UNIVERSIDAD DE ALCALÁ

Escuela Técnica Superior de Ingeniería Informática

Grado en Ingeniería Informática

Trabajo Fin de Grado

Estudio y análisis sobre el Software para Control Parental

Borja Casla Maroto

Julio / 2016

UNIVERSIDAD DE ALCALÁ

Escuela Técnica Superior de Ingeniería Informática

Grado en Ingeniería Informática

Trabajo Fin de Grado

Estudio y Análisis sobre el Software para Control Parental

Autor: Borja Casla Maroto

Director/es: Juana María López Fernández

TRIBUNAL:

Presidente: Rafael Rico López

Vocal 1: Rosa Estriégana Valdehita

Vocal 2: Juana María López Fernández

CALIFICACIÓN: .....

FECHA: .....

Agradecimientos

A mis padres y hermano, agradecerles todo el apoyo y paciencia que me han brindado durante estos años de estudio en los que ha habido buenos y malos momentos porque sin ellos hoy no estaría aquí superando la última barrera de esta complicada pero bonita carrera.

A mis compañeros y amigos, gracias por todos los momentos que hemos vivido juntos durante esta etapa que, simplemente, es el comienzo de una bonita amistad.

A mi tutor Juana María López Fernández, gracias por darme la oportunidad de realizar este Trabajo de Fin de Grado con el que tanto he aprendido.

A todos y cada uno de los profesores, gracias por vuestra labor.

Resumen

El presente documento es el resultado de la investigación llevada a cabo acerca del software de control parental disponible para poder ejercer un control sobre los menores cuando hacen uso de los dispositivos electrónicos, en especial del ordenador, para acceder a Internet u otras aplicaciones.

En Internet hay multitud de sitios web que suponen una amenaza para la educación de los menores, por lo que es necesario contrarrestar estos problemas con herramientas que se encarguen de filtrar el contenido al que pueden acceder y, en algunos casos, registrar la actividad que realizan en la web.

A lo largo del documento se localizan los principales riesgos activos en la red y se muestran soluciones para hacer frente a ellos.

Palabras clave

Internet, riesgos, control parental, software.

Abstract

This document is the result of research about parental control software available to control children when they use electronic devices to surfing the Internet or access other applications, especially computer.

There are many websites on the Internet that are a threat to the children education so it is necessary to counter these problems with tools that filter the content they can access and log the activity performed on the computer.

Throughout the document, the main risks of Internet are studied and propose solutions to avoid them.

Keywords

Internet, risks, parental control, software.

Índice

Resumen

Este Trabajo de Fin de Grado (TFG) que expongo se trata de una investigación sobre el software de control parental. El presente estudio pretende analizar las herramientas existentes para controlar la actividad de los menores cuando hacen uso de los dispositivos electrónicos (ordenador, Tablet, Smartphone) sin la supervisión de un adulto.

Para buscar una solución correcta es necesario localizar y estudiar el problema que provocó el desarrollo de este tipo de herramientas de supervisión y control. Por ello, antes de entrar a explicar en qué consiste un sistema de control parental, he realizado un estudio previo acerca del impacto que tiene Internet sobre los menores comentando brevemente los beneficios que supone la navegación online para éstos y analizando en profundidad los riesgos a los que están expuestos cuando acceden a la red sin ningún tipo de control y/o supervisión, así como una breve introducción a las redes sociales.

Una vez analizados los peligros de Internet que pueden afectar a los menores, es momento de buscar una solución. La solución es hacer uso de un sistema de control parental que se encargue de bloquear y filtrar el acceso a determinados contenidos web o aplicaciones, y de establecer un control sobre el equipo y las actividades que se realizan con él. Entre las funcionalidades más comunes de los sistemas de control parental está: controlar los tiempos de uso del dispositivo, denegar el acceso a páginas web, bloquear aplicaciones o monitorizar la actividad realizada por el menor. Estos sistemas emplean diferentes técnicas o algoritmos para filtrar el contenido web y decidir si es apto para menores o, por el contrario, se trata de contenido inapropiado que debe ser bloqueado, más adelante se explican estas técnicas.

Otra de las funcionalidades de los sistemas de control parental es la monitorización de las tareas llevadas a cabo en el equipo. Los propios equipos incorporan mecanismos para controlar la actividad. En el documento se explica en qué consisten estos mecanismos y cómo acceder a ellos.

Las herramientas de control parental se pueden clasificar en función del nivel de aplicación donde se desea realizar el control:

- Los sistemas de control parental integrados en el propio sistema operativo, realizan un control y seguimiento de la actividad que se realiza en cualquier aplicación del equipo y únicamente sirven para controlar ese dispositivo. Se estudian las herramientas integradas en Windows, Ubuntu y MAC.
- Las medidas de control parental relacionadas con las DNS se aplican en la tarjeta de red del equipo para controlar ese dispositivo o se configuran en el router para poder realizar un control de todos los dispositivos conectados a la misma red. Se trata de la herramienta OpenDNS.
- Las herramientas configuradas en los navegadores web sirven, exclusivamente, para controlar la actividad en dicho navegador y quedan inservibles cuando el menor accede a Internet con otro navegador diferente. Es la opción menos recomendada.
- Los desarrolladores de software comercializan este tipo de herramientas, muchas de ellas de código abierto puestas a disposición de los usuarios sin ningún coste de uso.

Se han analizado las dos herramientas más utilizadas de este tipo, Qustodio y K9 Web Protection. Estos sistemas se instalan en el dispositivo del menor y realizan un control de toda la actividad que se puede llevar a cabo, así como realizar un registro del uso que hacen del equipo.

- Los proveedores de Internet también ofrecen servicios de pago que incorporan software de control parental.

En el apartado de *Análisis de Resultados* se muestra una comparación de las herramientas analizadas en base a la funcionalidad que ofrece cada una de ellas, así como una valoración de los resultados obtenidos tras haber probado dichas herramientas.

Por último, expongo las conclusiones obtenidas tras haber finalizado la investigación y desarrollo del TFG.

1. Introducción

En los últimos años se ha incrementado notablemente el uso de las tecnologías de información y comunicación (TIC) en los hogares. Según un estudio realizado por el Instituto Nacional de Estadística en el año 2015, el 74,8 % de los hogares cuentan con al menos un ordenador y el 74,4% dispone de acceso a Internet. Este crecimiento de las TIC en los hogares se debe, en gran parte, a la necesidad de estar conectado a la Red.

Internet se ha convertido en la mayor fuente de información y búsqueda de recursos a la que los usuarios acceden por motivos de formación, entretenimiento o relaciones sociales. Estos usuarios son cada vez más prematuros y no es difícil encontrar a menores de cuatro o cinco años manejando un dispositivo con total fluidez sin que los padres se den cuenta del verdadero riesgo que ello puede conllevar.

Hoy en día, la mayoría de dispositivos tienen acceso a Internet para poder navegar por la Red por lo que el menor está expuesto a los beneficios y riesgos de la Red. No siempre se hace un uso adecuado de las herramientas que Internet pone a disposición de los usuarios y se puede navegar por páginas de contenido no apto para los menores que pueden poner en peligro su correcto desarrollo y educación.

Para tratar de evitar este tipo de situaciones y garantizar un acceso seguro a los menores en la Red se incorporaron los sistemas de control parental en sistemas operativos y navegadores Web. Los sistemas de control parental tienen por objetivo restringir el acceso de los menores a contenidos a los que padres o tutores consideran inadecuados para la seguridad y la educación del menor.

A día de hoy, no se ha encontrado una solución bien definida para poder controlar, con total seguridad, el acceso de los menores a todo tipo de contenido no apto. La mayoría de padres desconoce la existencia de herramientas que permiten controlar el acceso a los diversos contenidos de Internet y es por ello por lo que no realizan un control sobre sus hijos exponiéndoles a multitud de peligros.

El objetivo principal del presente Trabajo de Fin de Grado es realizar un estudio y análisis exhaustivo acerca de las diferentes herramientas disponibles para ejercer un control sobre los menores cuando hacen uso de Internet sin la supervisión de padres o tutores. Para ello, se analizarán los peligros a los que se exponen los menores cuando navegan por la red sin un sistema de control parental y, posteriormente, se realizará un estudio completo de las diferentes herramientas de control parental disponibles, mostrando resultados de las evaluaciones. Por último, se realizará una comparativa de lo que nos ofrece cada herramienta y cuál de ellas es la más efectiva.

2. Uso de Internet por los menores

2.1. Introducción

La popularización de Internet ha hecho que sea una parte cada vez más importante de la cultura actual, especialmente para los niños y jóvenes, quienes lo utilizan principalmente para:

- **Búsqueda de información**. Internet es la principal fuente de información en todo el Mundo y es por ello por lo que recurrimos a la Red en la mayoría de los casos para obtener la información necesaria. Sin embargo, localizar la información correcta y con exactitud no es una tarea fácil debido a que en la actualidad existen más de 3000 millones de páginas web con todo tipo de información.
  Cuando se busca información en Internet hay que tener en cuenta de donde se ha obtenido esa información y quién la ha publicado ya que hay una gran cantidad de contenido erróneo.

- **Comunicación**. A través de Internet nos podemos comunicar con personas situadas en cualquier parte del Mundo por medio del correo electrónico, redes sociales y demás aplicaciones de mensajería instantánea como, por ejemplo, Skype.

- **Entretenimiento**. En Internet hay una amplia variedad de formas de entretenimiento tales como escuchar música, ver películas, juegos online, etc.

Un estudio realizado por el Instituto Nacional de Tecnologías de la Comunicación a niños y adolescentes revela que el lugar habitual donde llevan a cabo los menores estas actividades es en el hogar y, en menor medida, en el centro escolar.

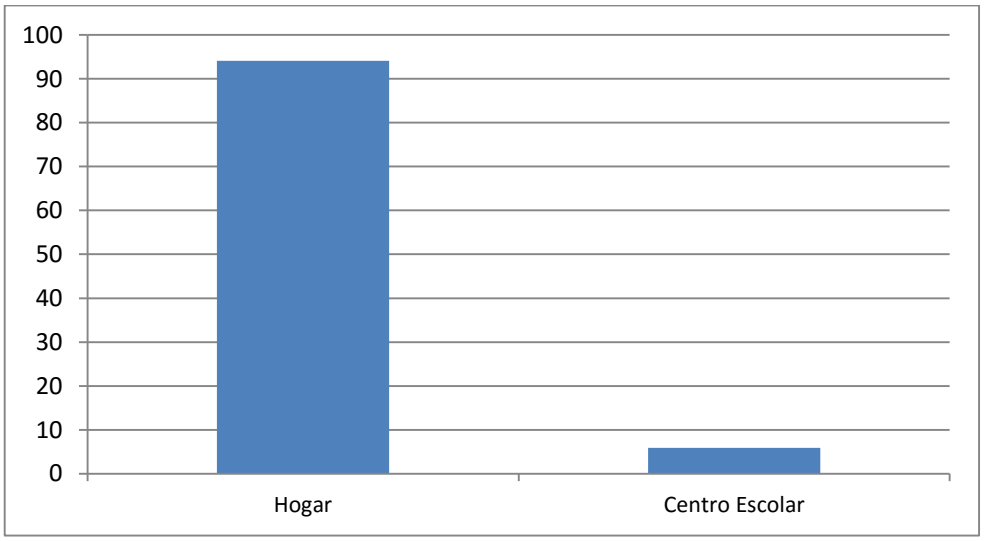

Ilustración 1: Lugar habitual de acceso a Internet por los menores entre 10 y 16 años

Hace unos años era habitual el uso de Internet, mayoritariamente, en los centros escolares pues no estaba al alcance de todos disponer de un ordenador con conexión de banda ancha en los hogares. El rápido crecimiento y evolución de las tecnologías, el abaratamiento del hardware y la facilidad de uso del software han propiciado un acercamiento masivo de los usuarios a Internet y a los servicios que ofrece. Por este motivo, ha aumentado el uso de

dispositivos electrónicos con acceso a Internet en los hogares y el 94,1% de los menores acceden a la Red habitualmente desde casa.

El acceso diario de los menores a la Red aumenta conforme lo hace su edad. Los adolescentes entre 15 y 16 años son los que se conectan a Internet desde casa con más frecuencia por motivos escolares y relaciones sociales. A continuación, se visualiza un gráfico que muestra la frecuencia de acceso a Internet de los menores entre 9 y 16 años:

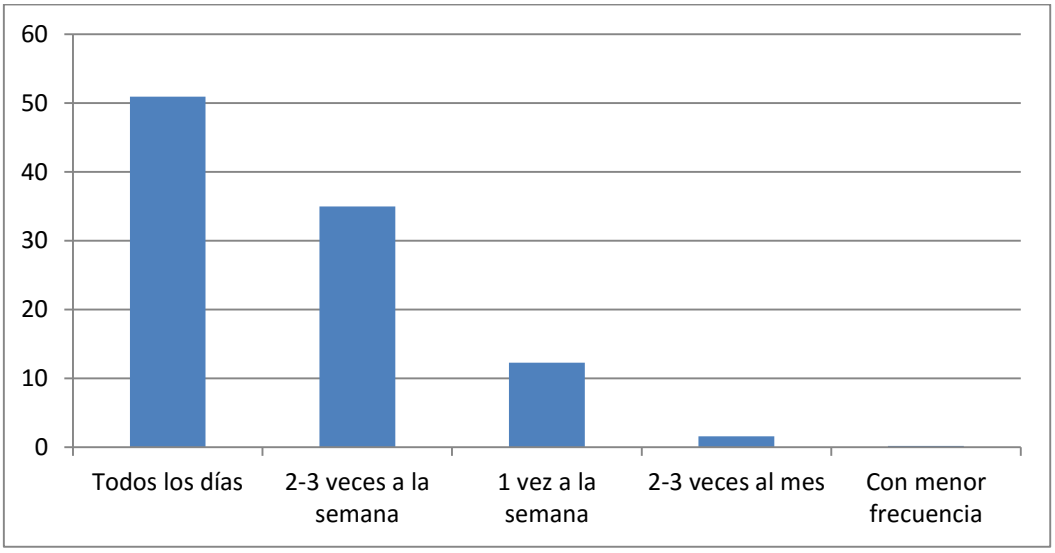

Ilustración 2: Frecuencia de acceso a Internet por los menores

Como se puede apreciar, los menores hacen uso de Internet muy frecuentemente por diferentes motivos: aproximadamente la mitad accede a diario a la Red y más de la tercera parte lo hace alrededor de dos o tres veces a la semana.

Los datos mostrados revelan que el uso de las nuevas tecnologías e Internet se han convertido en una parte fundamental en la vida de los menores. Por ello, es importante que los padres o tutores sean buenos conocedores de los beneficios que supone el uso de las tecnologías para el desarrollo y formación de los jóvenes, pero también deben conocer los peligros a los que están expuestos cuando acceden sin ningún tipo de supervisión a Internet. A continuación, se muestra una tabla resumida de las oportunidades y riesgos del uso de Internet por los menores que profundizaré en los siguientes apartados:

		Contenido: Menor como receptor	Contacto: Menor como participante	Conducta: Menor como actor
Oportunidades	**Aprendizaje, capacidad y conocimiento digital**	Recursos educativos	Contacto con otros niños que comparten los mismos intereses	Aprendizaje por iniciativa propia o en colaboración
	Participación y compromiso social	Información global	Intercambio con otros grupos de interés	Formas concretas de participación social
	Creatividad y expresión	Diversidad de recursos	Haber sido invitado/inspirado para crear o participar	Creador de contenido
	Identidad y conexión social	Recomendaciones (persona, salud, sexualidad, etc.)	Participar en redes sociales, compartir experiencias con otros	Expresión de la propia identidad
Riesgos	**Comercial**	Publicidad, spam, patrocinios	Ser observados, recopilación de información personal	Apuestas, descargas ilegales, hackeo
	Agresivo	Contenido violento, sanguinolento, agresivo	Ser victimizado, acosado o perseguido	Victimizar o acosar a otro
	Sexual	Contenido pornográfico / sexual dañino	Conocer extraños, sufrir grooming	Crear/subir a la red material pornográfico
	Valores	Racismo, información y sugerencias equivocas (ej. drogas)	Autolesionarse, ser víctima de sugerencias indeseables	Dar malos consejos (ej. suicidio)

Tabla 1: Oportunidades y riesgos del uso de Internet por los menores

2.2. Beneficios

Internet ha sido uno de los inventos más importantes en la historia de la civilización y, sin su invención, las tecnologías no serían lo que son hoy en día. Se trata de una red de computadoras que conecta millones de dispositivos informáticos a lo largo de todo el mundo, conectados por líneas telefónicas, satélites o cables. Esta interconexión permite comunicarse en tiempo real con cualquier dispositivo desde cualquier parte del mundo, lo que hace que se pueda obtener información, en directo, de lo que está pasando en un preciso momento.

Internet es la mayor fuente de información que hay disponible a nuestro alcance hoy en día. Cualquier tipo de información acerca de cualquier tema está disponible en la Red. Para facilitar la búsqueda de información existen motores de búsqueda como Google o Yahoo, entre otros, que, en función de los datos que el usuario envíe, realizan una búsqueda de páginas web en los diferentes servidores de Internet.

Otro de los beneficios que nos ofrece Internet es la inmensa cantidad de servicios de los que dispone tales como ver películas, escuchar música, juegos online, compras, banca online, etc…

Cuando niños y jóvenes hacen uso de Internet de una manera medida y responsable pueden obtener múltiples beneficios para su educación y desarrollo. Entre todas las ventajas que supone el uso de Internet por los menores, cabe destacar las siguientes:

- **Excelente comunicación**. A través de la Red pueden comunicarse de una forma inmediata, rápida y eficaz. Los niños pueden establecer una comunicación con otra persona que se encuentra en cualquier parte del mundo e intercambiar todo tipo de archivos tales como videos y música.

- **Información abundante y recursos**. Cuando es necesario buscar algún tipo de información o investigar acerca de cualquier tema, pueden hacerlo rápidamente accediendo a Internet sin necesidad de acudir a una biblioteca. Internet estimula la investigación y el descubrimiento de los pequeños cuando acceden para buscar información sobre un tema que les despierta interés y les ayuda a saber navegar por la red y ampliar sus conocimientos.

- **Herramienta de apoyo escolar**. En Internet pueden encontrar ejercicios y juegos para complementar lo que estudian en el centro escolar y, de esta manera, mejorar sus resultados académicos.

- **Herramienta de entretenimiento**. El juego controlado puede ser estimulante, didáctico y positivo en el desarrollo del menor. Además de jugar, existen muchas formas de entretenimiento en línea como música, vídeos, películas, libros.

- **Mejorar sus conocimientos tecnológicos**. Una de las principales ventajas de que los niños usen Internet es que les ayudará a reforzar y mejorar sus conocimientos sobre informática, algo fundamental ahora y de cara al futuro.

- **Socialización**. Los menores más tímidos pueden socializarse a través de Internet conociendo a otros jóvenes para compartir aficiones o intercambiar culturas, por ejemplo. Este tema requiere supervisión y control por parte de los padres o tutores del menor para que no entren en contacto con personas no deseadas.

Internet es realmente útil y cuenta con numerosas ventajas para los menores si se hace un uso adecuado y controlado, pero también existen riesgos a los que están expuestos los menores cuando navegan por la Red.

2.3. Riesgos

Internet es un “mundo abierto” que ofrece un amplio abanico de posibilidades a los menores para complementar su educación y desarrollo. Sin embargo, la falta de un acuerdo sobre el enfoque adecuado para educar y proteger a los niños añade nuevos retos a la experiencia en la red de los pequeños. Además, las diferencias culturales y geográficas en las normas legales y sociales reflejan el hecho de que no existe un criterio universalmente aceptado de lo que define a una persona como un niño, o de lo que es apropiado para los niños, por lo que no hay una definición explícita acerca del contenido y comportamiento inapropiado. Esto supone un problema cuando los menores navegan por la Web exponiéndoles a una gran cantidad de peligros.

El uso excesivo y descontrolado de Internet aumenta las probabilidades de sufrir cualquiera de los riesgos activos de la red que se pueden agrupar en:

1. **Relativos al contenido de Internet**

Internet ofrece infinitud de contenido para todo tipo de usuarios. No todos los contenidos deberían ser accesibles para niños y jóvenes, pero esto es muy difícil de conseguir por las diferencias culturales citadas anteriormente. Debería prestarse especial atención a aquellos contenidos que, sin ser ilegales en general, pueden herir a los usuarios más jóvenes.

El riesgo de acceder a contenidos inapropiados para una determinada edad puede ser consecuencia de la propia conducta del usuario al buscarlos intencionadamente o puede darse de forma involuntaria, topándose con ellos sin previa intención.

El riesgo de encontrarse con contenido incorrecto, por ejemplo, en Wikipedia o en un anuncio de productos falsos está directamente relacionado con la conducta de otros usuarios y se multiplica con la aparición de aplicaciones 2.0, donde la corrección es como mucho controlada por los propios usuarios en lugar de por un editor.
Los contenidos sesgados, por ejemplo, los diseñados para transmitir un mensaje concreto o resultados de búsquedas manipulados con una intención determinada, pueden ser tomados como ciertos por usuarios inexpertos.

El tipo de contenido clasificado como ilegal, depende principalmente de la legislación nacional, aunque cierto tipo de contenido es ilegal en la mayoría de los países. En cualquier caso, los contenidos ilegales están disponibles y tanto los jóvenes como los más pequeños pueden acceder a ellos de forma involuntaria y también intencionada.

Los contenidos violentos son otro ejemplo de contenido inapropiado por razón de la edad. El efecto que el contenido violento tiene sobre quien lo ve depende en gran medida de la edad del usuario, de sus hábitos de consumir contenidos online y de su entorno social. En especial, los niños más jóvenes deberían estar protegidos frente a este tipo de contenidos violentos con algún tipo de aplicación de control parental.

2. **Relativo al uso y funcionamiento de Internet**

Estos riesgos son producidos dentro de la propia red. En Internet continuamente se producen situaciones de riesgo derivadas de la tecnología utilizada. La descarga de archivos puede introducir software malicioso en el ordenador y pueden hacer que nuestro ordenador se vea vulnerado.
Cuando se navega por la Web existe el riesgo de recibir o estar expuesto a publicidad o anuncios de productos o servicios ajenos que no son adecuados para los menores, como anuncios de sexo o apuestas. Cuanta más información personal facilitan los usuarios más expuestos están a recibir publicidad. Dado que los niños no son, en muchos casos, conscientes de las consecuencias de introducir su información personal en formularios de la web, constituye para ellos un alto riesgo.

El uso excesivo y prolongado de Internet puede tener como consecuencia la ciberadicción o trastorno de adicción a Internet (IAD), uso excesivo del ordenador que interfiere con la vida

diaria. A medida que los usuarios pasan mayor tiempo en la red, el riesgo de volverse adicto a Internet crece. En especial los jóvenes son vulnerables al hecho de no ser capaces de dejar el ordenador. Por lo tanto, este riesgo está principalmente relacionado con la propia conducta del menor.

3. **Relativo a la comunicación en Internet**

Utilizar Internet como medio de comunicación tiene el riesgo de contactar con usuarios malintencionados por medio de herramientas de mensajería instantánea, chats, foros o correo electrónico.

Los pederastas utilizan Internet como medio para contactar con niños y jóvenes, ocultando su identidad adulta. Todos los espacios web que ofrecen plataformas para contactos e intercambios entre personas pueden suponer un riesgo de captación de menores o de grooming.

En el intercambio de mensajería instantánea por Internet también está muy presente el riesgo de sexting, una práctica que supone el envío de imágenes o vídeos de contenido erótico-pornográfico por parte de menores o jóvenes, principalmente, por medio del teléfono móvil. En sí mismo, incluso en un contexto de privacidad adecuado, puede suponer problemas ligados a la pornografía infantil. Otro incidente se produce cuando esas imágenes salen del ámbito privado, haciéndose públicas, suponiendo el menoscabo de la intimidad y el honor de la persona y, en muchos casos, el comienzo de campañas de ciberbullying.

4. **Relativo a temas económicos**

Los menores navegan por la web sin ser conscientes de que el acceso a determinadas páginas requiere facilitar datos que pueden incurrir un gasto importante con sólo introducir el nombre o DNI. A través de las compras online, existe un amplio abanico de opciones en la red que pueden suponer un engaño y su consiguiente fraude económico.
Por otro lado, los menores no son conscientes de las descargas ilegales que realizan sin darse cuenta de los prejuicios que ello supone para los propietarios.

Los riesgos a los que el menor está expuesto cuando accede a Internet son similares a los que puede sufrir en el "mundo físico". La continua evolución de la red y la naturalidad con la que se navega hacen que sea un lugar donde los delincuentes pueden actuar con total facilidad favorecidos por los siguientes factores:

- **Fácil acceso a la información**. En Internet es muy sencillo encontrar información de todo tipo, de una forma libre y gratuita, sin ningún tipo de restricción.
- **Fácil comunicación**. En el "mundo virtual" todo está a nuestro alcance, no existen distancias ni barreras que impidan conectarse mediante personalidades ficticias.
- **Accesibilidad**. Internet no tiene límites, un usuario puede estar conectado a todas horas y en el momento que lo desee de forma inmediata. Esto hace que se potencien adicciones como la violencia o la ludopatía.

