MEDIDAS DE CONTROL Y MEDIACIÓN PARENTAL para padres, madres y educadores

SEMINARIO ONLINE

ÍNDICE

INTRODUCCIÓN

La comunicación con los menores se hace fundamental para conocer acerca de qué conocen o no de la seguridad en Internet.

Las recomendaciones de los expertos, nos informan de que no es recomendable prohibir todo uso de Internet.

Al igual que les enseñamos a llamar por teléfono por si lo necesitan en una emergencia, es necesario que compartamos con ellos momentos para mostrarles el uso correcto de la navegación en la Red.

Para que la navegación de los menores puedan realizarse con precaución, es necesario que mantengamos nuestros equipos informáticos protegidos y que dispongamos de los programas adecuados y herramientas que nos proporcionen esta seguridad online.

COMUNICACIÓN

CONOCIMIENTO

PREVENCIÓN

MÓDULO 1

IDENTIDAD DIGITAL

1.1. IMPORTANCIA DE LA IDENTIDAD DIGITAL

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.

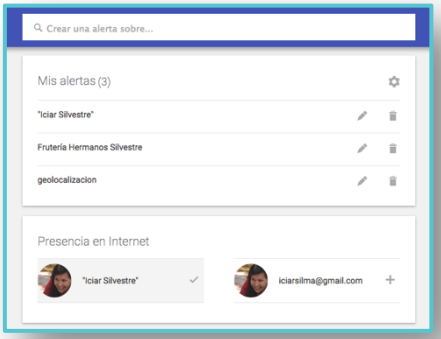
Por todo ello, es importante que sean precavidos sobre la información que comparten en Internet, ya que pueden traerles consecuencias tanto a corto y como a largo plazo.

1.2. COMPROBACIÓN DE NUESTRA HUELLA DIGITAL EN LA RED

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.



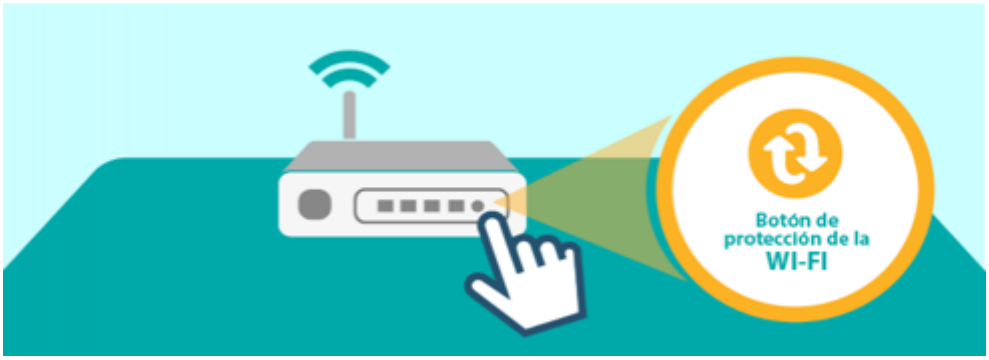
Con estas prácticas que podemos hacer junto con el menor, conocerá de una forma rápida la información sobre la identidad digital que los demás pueden conocer de él en Internet y la “reputación online” que se está construyendo y que afectará a su vida.

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.

MÓDULO 2

CONEXIONES SIEMPRE SEGURAS

5.2. RECOMENDACIONES CONFIGURACIÓN ROUTER



- Para mantener nuestra red WiFi segura, debemos renunciar a la comodidad de conectarnos mediante esta utilidad e introducir la contraseña WPA2 cada vez que queramos conectar un nuevo dispositivo a nuestra red.

- Para desactivarlo debemos acceder a la página de configuración de nuestro router:

  • La dirección de acceso por defecto suele ser la 192.168.1.1

  • Introducir el usuario y la contraseña de acceso. Si no las hemos cambiado suelen estar escritas en la parte posterior del router y en el manual del dispositivo, aunque es muy recomendable cambiar las credenciales por defecto.

  • Y deshabilitar la opción de WPS.

