: emoticones, símbolos, dibujos, etc. Así evitarás malentendidos.



Con estos consejos conseguiremos que el me / respeto en las redes sociales en las que particip

MÓDULO 2

MEDIDAS DE PROTECCIÓN EN EQUIPOS INFORMÁTICOS: ANTIVIRUS Y CORTAFUEGOS

2.1. INSTALACIÓN DE UN ANTIVIRUS GRATUITO

Es fundamental que nuestros equipos informáticos estén protegidos. Para ello, vamos a ver la instalación y los usos que podemos obtener de los antivirus.

Un antivirus es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso; lo que conocemos como virus, troyanos, gusanos, etc.

Para que realice su función, una vez instalado, debe estar activado y actualizado, ya que si no, no podrá evitar los nuevos virus que pueden haber afectado a nuestro equipo.

Existen muchos antivirus en el mercado, que ofrecen también una versión gratuita.

A continuación veremos cómo instalar el AVG Antivirus Free, que es un antivirus gratuito de fácil uso.

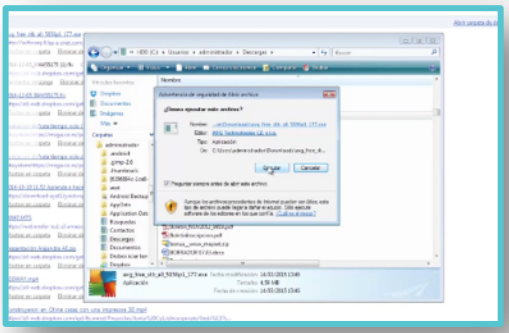
Entre sus acciones, realiza una verificación de los vínculos de una página web antes de hacer clic en ellos. Protege nuestra navegación en Redes Sociales y previene el espionaje y el robo de datos. Así como protección de correos electrónicos que puedan contener virus.

2.1. INSTALACIÓN DE UN ANTIVIRUS GRATUITO

Para instalarlo, nos dirigimos a la página de su descarga gratuita: free-avg.com/es-es/free

Hacemos clic en el botón verde indicado como "Descarga gratuita desde CNET" y esperamos a que el archivo se descargue.

Cuando ya esté listo, abrimos la descarga, hacemos clic en "Ejecutar" y vamos siguiendo las instrucciones del instalador.



Esta acción podrá durar varios minutos.

Será necesario reiniciar el equipo una vez completada la instalación.

Como veremos, este antivirus nos ofrece:

- Protección del equipo, protección en la navegación en páginas webs de Internet.
- Y protección contra robo de identidad.
- También nos protege de amenazas que puedan llegar a través de nuestro correo electrónico.

Las actualizaciones aparecerán de forma periódicamente con un aviso para poder instalarlas.

Ya hemos visto lo fácil que es instalar un antivirus. Por eso, ¡NO HAY EXCUSAS! para no tener protegidos nuestros equipos.

PÁGINA RECOMENDADA

OSI Oficina de Seguridad del Internauta

- La Oficina de Seguridad del Internauta, desde su web www.osi.es, ofrece información actualizada y soporte para evitar y resolver los problemas que pueden existir al navegar por Internet.
- Comparte multitud de herramientas para navegar de forma segura incluyendo un canal de “avisos” para estar actualizados sobre las últimas alertas de seguridad.
- Todo está explicado en un lenguaje sencillo para no tener que saber grandes conocimientos de informática y así estar siempre actualizados de posibles amenazas que estén surgiendo en la Red y evitar que nos afecten.
- Es una iniciativa del INCIBE, el Instituto Nacional de Ciberseguridad. En la que se proporciona la información y el soporte necesarios para evitar y resolver problemas de seguridad que pueden existir al navegar por Internet.

2.2. CONFIGURACIÓN DE CORTAFUEGOS EN EQUIPOS INFORMÁTICOS

Cuando conectamos nuestros equipos informáticos a Internet, corremos el riesgo de que alguien acceda a nuestra información almacenada: fotos, archivos,…; e incluso que descubra cuáles son las contraseñas que utilizamos para acceder a nuestro correo electrónico.