- **Anonimato**. En la red pueden realizarse muchas acciones de manera anónima lo que permite a algunas personas realizar actos en Internet que no se atreverían a hacer en el "mundo físico".

2.3.1. Malware

El malware, también conocido como código o software malicioso, es un software que se inserta en un sistema de forma encubierta con la intención de comprometer la confidencialidad, integridad y disponibilidad de los datos, aplicaciones o el sistema operativo. Malware tales como virus o gusanos son diseñados para realizar estas funciones que ponen en peligro la privacidad de los usuarios que no son conscientes, inicialmente, de la introducción de este tipo de software en el sistema.

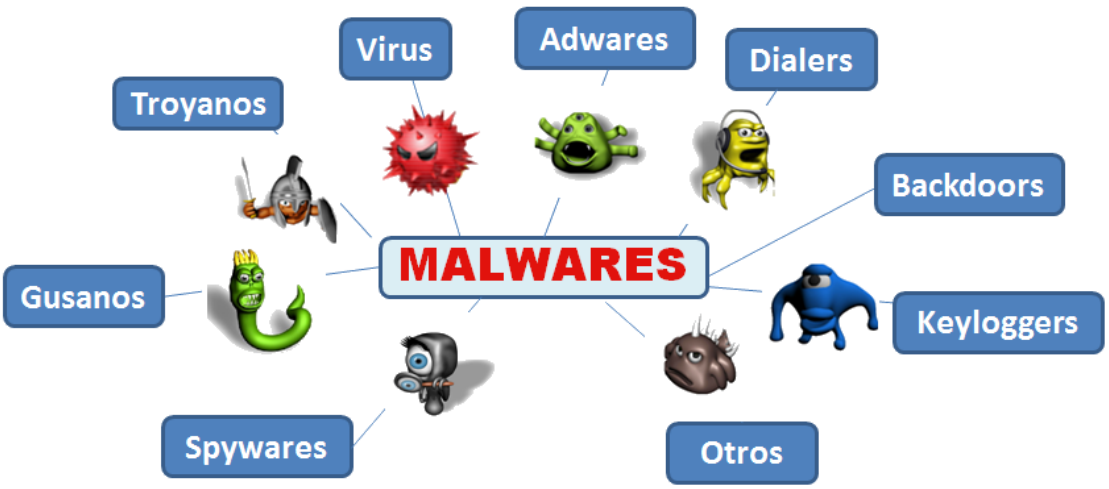

Ilustración 3: Diferentes tipos de malware

2.3.1.1. Virus

Un virus es un software diseñado para auto-replicarse y distribuir las copias, infectando a otros archivos ejecutables. Cuando se ejecuta un archivo infectado se activa el virus, produciendo los efectos dañinos que tenga programados como pueden ser la aparición de publicidad masiva, envío de información privada a terceros o la destrucción del sistema.

Su principal objetivo es modificar otros programas y destruir información.

2.3.1.2. Gusanos (worms)

Un gusano informático es similar a un virus por su diseño, y es considerado una subclase de virus, a diferencia de que los gusanos no necesitan la interacción del usuario para propagarse. Este tipo de malware es un programa independiente capaz de auto-replicarse y propagarse por sí mismo, sin modificar u ocultarse bajo otros programas. Se reproducen utilizando diferentes medios de comunicación como las redes locales, el correo electrónico, los programas de mensajería instantánea, redes P2P, dispositivos USB y las redes sociales.

Al contrario de lo que ocurre con los virus informáticos, el objetivo de los gusanos es reproducirse y alcanzar el máximo de distribución entre los equipos de la red. Como máximo, los gusanos tienden a replicarse en tal medida que saturan los recursos de las computadoras, provocando un ataque por denegación de servicio (caída del sistema). No obstante, algunos gusanos pueden incluir como parte de su código algún virus informático, bomba lógica, troyano o backdoor, que actúe sobre los equipos en los que se logren establecer.

2.3.1.3. Troyanos

Son programas maliciosos que llegan al sistema como aplicaciones aparentemente inofensivas, pero cuando se ejecutan, dejan instalado en el equipo un segundo programa oculto de carácter malicioso. Este programa oculto es lo que se conoce como troyano.

Los troyanos no son virus ni gusanos puesto que no tienen la capacidad de replicarse por sí mismos, pero en muchos casos, los virus y gusanos liberan troyanos en los sistemas que infectan para que cumplan funciones específicas, como, por ejemplo, capturar todo lo que el usuario ingresa por teclado. El principal uso de los troyanos es para obtener acceso remoto a un sistema infectado a través de una puerta trasera o backdoor.

2.3.1.4. Spyware

Los programas espía o spyware extraen cualquier tipo de información acerca del sistema o personal del usuario de manera oculta sin su consentimiento. Este tipo de malware es difícil de detectar ya que no se trata de software destructivo ni produce efectos visibles, puede producir ralentización cuando se usa Internet porque usan parte del ancho de banda para su propio servicio. Hacen uso de medios de comunicación tales como el correo electrónico o la red local para enviar la información recabada a sus propios servidores.

El spyware se instala en el sistema mediante un virus, un troyano enviado a través del correo electrónico, o bien puede estar oculto en la instalación de un software, aparentemente, seguro.

El objetivo del spyware es recopilar todo tipo de información del equipo, normalmente en forma de estadísticas, y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

2.3.1.5. Adware

Se trata de un tipo de malware similar al spyware, recopilan secretamente información personal a través de Internet y la reenvían a servidores propios, frecuentemente con fines publicitarios.

Al contrario que el spyware, el adware sí que tiene efectos visibles ya que exhibe una gran cantidad de banners publicitarios durante la navegación en Internet o la ejecución de determinados programas gratuitos. La instalación de este software provoca ralentizaciones en el funcionamiento del sistema.

Se instala en la computadora de la misma manera que el spyware, por medio de troyanos, o debido a la aceptación de los términos de licencia de determinados programas gratuitos que conlleva la instalación de estos banners publicitarios.

2.3.1.6. Dialers

Se trata de un tipo de troyano que modifica o suplanta el acceso telefónico sin consentimiento del usuario. Su funcionamiento consiste en cambiar el número de teléfono con el que se tiene conexión a Internet con lo que cada vez que el usuario se conecta a la red, el módem realiza una llamada a un número diferente con una tarifa especial. Los dialers se descargan en el sistema mediante el uso de pop-ups o la ejecución de archivos en la web.

Las consecuencias de este tipo de malware es la elevada cantidad económica que supone en la factura telefónica del cliente.

Este riesgo solo lo corren los usuarios que se conectan por medio de conexiones de marcado de modem a la red telefónica.

2.3.1.7. Backdoors

También conocidos como puertas traseras, se instalan en nuestro equipo por medio de virus y gusanos. Este tipo de malware abre una puerta trasera, o backdoor, que permite a un atacante acceder y controlar el PC de manera remota a través de Internet.

Un backdoor consiste en una conexión entre cliente y servidor. El cliente reside en el ordenador remoto del intruso, y el servidor es el sistema infectado. Cuando se establece una conexión entre el cliente y el servidor, el usuario remoto tiene un cierto grado de control sobre el sistema infectado. Las puertas traseras permiten a un atacante realizar un cierto conjunto de acciones en un sistema, tales como la transferencia de archivos, la adquisición de contraseñas, o ejecutar una serie de comandos.

2.3.1.8. Keyloggers

Un keylogger es un programa que registra las pulsaciones realizadas en el teclado de un equipo que ha sido infectado. Este malware se instala entre el software del teclado y el sistema operativo para interceptar y registrar la información introducida por el usuario, sin que éste se percate de ello. La información recogida se almacena en un fichero local del equipo infectado.

Este tipo de malware suele instalarse junto con virus, gusanos o troyanos, de manera que el atacante tiene acceso remoto al equipo y obtiene el fichero que contiene la información recogida por el keylogger.

2.3.1.9. Otros

- **Rootkit.** Un rootkit es un conjunto de herramientas que se instalan en un sistema para alterar el funcionamiento normal del sistema de una manera maliciosa y sigilosa. Estas herramientas sirven para ocultar programas o procesos al usuario que están llevando a cabo acciones maliciosas en el sistema. Por ejemplo, si en el sistema hay un backdoor para llevar a cabo tareas de espionaje, el rootkit ocultará los puertos abiertos que delaten la comunicación.

Los rootkits no pueden ser detectados porque muestran información falsa cuando un usuario intenta analizar el sistema para ver qué procesos se están ejecutando, mostrando todos los procesos excepto él mismo y los que está ocultando.
Se introducen en el sistema por medio de virus y troyanos.

- **Hoaxes.** Se trata de falsas advertencias de virus que se envían, generalmente, a través del correo electrónico cuyo contenido es la descripción de un virus que contiene el equipo y que sus consecuencias son devastadoras para la integridad de los datos que requiere la realización de una acción inmediata para proteger los datos y aplicaciones.
  Su objetivo es generar miedo e inseguridad en los usuarios para que reenvíen los mensajes a la mayor cantidad posible de direcciones y de esta manera realizar acciones como captar esas direcciones de correo, saturar la red y los servidores de correo, o cometer algún tipo de fraude.

- **Spam.** También conocido como correo basura, es la recepción de mensajes de correo electrónico que no han sido solicitados por el usuario. Estos mensajes tienen el fin de hacer publicidad ofertando productos y servicios que, en muchos casos, son fraudulentos.

- **Mailbomb o bomba de e-mail.** Consiste en el envío masivo de mensajes de correo electrónico excesivamente largos con el objetivo de saturar la capacidad de almacenaje del servidor de correo y evitar que los mensajes lleguen a su destinatario. También puede provocar la caída del sistema debido a la gran cantidad de datos que contienen los mensajes.

- **Bombas lógicas.** Programas maliciosos ocultos en el sistema que contienen una secuencia de código que activa el virus cuando se produce un acontecimiento determinado como una fecha o la combinación de teclas.

2.3.2. Ciberbullying

El desarrollo de Internet y las redes sociales como uno de los principales medios de comunicación entre los menores ha aumentado el riesgo de que los menores puedan sufrir ciberbullying. El ciberbullying, también conocido como ciberacoso, "implica utilizar información y comunicación tecnológica tal como el correo electrónico, teléfono móvil, sitio Web personal, foros y mensaje de texto inmediato, difamatorio, así como apoyar deliberadamente, y repetitivamente, el comportamiento hostil por parte de un individuo o grupo, con la finalidad de dañar a otro"[1].

Otra definición importante sobre lo qué es el ciberacoso fue la realizada por la asociación "Safe2Tell": "La intimidación por medio de Internet consiste en la promoción del comportamiento hostil de algún individuo que tiene la intención de hacer daño a otros individuos, por medio del uso de la tecnología informática y comunicaciones; por ejemplo, el

[1] Bill Belsey Profesor de Enseñanza Media. Springbank, Alberta Canadá. "Cyberbullying". www.cyberbullying.ca

correo electrónico, teléfonos móviles, mensajes de texto, mensajes instantáneos y sitios Web personales"[2].

Este tipo de acoso no necesariamente debe tener un objetivo sexual como en el caso del grooming.

2.3.2.1. Características

Las características más relevantes del ciberacoso son las siguientes:

- **Anonimato.** El acosador, que suele conocer a la víctima, se oculta tras una identidad falsa utilizando los datos de otra persona o por medio de un personaje ficticio creado para acosar en la web.
- **Recopilación de información.** Se obtiene información personal de la víctima rastreando su dirección IP para ver qué tipo de actividad realiza cuando accede a Internet.
- **Repetición.** Por lo general, los ataques no son incidentes aislados. La víctima sufre continuos acosos en forma de amenazas y chantajes que suelen consistir en la publicación de vídeos, fotos e información personal en diversos sitios web, tales como redes sociales, que compromete a la víctima.
- **Recursos utilizados**. El medio utilizado para realizar el acoso es de naturaleza tecnológica. Las herramientas más utilizadas para llevar a cabo este tipo de ataques son las redes sociales (Facebook, Twitter, Instagram), plataformas de correo electrónico, foros web y el uso de aplicaciones de mensajería instantánea como WhatsApp.

2.3.2.2. Cómo se produce

Como se ha comentado anteriormente, los jóvenes hacen uso de las redes sociales, blogs y sistemas de mensajería instantánea para intimidar a sus compañeros. Una de las técnicas más utilizadas es la difusión de fotografías, previamente retocadas, para ridiculizar a la víctima.

A continuación, se muestran algunas de las formas más habituales de realizar ciberacoso:

- **Teléfono móvil**. La telefonía móvil ha experimentado un gran crecimiento en los últimos años con la aparición de los Smartphones y su uso comienza a realizarse cada vez a edades más tempranas. El uso del teléfono móvil proporciona muchas ventajas al usuario, pero también se identifican algunos efectos negativos.
  El móvil se ha convertido en un medio propicio para acosar a través de llamadas ocultas con contenidos violentos, envío de mensajes amenazantes, grabaciones de vídeo o mensajes de voz. Con la aparición de aplicaciones de mensajería como WhatsApp, se puede difundir con facilidad videos y fotografías de las víctimas.

- **Correo electrónico.** Hoy en día, se ha extendido el uso del correo electrónico en los menores ya sea por motivos escolares (actualmente, los profesores utilizan el correo electrónico para enviar material didáctico a los alumnos), creación de una cuenta de correo para una plataforma de videojuegos, o para comunicarse. Una de las mayores

[2] Asociación Safe2Tell "¿Es su hijo víctima de intimidación por medio de Internet?"

ventajas del correo electrónico es la posibilidad de enviar archivos de texto, imágenes, vídeo y audio, así como de almacenar grandes cantidades de información.

Existen multitud de servidores de correo que permiten crear cuentas de correo de forma gratuita y sin necesidad de verificar los datos registrados. Por este motivo, ha aumentado la creación de identidades falsas y la suplantación de identidades.

Esta forma de ciberbullying consiste en el envío repetido de mensajes de correo electrónico con contenido ofensivo y violento a la víctima. Resulta complicado averiguar cuál es la verdadera identidad del acosador debido a los continuos cambios de IP que se producen en la red. No obstante, existen filtros que permiten bloquear o eliminar automáticamente mensajes de remitentes indeseables.

2.3.3. Grooming

El grooming es un problema relativo a la seguridad de los menores en Internet, se trata del conjunto de estrategias utilizadas para construir una conexión emocional con el menor y, de esta manera, ganarse su confianza con el único objetivo de obtener concesiones de índole sexual tales como el envío de imágenes o vídeos y propuestas de encuentros en persona.

Mientras que el ciberacoso es una situación que, generalmente, se produce entre iguales (ambos son menores) y su objetivo es amenazar causando pánico en la víctima, en el grooming el acosador es un adulto cuyo único objetivo es sexual. Por lo tanto, el grooming se produce cuando un adulto, mediante una identidad falsa, engaña a un menor a través de aplicaciones de mensajería instantánea como WhatsApp, correo electrónico o redes sociales intentando obtener imágenes de contenido sexual, para luego extorsionar al menor mediante chantajes y amenazas, dificultando que la víctima pueda salir de esa situación y que la relación se corte.

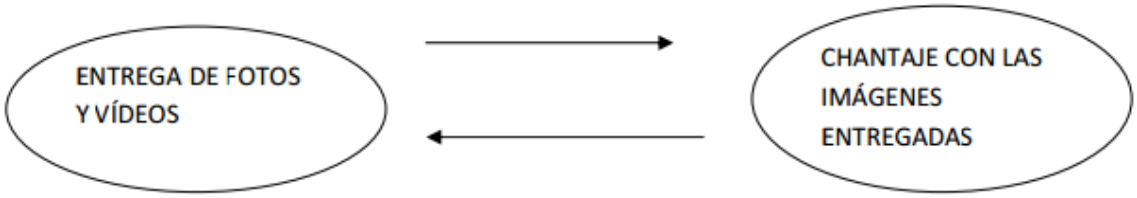

Ilustración 4: Grooming

2.3.3.1. Fases del Grooming

1. **Fase de acercamiento.** En esta primera fase, el adulto comienza investigando al menor acerca de las tareas que realiza en Internet. Una vez recogida la información, utiliza una identidad falsa para comunicarse con el menor e intenta establecer contacto con él mediante el intercambio de gustos e inquietudes.

2. **Fase de relación.** Con el fin de ganarse la confianza del menor, el adulto realiza confesiones íntimas personales e inventadas. El objetivo de esta fase es obtener información íntima del menor para después utilizarla como chantaje.

3. **Fase de envío de imágenes comprometidas.** Una vez que ha logrado hacerse con la confianza del menor, se lanza a pedirle imágenes de carácter sexual, vídeos o que lo haga delante de la webcam.

4. **Fase de chantaje.** Si ha conseguido hacerse con la alguna imagen del menor, la utiliza como medio de chantaje para que continúe enviando imágenes cada vez con mayor contenido sexual, amenazándole con que si no lo hace difundirá toda la información privada e imágenes que ha conseguido.

2.3.4. Sexting

El sexting consiste en la difusión de imágenes de carácter sexual a través de un teléfono móvil, redes sociales o una aplicación de mensajería instantánea. Este riesgo ha ido aumentando entre los adolescentes a medida que la tecnología ha avanzado y los Smartphone tienen la capacidad de grabar y enviar grabaciones de alta calidad.

Cuando esas imágenes y vídeos salen del ámbito privado, haciéndose públicas, pueden suponer la aparición de otros riesgos como grooming o ciberbullying.

2.4. Los menores en las redes sociales

Una red social es un medio de comunicación social que consiste en la creación de un perfil público, o privado, para encontrar gente con el objetivo de relacionarse a través de Internet. Las redes sociales sirven para compartir todo tipo de información y contenido entre las personas que han establecido un vínculo virtual. Su propósito es facilitar la comunicación y otros temas sociales en el sitio web.

Actualmente, las redes sociales se pueden clasificar en dos tipos:

- **Directas**. Son redes sociales en las que se produce un intercambio de información e intereses comunes entre los usuarios y pueden controlar la información que comparten. Los usuarios crean perfiles a través de los cuales gestionan su información personal y la relación con otros usuarios. El acceso a la información contenida en los perfiles suele estar condicionada por el grado de privacidad que dichos usuarios establezcan para los mismos.
  Las redes sociales directas se pueden clasificar según el enfoque empleado:

Según finalidad	Según modo de funcionamiento	Según grado de apertura	Según nivel de integración
De ocio	De contenidos	Públicas	De integración vertical
De uso profesional	Basada en perfiles: personales/profesionales	Privadas	De integración horizontal
	Microblogging		

Tabla 2: Clasificación redes sociales directas. FUENTE: ONTSI

- **Indirectas**. Son aquellas cuyos usuarios no suelen disponer de un perfil visible para el resto, existiendo un individuo o grupo que controla y dirige la información o las discusiones en torno a un tema concreto. Dentro de estas redes sociales se encuentran los foros y blogs.
  Los foros sirven para intercambiar información, valoraciones y opiniones sobre un tema produciéndose un debate bidireccional entre los usuarios.

Los blogs son sitios web donde un autor argumenta aspectos que pueden ser relevantes o de interés para los usuarios.

Un estudio realizado a jóvenes y menores muestra cuáles son las redes sociales más utilizadas por éstos.

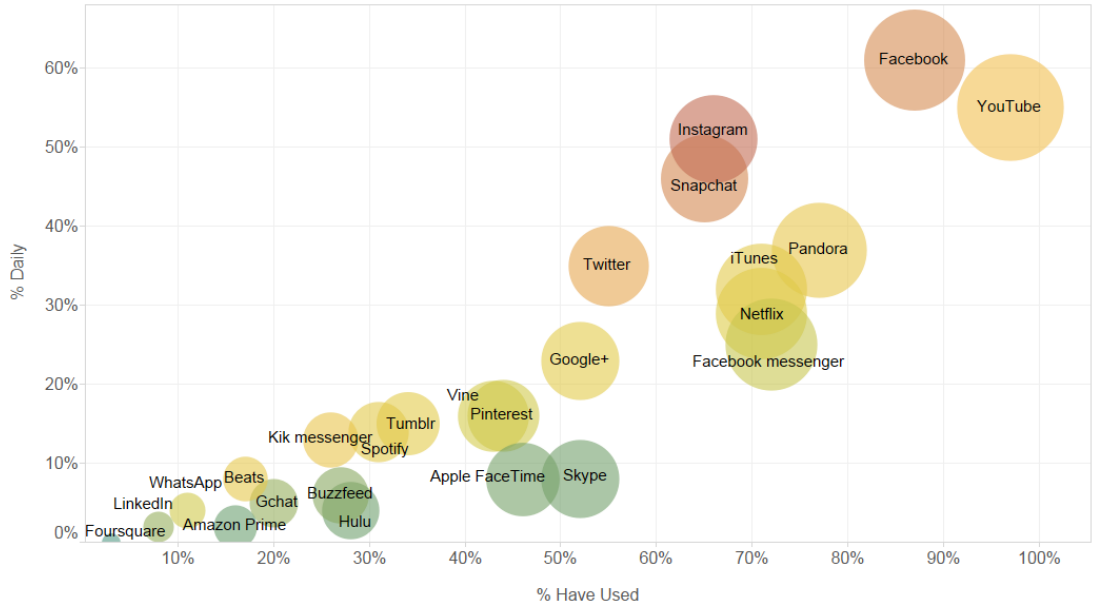

Ilustración 5: Redes sociales más utilizadas por los adolescentes

El uso de estas redes sociales por parte de los menores se está convirtiendo en una actividad habitual que, haciendo de ellas un uso adecuado y controlado, supone numerosas ventajas tales como el acceso a un nuevo medio de comunicación y relación social, que les permite crear y mantener tanto el contacto directo con sus amigos y conocidos como una nueva forma de identidad y compartir aficiones. Las redes sociales también pueden suponer un importante avance en su desarrollo y formación al acceder a foros o blogs donde se puede obtener información importante.

Sin embargo, los menores a pesar de tener ciertas nociones de seguridad descuidan ciertos aspectos y, en ocasiones, no otorgan la importancia que se merece a los datos personales e imágenes (tanto de los demás como de ellos mismos) y no piensan en las repercusiones. Uno de los principales problemas se produce cuando el menor tiene su perfil en estado público permitiendo que todos los usuarios, amigos o no, puedan acceder a toda la información publicada (nombre, edad, sexo, imágenes, aficiones, gustos, formación académica, …). Según un estudio de la Agencia Española de Protección de Datos y el Instituto de Tecnologías de la Comunicación, el 77% de los menores de 18 años tiene su perfil abierto al público.
Los problemas más importantes son los propios de la red comentados anteriormente. La compartición de imágenes, videos o cualquier tipo de información personal favorece la aparición de riesgos como el ciberbullying y grooming.