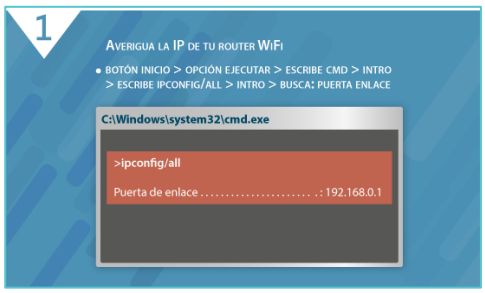
- Estos pasos son válidos para la mayor parte de los dispositivos pero podrían variar en función del modelo de router utilizado.

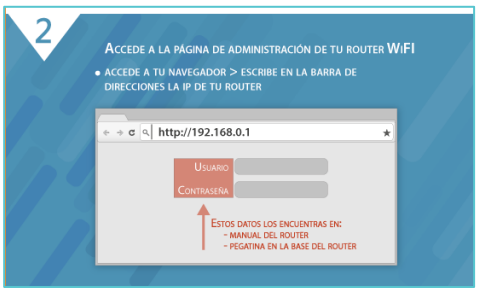
- Una vez desactivada la funcionalidad de WPS, lo correcto sería cambiar la contraseña WPA/WPA2 y también podemos aprovechar para cambiar el nombre de usuario y la contraseña por defecto.

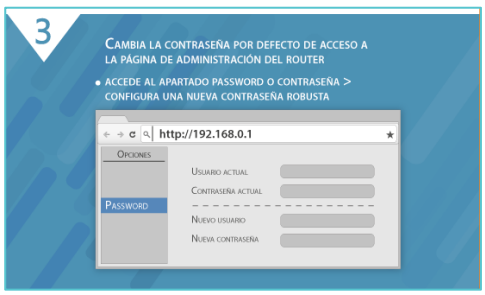
5.2. WIFIS SEGURAS

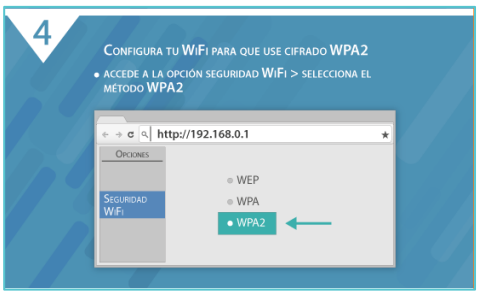
También deberemos cambiar el nombre que por defecto aparece en la wifi y la contraseña, ya que de este modo podrían conectarse a ella gente que no deseamos. Con todo lo que ello implica, ya que si algún ciberdelincuente realiza algo ilegal desde nuestra conexión, a quien pedirían responsabilidades sería a nosotros.

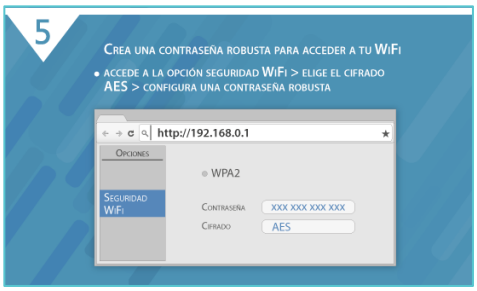
La OSI (Oficina de Información del Internauta) nos informa a través de esta infografía los pasos a seguir para configurar de forma segura nuestra WIFI). Se puede consultar en:
https://www.osi.es/sites/default/files/actualidad/blog/201503/infografia_asegurandolawifi.png

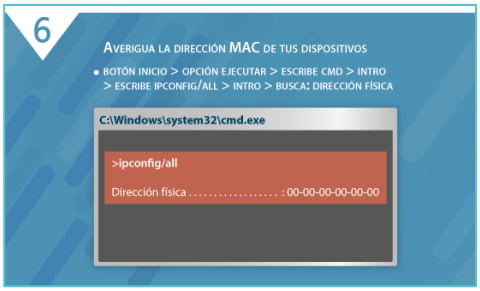












MÓDULO 3

MEDIDAS DE PROTECCIÓN EN EQUIPOS INFORMÁTICOS: ANTIVIRUS Y CORTAFUEGOS

3.1. 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.