También existe la posibilidad de que se hayan instalado programas sin nosotros saberlo y que estén ejecutando rutinas que hacen que cambie la configuración o que el equipo esté enviando datos.

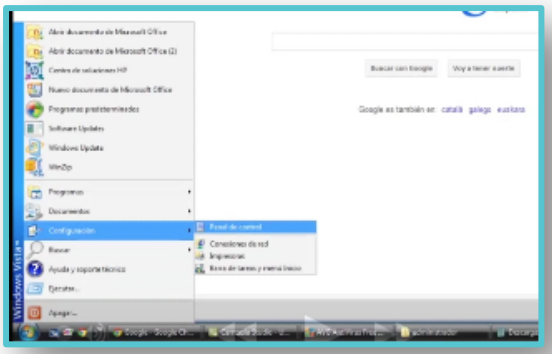
Para evitarlo, existen los programas que se llaman cortafuegos o dicho en inglés “Firewall”. Este tipo de programas, lo que evitan es que salga información que nosotros no deseamos y que tampoco entre información que no hemos aceptado.

El cortafuegos lo que va evitar es que haya programas que estén enviando y recibiendo información a través de Internet a nuestros equipos informáticos.

Podremos configurarlos para que entre o salga información y las nuevas actualizaciones del antivirus, por ejemplo.

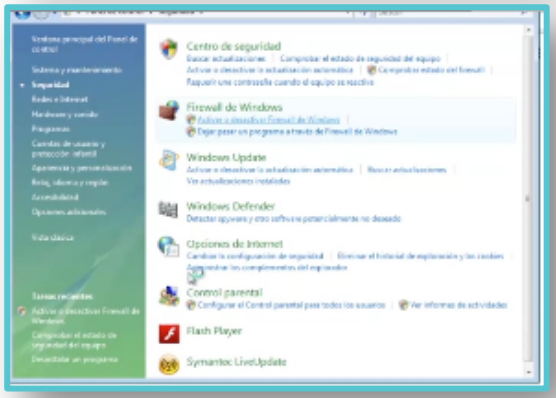
2.3. CONFIGURACIÓN DE CORTAFUEGOS EN EQUIPOS INFORMÁTICOS CON SISTEMA OPERATIVOS WINDOWS

El cortafuegos de Windows permite proteger al equipo de software malicioso o atacante que intente conectarse al equipo de forma remota.



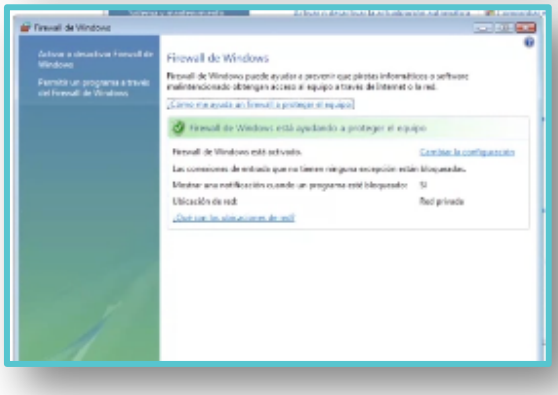
Para configurar el cortafuegos de Windows accederemos al “Panel de control” desde el apartado de “Configuración”.

- Una vez en esta ventana, pulsaremos en la opción “Seguridad”. Como vemos, uno de sus apartados es el indicado como “Firewall de Windows”.



- Abriremos la “Configuración” y comprobaremos que está activado. Es recomendable bloquear las comunicaciones de los programas a excepción de, por ejemplo, el antivirus que tenemos instalado en el equipo; ya que si no, no podrá actualizarse y nuestro equipo no estará protegido totalmente.