3. Control Parental

3.1. Introducción

Durante el tiempo que los niños y adolescentes están conectados en la red los contenidos a los que pueden acceder pueden ser impredecibles. La probabilidad de que un menor llegue a contenidos no aptos para su edad es cada día más alta. ¿Qué contenidos se podrían considerar como no aptos para un menor? Se considera contenido no apto, según la Ley Orgánica para la Protección del Niño y del Adolescente, a "*aquellos que promuevan, hagan apología o inciten a la violencia, a la guerra, a la comisión de hechos punibles, al racismo, a la desigualdad entre el hombre y la mujer; a la xenofobia, a la intolerancia religiosa y cualquier otro tipo, al uso y consumo de cigarrillos y derivados del tabaco, de bebidas alcohólicas y demás especies previstas en la legislación sobre la materia y de sustancias estupefacientes y psicotrópicas, así como aquellos de carácter pornográfico, que atenten contra la seguridad de la Nación o que sean contrarios a los principios de una sociedad democrática".*

Se debe tener presente que, dependiendo de las opiniones o creencias de padres o tutores, el nivel de gravedad de los contenidos puede variar. Debemos ser conscientes de que cada vez más las redes sociales, los programas de mensajería instantánea y las salas de chat, que tanto gustan a los menores, pueden ser utilizados por depredadores sexuales y acosadores que se aprovechan de la inocencia y la vulnerabilidad de los menores. Una estadística publicada por el Portal Statista[3], muestra las mayores preocupaciones que tienen los padres cuando los menores hacen uso de Internet:

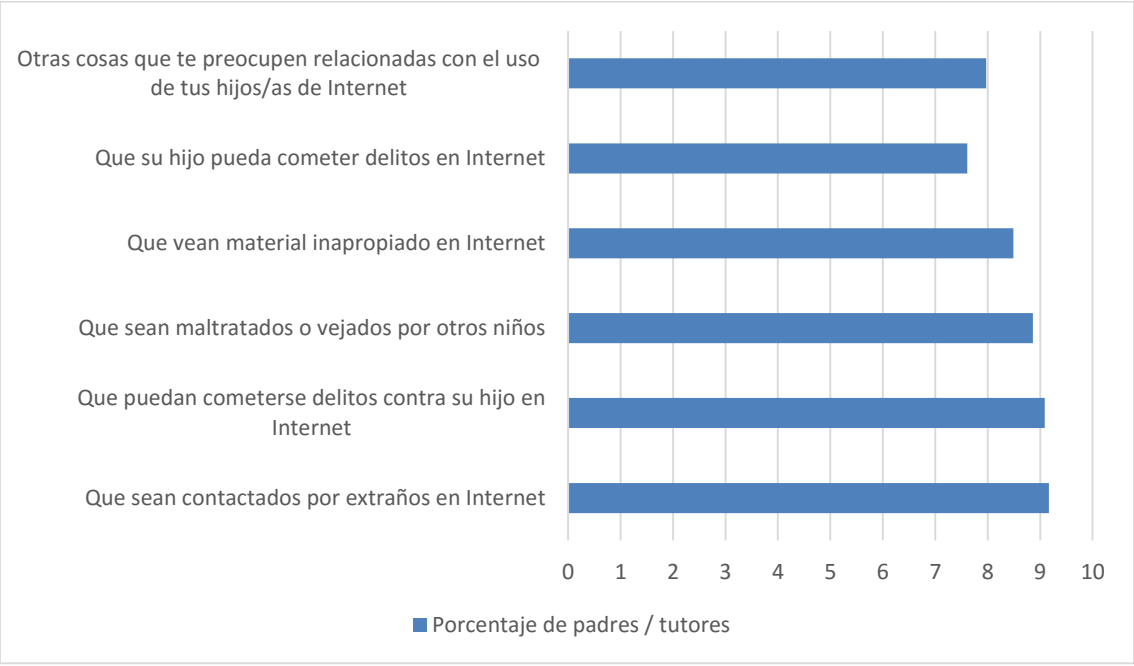

Ilustración 6: Preocupaciones de los padres cuando los menores hacen uso de Internet

[3] Portal Statista. http://es.statista.com/estadisticas/476535/preocupaciones-padres-con-hijos-uso-internet-espana/

Por todos estos motivos, además de los riesgos expuestos en el apartado 2.3, es necesario el uso de servicios de control parental cuando los menores navegan por la red, es decir, medidas de prevención para evitar que accedan sin ningún control a cualquier contenido que ofrece la red.

Estas medidas de control cada vez son más frecuentes en los desarrollos de productores de software, herramientas web, aplicaciones o hardware que están centrándose en utilizar sus recursos para prevenir los riesgos en la red, proporcionándoles a padres y tutores un amplio abanico de herramientas que les permitan controlar y supervisar la actividad de sus niños, tanto en los entornos propios (ordenador, Smartphone, tableta, videoconsola), como en los entornos compartidos en una LAN familiar, desde la regulación del acceso a internet en el ISP, hasta la implementación de filtros MAC en el router, la creación de una lista negra para páginas no toleradas según URL o lista de palabras bloqueadas, filtros establecidos por niveles de permeabilidad de la navegación (alto, medio, bajo), configuración de franjas horarias con acceso abierto y permitido, pero también desde la perspectiva del sistema operativo (Windows, Linux, Mac) mediante la prohibición de la utilización de ciertas aplicaciones de mensajería instantánea (Yahoo! Messenger, Skype), aplicaciones P2P (Ares, Emule), o simplemente por medio de la creación de cuentas de usuario con un régimen de permisividad menor en cuanto a la ejecución, creación o modificación de las aplicaciones instaladas en el sistema.

¿Qué deben esperar obtener los padres y tutores de estas herramientas de control parental?

- Evitar que los niños entren en contacto con personas desconocidas o peligrosas y prevenir problemas de lo que denominamos grooming, ciberbullying, sexting, etc.
- Configurar la herramienta para que bloquee o muestre el contenido sobre el tema que se indique, una lista de URLs o algunas palabras clave específicas. Además, podrán fijar un nivel de filtrado (bajo, medio, alto).
- Limitar el uso de algunas aplicaciones.
- Recibir informes sobre la actividad de los menores en Internet, obtener información sobre los lugares a los que se ha accedido o han sido bloqueados, qué aplicaciones han sido utilizadas, etc.
- Reducir las posibilidades de que los niños abusen de internet y del ordenador, en términos de tiempo y horario.

Hay que tener en cuenta que todavía no se ha encontrado una solución efectiva, por tanto, se deben complementar las herramientas de control parental con una educación y una concienciación adecuadas para minimizar los riesgos.

3.2. ¿Qué es un sistema de control parental? ¿Para qué sirve?

La definición más completa acerca de lo que es un sistema de control parental, es la proporcionada por INTECO (Instituto Nacional de Tecnologías de la Comunicación)[4] según el cual, un sistema de control parental es "*toda herramienta o aplicación que tiene la capacidad de bloquear, restringir o filtrar el acceso a determinados contenidos o programas, accesibles a través de un ordenador o de la Red, y de dotar de un control sobre el equipo y las actividades que se realizan con él, a la persona que sea el administrador del mismo, que normalmente deberá ser el padre o tutor del menor*". Por lo tanto, se llama Control Parental a cualquier herramienta que permite a los padres y tutores controlar y/o limitar el uso que un menor puede hacer del dispositivo o de Internet.

Así, de ambas definiciones, se concluye que un sistema de control parental sirve, básicamente, para los siguientes aspectos:

1. Realizar un control y monitorización de la actividad de los menores en Internet. De este modo con el control parental se puede obtener información de las páginas web que se visitan, participación en las redes sociales, etc.

2. Evitar que los menores abusen de Internet y del ordenador evitando que se conecten durante demasiadas horas o en horarios poco recomendables.

3. Evitar las visitas a sitios web inapropiados como por ejemplo webs eróticas, que fomenten el racismo, que fomenten la violencia u otros sitios de contenidos para adultos.

4. Evitar el uso de determinadas aplicaciones porqué las consideramos peligrosas.

5. Evitar el contacto con personas desconocidas o peligrosas como por ejemplo acosadores y depredadores sexuales.

Estos sistemas de control parental podemos encontrarlos preinstalados hoy en día en la mayor parte de los sistemas operativos que utilizamos, software específico de control parental para el ordenador, navegadores o exploradores, videoconsolas, y también en aplicaciones para tabletas y Smartphones.

Un sistema de control parental se puede aplicar en diferentes entornos dependiendo del tipo de control que se quiere realizar:

- **Control a nivel de red**. Se establece en el hub o router y se aplican a todos los dispositivos conectados a ese hub o router. Se utiliza cuando se quiere realizar un control de todos los dispositivos del hogar conectados a una determinada red.
- **Control a nivel de dispositivo**. Se establece en el propio dispositivo utilizado por el menor y se aplica con independencia de cómo y dónde se encuentra conectado a Internet.

[4] INTECO. Guía sobre cómo activar y configurar el control parental de los sistemas operativos. https://www.incibe.es/CERT/guias_estudios/guias/guiaManual_activacion_contol_parent

- **Control a nivel de aplicación**. Se fijan en la aplicación que se está utilizando. Este tipo de control se aplica independientemente del lugar donde se encuentra el dispositivo. Ejemplos de esto serían los ajustes aplicados a Google o YouTube.

3.3. Características de los Sistemas de Control Parental

Actualmente existen dos tipos de soluciones de control parental:

- Las soluciones que vienen establecidas por defecto en los sistemas operativos.
- Las soluciones de control parental comercializadas por empresas dedicadas al desarrollo de este tipo software.

La diferencia entre ambos tipos de soluciones, se encuentra en las opciones de seguridad que ofrece cada solución. Las soluciones preinstaladas en los sistemas operativos establecen niveles de seguridad más básicos, entre los que cabe destacar el registro de las actividades que los menores llevan a cabo cuando hacen uso del ordenador como las comunicaciones que realizan, las páginas web a las que acceden o las aplicaciones informáticas utilizadas. Las soluciones comercializadas por productores de software presentan niveles de seguridad más completos, avanzados y especializados. Pese a ofrecer diferentes niveles de seguridad, comparten ciertas características que permiten realizar una enumeración de las mismas.

3.3.1. Control de tiempo

El software de control parental permite limitar el tiempo que un menor puede estar utilizando un ordenador, un dispositivo, o conectado a la red. La mayoría permite controlar a qué horas es posible conectarse y en qué franja horaria no está permitido utilizar el dispositivo.

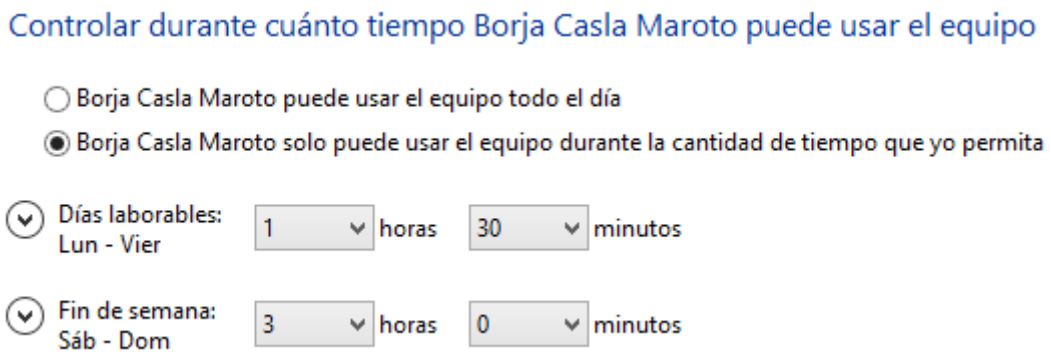

Ilustración 7: Control de tiempo de un sistema de control parental.

De esta manera es posible limitar el tiempo real que pueden estar conectados y a qué hora lo hacen. Así, se evita que los menores no estén demasiado tiempo conectados o jugando excesivamente con los dispositivos. Esta solución protegería de un uso excesivo de los dispositivos debido a ciertas aplicaciones que pueden resultar adictivas, estableciendo un tiempo máximo de uso.

3.3.2. Roles de usuario

Los padres pueden controlar y monitorizar el acceso a Internet de los menores configurando un rol para cada uno de los usuarios que utilizan los dispositivos. De este modo, se pueden personalizar distintos permisos de acceso a Internet, privilegios sobre archivos importantes e incluso la restricción de la instalación de aplicaciones.

3.3.3. Bloqueo de Páginas Web

Una de las principales características del control parental es la capacidad de restringir el acceso a contenido inapropiado por medio del bloqueo de ciertas páginas web.

En función del rol que se desee proteger, se pueden restringir o permitir los accesos. En esta sección podríamos bloquear sitios de contenido violento o sexual, e incluso aquellos sitios que posean una baja reputación.

También es importante mencionar que en muchos casos esta funcionalidad permitirá el bloqueo de ventanas emergentes (también conocidas como pop-ups) de sitios pornográficos o inadecuados, a los que muchas veces los menores llegan por error.

3.3.4. Bloqueo de aplicaciones

Permite bloquear la ejecución de determinadas aplicaciones que puedan suponer un problema para el menor como, por ejemplo: las aplicaciones de mensajería instantánea, correo electrónico, descarga de programas, etc.

3.3.5. Registro de actividad

Las herramientas de control parental permiten a los padres registrar la actividad de los menores cuando acceden a los dispositivos. Realizan un recuento de las aplicaciones ejecutadas y las páginas web que han sido visitadas o a las que se ha intentado acceder, pero han sido bloqueadas y por qué.

3.3.6. Geolocalización

Esta característica está presente en el software de control parental para dispositivos móviles mediante la cual se puede saber la ubicación del dispositivo del menor en cada momento.

3.3.7. Servicio de alertas y notificaciones

Entrar todos los días a la herramienta de control parental para revisar la actividad del menor, aunque es posible, no resulta práctico. Para facilitarlos la vida a los padres y educadores, las aplicaciones entre sus funcionalidades, ofrecen la posibilidad de enviar resúmenes periódicamente que recogen la actividad del menor de un periodo de tiempo determinado. También hay herramientas que permiten enviar alertas vía email o SMS en caso de que el menor esté intentando realizar una de las opciones no permitidas: intentar acceder a páginas web restringidas por el tipo de temática, conectarse a Internet fuera de la franja horaria establecida, intentar acceder a aplicaciones no permitidas.

3.4. Técnicas de filtrado de contenidos

Los filtros de contenidos cortan el acceso, a través de Internet, a contenidos ilícitos e inapropiados. Antes de explicar las diferentes técnicas de filtrado de contenidos, es conveniente saber que se entiende por contenidos ilícitos y contenidos inapropiados.

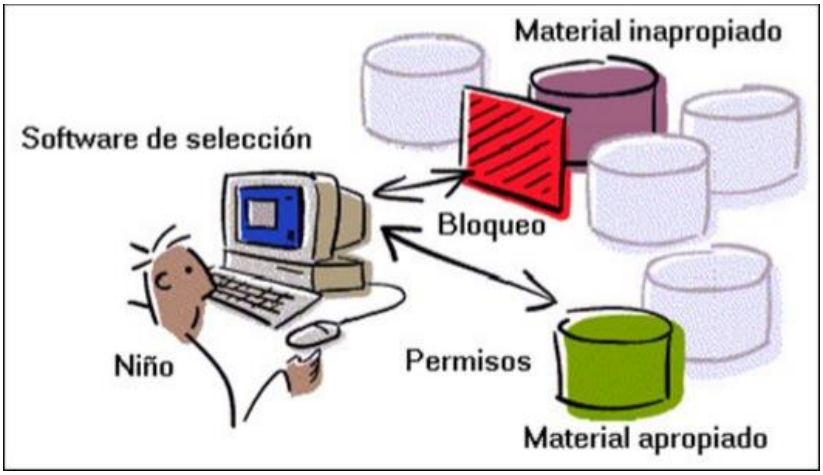

Ilustración 8: Funcionamiento de un filtro de contenido.

Son contenidos ilícitos aquellos que están prohibidos, es decir, van contra la norma penal y su publicación en Internet puede considerarse como delito. Por ejemplo, material relacionado con la pederastia, la pornografía infantil, apología del terrorismo, estafa.

Son contenidos inapropiados aquellos que, aunque no van contra la ley, son perjudiciales para los menores por su naturaleza o finalidad ya que pueden interferir en su proceso de formación. Por ejemplo, contenidos pornográficos, relacionados con las drogas, violencia escolar y acoso, juegos de azar, incitación a la anorexia, elaboración de explosivos.

Para cualquiera de ambos tipos de contenidos existen técnicas y herramientas que ayudan a realizar un filtrado previo y no lleguen a aparecer en las pantallas de los dispositivos que utilizan los menores.

3.4.1. Características de los filtros de contenido

- ✓ Permite/deniega el acceso a determinados servicios de Internet, como chats, conexiones P2P, comercio electrónico, juegos de azar, ...
- ✓ Permite limitar el tiempo de conexión de forma diaria, semanal, etc.
- ✓ Controla y limita la navegación web en un equipo determinado.
- ✓ Define filtros personalizados de forma que se pueden establecer filtros diferentes en función de las edades de los jóvenes.
- ✓ Registra los intentos de acceso a páginas web que han sido filtradas.

- ✓ Bloquea el acceso a páginas web con contenidos inapropiados para los menores. Estas listas de páginas deben ser actualizadas periódicamente ya que continuamente aparecen nuevas páginas en Internet de todo tipo.

3.4.2. Listas Blancas y Negras

Las listas blancas son un conjunto de direcciones web a las que sí está permitido acceder. Cuando se configura esta restricción, cualquier intento de ir a un sitio web que no esté en el listado será prohibido. Por tanto, es un filtrado más seguro, pero muy limitante y sólo suele ser eficaz en equipos de uso exclusivo por niños pequeños, donde se configura un entorno de navegación segura sin grandes cambios.

Las listas negras son un conjunto de direcciones web a las que no está permitido acceder. En este caso, se permite la navegación libremente, salvo a las direcciones que están en el listado. Se trata de un filtrado menos limitante, más funcional, pero más inseguro y siempre desactualizado pues es fácil encontrar nuevas páginas web con contenidos similares a las no permitidas. Se suelen emplear en entornos más adolescentes donde necesitan poder buscar y seleccionar información de múltiples fuentes y por tanto las listas blancas no serían operativas. Otro inconveniente es que existen páginas que utilizan técnicas para codificar la URL, de tal manera que no coincidan con las listas de sitios no permitidos.

3.4.3. Bloqueo por palabras clave

Las herramientas que emplean esta técnica de filtrado verifican el contenido de los sitios web y bloquea el acceso a aquellos que contengan ciertas palabras asociadas a un contenido no apto (por ejemplo, “sexo”, “porno”, “droga”, “matar”, “apuestas”, …). Muchas herramientas permiten personalizar los grados de severidad (¿cuántas veces debe aparecer cierta palabra para considerar el sitio web no apto?), e incluso seleccionar las palabras por categorías y añadir palabras específicas.

El problema fundamental es que es preciso cargar las palabras en diferentes idiomas y teniendo muy claro lo que se desea bloquear. Otro inconveniente es que pueden producirse los denominados falsos positivos, es decir, cabe la posibilidad de bloquear contenidos que pueden no ser peligrosos para los menores ya que el bloqueo de las palabras se realiza aisladamente, sin tener en cuenta el contexto en el que se encuentran integradas.

3.4.4. Bloqueo por categorías

Esta metodología de filtrado es propia de productos dedicados o de primer nivel, y permiten seleccionar la temática de las webs que permitiremos visitar en base a una lista de categorías que tiene la aplicación. Así, las webs catalogadas en una categoría no autorizada o no catalogada por la base de datos del fabricante, simplemente se bloquearán, y aquellas que estén dentro de las categorías autorizadas se podrán visitar sin problemas.

3.4.5. Bloqueo de aplicaciones e información

Mediante esta técnica se bloquea la entrada o salida de información del dispositivo en ciertas aplicaciones y/o servicios como pueden ser aplicaciones de mensajería instantánea, chat, correo electrónico, FTP, entretenimiento.

El inconveniente de hacer uso de esta metodología es que no importa si el contenido de la información es apropiado o no. Para contrarrestar este problema, hay disponibles herramientas de filtrado de contenido que permiten especificar y filtrar únicamente datos específicos. De tal manera que un padre puede no permitir que desde el dispositivo salgan datos como el apellido, dirección, teléfono, datos bancarios.

3.4.6. Etiquetado de páginas

Las páginas web contienen una serie de etiquetas de clasificación que determinan el contenido de la misma. Así, algunas herramientas permiten el bloqueo por parte de los navegadores web de las páginas que contengan ciertos contenidos determinados como no aptos por terceras empresas. Mediante un sistema de autoetiquetado de contenidos se indica a las herramientas de filtrado qué bloquear y que no.

La ventaja de utilizar una técnica basada en el autoetiquetado es que es independiente del idioma, muy optimizable, y además es el administrador de la herramienta el que determina que tipos de contenidos bloquear y cuáles no. Con esta técnica se facilita el bloqueo de determinadas páginas desde el navegador y herramientas, pero tiene el problema de que es el propio proveedor de la página el que tiene que autoclasificarse de forma voluntaria, ya que no existe una legislación al respecto que obligue a ello.

La tecnología de etiquetado más popular y estandarizada es RDF (Resource Description Framework, Marco de Descripción de Recursos en español), una terminología descriptiva por la que los mismos proveedores de contenidos indican mediante etiquetas que tipo de información está presente o ausente en sus sitios Web. De este modo se pueden configurar las herramientas de control para que sólo se acceda a aquellas páginas marcadas con contenido no perjudicial para los menores.

Dos de los principales sistemas de clasificación mediante etiquetas son ICRA (Internet Content Rating Association) y SafeSurf.

3.4.6.1. Etiquetado ICRA

El sistema de clasificación mediante etiquetas ICRA (Internet Content Rating Association, Asociación para la Clasificación de Contenidos de Internet) comenzó a utilizarse en 1994. Hoy en día es parte de FOSI, Family Online Safety Institute, una organización internacional sin fines de lucro, en donde se trabaja para desarrollar una Internet más segura y proteger a los menores de contenidos potencialmente dañinos en la Web.

El etiquetado ICRA consiste en un cuestionario que los proveedores de contenido deben de comprobar qué elementos del mismo se hallan presentes o ausentes en sus sitios Web. Posibilitándose que se genere un pequeño archivo que contiene las etiquetas que luego se

vincula con el contenido de uno o más dominios. Las etiquetas que contiene este archivo indican que el sitio web está libre de contenido nocivo para los menores y son como la que se muestra a continuación:

<link rel="meta" href="http://www.(*nombreWeb)*.com/Files/12345/labels.xml" type="application/rdf+xml" title="ICRA labels" />

Este cuestionario fue elaborado por un panel internacional y diseñado para ser lo más neutral y objetivo posible. Fue revisado en el año 2005 para permitir una aplicación más fácil a una amplia gama de contenido digital.

De esta manera los padres pueden mediante un software de filtrado permitir o no, ciertos contenidos basándose en la información declarada en las etiquetas.

Los temas abordados en el cuestionario son:

- Presencia o ausencia de imágenes de desnudez.
- Presencia o ausencia de contenido sexual.
- Representación de la violencia.
- Lenguaje utilizado.
- Presencia o ausencia de contenidos generados por usuarios, y si estos están moderados.
- Representación de otros contenidos peligrosos, como juegos, drogas y alcohol.

El sistema de etiquetado ICRA es independiente del idioma y se expresa mediante el estándar de etiquetado RDF, tecnología en la cual ICRA jugó un papel decisivo para su definición.

3.4.6.2. SafeSurf

El estándar de clasificación Web SafeSurf es un sistema de etiquetado de páginas diseñado para proteger a los niños. Fue desarrollado con la ayuda de miles de padres y usuarios de Internet, de todo el mundo.

Su estructura es diferente a la de otros sistemas de clasificación en varios aspectos. En primer lugar, es más detallada. En segundo lugar, su objetivo es describir objetivamente tanto el contenido como la forma en que se presenta el contenido. En tercer lugar, fue el primer sistema diseñado para permitir la auto clasificación y aquellos que evalúan tienen la suficiente flexibilidad para llegar a un acuerdo sobre una calificación sin comprometer la finalidad de SafeSurf de proteger la inocencia de los menores.

Dado que el sistema sólo se emplea cuando el ordenador está en uso, el propio PC se utiliza para realizar un seguimiento de todas las marcas, y traducir la información al usuario.

El estándar de clasificación de SafeSurf es reconocido por la marca de certificación registrada SS ~~(R). Esto se conoce como SafeSurf Wave. Esto va seguido por un grupo de 3 dígitos, un espacio y un valor numérico. Los tres dígitos identifican el tipo de clasificación (van de 0-9) y se requiere el cero como marcador de posición. El valor numérico identifica el nivel y el rango es

de 1-9 para las clasificaciones de temas de adultos y el rango de 1-100 es para otras clasificaciones de la información. El valor numérico no puede ser cero porque eso significa que la clasificación no tiene un nivel o no existe. En caso de que el valor sea cero, no se incluye en la lista. Por lo tanto, el código quedaría de la siguiente forma: SS 000 ~~ 1 (requiere un espacio antes del último dígito).

Los códigos informáticos se convierten en calificaciones legibles por los humanos gracias al software de filtrado.

Un ejemplo del sistema SafeSurf Wave en un documento web HTML en el formato PICS (Plataforma para la Selección de Contenido en Internet):

<META http-equiv="PICS-Label" content='(PICS-1.1 " *http://www.classify.org/safesurf/*" l r (SS~~000 1))'>

Esto debe aparecer antes o dentro de la sección <HEAD> del documento HTML:

<HTML>
<HEAD>
<META http-equiv="PICS-Label" content='(PICS-1.1 "http://www.classify.org/safesurf/" l r (SS~~000 1))'>
<TITLE> Título del Documento </TITLE>
</HEAD>

Realizando una clasificación de cada página HTML, de forma individual, se puede conseguir un filtrado específico de una manera sencilla. Una vez que se ha calificado el documento completo, se tendrán en cuenta todas las imágenes y archivos de sonido a los que se puede acceder mediante la página HTML para obtener la misma clasificación. Si una página contiene un vínculo a otra página, la nueva página se clasifica por separado.

Otra de las posibilidades que nos permite SafeSurf es clasificar directorios completos mediante un comando en la página *index.html* de ese directorio utilizando el PICS "generic true for" junto con el nombre del directorio. Suponer que el sitio web es *sample.com* y el subdirectorio se llama *subdir*. Se puede clasificar todo el subdirectorio del sitio *sample.com* mediante el comando META en la página *index.html* de *subdir* de la siguiente forma:

<META http-equiv="PICS-Label" content='(PICS-1.1 "http://www.classify.org/safesurf/" labels generic true for "http://www.sample.com/subdir/" ratings (SS~~000 1))'>

Aunque es posible bajo el protocolo PICS utilizar el comando "generic true for" para clasificar un sitio completo, se aconseja que cada directorio contenga su propia calificación en el *index.html* de ese directorio.