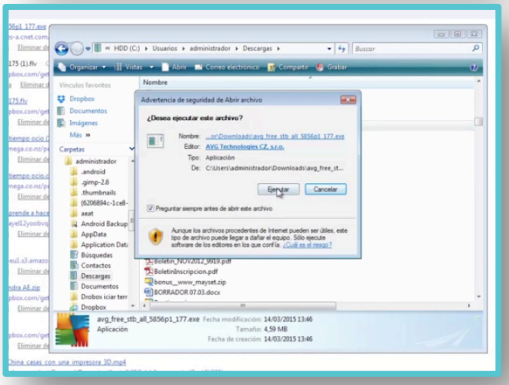
Entre sus acciones, realiza una verificación de los vínculos de una página web antes de hacer clic en ellos. Protege nuestra navegación en Redes Sociales y previene el espionaje y el robo de datos. Así como protección de correos electrónicos que puedan contener virus.

3.1. 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.

3.2. 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.

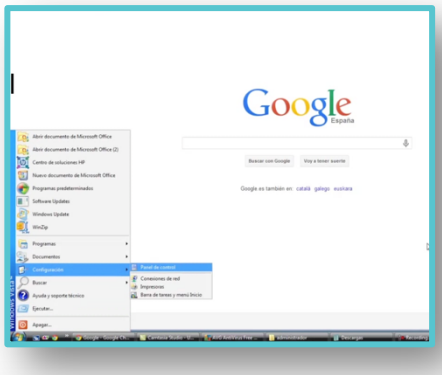
Para evitarlo, existen los programas que se llaman cortafuegos o dicho en inglés “Firewall”. Este tipo de programas, lo que evitan es que salga información que nosotros no deseamos y que tampoco entre información que no hemos aceptado.

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.

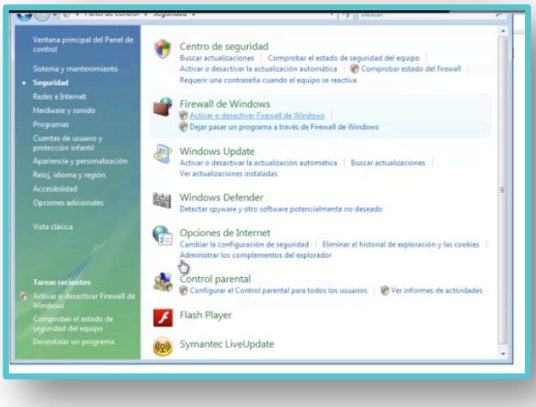
3.3. CONFIGURACIÓN DE CORTAFUEGOS EN EQUIPOS INFORMÁTICOS CON SISTEMA OPERATIVOS WINDOWS

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



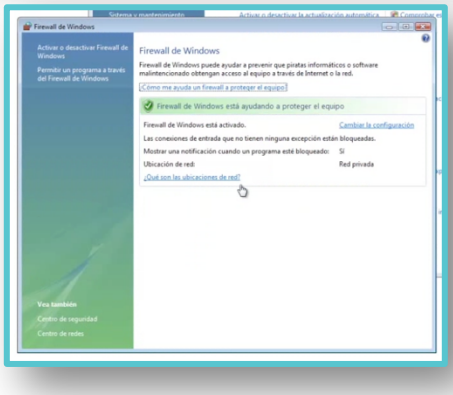
Para configurar el cortafuegos de Windows accederemos al "Panel de control" desde el apartado de "Configuración".

- 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 4

FILTROS PARENTALES COMO MEDIDA DE PRECAUCIÓN Y CONTROL

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

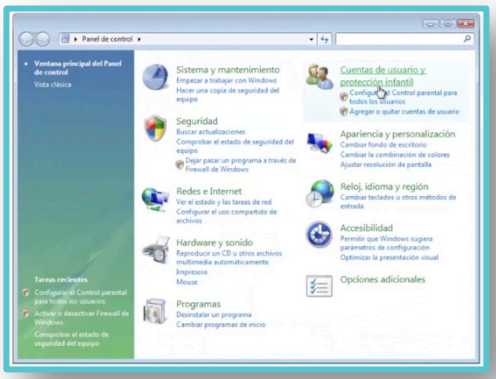
Para los menores, los ordenadores, las tabletas o los Smartphones son instrumentos cotidianos que utilizan de forma habitual.

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.

- Aseguraremos 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.