- Podemos acceder a cambiar la Configuración y en la opción “Excepciones”, elegir entre todos los programas que tenemos, activando o desactivando esa excepción.



Con estos sencillos pasos, tendremos configurado el cortafuegos del equipo, evitando así las conexiones de usuarios malintencionados y virus que se propagan por la Red.

MÓDULO 3

FILTROS PARENTALES COMO MEDIDA DE PRECAUCIÓN Y CONTROL

3.1. INSTALACIÓN Y CONFIGURACIÓN DE FILTROS PARENTALES EN ORDENADORES CON SISTEMA OPERATIVOS WINDOWS

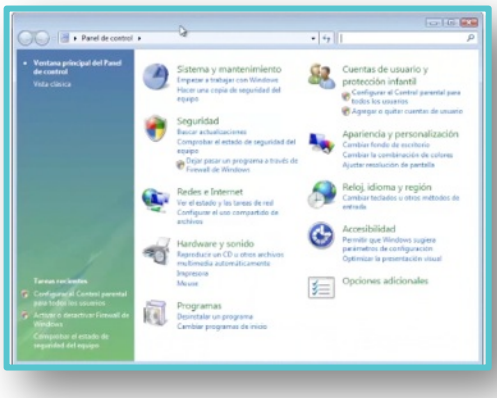
Para los menores, los ordenadores, las tabletas o los Smartphones son instrumentos cotidianos que utilizan de forma habitual.

Se sienten tan cómodos utilizándolos, que en ocasiones les puede crear una falsa sensación de seguridad.

Una de las herramientas que tenemos a nuestra disposición para ayudarles, sobre todo a edades tempranas, es el "Control parental", que realiza acciones de control, supervisión y dirige el uso que hacen los menores de la Tecnología.

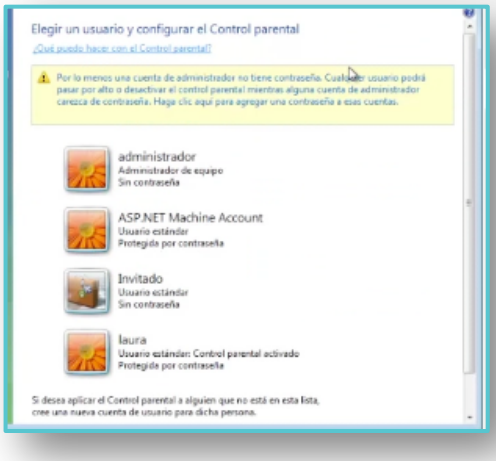
A continuación, veremos cómo configurar el Control Parental en un ordenador con sistema operativo Windows.

Para ello, accedemos desde el botón "Inicio" a la "Configuración" y al "Panel de Control".



- Dentro del apartado "Cuentas de usuario y protección infantil", entraremos en la opción "Configurar el Control parental para todos los usuarios".

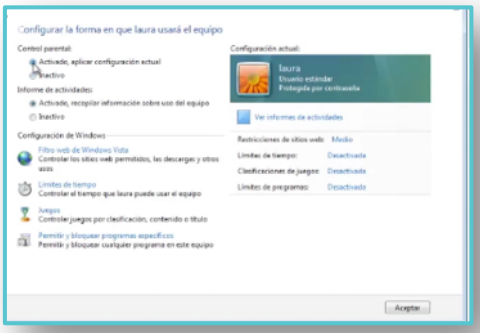
- Una vez dentro, comprobaremos que el usuario de "Administrador del equipo" posee una contraseña. Si no es así, la agregaremos, ya que si no, cualquier usuario podrá activar o desactivar el control parental.



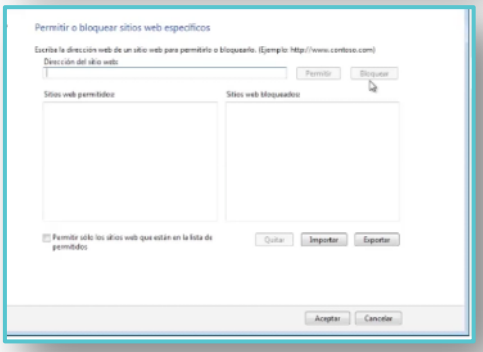
- Asegurauremos la contraseña del usuario "Administrador" y ya podremos continuar con la activación del control parental en el equipo.