Criterios de clasificación

SafeSurf basa su metodología en diez criterios de clasificación y nueve subniveles en cada uno. A continuación, se muestra cada criterio con sus correspondientes subniveles:

SS~~000 - Edad	1) Todas las edades 2) Niños mayores 3) Adolescentes 4) Adolescentes mayores 5) Supervisión de adultos recomendada 6) Adultos 7) Se limita a adultos 8) Sólo para adultos 9) Explícito para adultos

Tabla 3: Clasificación de SafeSurf basada en la edad

SS~~001 - Creencias	1) Insinuación sutil 2) Insinuación explícita 3) Referencia técnica (Diccionario, noticias, enciclopedia) 4) No gráfico-artístico (limitación de palabrotas no sexuales utilizadas de una manera artística) 5) Gráfico-artístico (palabrotas no sexuales utilizadas de una manera artística) 6)Gráfico (El uso limitado de palabrotas y gestos obscenos) 7)Gráfico detallado (El uso casual de palabrotas y gestos obscenos) 8) Vulgaridad explícita (El uso intensivo del lenguaje vulgar y gestos obscenos. Salas de Chat sin supervisión) 9) Explícito y vulgar (Abuso de referencias sexuales y gestos vulgares. Salas de Chat sin supervisión)

Tabla 4: Clasificación de SafeSurf basada en las creencias

SS~~002 – Temas heterosexuales	1) Insinuación sutil (sutilmente implícita a través del uso de la metáfora) 2) Insinuación explícita (Explícita (no mostrado) a través del uso de la metáfora) 3) Referencia técnica (Diccionario, noticias, enciclopedias) 4) No gráfico-artístico (Limitación de descripciones metafóricas utilizadas de manera artística) 5) Gráfico-artístico (Descripciones metafóricas utilizadas de manera artística) 6)Gráfico (Descripciones de actos sexuales íntimos) 7)Gráfico detallado (Descripciones de detalles íntimos de actos sexuales) 8) Gráfico explícito o invitación a participar (Descripciones explícitas de los detalles íntimos de actos sexuales diseñados para excitar o invitando a la participación interactiva sexual. Sin supervisión de salas de chat sexuales o grupos de noticias.) 9) Explícita y vulgar o invitación explicita a participar (Descripciones gráficas vulgares de los detalles íntimos de actos sexuales diseñados para excitar o invitando a la participación interactiva sexual)

Tabla 5: Clasificación de SafeSurf basada en temas heterosexuales

SS~~003 – Homosexualidad	1) Insinuación sutil (sutilmente implícita a través del uso de la metáfora) 2) Insinuación explícita (Explícita (no mostrado) a través del uso de la composición, la iluminación, la configuración o la ropa que revela) 3) Referencia técnica (Diccionario, noticias, enciclopedias) 4) No gráfico-artístico (Limitación de descripciones metafóricas utilizadas de manera artística) 5) Gráfico-artístico (Descripciones metafóricas utilizadas de manera artística) 6)Gráfico (Descripciones de actos sexuales íntimos) 7)Gráfico detallado (Descripciones de detalles íntimos de actos sexuales) 8) Gráfico explícito o invitación a participar (Descripciones explícitas de los detalles íntimos de actos sexuales diseñados para excitar o invitando a la participación interactiva sexual. Sin supervisión de salas de chat sexuales o grupos de noticias) 9) Explícita y vulgar o invitación explicita a participar (Descripciones gráficas vulgares de los detalles íntimos de actos sexuales diseñados para excitar o invitando a la participación interactiva sexual)

Tabla 6: Clasificación de SafeSurf basada en la homosexualidad

SS~~004 – Nudismo	1) Insinuación sutil (Sutilmente implícita a través del uso de la composición, la iluminación, la conformación, revelando la ropa) 2) Insinuación explícita (Explícita (no mostrado) a través del uso de la composición, la iluminación, revelando la ropa) 3) Referencia técnica (Diccionario, noticias, enciclopedias) 4) No gráfico-artístico (obras de arte clásicas que se presentan en los museos públicos para ver en familia) 5) Gráfico-artístico (Artísticamente presentados sin desnudez frontal completa) 6)Gráfico (Artísticamente presentados con desnudos frontales) 7)Gráfico detallado (desnudos frontales eróticos) 8) Vulgaridad explícita (espectáculo pornográfico, diseñado para atraer a intereses lascivos) 9) Explícito y vulgar (espectáculo pornográfico explícito)

Tabla 7: Clasificación de SafeSurf basada en el nudismo

SS~~005 – Violencia	1) Insinuación sutil 2) Insinuación explícita 3) Referencia técnica 4) No gráfico-artístico 5) Gráfico-artístico 6) Gráfico 7) Gráfico detallado 8) Invitando a la participación en el formato gráfico interactivo 9) Incitación a la participación del usuario (venta de armas)

Tabla 8: Clasificación de SafeSurf basada en la violencia

SS~~006 – Sexo	1) Insinuación sutil 2) Insinuación explícita 3) Referencia técnica 4) No gráfico-artístico 5) Gráfico-artístico 6) Gráfico 7) Gráfico detallado 8) Invitando a la participación en el formato gráfico interactivo (salas de chat sexual) 9) Incitación a la participación del usuario (Participación en un espectáculo pornográfico)

Tabla 9: Clasificación de SafeSurf basada en el sexo

SS~~007 – Intolerancia	1) Insinuación sutil 2) Insinuación explícita 3) Referencia técnica 4) No gráfico-literario 5) Gráfico-literario 6) Discusiones gráficas 7) Aprobar el odio 8) Aprobar la acción violenta o de odio 9) Promocionar la acción violenta o de odio

Tabla 10: Clasificación de SafeSurf basada en la intolerancia

SS~~008 – Drogas	1) Insinuación sutil 2) Insinuación explícita 3) Referencia técnica 4) No gráfico-artístico 5) Gráfico-artístico 6) Gráfico 7) Gráfico detallado 8) Participación interactiva simulada 9) Solicitar la participación de personal

Tabla 11: Clasificación de SafeSurf basada en las drogas

SS~~009 – Otros temas de adultos	1) Insinuación sutil 2) Insinuación explícita 3) Referencia técnica 4) No gráfico-artístico 5) Gráfico-artístico 6) Gráfico 7) Gráfico detallado 8) Vulgaridad explícita 9) Explícito y ordinario

Tabla 12: Clasificación de SafeSurf basada en otros temas de adultos

SS~~00A – Juegos	1) Insinuación sutil 2) Insinuación explícita 3) Referencia técnica 4) No gráfico-artístico, publicidad 5) Gráfico-artístico, publicidad 6) Simulación de apuestas 7) Juegos de la vida real sin apuestas 8) Fomentar la participación interactiva de las apuestas en la vida real 9) Promocionar medios mediante apuestas

Tabla 13: Clasificación de SafeSurf basada en el juego

El dígito final (SS~~00A **1**) es el nivel de precaución de los padres o tutores. Se puede ir de 1 a 9. El nivel 0 no se pone porque eso significaría el adulto no estaba presente. Si no está presente, no se menciona. Sin embargo, al crear e nivel de la interfaz de usuario, se puede usar cero para permitir que un padre pueda bloquear completamente el acceso a un tema específico para adultos. El nivel más leve es el número uno y el nivel más grave es nueve.

Lo ideal sería tener un sitio seguro para los niños con una clasificación para todas las edades (SS 000 ~~ 1) y que no contenga temas para adultos. Este tipo de sitio sería considerado apto para el acceso de los menores.

Actualmente, se están proporcionando capas especiales de filtrado para los padres que desean controlar el acceso de sus hijos a los niveles de precaución personalizados, ya sea por los proveedores como un servicio adicional o a través de productos de software de terceros.

Un sitio web puede contener varios temas de adultos e identificar a todos ellos. El siguiente ejemplo demuestra esta característica:

<Meta http-equiv = "PICS-Label" content = '(PICS 1.0 "http://www.classify.org/safesurf/" lr (SS~~000 4 SS~~001 5 SS~~004 2 SS~~007 2 SS~~008 3)) '>

Esto se traduce en el sentido de que esta página Web contiene y clasifica temas adecuados para los adolescentes más mayores, creencias con un nivel de precaución 5, nudismo con un nivel de precaución 2, Intolerancia con un nivel 2, y el consumo de drogas con el nivel de precaución 3.

Explicación de los niveles de precaución

Cuando una página web utiliza un nivel de calificación de 1 o 2 para identificar un tema de adultos, significa que la presentación de ese tema se realiza de la forma más sutil posible, o presentado más abiertamente. Por ejemplo, la desnudez podría estar implicada como una silueta o como formas descritas a través de la ropa.

El nivel tres está reservado para los servicios de información puros como bases de datos de referencias, diccionarios o noticias. Por ejemplo, los sitios de publicación de temas sobre la homosexualidad, tales como las discusiones sobre cuestiones psicológicas podrían ser clasificados con un nivel tres.

Los niveles cuatro y cinco son para presentaciones artísticas sobre tema de adultos. Una película como el "Padrino" claramente podría ser clasificado como un cuatro o un cinco. Una revista Playboy en la que aparecen representaciones artísticas de mujeres en topless es un nivel cinco, y un nivel seis es cuando aparece un desnudo frontal.

El nivel siete es para representaciones gráficas con mayor contenido material para adultos. El valor artístico es menor o inexistente en estos niveles más altos y con el objetivo principal de atraer a los intereses lascivos.

Los niveles ocho y nueve son para los sitios web que pueden colocar al espectador en una posición participativa simulada, tal como la visualización de imágenes en primer plano detallado de contacto sexual, o conexiones "en vivo".

3.4.7. Filtrado de imágenes

Estudia las imágenes analizando técnicamente la imagen y buscando características típicas de las imágenes con contenidos ilegales o inapropiados.

3.5. Herramientas de Monitorización

Las herramientas de control parental pueden agruparse en dos bloques dependiendo de la finalidad para la que haya sido desarrollada la herramienta:

- Herramientas de monitorización. Llevan a cabo un registro de las páginas visitadas y tiempo de permanencia en ellas, pero no prohíben el acceso a páginas web de contenido inapropiado.

- Filtros de contenido. Como se ha comentado anteriormente, permiten bloquear el acceso a páginas web cuya dirección contenga un determinado patrón o el propio contenido de la página web contenga determinadas palabras. También permiten bloquear el acceso a ciertos servicios de Internet como a chats, así como limitar el tiempo de conexión.

3.5.1. Herramientas de monitorización

Los sistemas operativos y los navegadores web incorporan mecanismos integrados para poder realizar un control desde el propio sistema de algunos aspectos de la navegación. Por ejemplo, permiten conocer las páginas visitadas, la permanencia en ellas o qué documentos se han abierto recientemente tanto locales como de la web.

Independientemente del sistema operativo que tenga instalado el sistema es muy importante que cada miembro de la familia en el hogar, disponga de su propia cuenta con su usuario de conexión y contraseña. En base a esta premisa, el perfil del usuario de los padres o tutores deberá ser de administrador del sistema para tener el control del mismo.

El propio sistema proporciona los siguientes mecanismos de control:

- Historial de navegación.
- Cookies.
- Documentos recientes.

3.5.2. Historial de navegación

Los navegadores web proporcionan una opción de menú denominada Historial que muestra y almacena en un registro todas las páginas web que han sido visitadas.

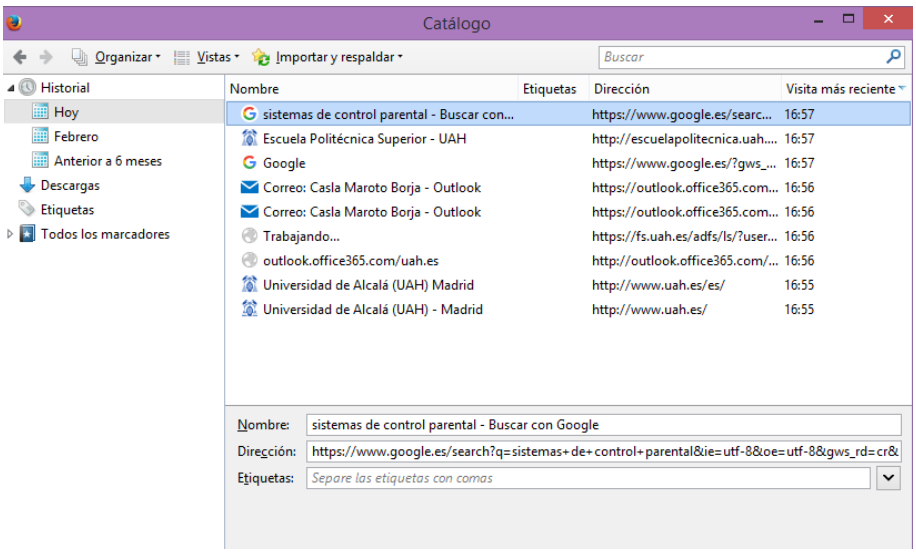

Ilustración 9: Historial de navegación

El historial de navegación se encuentra en *Menú > Historial* o se puede acceder directamente con la combinación de teclas *Ctrl + H* o *Ctrl + Shift + H*. Accediendo a este historial se puede visualizar qué paginas han sido visitadas, cuándo y cuántas veces. Como cualquier herramienta de monitorización, no es una opción que establezca una limitación, pero puede ayudar para hacer un seguimiento de la navegación que se está realizando.

En el navegador web Mozilla Firefox (*Ctrl + Shift + H*) se puede personalizar la vista del historial añadiendo otras columnas como la fecha de la visita, un contador de visitas a esa página, palabras clave, etiquetas, …. También es posible anclar en el panel izquierdo el historial mediante la combinación *Ctrl + H*.

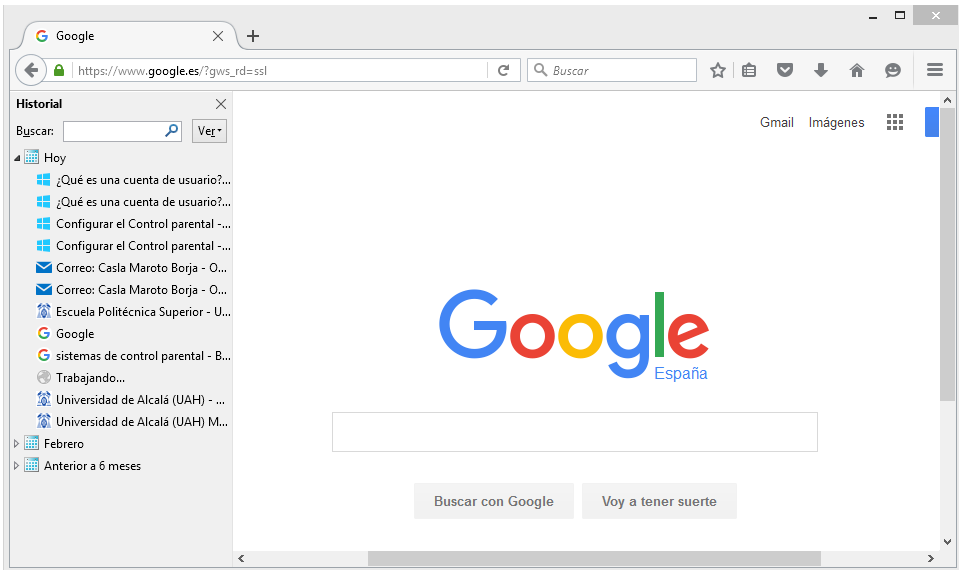

Ilustración 10: Historial web anclado en panel izquierdo (Ctrl + H)

Junto a la etiqueta Buscar está el botón Ver que permite organizar las webs visitadas bajo diferentes criterios: por lugar, por fecha, por lugar y fecha, la más visitada o la última visitada.

Acceder al historial no modifica su contenido ni deja rastro de que ha sido consultado. Eso quiere decir que, si los menores lo conocen pueden entrar y eliminar las páginas visitadas que quieran simplemente situados sobre la referencia pulsar el botón derecho del ratón y seleccionar Borrar. Otra opción que incorporan los navegadores y que pueden utilizar los menores para evitar el rastreo de los sitios web a los que acceden, es la navegación en modo incógnito. El modo incógnito no deja rastro de los sitios que se han visitado e impide el almacenamiento de las cookies.

3.5.3. Cookies

Las cookies fueron desarrolladas en el año 1994 por ingenieros de la compañía Netscape, y su navegador, hoy en día desaparecido, fue el primero en aceptarlas. Desde entonces, las cookies son un elemento imprescindible para que funcione la Web tal y como la conocemos hoy en día. Se trata de paquetes de datos que los servidores web envían a los navegadores y estos los almacenan de forma automática en el ordenador del usuario cuando este visita una página web. Posteriormente, cada vez que el usuario visite esa misma página web o alguna otra del

mismo dominio, la cookie será leída por el navegador web, sin ser modificada, y devuelta al servidor web.

Por tanto, una cookie son sólo datos que se almacenan en el ordenador del usuario. Pero como el almacenamiento se realiza por orden del servidor web, siempre ha existido el miedo de que se pudiera hacer algo malicioso. Sin embargo, las cookies no son software, tampoco son fragmentos de código, son simplemente datos. En principio, las cookies no pueden transmitir y ejecutar virus, ni instalar malware como troyanos o programas de espionaje.

Sin embargo, las cookies sí que pueden ser utilizadas para realizar un seguimiento de la actividad de un usuario en la Web.

Su propósito principal es identificar al usuario almacenando su historial de actividad en un sitio web específico, de manera que se le pueda ofrecer el contenido más apropiado según sus hábitos. Esto quiere decir que cada vez que se visita una página web por primera vez, se guarda una cookie en el navegador con un poco de información. Luego, cuando se visita nuevamente la misma página, el servidor pide la misma cookie para arreglar la configuración del sitio y hacer la visita del usuario tan personalizada como sea posible.

Tipos de Cookies

- **Cookies de sesión o temporales.** Son cookies que usualmente se eliminan cuando el navegador se cierra.

- **Cookies persistentes**. Estas son cookies que se mantienen a pesar de que el navegador sea cerrado. Se mantienen por un tiempo específico (tienen fecha de expiración), durante el cual una página puede conocer lo último que hiciste o algunas de tus preferencias. A este tipo de cookies también se les conoce como tracking cookies, porque pueden ser usadas por compañías de publicidad para conocer tus hábitos de navegación.

- **Cookies seguras**. Almacenan información cifrada para evitar que los datos almacenados en ellas sean vulnerables a ataques maliciosos de terceros. Se usan sólo en conexiones HTTPS.

- **Cookies de terceros**. Las cookies de terceros proceden de anuncios de otros sitios web (como anuncios emergentes) situados en el sitio web que está viendo. Los sitios web pueden usar estas cookies para realizar un seguimiento del uso que da a Internet a efectos de marketing.

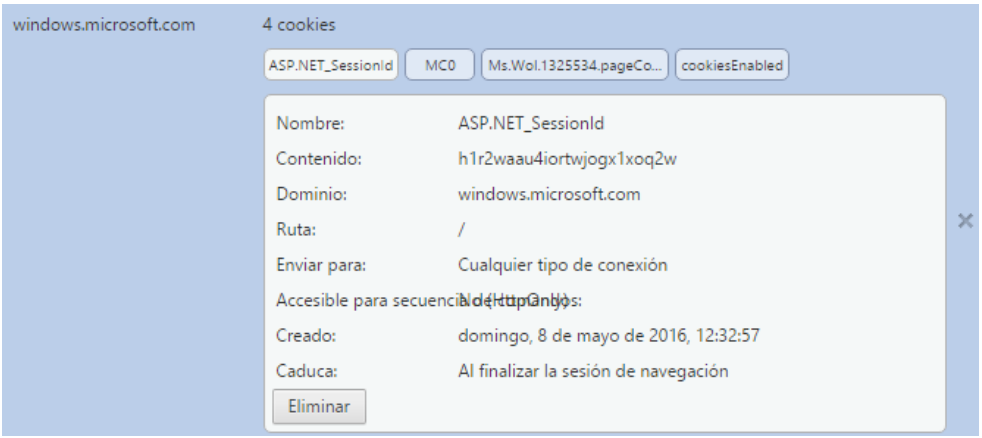

Ilustración 11: Ejemplo de Cookie temporal.

Qué almacenan las cookies

Los contenidos de una cookie los determina el sitio web que la creó. En su mayor parte, las cookies contienen cadenas de texto con información acerca del navegador web. Las cookies están pensadas para ayudar a los usuarios a acceder a la web de una forma más rápida y efectiva. Por lo tanto, pueden almacenar información para ayudar a entrar a un sitio sin tener que iniciar sesión.

Una vez creadas, las cookies normalmente no contienen ninguna información personal. Toda la información personal que puedan contener es únicamente la que el usuario ha introducido en un formulario del sitio (usuario, contraseña, correo, …). Cuando una cookie contiene información personal, ésta está codificada de forma que es ilegible para cualquier tercera parte que pudiera tener acceso al archivo de cookies. El único ordenador que puede leer y decodificar la información es el del servidor que la creó originalmente

Las cookies cambian dependiendo del servidor web que las generó, pero todas contienen seis parámetros básicos:

- **Nombre**.
- **Contenido**.
- **Fecha de caducidad**. Esto determina el tiempo que la cookie se mantendrá activa en el navegador.
- **Ruta**. Ruta donde se almacena el archivo de la cookie en el disco duro.
- **Dominio**. Esto hace que la cookie pueda acceder a las páginas de cualquiera de los servidores cuando un sitio utiliza varios servidores de un dominio.
- **Enviar para** - Esto indica que la cookie sólo se puede utilizar bajo una condición de servidor seguro utilizando SSL. En caso de que el campo esté vacío, indica que se puede utilizar en cualquier sitio web.

3.5.4. Documentos recientes

Los sistemas operativos tienen un registro de los documentos locales abiertos por el usuario que se ha conectado y así agilizar el acceso a ellos en cualquier momento. Esta opción sirve para poder ver los archivos a los que ha accedido el menor mientras estaba utilizando el ordenador.

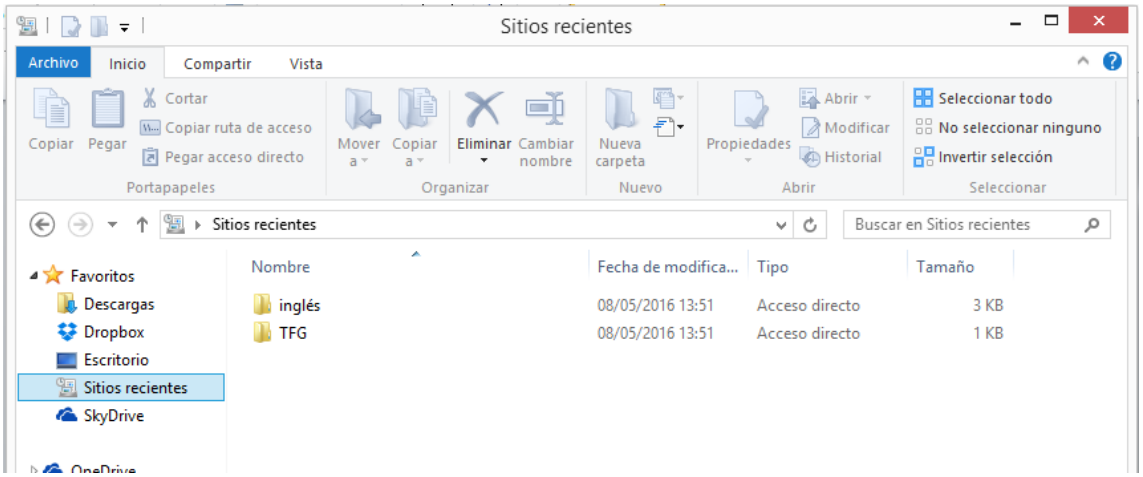

Ilustración 12: Documentos recientes en Windows.

En el caso de Ubuntu ir a Lugares > Documentos recientes.

Con la opción Vaciar documentos recientes se pueden eliminar todas las referencias (no los archivos propiamente).

4. Herramientas de Control Parental

Existen diferentes herramientas de control parental que permiten limitar el acceso de los menores de edad a contenidos que no son apropiados para su edad, que afectan su integridad, que promueven conductas no apropiadas o que van en contra de los valores familiares. Estas herramientas además ofrecen la posibilidad de controlar el tiempo en que los niños pueden navegar en Internet o usar sus dispositivos, con el fin de promover la realización de otras actividades.

Algunas de estas herramientas se pueden obtener de forma gratuita en Internet o en la tienda de aplicaciones de los dispositivos, además los principales navegadores como Google Chrome, Internet Explorer o Mozilla Firefox, así como los diferentes sistemas operativos ofrecen opciones de seguridad para monitorizar la actividad y filtrar el contenido al que pueden acceder los menores.

Hay dos clases de software de control parental: el del equipo y el de la nube. El primero consiste en software que se instala en el ordenador, como si de un programa normal se tratase, y todos los controles se realizan desde el dispositivo donde se encuentra instalado. El problema de este tipo de software es que puede ser desinstalado o reconfigurado por el menor si posee ciertos conocimientos de informática.