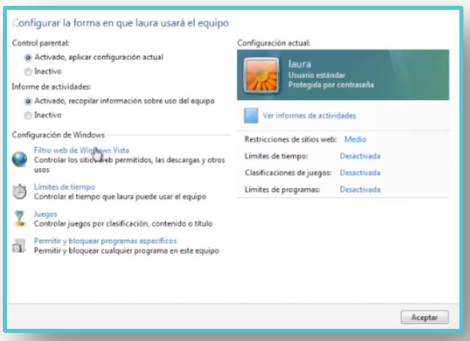
- Podremos escoger las direcciones web de los sitios que deseemos permitir así como los sitios que decidamos bloquear. Añadimos la URL en el apartado “Dirección de sitio web” y pulsamos en “Permitir” o “Bloquear” según corresponda.

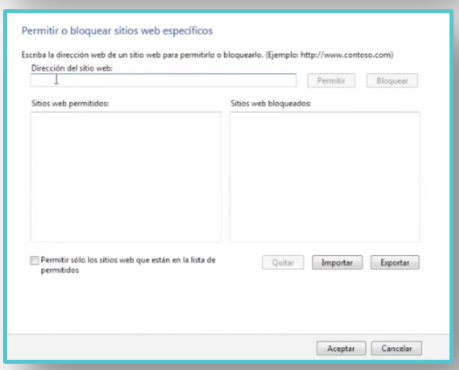
- También podremos bloquear el contenido web de forma automática eligiendo el nivel de “restricción de web”.

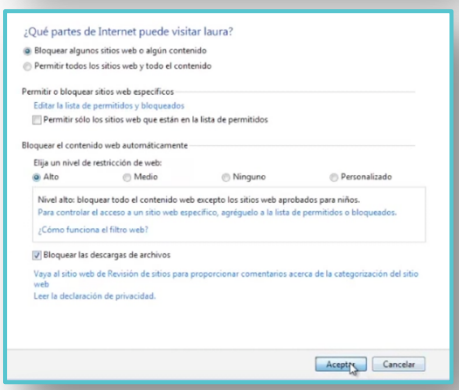
- Si queremos bloquear las descargas de archivos cuando Laura utilice el ordenador, activaremos dicha opción. Después de todos estos cambios, pulsaremos en “Aceptar”.

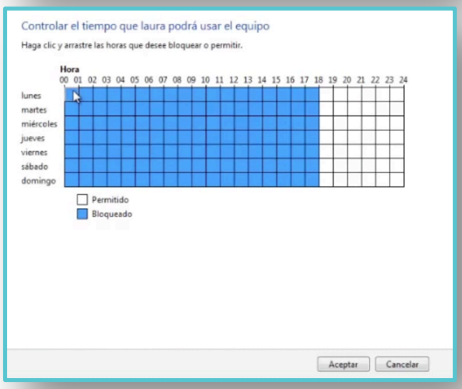
- Otra de las opciones que podemos hacer con el control parental es establecer unos límites de tiempo. De esta forma, podremos indicar el tiempo que el menor podrá usar el equipo.

- 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”.







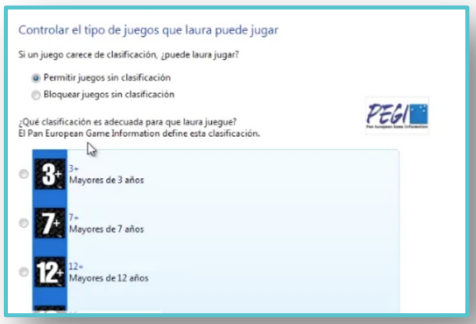


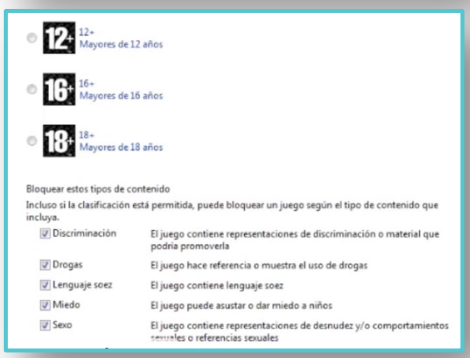
- Continuamos con los “Juegos”, donde podremos limitar el tipo de juegos que Laura podrá utilizar. Estableceremos por clasificación y tipos de contenido. De esta forma, podremos bloquear juegos que no tengan la clasificación PEGI, que es el sistema de clasificación por edades, utilizado en Europa.