- Crearemos una nueva cuenta de usuario para ser utilizada por el menor.

- A continuación, activaremos el Control parental y el “Informe de actividades”. Seleccionaremos el “Filtro Web” para indicar los sitios que el menor podrá visitar en Internet.

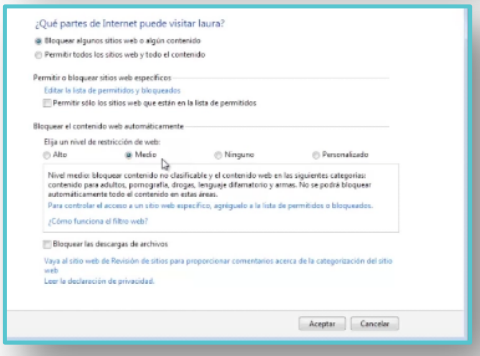


- Podremos escoger las direcciones web de los sitios que deseemos permitir así como los sitios que decidamos bloquear. Añadimos la URL en el apartado “Dirección de sitio web” y pulsamos en “Permitir” o “Bloquear” según corresponda.



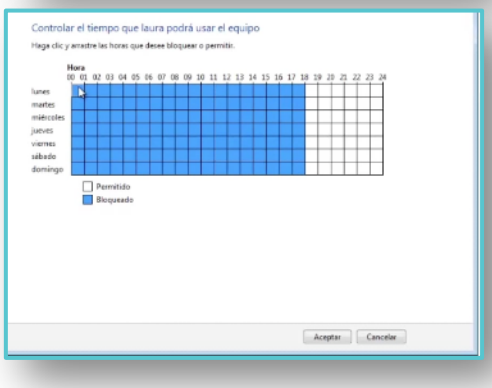
- También podremos bloquear el contenido web de forma automática eligiendo el nivel de “restricción de web”.

- Si queremos bloquear las descargas de archivos cuando Laura utilice el ordenador, activaremos dicha opción. Después de todos estos cambios, pulsaremos en “Aceptar”.



- Otra de las opciones que podemos hacer con el control parental es establecer unos límites de tiempo. De esta forma, podremos indicar el tiempo que el menor podrá usar el equipo.

- Haremos clic en las horas que queramos bloquear el uso y en blanco estarán las horas en las que Laura podrá utilizar el ordenador. Una vez elegido todo, pulsaremos en “Aceptar”.



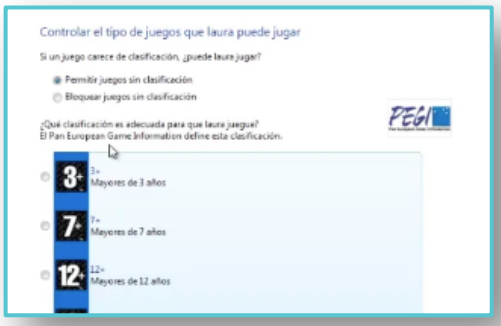
3.1. INSTALACIÓN Y CONFIGURACIÓN DE FILTROS PARENTALES EN ORDENADORES CON SISTEMA OPERATIVOS WINDOWS

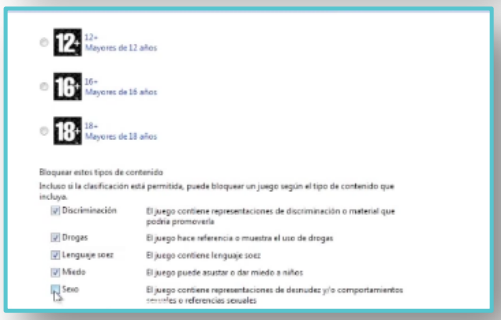
- Continuamos con los “Juegos”, donde podremos limitar el tipo de juegos que Laura podrá utilizar. Estableceremos por clasificación y tipos de contenido. De esta forma, podremos bloquear juegos que no tengan la clasificación PEGI, que es el sistema de clasificación por edades, utilizado en Europa.