En el caso de la nube, el servicio se carga localmente y, todos los ajustes, informes y control, se realizan desde la web del desarrollador empleando cualquier equipo con conexión a Internet. Este último formato es el más habitual en los productos de última generación, y también el más práctico a la hora de gestionar el control, incluso, si el padre o tutor se encuentra fuera de casa o en el trabajo.

A continuación, se ha realizado una clasificación de las herramientas de control parental, siguiendo una evolución en función de la comodidad en la adopción, del medio o entorno usado para su implementación, del grado de control que se desee realizar y de las necesidades ofrecidas.

4.1. Medidas de control parental integradas en Sistemas Operativos

Las últimas versiones de los sistemas operativos más utilizados como son Windows y Mac Os X disponen de sistemas para activar un control parental y limitar el uso y acceso a diferentes partes del ordenador o a Internet. Son de sencilla configuración y permiten controlar las aplicaciones y juegos que los menores podrán utilizar. Es primordial disponer de diversas cuentas de usuario de acceso para que se puedan asignar diferentes tipos de privilegios para limitar el uso del ordenador.

Estas herramientas son gratuitas ya que vienen integradas en el propio sistema operativo y son una buena opción para aquellos usuarios adultos que no tienen conocimientos avanzados de informática ni conocen ningún software de control parental para poder ejercer un control sobre sus menores.

En cualquier sistema operativo que se implemente, debe ser el Administrador el que configure las cuentas de control parental.

4.1.1. Windows 8

Windows 8 proporciona en su distribución original una herramienta de control parental muy interesante y más potente que en versiones anteriores de Windows. Resulta una opción adecuada que padres y tutores deben conocer si desean ejercer control sobre la forma en que los menores utilizan el equipo. El modo Protección infantil que proporciona Windows 8 consta básicamente de las siguientes funciones:

- Filtrado de contenidos. Realiza un control de los sitios web a los que se accede en línea.
- Restricciones de uso. Permite establecer un límite de las horas en que se utiliza el ordenador.
- Restricciones de juego. Se pueden elegir los tipos de juegos a los que el menor puede tener acceso.
- Restricciones de aplicaciones. Es posible bloquear el uso de ciertos programas y permitir otros.

- Informe de actividad. Permite registrar información sobre el uso que el menor hace del equipo.

4.1.1.1. Cómo configurar el control parental en Windows 8

El control parental de Windows 8 se aplica sobre una cuenta de usuario específica. Esta cuenta será la que utilice el menor para iniciar sesión en el equipo. Para poder crear un usuario y manejar el control parental es necesario haber abierto sesión con un usuario administrador del equipo. Los pasos para crear una cuenta de usuario para el menor:

1. Ir a la esquina superior derecha de la pantalla y en la barra que se muestra hacer clic en el icono Configuración.
2. Clic en Cambiar configuración de PC.
3. En el panel Configuración seleccionar en la barra lateral izquierda la opción Cuentas/ Otras Cuentas.
4. Para crear la cuenta del menor ir a Agregar Cuenta y en las opciones que aparecen seleccionar Agregar cuenta de un menor/Agregar cuenta de un menor sin correo electrónico y rellenar los datos solicitados.

La configuración del control parental se realiza en Panel de control/Cuentas de usuario y protección infantil/Configurar Protección infantil para todos los usuarios. A continuación, se debe seleccionar la cuenta del menor para la que se desea realizar el control.

Ilustración 13: Seleccionar cuenta control parental Windows 8

Al seleccionar la cuenta del menor, se accede a la configuración de control parental.

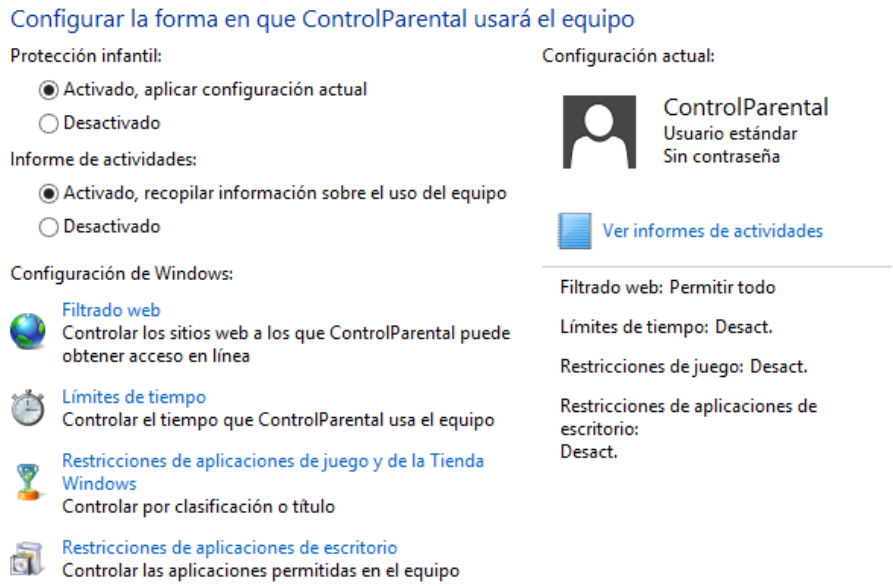

Ilustración 14: Configurar control parental Windows 8

Filtrado web. El filtrado web permite seleccionar el de contenido que se puede ver o decidir específicamente que páginas web se quieren bloquear.

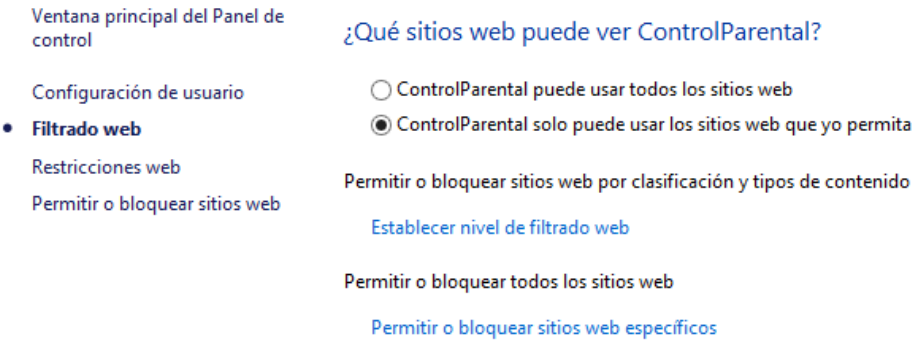

Ilustración 15: Filtrado web Windows 8

Windows 8 dispone de dos sistemas de filtrado web:

- **Por clasificación y tipos de contenido**. Si optamos por ese sistema de restricción web se puede elegir uno de estos niveles:
  - *Solo la lista de permitidos*. El usuario solo podrá navegar por los sitios web incluidos en la lista de permitidos. Se bloqueará el acceso al resto.
  - *Diseñado para menores*. Podrá acceder a la lista de permitidos y los sitios para menores. Se bloquearán los sitios para público adulto.
  - *Interés general*. Se accederá a la lista de permitidos, sitios para menores y de interés general. Se bloquearán los sitios para público adulto.
  - *Comunicación en línea*. Se accederá a la lista de permitidos, sitios para menores y de interés general: redes sociales, chat en web y correo web. Se bloquearán los sitios para público adulto.
  - *Advertir de contenido para adultos*. Se mostrará una advertencia cuando se trate de acceder a contenido supuestamente dirigido a adultos.

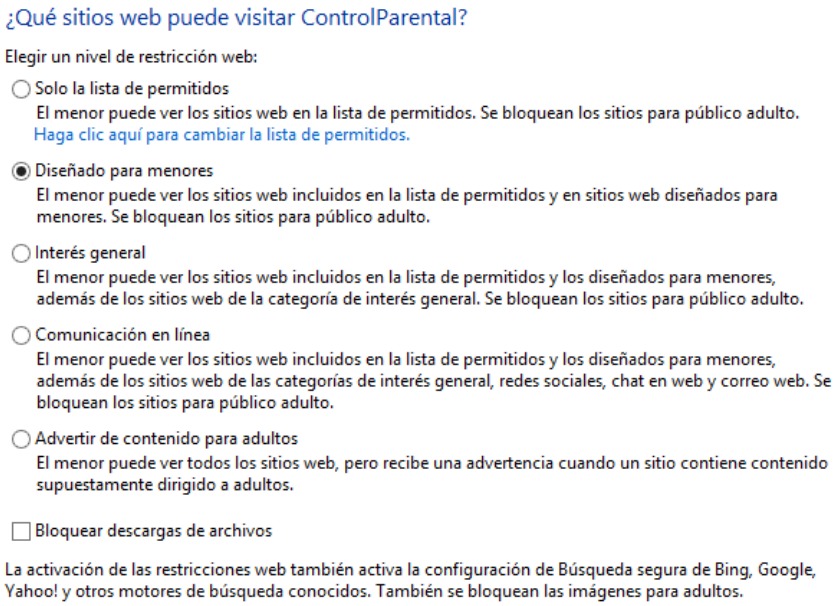

Ilustración 16: Filtrado web por clasificación y tipos de contenido.

- **Permitir o bloquear sitios web**. Desde esta página es posible crear una lista de sitios permitidos y otros bloqueados introduciendo sus URL y usando los botones Permitir o Bloquear.

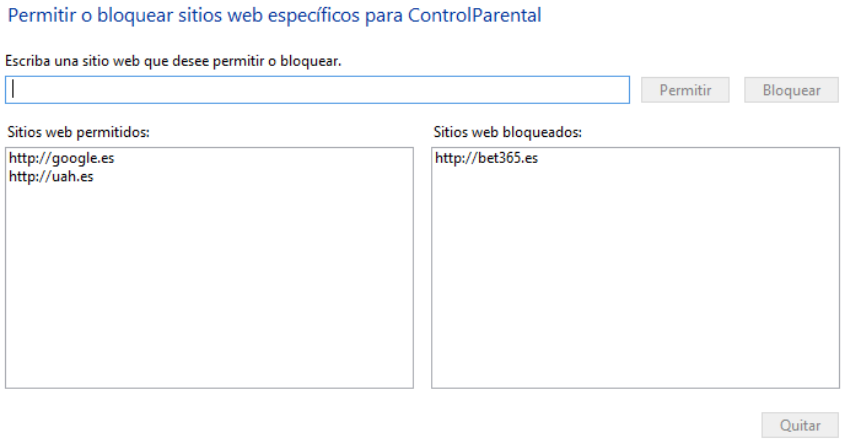

Ilustración 17: Filtrado web mediante listas blancas y negras.

Límites de tiempo. Permite controlar el tiempo que el usuario utilizará el equipo. Se puede controlar mediante dos parámetros:

- *Establecer tiempo permitido*. Establece el tiempo de uso del equipo los días laborales y festivos.

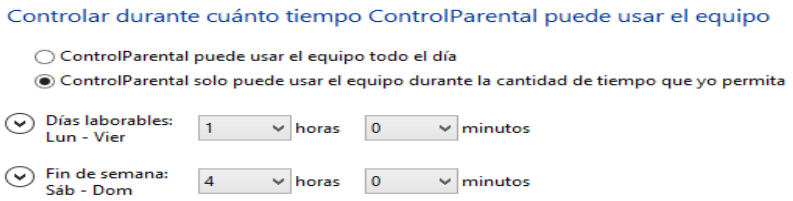

Ilustración 18: Establecer tiempo de uso del equipo Windows 8.

- *Establecer horario restringido*. Permite indicar las horas semanales donde se bloqueará el acceso al equipo de ese usuario. Para ello basta con pulsar y arrastrar con el ratón sobre la parrilla horaria. En azul se mostrarán las horas bloqueadas y el blanco las horas permitidas.

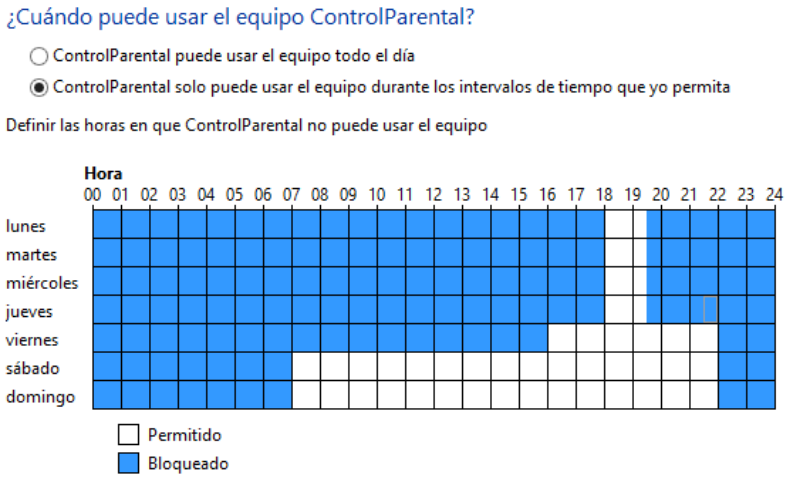

Ilustración 19: Restricción horaria Windows 8.

Restricciones de juego y tienda Windows. Permite seleccionar a que juegos y aplicaciones de la tienda de Windows puede acceder el menor según la clasificación seleccionada. Si existen juegos instalados en el ordenador, permite seleccionar a cuales puede acceder el menor y a cuáles no.

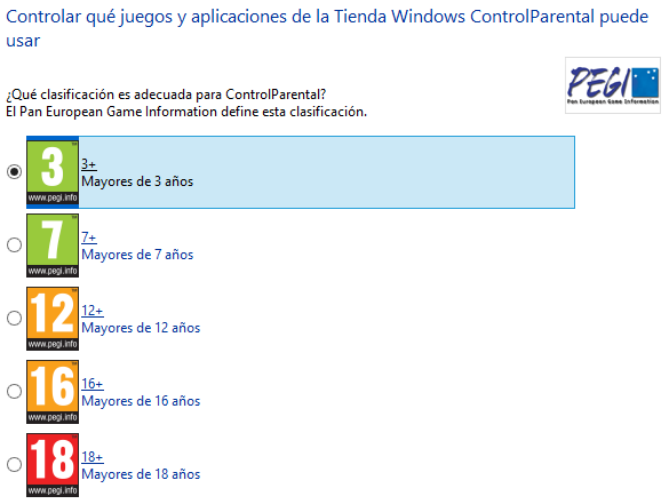

Ilustración 20: Clasificación de juegos Windows 8.

Restricciones de aplicaciones. Permite seleccionar las aplicaciones instaladas a las que el menor puede acceder o no.

4.1.1.2. Prueba control parental Windows 8

A continuación, se muestran los resultados de aplicar el control parental de Windows 8 a la cuenta de un menor para probar las diferentes opciones que éste nos proporciona.

Filtrado Web

Se ha establecido el filtrado web *Diseñado para menores.* Al intentar acceder a una página de apuestas, el sistema de control parental detecta que no es un sitio web adecuado para los menores y bloquea la web.

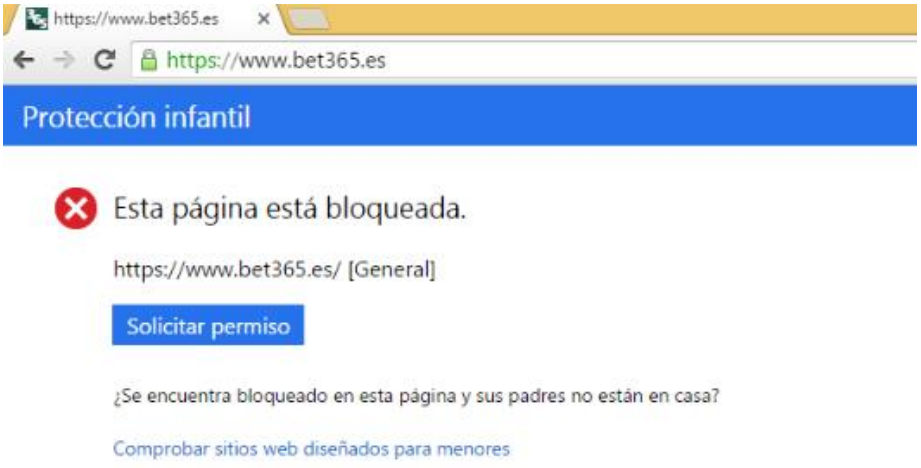

Ilustración 21: Sitio Web bloqueado Windows 8.

Límite de tiempo

El horario de uso establecido para la cuenta del menor es de 18:00-19:30 los días laborales. Si se accede fuera de ese horario, no se permite iniciar sesión y muestra un mensaje informando de ello.

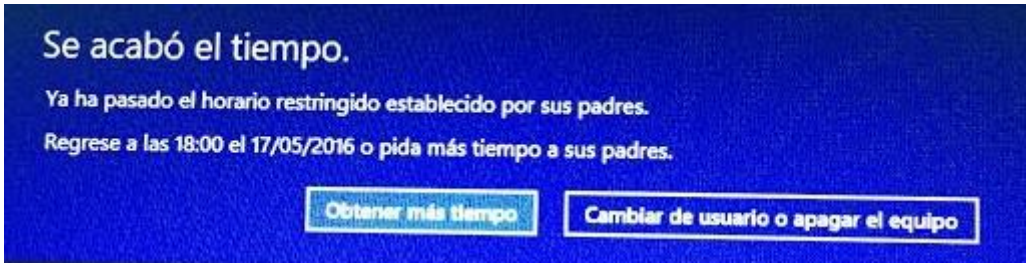

Ilustración 22: Acceso fuera del horario permitido Windows 8.

Restricciones de juegos y tienda Windows

El sistema se ha configurado para poder acceder únicamente a juegos y aplicaciones con una clasificación apta para mayores de tres años de edad. Por ejemplo, en la tienda Windows la aplicación de Facebook está clasificada para mayores de doce años por lo que si entramos con la cuenta del menor y buscamos la aplicación, no se obtienen resultados. Se muestra la comparación de la búsqueda realizada sin control parental y realizada con un filtro de control parental.

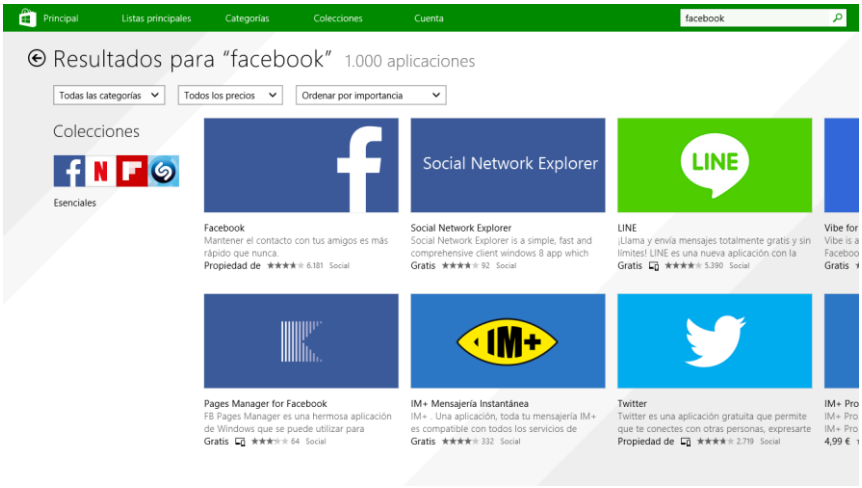

Ilustración 23: Búsqueda de aplicaciones sin control parental.

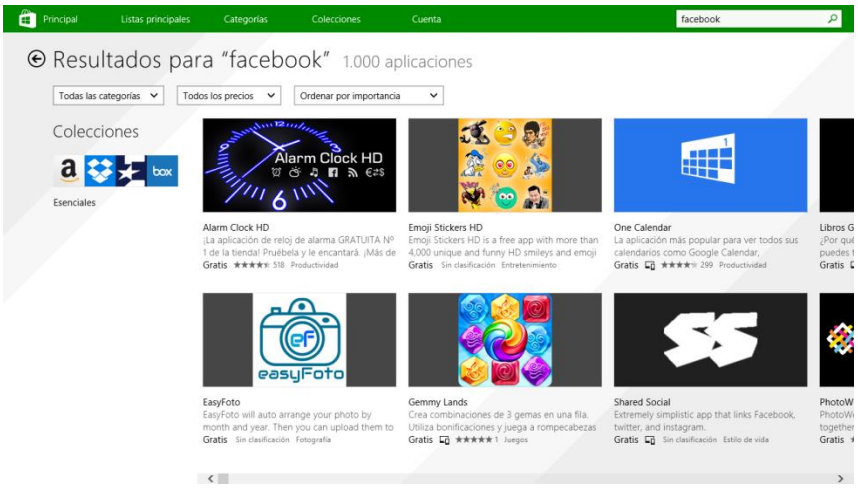

Ilustración 24: Búsqueda de aplicaciones con control parental.

4.1.2. Windows 10

Con la nueva versión del sistema operativo de Windows, ha desaparecido la herramienta de control parental que venía integrada en las anteriores versiones. Ahora, el control parental se gestiona desde la cuenta online de Microsoft del usuario donde se puede:

- Realizar un seguimiento de la actividad del menor en el ordenador (aplicaciones utilizadas, sitios web visitados y tiempo que el menor ha permanecido en el sistema). Se puede programar el envío de informes periódicos sobre la actividad del menor a una cuenta de correo electrónico.
- Gestión de listas de sitios permitidos y denegados para filtrar el contenido en la web.
- Posibilidad de activar un filtro de contenido que bloquea el acceso a todos los sitios web que contengan contenido inapropiado para los menores.
- Establecer límites de acceso y uso del ordenador.
- Establecer restricciones del uso de aplicaciones según la edad del menor.
- Limitar la descargar de aplicaciones desde Windows Store.

- Si el menor dispone de un Smartphone con Windows 10 Mobile, se puede activar la geolocalización para saber dónde se encuentra el menor.

Añadir cuenta de un menor

En primer lugar, es necesario añadir una nueva cuenta al sistema para poder aplicar el control parental. Para ello:

1. Ir a Configuración > Cuentas > Familia y otros usuarios.
2. En el apartado *Familia,* Agregar familiar.
3. Agregar un menor. Se puede continuar sin introducir una dirección de correo, pero es conveniente añadir el correo del menor para establecer mayor nivel de protección.
4. Se enviará una invitación al correo electrónico que el menor debe aceptar para poder iniciar sesión. Cuando acepte la invitación del correo electrónico, tendrá que iniciar sesión en Windows 10 con la misma dirección de correo electrónico en la que recibió la invitación.

Configurar control parental

Como se ha comentado anteriormente, la gestión se realiza online a través de la cuenta de Microsoft del Administrador. Para acceder a la cuenta se puede a través de *https://account.microsoft.com/about* o:

1. Ir a Configuración > Cuentas > Familia y otros usuarios.

2. Hacer clic en Administrar la configuración de la familia.

Una vez que se ha iniciado sesión, en la sección *Familia* se realizan las configuraciones oportunas para establecer límites en la cuenta del menor agregado.

El inconveniente de hacer uso del filtrado de contenido en Windows 10 es que únicamente se aplica al navegador Microsoft Edge. Si el menor tiene acceso a otros navegadores, podrá acceder a cualquier tipo de contenido. Para evitarlo, se debe bloquear la instalación y el uso de otros navegadores desde la sección de aplicaciones.

4.1.3. Linux

La investigación de herramientas de control parental disponibles para los usuarios que usan el sistema operativo Linux ha sido realizada en Ubuntu, una de las distribuciones más populares del sistema, debido a que es un sistema operativo gratuito y con una interfaz bastante más sencilla e intuitiva que el resto.

El sistema, a diferencia de Windows, no lleva integrado una herramienta de control parental para poder llevar a cabo un control de los menores. Existe una serie de herramientas independientes específicas para Linux que permiten realizar este control. Al igual que en el resto de sistemas operativos actuales, estas herramientas se aplican a cuentas de usuario específicas. Para ello en Ubuntu se pueden crear usuarios con permisos limitados, así como grupos de usuarios para organizar mejor la gestión de los mismos, e incluso controlar los permisos otorgados a diferentes servicios que se ejecutan en el sistema mediante la función IPTABLES.

4.1.3.1. TimePKR

TimePKR es una aplicación de control parental en el sistema operativo Ubuntu que permite establecer un control de acceso y de las horas en que se puede hacer uso del sistema. Las principales características de la herramienta son las siguientes:

- Limitación del uso diario del ordenador por parte del administrador del sistema basado en una duración del tiempo de acceso.
- Configuración de las horas del día en las que se puede y no se puede acceder al ordenador.
- Permite bloquear cuentas de usuario.
- Permite saltarse las restricciones hasta que termine el día.
- Se pueden añadir recompensas y castigos de tiempo.
- Tiene un sistema de notificaciones.

A diferencia de otras herramientas de control parental, Timekpr no permite controlar a qué sitios web pueden acceder los menores y a cuáles no y tampoco posibilidad de seleccionar qué aplicaciones pueden usar y cuáles no. A pesar de que sus opciones sean limitadas, Timekpr es una gran herramienta para controlar que los menores no pasan todo su tiempo delante de un ordenador.

Únicamente puede ser ejecutada por el administrador del sistema quién puede establecer diferentes controles de acceso y uso a cada usuario del sistema.