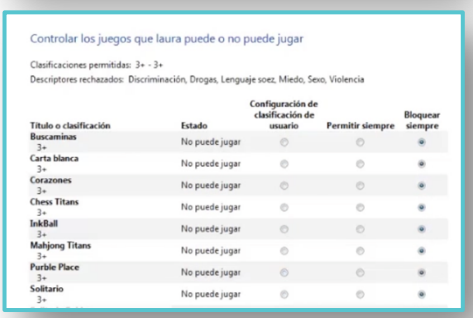
- También, podremos bloquear por tipo de contenido que incluyan los juegos. Una vez escogido todo, pulsamos en “Aceptar”.

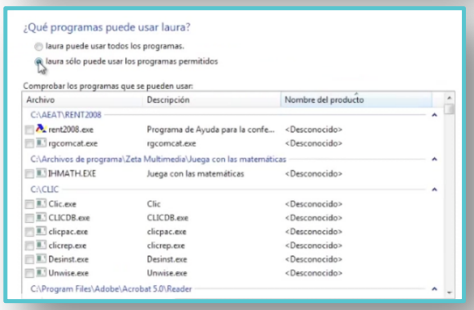
- Existe la opción de bloquear o permitir en el equipo cualquier juego por “nombre”, así se hará un rastreo de todos los que tenemos instalados en el equipo y estableceremos si bloquear, permitir o configurar según el usuario.

- 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.

4.2. 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.

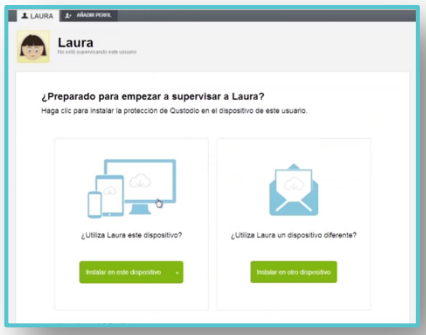
- Nos registramos en el formulario y creamos nuestra cuenta.

- 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.

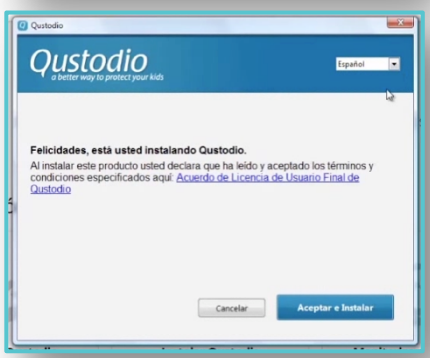
4.2. CONTROL PARENTAL EN MÚLTIPLES ORDENADORES Y DISPOSITIVOS MÓVILES: QUSTODIO PARA FAMILIAS

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



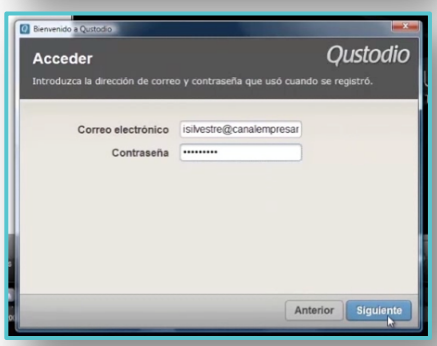
- Elegimos el sistema operativo y una vez completada la descarga, pulsamos en el archivo para su instalación.

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

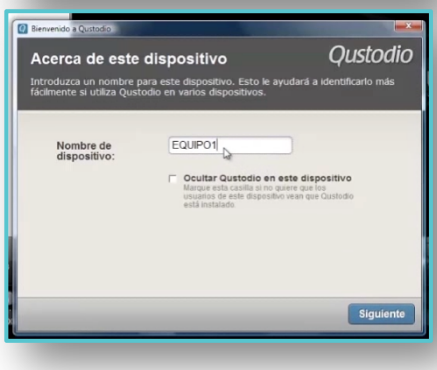


- Indicaremos que ya tenemos cuenta en Qustodio y continuaremos. Pondremos nuestro correo electrónico y nuestra contraseña de acceso.