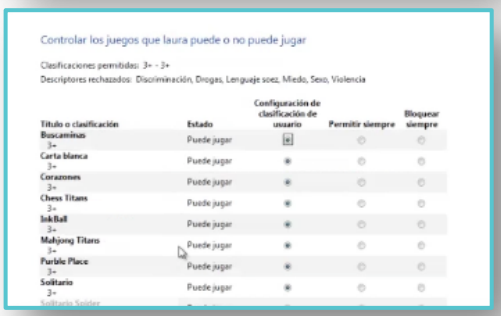
- También, podremos bloquear por tipo de contenido que incluyan los juegos. Una vez escogido todo, pulsamos en “Aceptar”.

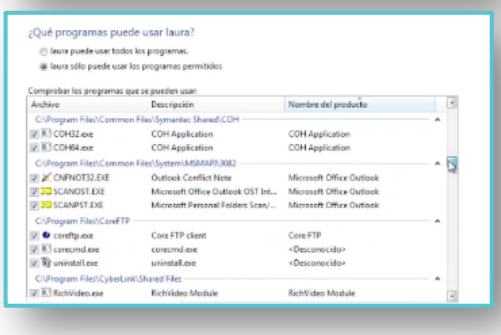
- Existe la opción de bloquear o permitir en el equipo cualquier juego por “nombre”, así se hará un rastreo de todos los que tenemos instalados en el equipo y estableceremos si bloquear, permitir o configurar según el usuario.

- Por último, podremos escoger los programas que el menor podrá usar. De esta forma, evitaremos el uso, por ejemplo, de la webcam del equipo si así lo establecemos.









Después de toda esta configuración, el control parental ya estará listo en el equipo para que el menor pueda usar el ordenador de forma segura.

3.2. CONTROL PARENTAL EN MÚLTIPLES ORDENADORES Y DISPOSITIVOS MÓVILES: QUSTODIO PARA FAMILIAS

El programa de control parental “Qustodio” permite de una forma sencilla visualizar las páginas visitadas por un menor en el equipo en el que se instale la aplicación.

También bloquea resultados de búsquedas inapropiadas, limita el tiempo de uso de un dispositivo según lo deseemos y restringe el uso de juegos y aplicaciones.

Está disponible para equipos que usan como sistema operativo Windows o Mac y también para teléfonos inteligentes y tabletas.

- Para instalarlo en el equipo que deseemos, accedemos a http://www.qustodio.com/es/ y pulsamos en “Comenzar ahora”. En tres sencillos pasos podremos completar la instalación y crear nuestra cuenta en Qustodio.

- Nos registramos en el formulario y creamos nuestra cuenta.

- Pulsamos en el botón verde de “Siguiente. Añadir mi primer usuario” y ponemos el nombre del menor. El año de nacimiento para que el programa sepa la edad y el género del niño.

- Elegimos también una imagen y guardamos.

3.2. CONTROL PARENTAL EN MÚLTIPLES ORDENADORES Y DISPOSITIVOS MÓVILES: QUSTODIO PARA FAMILIAS

- Podremos instalar Qustodio tanto en el equipo en el que estamos creando la cuenta como en otro dispositivo.

- Elegimos el sistema operativo y una vez completada la descarga, pulsamos en el archivo para su instalación.