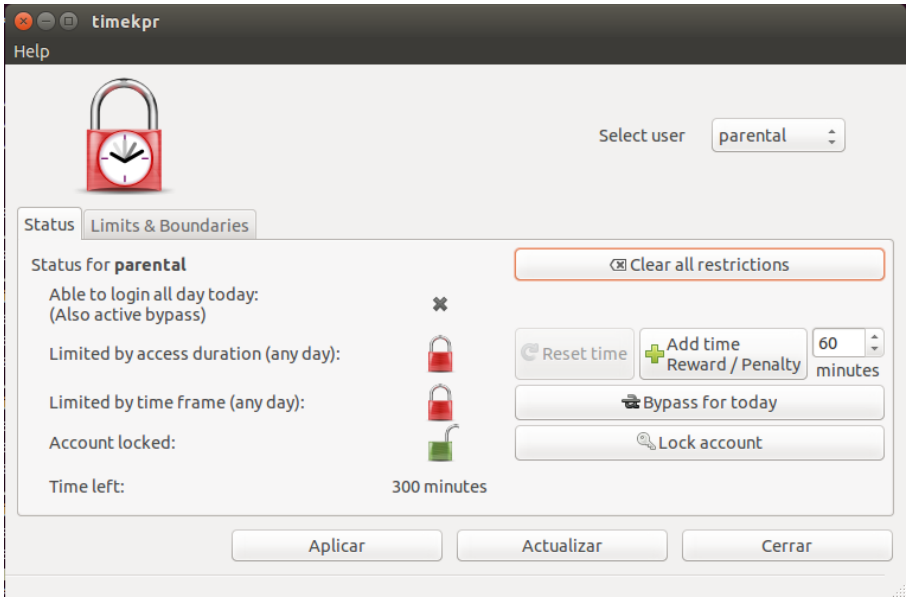

Ilustración 25: TimePKR

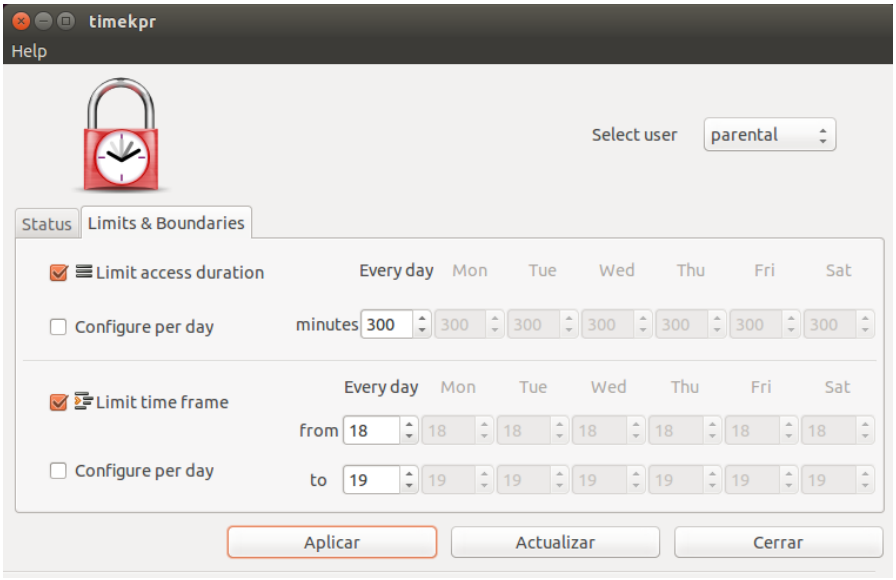

Ilustración 26: Configuración TimePKR

4.1.3.2. Gnome Nanny

Gnome Nanny es una aplicación de control parental que actúa tanto de herramienta de filtrado web como de gestión de acceso al sistema y sus funcionalidades. Nanny nos ofrece las siguientes características:

- **Control de usuarios**. Permite establecer restricciones de uso del PC a los diferentes usuarios del sistema e incluso restringir completamente su utilización asignando un uso del equipo de 0 horas al día.
- **Gestión del tiempo**. Desde la consola de administración de Nanny se puede planificar el tiempo que cada usuario podrá hacer uso del PC, el tiempo que se puede navegar por Internet, el uso del correo electrónico y de aplicaciones de mensajería.
- **Control web**. Del mismo modo que Nanny puede restringir el uso del navegador, también permite definir cuáles son los sitios web por los que permitirá navegar al usuario y cuáles no. Para ello, proporciona tres listas donde se podrán indicar los sitios prohibidos, los permitidos y las listas negras pudiendo realizar un filtrado de páginas.

Para realizar la instalación de la herramienta, que en mi caso es la versión 14.04 de Ubuntu, ha sido necesaria la instalación de un repositorio de terceros ya que no se encuentra disponible para esta versión en el repositorio principal. Para ello hay que ejecutar las siguientes sentencias como administrador en la terminal del sistema:

1. **sudo add-apt-repository ppa:boamaod/nanny-test**
2. **sudo apt-get update**
3. **sudo apt-get install nanny**

A continuación, se muestra la interfaz gráfica de la aplicación, así como una prueba de acceso a la página de apuestas bet365 que ha sido incluida en la lista de sitios prohibidos para comprobar si realmente funciona el filtrado web y el resultado ha sido satisfactorio.

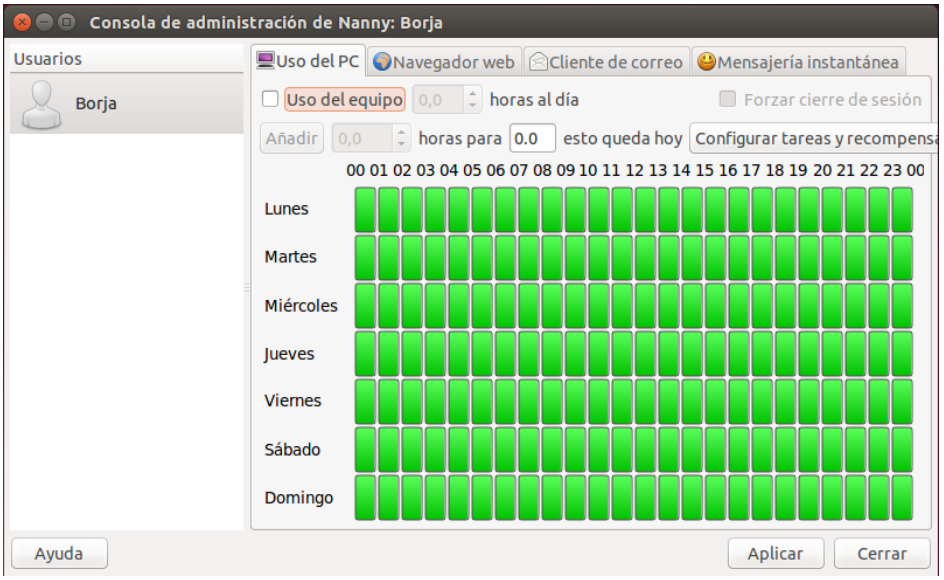

Ilustración 27: Interfaz gráfica Gnome Nanny

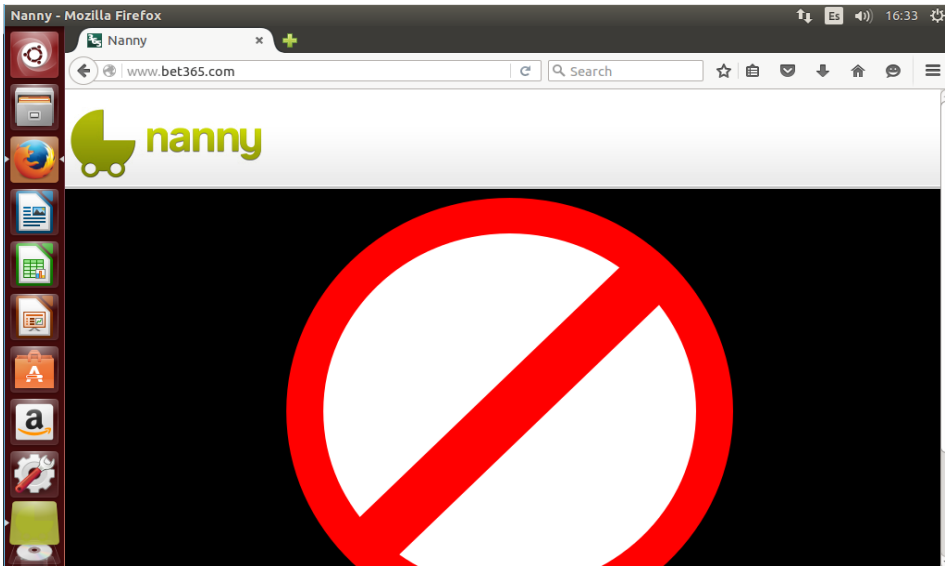

Ilustración 28: Filtrado web Gnome Nanny

La sencillez de la interfaz gráfica hace que la configuración de la consola de administración sea sumamente intuitiva. Una vez ejecutada, con privilegios de administrador, se listan a la izquierda los usuarios configurados en el sistema, y a la derecha, una serie de pestañas permiten acceder a la funcionalidad de la aplicación. En cada pestaña aparece un pequeño calendario dividido en semanas y un combo donde definir el tiempo de uso que cada usuario dedicará a cada actividad.

Otro de los aspectos positivos de la aplicación es que, en el caso de que a un usuario se le agote el tiempo permitido de uso, permite posponer cinco minutos el cierre de sesión para poder almacenar el trabajo que se esté realizando y éste no se pierda.

Una funcionalidad a mejorar es la configuración del filtrado web que, aunque funciona correctamente permitiendo y denegando el acceso a los sitios indicados, se hace complicado gestionar los sitios web manualmente ya que hay que introducir todas las URL que se quieran permitir o denegar.

4.1.3.3. DansGuardian

DansGuardian actúa como un filtro de contenido de sitios web muy potente trabajando conjuntamente con un servidor proxy caché, como por ejemplo Squid, presente en la red local del usuario. Este filtro se sitúa entre el navegador cliente y el proxy, interceptando y modificando la comunicación entre ambos. De esta forma facilita la tarea de filtrado de páginas visitadas por el usuario desde el equipo cliente.

Se trata de una herramienta de código abierto, desarrollada en C++ que permite una configuración flexible adaptándose a las necesidades del usuario para garantizar un buen sistema de control parental. Al instalar DansGuardian, la configuración por defecto ya limita las visitas a páginas prohibidas para menores, pero dispone de gran cantidad de archivos de configuración para llevar a cabo un ajuste del servicio más personalizado.

Su funcionamiento es el siguiente: los clientes mediante sus navegadores web hacen peticiones de direcciones URL que son recibidas por DansGuardian y sólo son redireccionadas al servidor proxy Squid aquellas que superan la fase de filtrado.

Instalación y configuración DansGuardian

Para instalar y configurar correctamente la herramienta hay que seguir los siguientes pasos:

1. Instalación. Introducir la siguiente sentencia en la terminal:
   Sudo apt-get install dansguardian
2. Editar el archivo de configuración para establecer el idioma de la herramienta en español.
   - Ejecutar en la terminal: *sudo gedit /etc/dansguardian/dansguardian.conf.*
   - Modificar la directiva del lenguaje: *language = "spanish".*
   - Una vez realizada la modificación, comentar la siguiente línea que aparece al principio del archivo:
     #UNCONFIGURED – Please remove this line after configuration
3. Configurar el navegador (por ejemplo, Mozilla Firefox) para que funcione correctamente la herramienta. DansGuardian escucha las peticiones en el puerto 8080. Para ello, nos vamos a: *Menú > Preferencias > Avanzado > Red > Configuración > Configuración manual de proxy*
   - Proxy HTTP: 127.0.0.1
   - Puerto: 8080
4. Reiniciar el servicio de DansGuargian para que los cambios se hagan efectivos. Cada vez que se realice un cambio se debe reiniciar.
   sudo /etc/init.d/dansguardian restart

Métodos de filtrado

DansGuardian utiliza un sistema de peso de las frases para mejorar el objetivo de bloqueo y permite filtrar por un gran número de criterios. Los métodos utilizados son:

1. Utiliza el sistema de etiquetas PICS (Platform for Internet Content Selection).

2. Comprueba que las extensiones de los archivos y los tipos MIME no estén en una lista de extensiones y tipos MIME prohibidos.

3. Filtra de acuerdo con las URLs, incluyendo expresiones regulares.

4. Trabaja con listas blancas y listas negras.

DansGuardian se basa en una serie de archivos de configuración para realizar el filtrado. Estos archivos se encuentran en */etc/dansguardian/lists*:

Archivo	Descripción
bannedextensionlist	Contiene una lista de extensiones de archivos no permitidas. Si una URL termina con alguna extensión contenida en esta lista, será bloqueada.
bannediplist	Contiene una lista de direcciones IP que no van a tener acceso.
bannedmimetypelist	Contiene una lista de tipos MIME prohibidos. Si una URL devuelve un tipo MIME incluido en la lista, quedará bloqueada.
bannedphraselist	Contiene una lista de frases prohibidas. Las frases deben estar entre <>. Se puede también utilizar combinaciones de frases, que si se encuentran en una página, serán bloqueadas.
bannedregexpurllist	Contiene una lista de expresiones regulares que si se cumplen sobre la URL ésta será bloqueada.
bannedsitelist	Contiene una lista de sitios prohibidos. Si se indica un nombre de dominio todo él será bloqueado. Si se quiere sólo bloquear partes de un sitio hay que utilizar el archivo bannedurllist.
bannedurllist	Permite bloquear partes específicas de un sitio web.
exceptionphraselist	Lista de las frases que, si aparecen en una página web, pasará el filtro.
exceptioniplist	Contiene una lista de las direcciones IP de los clientes a los que se permite el acceso sin restricciones.
exceptionsitelist	Lista de los nombres de usuarios que no serán filtrados en el caso de utilizar control de acceso por usuario.
exceptionurllist	Parte de un dominio que no se bloqueará.

Tabla 14: Archivos de configuración DansGuardian

Demostración DansGuardian

A continuación, se muestran las pruebas realizadas para comprobar el grado de efectividad de la herramienta.

Bannedsitelist. Incluir en el archivo el sitio web *bet365.com.*Si el usuario accede a cualquier sitio web que se encuentra en el archivo, ocurre lo siguiente:

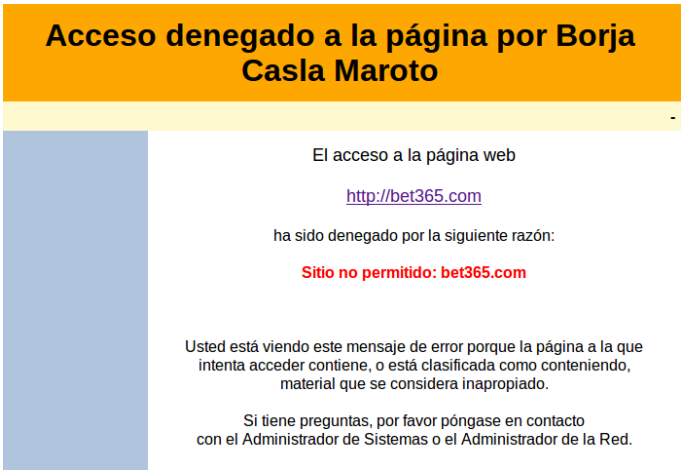

Ilustración 29: Bannedsitelist Dansguardian

Bannedphraselist. Se ha añadido al fichero la palabra “porno” para evitar el acceso a todas las páginas que lo contengan. Por ejemplo, si se intenta acceder a un enlace de google que contiene la palabra “porno”:

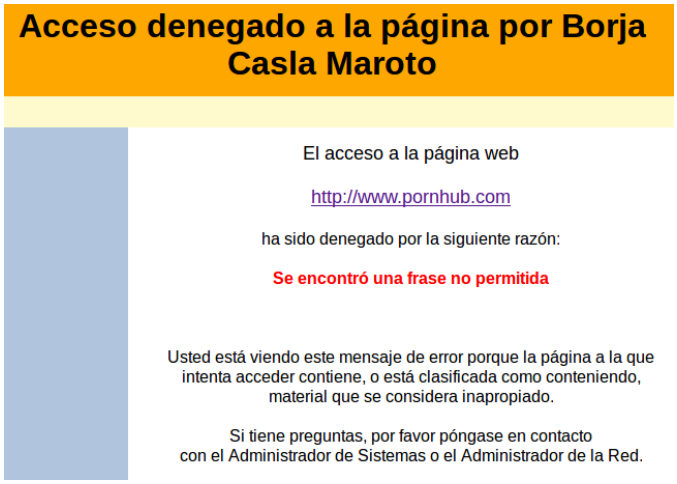

Ilustración 30: Bannedphraselist Dansguardian

Bannedextensionlist. Prohibición de descargas de ficheros .exe añadiendo la extensión en el archivo de configuración.

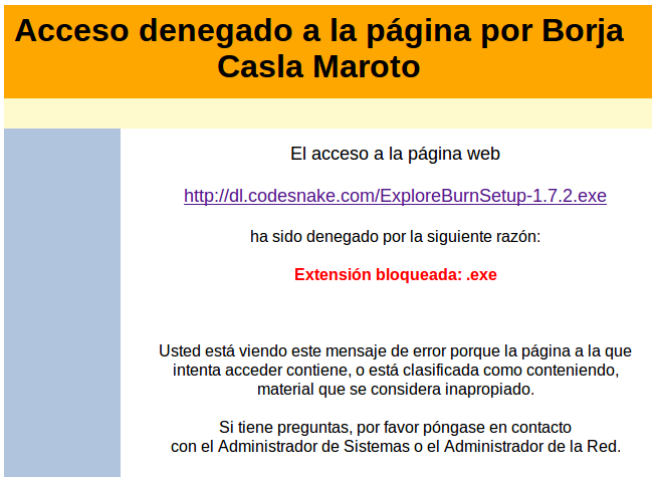

Ilustración 31: Bannedextensionlist DansGuardian

4.1.4. MAC

El sistema operativo MAC OS X incorpora una herramienta de control parental con una interfaz sencilla e intuitiva que hace que la herramienta sea fácil de configurar por cualquier tipo de usuario.

Su funcionalidad es eficaz y completa, actúa como herramienta de filtrado web y monitorización del sistema permitiendo gestionar la utilización del ordenador por parte de los menores, las aplicaciones a las que tendrán acceso y el acceso a los contenidos ubicados en Internet.

Esta herramienta se encuentra en **Preferencias del Sistema > Controles Parentales.**

En la pestaña de *Aplicaciones* se puede seleccionar, entre otras cosas, un Finder simplificado para que los menores únicamente puedan acceder a la carpeta de aplicaciones y al escritorio. Si se marca la opción *Limitar aplicacione,* solamente se tendrá acceso a las aplicaciones especificadas.

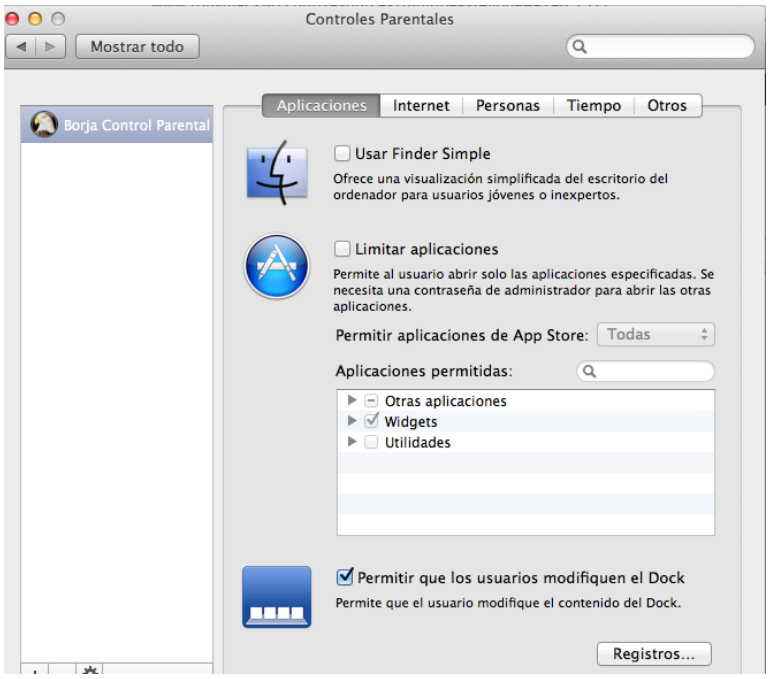

Ilustración 32: Pestaña aplicaciones Control parental MAC OS X

Pulsando el botón *Registros* se accede a la parte de monitorización del sistema donde se realiza un seguimiento de la actividad del menor. Se pueden ver los sitios web visitados por el menor, así como los sitios a los que se le ha bloqueado el acceso, aplicaciones utilizadas y personas con las que ha intercambiado mensajes.

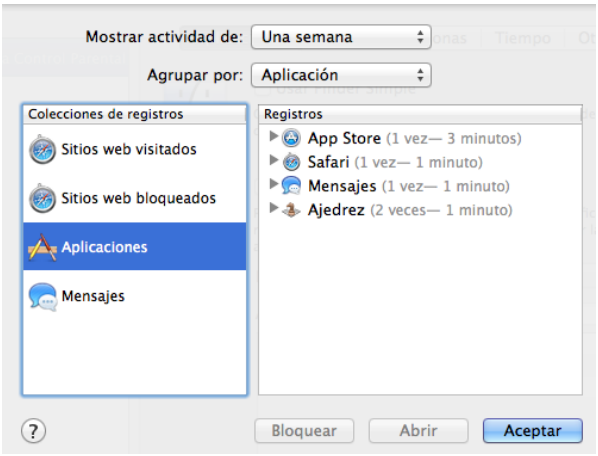

Ilustración 33: Registro de actividad MAC OS X

En la sección *Internet* es donde se realiza la configuración del filtrado web. Se puede elegir entre tres niveles de seguridad:

- Acceso ilimitado a la web.
- Denegar el acceso a algunas webs determinadas.
- Permitir el acceso únicamente a las páginas que nosotros indiquemos previamente.

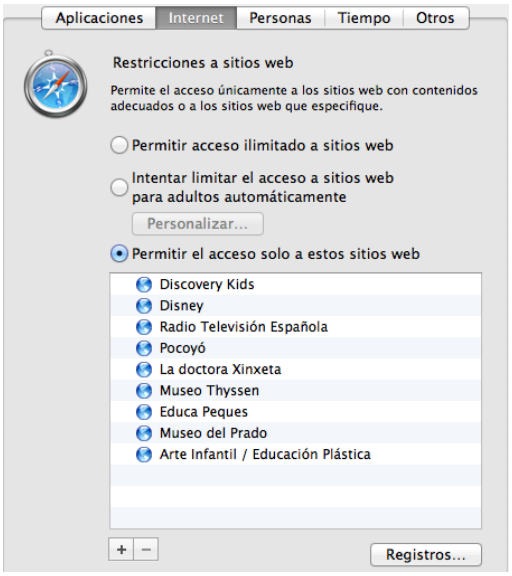

Ilustración 34: Pestaña Internet Control parental MAC OS X

En la sección *Personas* se pueden establecer restricciones en el correo electrónico y aplicaciones de mensajería instantánea para que el usuario únicamente pueda intercambiar mensajes con las personas indicadas en una lista introducida por el administrador del sistema.

En la pestaña *Tiempo,* al igual que en la herramienta de Windows, se configuran las restricciones de tiempo de uso y acceso al ordenador.

Por último, en *Otros* vienen preestablecidas unas restricciones que se pueden activar o desactivar relativas al uso de la impresora y grabación de CD y DVD, cambio de contraseñas

por parte del usuario que se está controlando o limitación de acceso a contenidos inadecuados en fuentes de referencia tales como diccionarios, vocabularios y Wikipedia.

4.1.4.1. Demostración Control Parental MAC OS X

Limitación de Aplicaciones

He configurado la cuenta del usuario para que únicamente tenga acceso a las aplicaciones de App Store, Safari y Mail. Al intentar acceder a una aplicación que no esté seleccionada en la lista de permitidas, aparecerá el siguiente mensaje en pantalla:

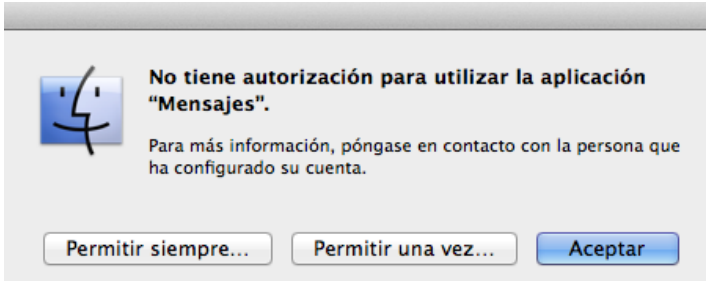

Ilustración 35: Bloqueo de aplicaciones en MAC OS X

Cuando se muestra el mensaje, da la opción de permitir una vez o siempre el acceso a la aplicación o cualquier herramienta que haya sido bloqueada, con el requisito indispensable de que sea el administrador del sistema el que introduzca su contraseña para dar permiso.