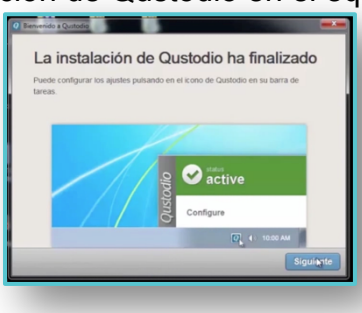
- Pulsaremos en siguiente y asignaremos un nombre al dispositivo. Podremos ocultar Qustodio en el dispositivo que estemos utilizando y así el menor no lo verá.



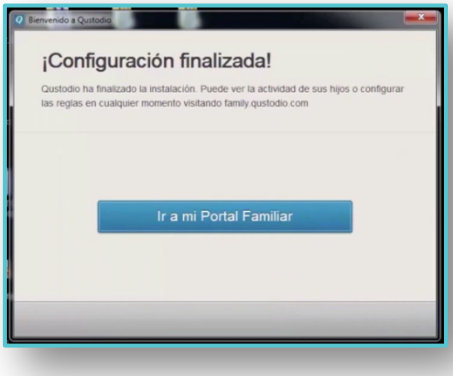
- Asociaremos al menor con el equipo en el que acabamos de hacer la instalación. Pondremos una contraseña y guardaremos.



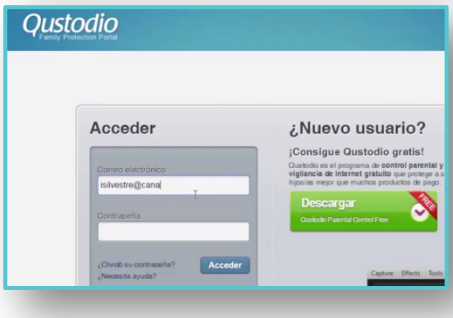
- De esta forma, habremos finalizado la instalación de Qustodio en el equipo.



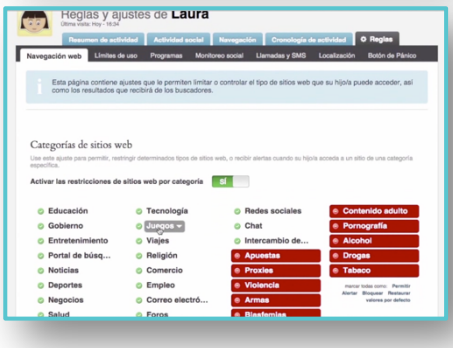
- Pulsamos en “Ir a mi Portal Familiar” y accederemos con nuestro correo electrónico y la contraseña indicada.



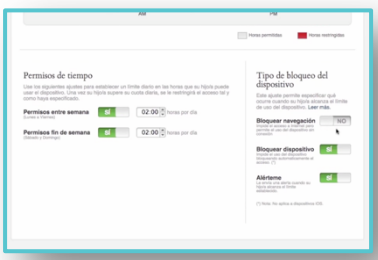
- Una vez dentro de nuestra cuenta, veremos cómo podemos configurar las “Reglas”. Lo primero, la navegación web. Aquí tendremos las categorías de los sitios web que están indicados para menores. Podríamos permitir, alertar o bloquear la página web que indiquemos y añadimos. También tendremos activados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

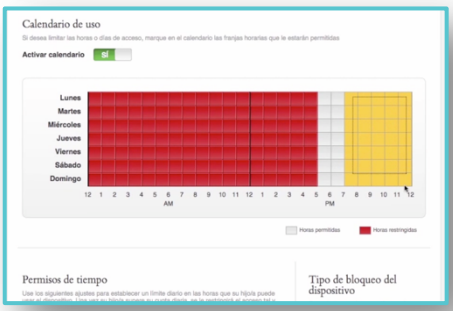


- Otra de las reglas que podemos configurar es el calendario de uso. Si lo activamos, podremos escoger los momentos en los que el menor pueda utilizar el ordenador. Otra forma de permisos de tiempo, es activar las horas por día que puede utilizar dicho equipo.



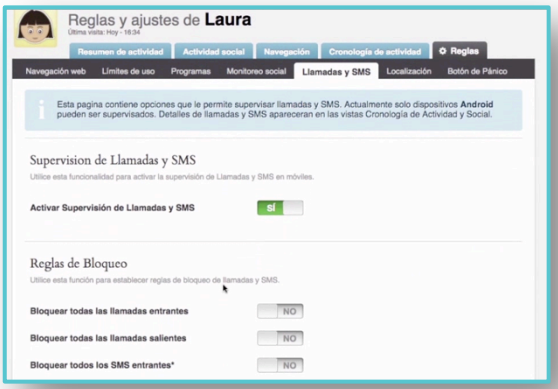
- También podremos bloquear la navegación, bloquear un dispositivo móvil si lo hemos asignado y también que nos envíen una alerta cuando alguna de las reglas se haya incumplido. Podremos boquear incluso números de teléfonos concretos, permitiéndolo o bloqueándolo.