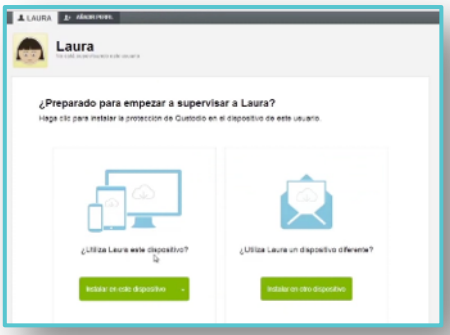
- Continuamos con los pasos indicados. Elegimos el idioma correspondiente, aceptamos e instalamos.

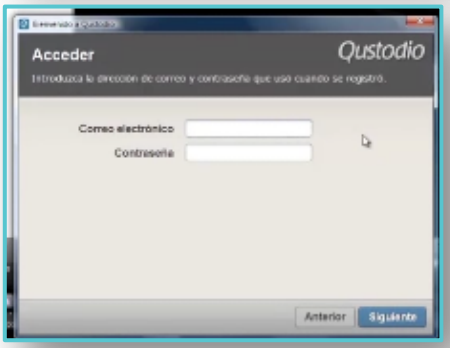
- Indicaremos que ya tenemos cuenta en Qustodio y continuaremos. Pondremos nuestro correo electrónico y nuestra contraseña de acceso.

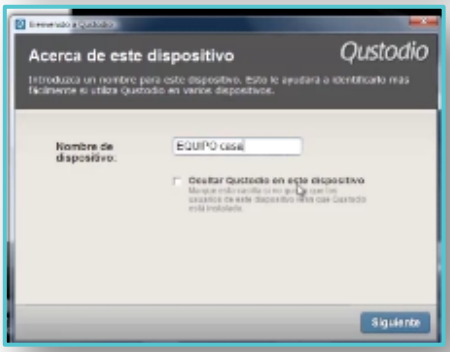
- Pulsaremos en siguiente y asignaremos un nombre al dispositivo. Podremos ocultar Qustodio en el dispositivo que estemos utilizando y así el menor no lo verá.

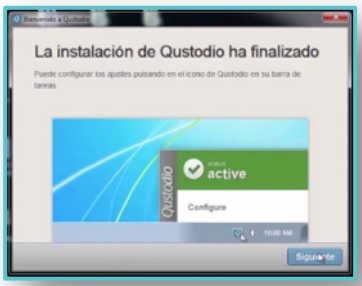
- Asociaremos al menor con el equipo en el que acabamos de hacer la instalación. Pondremos una contraseña y guardaremos.

- De esta forma, habremos finalizado la instalación de Qustodio en el equipo.



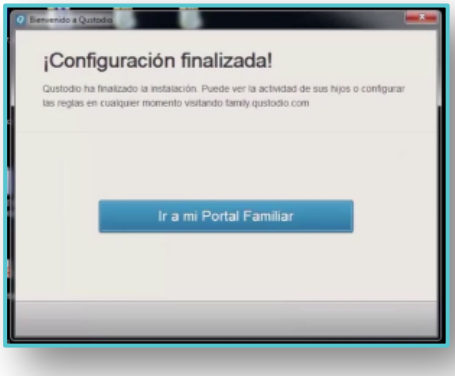




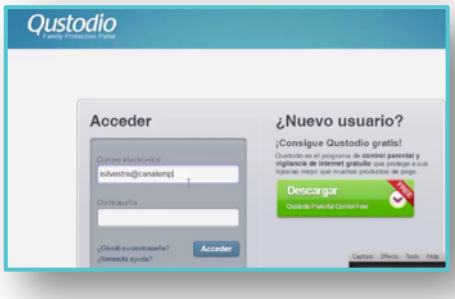


3.2. CONTROL PARENTAL EN MÚLTIPLES ORDENADORES Y DISPOSITIVOS MÓVILES: QUSTODIO PARA FAMILIAS

- Pulsamos en “Ir a mi Portal Familiar” y accederemos con nuestro correo electrónico y la contraseña indicada.