Filtrado Web

Al igual que ocurre en Windows o Ubuntu, al tratar de conectarse a una dirección web especificada en una lista negra, la herramienta bloquea el acceso al contenido de dicha web mostrando un mensaje explicativo.

Ilustración 36: Bloqueo Web MAC OS X

Restricciones Mail

Si se establece la opción de limitar el correo electrónico, únicamente se pueden enviar mails a los contactos que se encuentren en una lista de permitidos definida por el administrador. Si el destinatario del mensaje no se encuentra en dicha lista, la herramienta bloquea el envío.

Adicionalmente, el administrador recibirá un correo informando de que se ha tratado de enviar un mail a un usuario bloqueado.

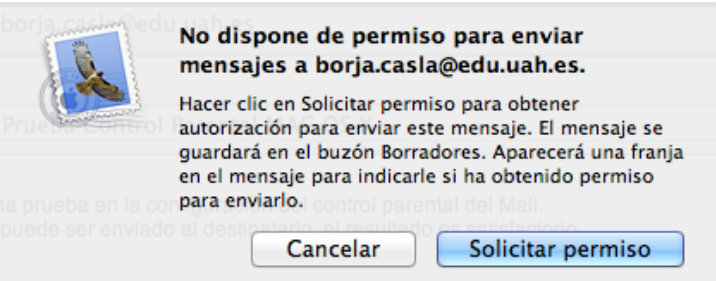

Ilustración 37: Bloqueo de envío de correo electrónico MAC OS X

4.2. Medidas de control parental relacionadas con el DNS (Domain Name Server)

Cada vez que se realiza la búsqueda de una dirección web en Internet, el navegador realiza una consulta a un servidor DNS para averiguar la dirección IP de la página. Por defecto, las consultas se realizan a los servidores DNS del proveedor de servicios de Internet que se tiene contratado, pero se puede utilizar otros servidores diferentes.

OpenDNS nos permite utilizar sus servidores DNS, de forma gratuita, en lugar de los de nuestro proveedor de acceso a Internet con el objetivo de mejorar el rendimiento de la navegación, acortando el tiempo de traducción de las direcciones. Otra de las ventajas de OpenDNS es que ofrece un servicio proxy que permite controlar y restringir el contenido al que puedan acceder los menores en el ordenador o dispositivos conectados a nuestra red.

OpenDNS permite aplicar el filtrado de contenido en dos niveles de aplicación. Por un lado, si se desea configurar un filtro de contenido para un único ordenador basta con modificar las direcciones DNS a las que se conecta el equipo. Por otro lado, la opción más segura es establecer el filtrado de contenido en la configuración del router. De esta manera, se realizará un control del acceso a los contenidos de Internet a cualquier equipo que se conecte a la Red. Aparte de realizar un filtrado de contenido, también permite realizar un seguimiento de la actividad del menor en la red registrando las direcciones web consultadas y las que han sido bloqueadas.

4.2.1. ¿Cómo funciona OpenDNS?

Cuando se introduce la dirección de una página web en la barra de direcciones del navegador, por ejemplo, http://www.google.es, el ordenador se dirige a un servidor de nombres DNS para saber la dirección IP del servidor que contiene la página. Este es un paso previo para obtener esta página y descargarla al equipo para su visualización a través del navegador.

Por lo general se suelen utilizar los servidores DNS de nuestro proveedor de acceso a Internet, pero podemos utilizar otros. Si utilizamos los servidores DNS de OpenDNS entonces navegaremos usando el acceso proporcionado por nuestra empresa de telefonía, pero aprovechándonos de las prestaciones de filtrado que nos ofrece de forma gratuita OpenDNS.

Los servidores DNS de OpenDNS son: 208.67.222.222 y 208.67.220.220.

Para activar el filtro de contenidos es necesario asignarle manualmente estas IP como servidor de DNS en la configuración de la tarjeta de red o bien configurar el router para que lo haga de forma automática cuando un ordenador se inicia y solicita una dirección IP con que conectarse a Internet.

4.2.2. Configuración OpenDNS

Para configurar OpenDNS hay que seguir los siguientes pasos:

1. En primer lugar, se establecen las direcciones DNS en la tarjeta de red de nuestra conexión. Para ello ir a *Panel de control > Redes e Internet > Conexiones de red.* Una vez dentro, acceder a las propiedades de la conexión y editar las propiedades del *Protocolo de Internet versión 4*, e incluir las dos direcciones DNS a las que se conecta OpenDNS, 208.67.222.222 y 208.67.220.220.

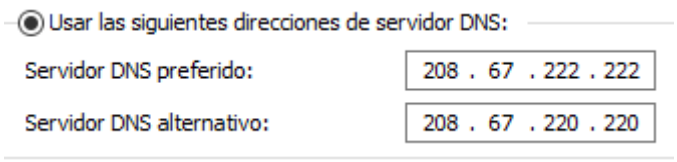

Ilustración 38: Direcciones de servidor OpenDNS

2. Crear una cuenta en la dirección web de OpenDNS (https://www.opendns.com/) para poder configurar el filtro de contenidos.

3. Introducir los credenciales registrados y, automáticamente, nos redirigirá a la interfaz principal de nuestro usuario. Ir a la sección de configuración "*Settings*" y añadir la Red con la dirección IP del equipo (OpenDNS detecta automáticamente la IP del equipo).

4. De entre todas las opciones que se pueden configurar, la más importante es el apartado de filtro de contenido web. Permite seleccionar entre varios grados de control (alto, moderado, bajo, ninguno y personalizado).
   Es recomendable realizar un filtrado personalizado para así poder seleccionar qué contenido se permite mostrar y a qué tipo de sitios se restringirá el acceso.

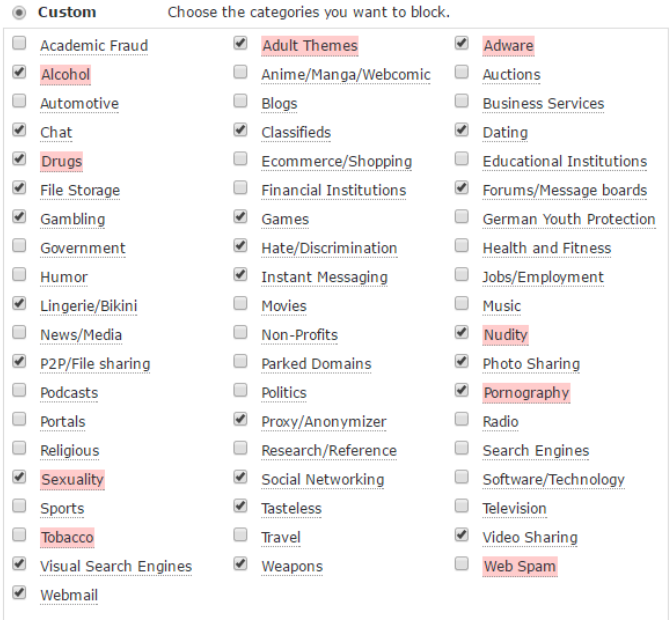

Ilustración 39: Filtro de contenido personalizado OpenDNS

Si el menor intenta acceder a cualquier sitio web cuyo contenido esté relacionado con alguna de las categorías seleccionadas, se bloqueará el acceso y se muestra un mensaje en pantalla.

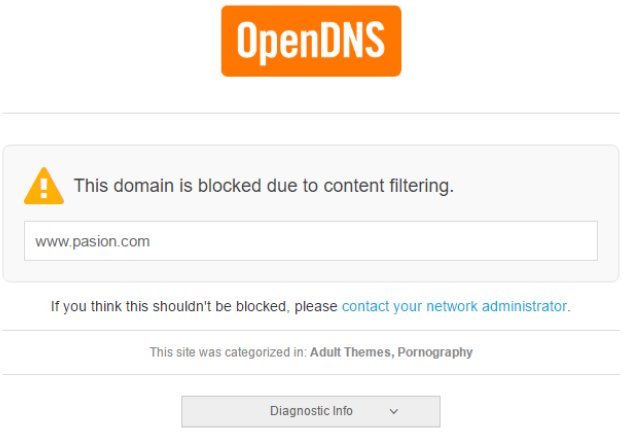

Ilustración 40: Bloqueo Web OpenDNS

En la sección "*Manage individual domains*" se puede definir un listado de dominios que siempre se bloquearán y un listado de dominios que nunca se bloquearán. Para ello basta introducir el dominio, desplegar el combo *Always block/Never block* para seleccionar una de las dos opciones y hacer clic en el botón *Add domain*.

Se puede utilizar en cualquier sistema operativo.

4.3. Medidas de control parental relacionadas con el ISP (Internet Service Provider)

Algunos proveedores de Internet (ISP) ofrecen sin costes adicionales la posibilidad de configurar perfiles de usuarios distintos para cada miembro de una familia, con acceso personalizable en función de la edad, como solución de seguridad integrada.

En España nos encontramos con las soluciones integradas ofrecidas por dos de los principales proveedores de Internet como son Telefónica y Ono.

4.3.1. Canguro Net

Canguro Net es un servicio de filtrado de contenido en Internet que permite bloquear ciertas páginas web en función del potencial de riesgo de sus contenidos (racismo, violencia, tráfico y consumo de drogas, pornografía, manifestaciones sectarias o construcción de explosivos), utilizando un doble-mecanismo basado en un analizador semántico que se encarga de la detección de los contenidos, su posterior comparación con las listas de categorías restringidas y bloquea su acceso en caso de coincidencia, y unas listas de protección predefinidas que serán simples listas de direcciones web preclasificadas por su contenido.

Este servicio supone múltiples ventajas para aquellos usuarios que quieren realizar un control sobre sus menores:

- Protege el acceso web desde cualquier dispositivo (PC, videoconsolas, Smartphone) que esté conectado a la red Movistar ya sea por cable o wifi, desde cualquier tipo de dispositivo.
- Es posible activar o desactivar la lista de control por categorías. Esta lista presenta una configuración por defecto que se puede modificar, ajustándola a las necesidades del usuario.
- Uso de listas blancas y negras para los servicios de filtrado de contenidos.
- Elimina pop-ups, filtra los banners por sus dimensiones, bloquea peticiones categorizadas como publicidad.
- Trabaja en la nube por lo que no hay que realizar ningún tipo de instalación.
- Utiliza una tecnología que combina listas de palabras con análisis de contenido en el que aparecen, lo que garantiza una mayor efectividad en el proceso de filtrado.
- Posibilidad de prohibir cualquier tipo de comunicación que suponga transferencias de archivos en distintos formatos.
- Permite establecer horarios de uso de la red.

Valorando la funcionalidad que nos ofrece este servicio, es una buena opción para los usuarios que tengan contratada su red ADSL con Movistar que por una tarifa mensual de 4,99€ pueden obtener el servicio y evitar que los menores estén expuestos a los riesgos de la red.

4.3.2. Centinela Ono

Ono ofrece un pack de seguridad total comercializado bajo el nombre “Centinela Ono”, se trata de un paquete de tres licencias de uso (para tres equipos informáticos distintos, que compartan la misma conexión) que consiste en un conjunto de aplicaciones de seguridad. Es, por tanto, un paquete software que el ISP ofrece a sus clientes, e incluye:

- Antivirus. Protege el equipo informático frente a los virus, gusanos y troyanos.
- Firewall. Evita los accesos intrusivos o no autorizados al PC.
- Aplicaciones antispyware Detectan y eliminan las potenciales aplicaciones espía.
- Antifraude. El sistema evita que se realicen compras online en sitios web no seguros.
- Antipop-ups. Evita la aparición de ventanas emergentes y de la publicidad no deseada.
- Control parental. Únicamente tiene la función de filtrar contenidos.
- Gestor de privacidad. Borra o controla las cookies guardadas en el ordenador y avisa sobre las eventuales fugas de información personal, no consentidas.

El mayor inconveniente de esta herramienta es que no permite realizar la monitorización de la actividad del menor cuando está utilizando el dispositivo. En cambio, Ono lo compensa con un fuerte filtrado de contenidos para evitar acceder a sitios web inapropiados, que hace que no

haya que preocuparse por las actividades que se realicen cuando el menor navega por Internet sin la supervisión de un adulto.

4.4. Medidas de control parental ofrecidas por los navegadores

Los diferentes navegadores web también ofrecen la posibilidad de limitar el acceso a determinados contenidos mediante la instalación de extensiones propias que son las encargadas de realizar el filtrado web. La ventaja que tiene utilizar herramientas de control parental desde el navegador es que se pueden instalar bajo cualquier sistema operativo ya que los navegadores más utilizados son compatibles con los sistemas operativos más importantes. Actualmente, el navegador Microsoft Edge, antiguo Internet Explorer, se configura con la misma configuración de Windows 10.

4.4.1. Mozilla Firefox

La herramienta principal para filtrar el contenido en el navegador Mozilla Firefox es la extensión **Procon Latte Content Filter.** Puede instalarse desde la siguiente dirección: *https://addons.mozilla.org/es-ES/firefox/addon/1803*, o buscando la aplicación en la pestaña de complementos del navegador.

Las características de ProCon Latte son las siguientes:

- Filtra cualquier tipo de contenido.
- Puede bloquear todo el tráfico hacia páginas no incluidas en una lista blanca de páginas web a las que se permite el acceso.
- Incorpora un filtro por palabras clave que bloquea páginas web que contienen determinadas palabras en su URL, título o contenido.
- Permite la personalización de las listas blancas y/o palabras clave, así como la posibilidad de importar otras listas desde otros equipos.
- Dispone de un sistema llamado *profanity filter* que busca en la página todas las veces que aparecen palabras de una lista prohibida que, además es configurable, y las sustituye por otra palabra.
- El entorno de la extensión está protegido por contraseña para impedir cambiar la configuración.
- En caso de que se bloquee una página, podemos mostrar una advertencia y/o redirigir a otra página.

Configuración

En la pestaña *General* se establece el nivel de filtrado que se quiere realizar: uso de lista blanca y negra, sitios bloqueados, palabras prohibidas, lista de palabras malsonantes, personalización de los mensajes de bloqueo, así como personalizar una página a la que se redireccionará en caso de bloqueo. Un aspecto importante a configurar en esta pestaña es el uso de contraseña para poder configurar la aplicación, si no se especifica una contraseña de acceso, el menor puede reconfigurar la herramienta.

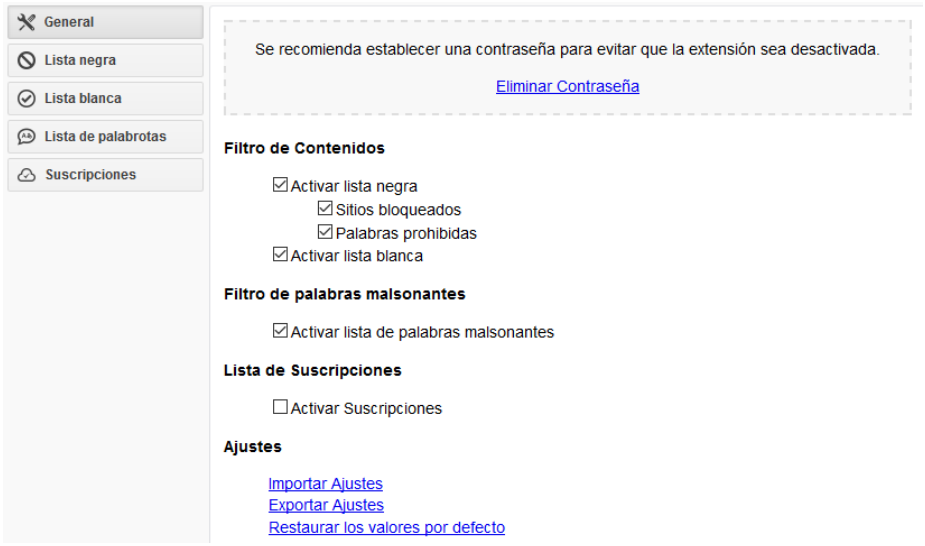

Ilustración 41: Interfaz Procon Latte

En *Lista Negra* se especifica una lista de sitios bloqueados y una lista de palabras prohibidas que sirve para bloquear el acceso a los sitios web cuyo contenido coincida con, al menos, una palabra de la lista.

En la sección *Lista Blanca* se establecen los sitios a los que se permitirá el acceso de manera permanente.

Lista Palabrotas es una lista donde se incluye una serie de palabras que se van a censurar si alguna de estas aparece en cualquier sitio web. Se puede personalizar para que se sustituya la palabra censurada por una palabra que el usuario desee.

Cuando se produce un bloqueo en el navegador porque se ha activado el filtro de control parental, aparece un mensaje informativo en pantalla. En este caso se ha utilizado la palabra prohibida *'porn'* en el navegador y ha sido bloqueada la búsqueda mostrando lo siguiente:

Ilustración 42: Bloqueo web Procon Latte

4.4.2. Google Chrome

Blocksi (*https://goo.gl/OSdEgw*) es la extensión de filtrado de contenido más completa y utilizada en el navegador Google Chrome, también disponible para el navegador Opera y Mozilla Firefox. Se trata de una especie de control parental todo-en-uno que agrupa las principales características que un sistema de control parental debe tener para realizar un correcto funcionamiento. Actualmente, dispone de dos versiones, una gratuita y otra de pago, pero para cumplir con su función de filtro de contenido basta con instalar la versión gratuita.

Las principales características de la versión gratuita son:

- Realiza un filtrado web basado en la clasificación de 79 categorías de tipo de contenido, incluyendo temas para adultos, seguridad y contenido malicioso. Contiene una base de datos con más de 45 millones de sitios web clasificados.
- Filtrado de contenido en YouTube a través de 20 categorías, permite bloquear determinados canales de YouTube y filtro de contenido por palabras clave.
- Búsqueda segura de texto, imágenes y vídeos en los principales motores de búsqueda.
- Filtrado de contenidos basado en palabras clave.
- Gestión de listas negra y blanca para denegar o permitir el acceso a determinados sitios web.
- Permite controlar el tiempo de acceso y uso del navegador.

La versión de pago incluye, además de esta funcionalidad, un registro de los sitios web que se han visitado y los que se han bloqueado, así como un servicio de análisis estadísticos para estudiar el tipo de navegación que se está realizando.

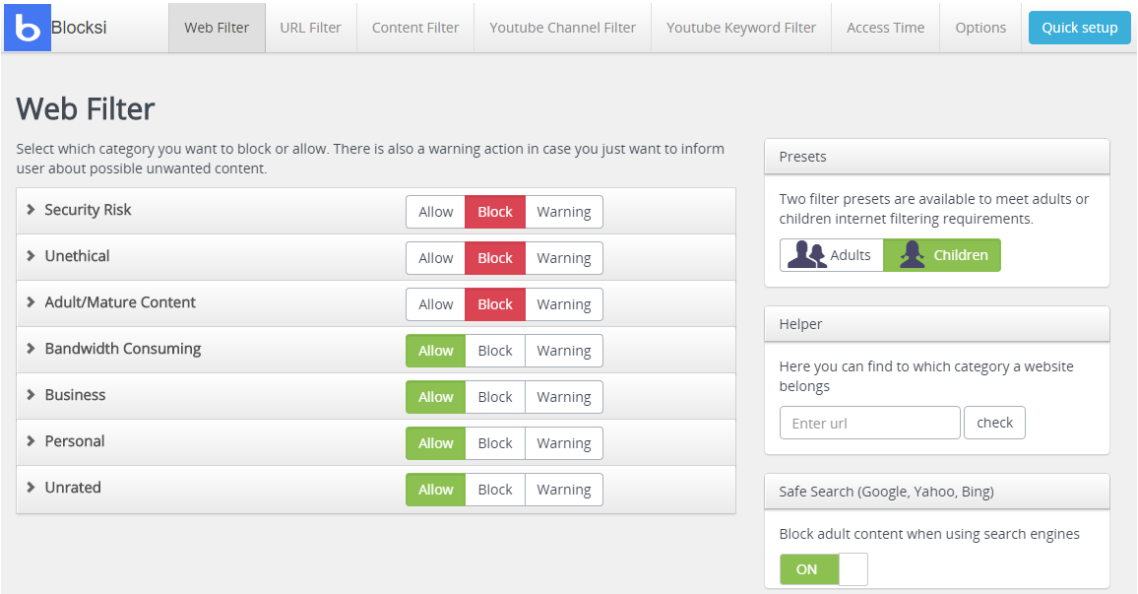

Ilustración 43: Extensión Blocksi

Una diferencia importante con el resto de herramientas de filtrado web es a la hora de realizar una búsqueda en cualquiera de los motores de búsqueda web (Google, Yahoo, …). En otras herramientas cuando se busca, por ejemplo, información sobre el sexo se muestra todo tipo

de páginas, aptas y no aptas, que contienen esta categoría, así como imágenes para adultos. Blocksi realiza una búsqueda exhaustiva de páginas que contienen información didáctica sobre el sexo sin mostrar imágenes que puedan dañar al menor.

Cuando el filtro de contenido deniega el acceso a un sitio web muestra un mensaje informativo con la URL del sitio web bloqueado y la categoría en la que se clasifica y por la que se ha prohibido el acceso.

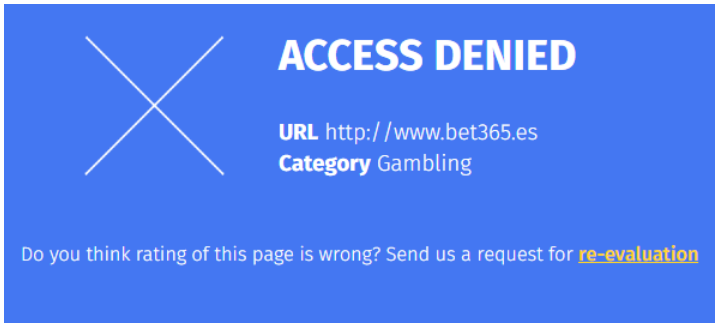

Ilustración 44: Bloqueo web Blocksi

Filtro de contenido YouTube

Como se ha visto en las características, Blocksi permite realizar un filtrado exclusivo para el sitio web de YouTube mediante la clasificación en categorías del contenido de los vídeos, bloqueo por palabras clave contenidas en la descripción del video y el bloqueo de determinados canales que pueden ser perjudiciales para los menores.

Por ejemplo, estableciendo el bloqueo por categoría de los videos clasificados para mayores de 18, el filtro actúa redirigiendo a un video que contiene un mensaje del bloqueo impidiendo la visualización del video.

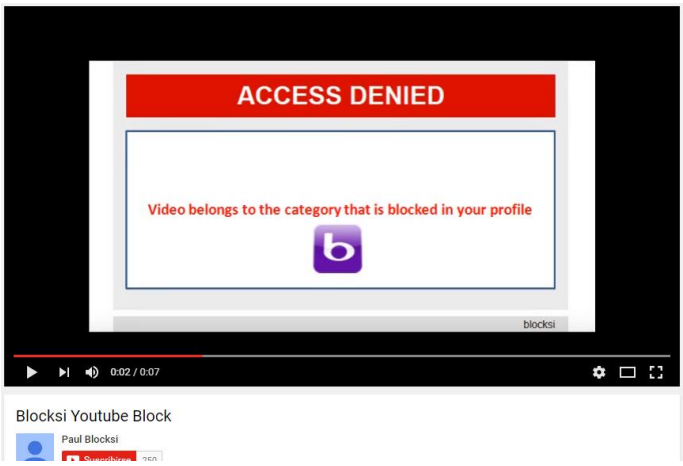

Ilustración 45: Filtro de contenido YouTube

4.5. Software de control parental de terceros

Además de las soluciones propuestas, existen muchas otras herramientas comercializadas en el mercado, de código abierto o puestas a disposición de los usuarios sin ningún tipo de contraprestación. Existe gran variedad de herramientas, pero voy a centrarme en dos de ellas,

Qustodio y K9Web Protection, que son gratuitas y cumplen a la perfección con los requisitos que debe tener un sistema de control parental para ser correcto y efectivo

4.5.1. Qustodio

Qustodio es una herramienta de monitorización de actividad y filtrado de contenido multiplataforma, es decir, se puede instalar en cualquier dispositivo conectado a la red sea cual sea el sistema operativo instalado.

Las principales características de Qustodio son:

- Permite bloquear temas o sitios específicos con contenido inadecuado.
- Permite realizar un seguimiento de la actividad del menor en el dispositivo. Incluye una función de envío de notificaciones al administrador cuando el menor intenta acceder a un sitio web catalogado como inapropiado.
- Qustodio se mantiene oculto para los perfiles que están siendo monitorizados, de modo que el menor no sabe que está siendo controlado.
- Permite controlar la cantidad de horas que los más pequeños pasan frente al dispositivo.
- Control de las aplicaciones de las que puede hacer uso el menor.
- Permite realizar un control del uso de las redes sociales.
- Si se aplica en un Smartphone, permite monitorizar y bloquear llamadas y envío de SMS. Permite establecer una lista de contactos permitidos y bloqueados para controlar con quien puede comunicarse el menor.
- Geolocalización. Permite saber dónde se encuentra el menor en todo momento. En dispositivos móviles, incluye un botón de pánico en caso de que el menor necesite ayuda y envía un mensaje al administrador informando de la situación.