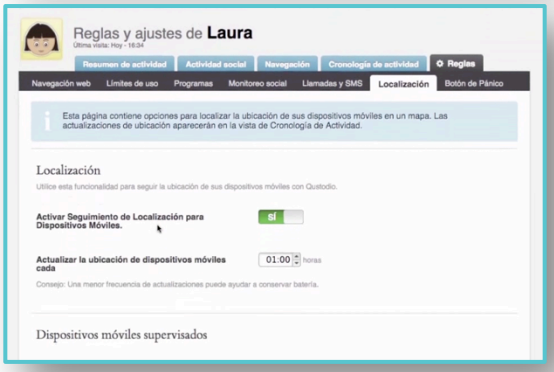


4.2. CONTROL PARENTAL EN MÚLTIPLES ORDENADORES Y DISPOSITIVOS MÓVILES: QUSTODIO PARA FAMILIAS

- 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.

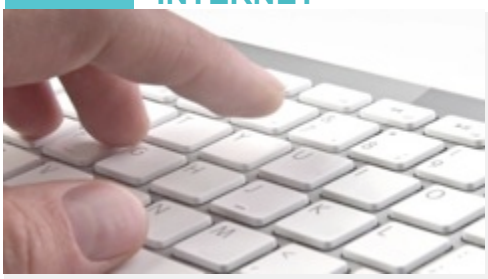
MÓDULO 5

RECOMENDACIONES FINALES DEL USO SEGURO DE INTERNET

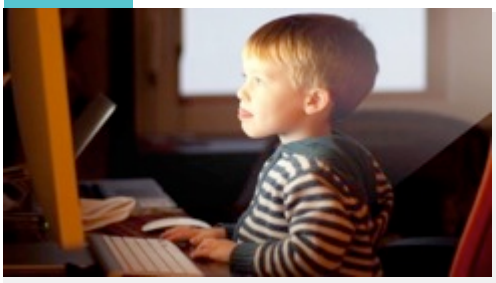
RECOMENDACIONES

Como resumen de todo lo visto hasta ahora, será necesario hablar y recordar en familia con los menores los siguientes mensajes que trasmitirles sobre seguridad en Internet:

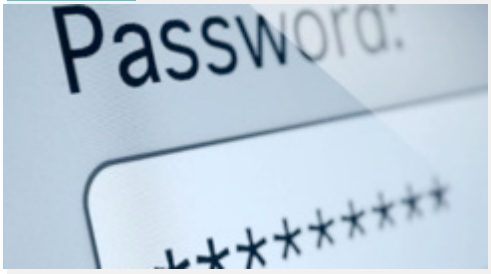
1 PENSAR BIEN LA INFORMACIÓN QUE PUBLICAMOS EN INTERNET



2 ORDENADOR SITUADO EN LUGAR COMÚN DEL HOGAR

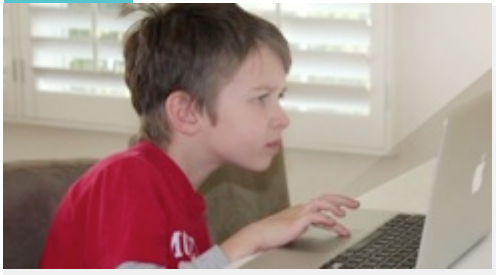


3 CONTRASEÑAS SEGURAS Y EQUIPOS CON ANTIVIRUS Y CORTAFUEGOS



4 VIGILAR LOS JUEGOS, CONSOLAS Y DISPOSITIVOS DEL MENOR

5 USAR SISTEMAS DE CONTROL PARENTAL



6 TAPAR LA WEBCAM DE LOS EQUIPOS INFORMÁTICOS DEL HOGAR

ANEXO

PÁGINAS RECOMENDADAS

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 nuestra 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.

Aviso Legal