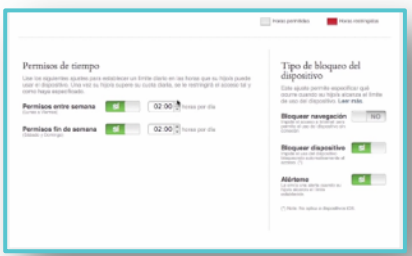


- Una vez dentro de nuestra cuenta, veremos cómo podemos configurar las “Reglas”. Lo primero, la navegación web. Aquí tendremos las categorías de los sitios web que están indicados para menores. Podríamos permitir, alertar o bloquear la página web que indiquemos y añadimos. También tendremos activados los sitios no categorizados así como el hacer búsquedas seguras a través del navegador.



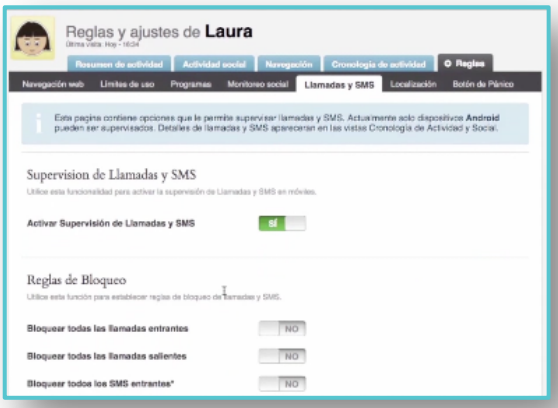
- Otra de las reglas que podemos configurar es el calendario de uso. Si lo activamos, podremos escoger los momentos en los que el menor pueda utilizar el ordenador. Otra forma de permisos de tiempo, es activar las horas por día que puede utilizar dicho equipo.

- También podremos bloquear la navegación, bloquear un dispositivo móvil si lo hemos asignado y también que nos envíen una alerta cuando alguna de las reglas se haya incumplido. Podremos boquear incluso números de teléfonos concretos, permitiéndolo o bloqueándolo.

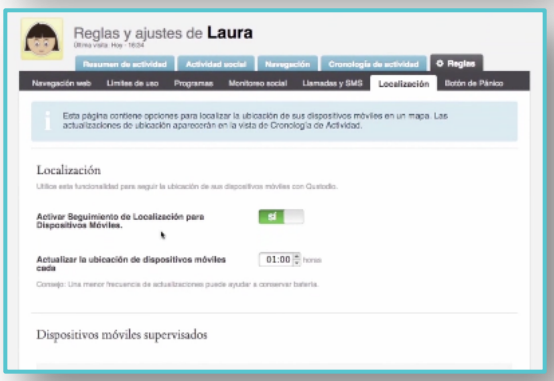


3.2. CONTROL PARENTAL EN MÚLTIPLES ORDENADORES Y DISPOSITIVOS MÓVILES: QUSTODIO PARA FAMILIAS

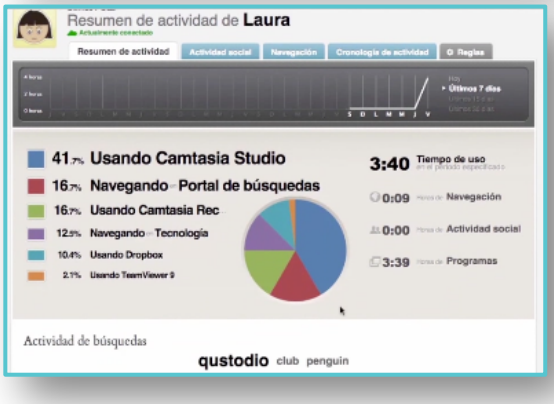
- Podremos supervisar las llamadas y mensajes de texto si hemos asignado un móvil a Laura. Tendremos algunas opciones de reglas bloqueo para las llamadas entrantes, salientes o bloquear todos los mensajes de texto entrantes.



- Otra de las funciones que nos permite Qustodio es la "Localización" y podremos activar ese seguimiento para el dispositivo móvil que hayamos asignado a Laura.



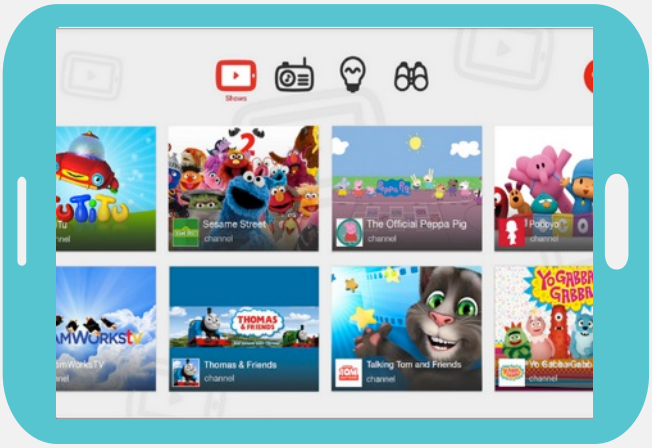
- Cuando hayan pasado unos días, Qustodio nos ofrecerá un resumen de la actividad del menor en el equipo. Como vemos, nos indica el tiempo de uso, la navegación y los programas que se han estado utilizando. Podremos ver esos programas y también las páginas web que ha visitado. En la sección de navegación, veremos esas páginas que Laura ha ido visitando.



- Y en la cronología de la actividad veremos las horas exactas en las que ha ido utilizando cada uno de los servicios.

Como vemos, Qustodio nos ofrece la posibilidad de establecer unas reglas de uso de los equipos, pero siempre tendríamos que tener en cuenta, hablar con los menores y llegar a un acuerdo para que entiendan que esta medida de protección es por su seguridad.

APLICACIÓN RECOMENDADA



YouTube KIDS

- Google ofrece su plataforma de vídeos adaptada para niños en YouTube Kids. Se trata de una aplicación que está disponible en Google Play, donde se puede ver contenido dedicado a los más pequeños.
- Dispone de una serie de opciones para que, como padres, podamos controlar el tipo de vídeos que los menores vean.
- En el Control Parental de YouTube Kids, se incluyen opciones como:
  - Temporalizador. Para limitar el tiempo de visualización de los vídeos. Avisando con una alarma cuando se cumpla el tiempo que establezcamos.
  - Ajustes de sonido. Para poder silenciar o aflojar la música.
  - Ajuste del buscador. Para seleccionar el tipo de vídeos que se pueden ver.
- Una nueva opción para que los menores disfruten de los contenidos que les gusten sin peligro a que aparezcan vídeos que no son aptos para su edad.

MÓDULO 6

RECOMENDACIONES FINALES DEL USO SEGURO DE INTERNET

6.2. CONCLUSIONES

Esperamos que hayáis descubierto algunas conceptos que desconocíais sobre la seguridad en Internet y en Redes Sociales.

Ahora es el momento de comunicarse toda la familia, prevenir con todas estas medidas que hemos comentado para evitar situaciones que no queremos que ocurran en Internet y sobre todo, fomentar una comunicación y conocimiento de todas estas funcionalidades que nos ofrece la Red.

PÁGINA RECOMENDADA

La Policía Nacional pone a disposición de los ciudadanos la Brigada de Investigación Tecnológica con el fin de mantener informados a los ciudadanos a través de las alertas tecnológicas todo lo que pudiera afectar a nesutra seguridad online como timos en internet o spam.

De esta forma, a través de http://www.policia.es/org_central/judicial/udef/alertas_1.html podremos seguir las últimas novedades en cuanto a seguridad en Internet.

PÁGINA RECOMENDADA

En la web https://www.gdt.guardiacivil.es/webgdt/home_alerta.php la Guardia Civil nos alerta de las últimas noticias sobre seguridad tecnológica para que estemos informados y tengamos precaución de los delitos online que se están detectando y así poder comentarlos en familia para que no lleguen a afectarnos.