Su funcionamiento está basado en un sistema de perfiles, a los que se asocia uno o varios dispositivos (en la versión gratuita solo se puede asociar un dispositivo). De esta manera, se obtiene información de cada uno de los menores que hacen uso del dispositivo.

La configuración de la herramienta y el seguimiento de la actividad se realiza desde cualquier navegador de internet, sin necesidad de que la aplicación se encuentre instalada en el dispositivo del menor. Basta con asociar un perfil al instalar Qustodio en el dispositivo. La ventaja de que el control se realice de forma “remota” es que no hay posibilidad de que el menor desinstale o cambie la configuración de la herramienta.

Instalación

A continuación, se enumeran los pasos a seguir para realizar la instalación de la herramienta:

1. Crear una cuenta en la web oficial de Qustodio (*https://www.qustodio.com/es/*).
2. Añadir un perfil con los datos del menor (nombre y año de nacimiento).
3. Indicar si se desea instalar la aplicación en el propio dispositivo desde el que se añade la cuenta o desde otro dispositivo. En caso de que señale que desea aplicarlo en otro

dispositivo, se enviará un correo electrónico con los datos de la descarga para iniciar sesión desde dicho dispositivo.

4. Descargar el ejecutable si se desea instalar en el mismo dispositivo o acceder al enlace de descarga enviado, en caso de que se haya seleccionado la instalación en otro dispositivo.
5. Instalación. Es un proceso sencillo en el que se debe indicar el perfil del usuario creado en el paso 2. Una opción muy importante que hay que indicar es la de ocultar la aplicación en el dispositivo para que el menor no tenga constancia de ello.

Configuración

Una vez finalizada la instalación, se debe configurar la aplicación para que actúe acorde a nuestras necesidades.

Ilustración 46: Qustodio

Como he explicado anteriormente, la configuración de la herramienta se realiza a través de la propia web en el Portal Familiar de Qustodio. Se muestran los siguientes apartados:

- **Resumen de actividad.** Muestra un informe general de las actividades realizadas por cada usuario. Están representadas en forma de gráfico circular y el tiempo dedicado a cada actividad se muestra como porcentaje. Además, facilita la siguiente información:
  - Actividad de búsquedas**:** muestra las palabras clave de búsqueda utilizadas por el usuario (en Google, Yahoo, ...).
  - Programas: Muestra las aplicaciones utilizadas, así como el tiempo activo en cada aplicación.
  - Dispositivos usados y sus cifras de utilización.
- **Actividad social.** Monitorización de la actividad realizada en Facebook.

- **Navegación.** Muestra un resumen de los sitios web visitados por el usuario en los últimos 30 días. Cuando se selecciona un sitio web, se muestra la información sobre el sitio web, el resumen de la visita y el historial de navegación.

- **Cronología de actividad.** Muestra una lista de las actividades realizadas por el usuario, el dispositivo utilizado y el tiempo que el usuario empleó en estas actividades. Puede filtrar por las siguientes secciones:
  - **Toda la actividad:** muestra todas las actividades en la red, aplicaciones ejecutadas en el dispositivo y el tiempo empleado en cada actividad.
  - **Actividad cuestionable:** muestra la lista de actividades que Qustodio ha clasificado como potencialmente inseguras.
  - **Navegación:** muestra una lista de la actividad realizada por el usuario en la web.
  - **Programas:** muestra la lista de aplicaciones utilizadas.
  - **Llamadas y SMS:** muestra una lista de llamadas y SMS enviados y recibidos. Permite monitorizar y bloquear las llamadas telefónicas y mensajes de texto SMS.
  - **Ubicación:** muestra la última y las anteriores ubicaciones del dispositivo monitorizado.

- **Reglas**. En esta sección se realiza la configuración que le permite controlar el tipo de sitios web a los que puede acceder el menor, así como los resultados que recibirá de los buscadores. Al crear un nuevo perfil, se aplica automáticamente la configuración por defecto de Qustodio. Está compuesto de diferentes secciones:
  - **Navegación web**
    - *Categorías de sitios web*: se puede permitir o restringir determinados tipos de sitios web, o recibir alertas cuando el menor acceda a un sitio de una categoría específica.
    - *Excepciones de sitios web*: introducir sitios web específicos que se desea vigilar, bloquear o permitir.
    - *Sitios no categorizados*: activar este ajuste si desea que Qustodio permita o bloquee el acceso a sitios web que no pueden ser categorizados por cualquier motivo.
    - *Búsqueda segura*: especificar si quiere que Qustodio limite los resultados de búsqueda eliminando contenido potencialmente inseguro.
  - **Límites de uso.** Permite limitar la cantidad de tiempo que el menor puede utilizar el dispositivo o acceder a internet. Por defecto, todos los límites de uso están desactivados. Se puede configurar:
    - *Calendario de uso*: permite activar o desactivar el control de tiempo. Si se desea limitar las horas o días de uso, marca en el calendario las franjas horarias que le estarán permitidas.
    - *Tipo de bloqueo de dispositivo*: este ajuste permite especificar qué ocurre cuando el menor alcanza el límite de uso del dispositivo. Permite seleccionar entre bloquear la navegación, bloquear el dispositivo o enviar una alerta.

- **Programas.** Permite limitar el acceso de un usuario supervisado a ciertas aplicaciones o fijar límites de tiempo para cada aplicación específica.
- **Monitoreo social.** Permite activar un Monitoreo Avanzado para Facebook (función disponible para cuenta premium). Esta prestación permite a Qustodio conectarse directamente a la cuenta de Facebook del usuario supervisado con el fin de monitorear la actividad social con mayor detalle.
- **Llamadas y SMS.** Esta página contiene opciones que le permite supervisar llamadas y SMS. Actualmente solo se pueden supervisar los dispositivos Android.
- **Localización.** Contiene opciones para localizar la ubicación de sus dispositivos móviles en un mapa.
- **Botón de pánico.** Permite activar un Botón del Pánico en teléfonos Android asociados a este perfil. Cuando está activado, envía alertas de emergencia con la localización del dispositivo a una lista de contactos de confianza.

En definitiva, Qustodio es una herramienta muy interesante debido a la totalidad de su funcionalidad, protegiendo todos los lugares a los que tiene acceso el menor desde un dispositivo, y que se puede obtener de forma gratuita. La única diferencia con su versión de pago es el número de dispositivos en los que se puede instalar y la monitorización de la red social Facebook.

4.5.2. K9 Web Protection

K9 es una herramienta de control parental gratuita, desarrollada por Blue Coat, que permite controlar y monitorizar la actividad de los menores en Internet con una aplicación sencilla de instalar, configurar y aplicar. Para realizar el filtrado de contenido, K9 cuenta con una clasificación de contenido de 60 categorías diferentes para poder realizar un control efectivo.

Al igual que en la herramienta Qustodio, la configuración del filtrado de contenido y el seguimiento de la actividad se realiza a través de Internet, pero, en este caso, debe ser desde el mismo dispositivo en el que se ha instalado la aplicación porque para acceder al sitio web de K9 hay que ejecutar la aplicación de escritorio instalada.

Las principales características que nos ofrece la aplicación son las siguientes:

- Filtrado web que permite bloquear categorías de contenido completas, como pornografía o juegos.
- Protección contra malware en tiempo real que bloquea el contenido ilegal o malintencionado.
- Clasificaciones automáticas de contenido que identifican la categoría de una página web sin clasificar.
- Políticas personalizadas para permitir o bloquear cualquier sitio web específico, como Facebook o YouTube.
- Restricciones de tiempo de uso de Internet.
- Filtrado por palabras clave.

- Modo Safe Search que filtra las búsquedas realizadas en los motores de búsqueda.
- Disponible para Windows, Mac e IOS.

Instalación

La descarga de la aplicación se realiza desde la página oficial de la herramienta (*http://www1.k9webprotection.com/*) y hay que seguir una serie de pasos para obtener el instalador:

1. Rellenar el formulario que se encuentra en *http://www1.k9webprotection.com/get-k9-web-protection-free* para recibir, en el correo electrónico registrado, una licencia necesaria durante el proceso de instalación. En este paso se deberá especificar una contraseña de administrador que será necesaria, posteriormente, para acceder a la aplicación.
2. Descargar el ejecutable accediendo al link indicado en el correo recibido e instalar. A pesar de que en la herramienta para Windows aparezca disponible hasta la versión de Windows 7, también es compatible con Windows 8 y Windows 10. Durante el proceso de instalación se solicitará la clave obtenida en el paso 1 y se debe reiniciar el sistema para que funcione correctamente. Una vez instalado, proceder a configurar la herramienta.

Configuración

Cuando se ejecuta la aplicación, se abre automáticamente en el navegador que tengamos instalado por defecto.

Ilustración 47: K9 Web Protection

K9 Web Protection monitoriza toda la actividad relacionada con la navegación web y se puede consultar a través del apartado **View Internet Activity**. Para mostrar toda la información de manera sencilla, agrupa los sitios web visitados por categorías. Haz clic en una de ellas si deseas datos específicos de qué sitios se han visitado. Para consultar el listado exhaustivo de páginas consultadas, pulsa sobre View activity detail. Además de la dirección URL de los sitios visitados, muestra la fecha y la hora de acceso.

La configuración de la herramienta se realiza en el apartado **Setup**, que contiene las siguientes secciones:

- **Web Categories to Block.** Permite seleccionar el nivel de filtrado que se desea realizar, cada nivel contiene una serie de categorías a bloquear.
  - *Hight*: Esta opción es la más restrictiva, bloquea todas las páginas de contenido sexual, programas de mensajería que se utilizan para chatear, grupos de noticias, redes sociales como Facebook y MySpace, sitios sin censura, páginas sospechosas y páginas de actividad ilegal.
  - *Default*: Bloquea todas las páginas de contenido sexual, amenazas de seguridad y sitios web no clasificados. Es la opción que viene establecida por defecto.
  - *Moderate*: bloquea todas las páginas de contenido sexual, paginas sospechosas y páginas de actividad ilegal.
  - *Minimal*: esta opción es la menos restrictiva, únicamente bloquea páginas de contenido sexual y páginas de actividad ilegal.
  - *Monitor*: esta opción no filtra ningún tipo de contenido. Se limita a registrar la actividad web del menor y almacena las páginas que se han visitado.
  - *Custom*: si ninguno de los niveles de protección satisface sus necesidades, esta opción permite seleccionar las categorías que se deseen bloquear.

- **Time Restrictions.** Permite configurar el horario que los usuarios tendrán permitido o denegado el acceso a la Web. Hay tres opciones:
  - *Sin restricciones*.
  - *NightGuard*: prohíbe la navegación durante la noche
  - Custom: permite determinar a qué horas se puede navegar y a cuáles no.

- **Web Site Exceptions**. Permite indicar sitios web que se desean bloquear o permitir su acceso, sin tener en cuenta su categoría.
  Si se quiere denegar siempre el acceso a una página web, teclear en la casilla de la sección *Always Block* el nombre del sitio o la URL de la página. El acceso quedará autorizado independientemente de las opciones seleccionadas en *Web Categories to Block*.
  Por el contrario, si se desea permitir el acceso permanente a un sitio web, teclear su dirección en la casilla de la sección *Always Allow*.

- **Blocking Effects**. Se puede determinar que comportamiento debe tener el programa al bloquear una web. Seleccionar entre que emita un sonido, que muestre las opciones administrativas, e incluso cancelar la navegación si comprueba que hay reiterados intentos de acceder a páginas bloqueadas.

- **URL Keywords**. Mediante esta sección podemos crear una lista de palabras que, en caso de aparecer en la URL de una web, provocan que ésta se bloquee inmediatamente.

- **Safe Search**. Permite configurar el comportamiento de los motores de búsqueda.

Es una herramienta que realiza un filtrado de contenido muy restrictivo bloqueando cualquier sitio web cuyo contenido esté relacionado con alguna de las 60 categorías en las que clasifica

la web. Por ejemplo, si se desea buscar información didáctica sobre el sexo no se obtienen resultados porque la aplicación considera que es una categoría peligrosa y bloquea el acceso. Es muy importante seleccionar el nivel de bloqueo que se quiere realizar y combinarlo con las excepciones web para obtener los mayores beneficios de la red.

K9 Web Protection también incorpora una tecnología de protección anti-phishing en tiempo real, es decir, cada página que se intenta visitar es analizada y comparada automáticamente con una base de datos actualizada de sitios fraudulentos, si la web se incluye entre los sitios considerados maliciosos, K9 Web Protection bloqueará la página o alertará al usuario. Este proceso de filtrado se realiza en cuestión de milisegundos y por lo tanto la ralentización es mínima.

5. Análisis de resultados

Una vez realizado el análisis y aplicación de las herramientas de control parental más relevantes de las que disponemos actualmente, se puede realizar una comparación de todas ellas en forma de tabla viendo qué ofrece y qué le falta a cada una de ellas.

Área	Funcionalidad	W8	W10	MAC OS X	TimePKR	Gnome Nanny	DansGuardian
Administración	Gestión de diferentes perfiles de usuario	✓	✓	✓	✓	✓	✗
	Gestionar varios dispositivos	✗	✗	✗	✗	✗	✗
	Registro de actividad	✓	✓	✓	✗	✓	✗
	Monitorización de forma remota	✗	✗	✗	✗	✗	✗
Personalizar el filtro de contenido	Personalizar categorías de filtrado	✗	✗	✗	✗	✓	✗
	Gestión de lista blanca y negra (modificación o creación)	✓	✓	✓	✗	✓	✓
	Lista blanca y negra por defecto	✗	✗	✗	✗	✗	✓
	Filtrado por palabras clave	✗	✗	✗	✗	✗	✓
Tiempo de uso y/o acceso	Gestionar el tiempo de uso y/o acceso al PC	✓	✓	✓	✓	✓	✗
	Gestionar el tiempo de uso y/o acceso a Internet	✗	✗	✓	✓	✓	✗
Notificaciones de bloqueo	Solicitar permiso para desbloquear	✓	✓	✓	✗	✓	✗
	Redirección a sitio web seguro	✗	✗	✓	✗	✗	✗
Restricciones de uso	Bloquea el acceso a sitios web	✓	✓	✓	✗	✓	✓
	Registra la actividad online	✓	✓	✓	✗	✗	✗
	Modo Safe Search	✓	✓	✗	✗	✗	✗
	Bloquea el acceso a redes sociales	✓	✓	✗	✗	✓	✓

	Monitoriza la actividad en redes sociales	✗	✗	✗	✗	✗	✗
	Bloqueo de aplicaciones	✓	✓	✓	✗	✗	✗
	Restringe el uso del correo electrónico	✓	✓	✓	✗	✓	✗
Seguridad. Controla que el usuario evite el filtrado de contenido mediante:	Uso de dirección IP en lugar de URL	✓	✓	✓	✗	✓	✓
	Navegador alternativo	✓	✗	✓	✓	✓	✓
	Desinstalar software	✓	✓	✓	✓	✓	✓
	Modo seguro	✓	✓	✓	✓	✓	✓
	Cambiar nombre de una aplicación bloqueada	✓	✓	✓	✓	✓	✓
	Modificación de ajustes de hora y fecha	✓	✓	✓	✓	✓	✓
	Cierre de la herramienta de control parental a través del administrador de tareas	✓	✓	✓	✓	✓	✓
	Llegar a un sitio web a través de sitios de traducción	✓	✓	✓	✗	✗	✗

Tabla 15: Comparación Herramientas Control Parental (I)

Área	Funcionalidad	OpenDNS	Procon Latte	Blocksi	Qustodio	K9 Web
Administración	Gestión de diferentes perfiles de usuario	✓	✗	✗	✓	✗
	Gestionar varios dispositivos	✓	✗	✗	✓	✗
	Registro de actividad	✓	✗	✗	✓	✓
	Monitorización de forma remota	✓	✗	✗	✓	✗
Personalizar el filtro de contenido	Personalizar categorías de filtrado	✓	✓	✓	✓	✓
	Gestión de lista blanca y negra (modificación o creación)	✓	✓	✓	✓	✓
	Lista blanca y negra por defecto	✓	✗	✓	✓	✗
	Filtrado por palabras clave	✗	✓	✓	✗	✗
Tiempo de uso y/o acceso	Gestionar el tiempo de uso y/o acceso al PC	✗	✗	✗	✓	✗
	Gestionar el tiempo de uso y/o acceso a Internet	✗	✗	✓	✓	✓

Notificaciones de bloqueo	Solicitar permiso para desbloquear	✗	✓	✗	✓	✓
	Redirección a sitio web seguro	✗	✗	✗	✓	✓
Restricciones de uso	Bloquea el acceso a sitios web	✓	✓	✓	✓	✓
	Registra la actividad online	✓	✗	✗	✓	✓
	Modo Safe Search	✓	✓	✓	✓	✓
	Bloquea el acceso a redes sociales	✓	✓	✓	✓	✓
	Monitoriza la actividad en redes sociales	✗	✗	✗	✓	✗
	Restringe el uso del correo electrónico	✗	✗	✗	✓	✗
Seguridad. Controla que el usuario evite el filtrado de contenido mediante:	Uso de dirección IP en lugar de URL	✓	✓	✓	✓	✓
	Navegador alternativo	✓	✗	✗	✓	✓
	Desinstalar software	✓	✓	✓	✓	✓
	Modo seguro	✓	✓	✓	✓	✗
	Cambiar nombre de una aplicación bloqueada	✓	✓	✓	✓	✓
	Modificación de ajustes de hora y fecha	✓	✓	✓	✓	✓
	Cierre de la herramienta de control parental a través del administrador de tareas	✓	✓	✓	✓	✓
	Llegar a un sitio web a través de sitios de traducción	✓	✓	✓	✓	✓

Tabla 16:Comparación Herramientas Control Parental (II)

Como se aprecia en las tablas, cada herramienta ofrece funcionalidades diferentes que permiten a los usuarios seleccionar el grado de control que desean ejercer. Es decisión del usuario final decantarse por la herramienta que más se ajuste a sus necesidades dependiendo del dispositivo y del sistema operativo en que se va a aplicar.

Windows 8

Usabilidad

Instalación. No precisa de instalación por venir integrada en el propio sistema operativo.

Configuración. El proceso de configuración es sencillo gracias a la interfaz que presenta la aplicación, que se encuentra dividida en secciones bien explicadas.

Uso. La información que muestra la aplicación es detallada mostrando mensajes a los usuarios. Los informes de actividad muestran toda la información sobre el uso que el menor ha hecho del dispositivo.

Funcionalidad

Filtrado web limitado ya que no permite personalizar qué categorías se desean bloquear y cuáles se desean permitir. Cuando se bloquea un sitio web no redirecciona a un sitio seguro. No se puede realizar un seguimiento de la actividad del menor en las redes sociales, únicamente se puede saber el tiempo que el menor ha permanecido en ellas.

Efectividad

Las pruebas realizadas han demostrado que es una herramienta eficaz contra las páginas de contenido para adultos bloqueando el acceso a ellas (si se ha establecido el nivel de filtrado).

Seguridad

La herramienta se resistió a los principales intentos de evitar el filtrado como acceder al sistema en modo seguro o intentar navegar en modo incógnito, por lo que los menores no se podrán deshacer de la herramienta y evitar el filtro de contenidos.

Windows 10

Usabilidad

Instalación. No precisa de instalación, la aplicación se gestiona de manera online.

Configuración. Cuenta con una interfaz web simple y fácil de utilizar debido a las explicaciones que ofrece de cada campo a configurar.

Uso. La información que muestra la aplicación es detallada mostrando mensajes a los usuarios. Además de los informes de actividad disponibles también en la versión de Windows 8, incluye un sistema de envío de informes semanales al correo electrónico con la actividad registrada.

Funcionalidad

No permite elegir el nivel de filtrado que se desea realizar como ocurría en Windows 8, ahora muestra una única opción que, si se activa, bloquea el acceso al contenido que la herramienta considera inapropiado. Al contrario que en Windows 8 que filtraba el contenido de cualquier navegador, únicamente se aplican las restricciones para el navegador Microsoft Edge

Efectividad

Las pruebas realizadas han demostrado que es una herramienta eficaz contra las páginas de contenido inapropiado.

Seguridad

Hay un único caso en que los menores pueden saltarse el filtrado web y es cuando éstos acceden desde otros navegadores que no sea el de Microsoft.

MAC OS X

Usabilidad

Instalación. La aplicación viene integrada en el sistema operativo.

Configuración. El proceso de configuración es comprensible y fácil de usar.

Uso. Cuando se activa el bloqueo web o de alguna aplicación, muestra información poco detallada y permite solicitar acceso al administrador. Permite retroceder a la página anterior

donde la navegación no se ha bloqueado. Registra el tiempo que el menor hace uso de cada aplicación.

Funcionalidad

Al contrario que en el control parental de Windows, permite seleccionar qué categorías se desean bloquear y cuáles no. No es posible bloquear el acceso a redes sociales. No fuerza al usuario a realizar una búsqueda segura. Permite restringir el uso del correo electrónico.

Efectividad

Funciona correctamente evitando el acceso a aplicaciones y sitios web restringidos.

Seguridad

No es posible evitar el filtrado de contenido.

TimePKR

Usabilidad

Instalación. A través de la terminal.

Configuración. Fácil de configurar, basta con seleccionar un usuario y asignarle un control del tiempo de uso y acceso al PC.

Uso. Muestra notificaciones cuando se termina el tiempo de uso permitido o cuando se accede fuera del horario.

Funcionalidad

Únicamente sirve para controlar el tiempo de acceso y uso del ordenador.

Efectividad

Restringe el horario correctamente.

Seguridad

No es posible evitar el control. Se necesita contraseña de administrador para abrir la aplicación.

Gnome Nanny

Usabilidad

Instalación. Puede darse el caso de que el archivo de instalación se encuentre en otro repositorio, por lo que antes habría que actualizar los repositorios. A través de la terminal.

Configuración. Proceso sencillo gracias a su interfaz intuitiva.

Uso. Cuando se bloquea un acceso web, muestra una imagen de bloqueo de la aplicación sin mostrar ningún tipo de mensaje de porqué se bloqueó.

Funcionalidad

Permite restringir el uso del correo electrónico y aplicaciones de mensajería, gestión del tiempo de uso del equipo y filtrado web. No registra la actividad del usuario.

Efectividad

Su único problema es al realizar una búsqueda en google que muestra las páginas inapropiadas, aunque después no permita el acceso, y se muestran imágenes con contenido inapropiado para los menores.

Seguridad

Al filtrar por palabras clave, si el menor entra mediante traducciones de las páginas se puede saltar el filtro y acceder a la web.

Dansguardian

Usabilidad

Instalación. La instalación de la herramienta se realiza a través de la terminal, puede estar ubicada en otro repositorio.

Configuración. Es complicado configurar la herramienta ya que no dispone de interfaz gráfica. La configuración se realiza a través de archivos de configuración que hay que editar. Requiere conocimientos sobre Linux.

Uso. El software cumple, en general, las expectativas de los usuarios. El mensaje de se puede personalizar.

Funcionalidad

Se limita a filtrar los contenidos en la navegación web. No gestiona tiempos de acceso a la web ni registra la actividad. No realiza una búsqueda segura.

Efectividad

Los filtros configurados cumplen correctamente su función.

Seguridad

Si el menor accede mediante traducciones de las páginas se puede saltar el filtro y acceder a la web.

OpenDNS

Usabilidad

Instalación. No es un proceso de instalación como tal, lo que hay que hacer es cambiar las direcciones DNS de nuestra red y añadir la IP en la cuenta creada. Siguiendo los pasos, es un proceso sencillo.

Configuración. Interfaz web sencilla y fácil de utilizar.

Uso. Permite personalizar el mensaje de alerta cuando se bloquea un sitio web, el mensaje que incluye por defecto no es muy detallado para los menores. Muestra una serie de estadísticas de actividad online.

Funcionalidad

La herramienta ha sido probada en Windows 10.

Permite seleccionar las categorías a bloquear/permitir. No restringe el uso del correo electrónico y aplicaciones de mensajería, pero sí que se puede bloquear el acceso a sitios web

específicos como pueden ser las redes sociales. Incluye un control de sitios P2P bloqueando sitios web donde el usuario puede descargar archivos.

Efectividad
Filtra correctamente las categorías seleccionadas.

Seguridad
El menor puede cambiar la configuración de las DNS y hacer inutilizable el filtro de control.

Procon Latte

Usabilidad
Instalación. Se instala a través de la herramienta de extensiones de Mozilla Firefox.

Configuración. Interfaz fácil de comprender.

Uso. Al saltar el boqueo, muestra un mensaje y ofrece diferentes opciones para solicitar permiso al administrador.

Funcionalidad
No incluye una búsqueda Safe Search. Filtro de palabras clave que son sustituidas por otra palabra que el administrador establezca y restringe el acceso. Redirección a un sitio web seguro. Únicamente filtra sitios web introducidos en la configuración de las listas y que contengan alguna de las palabras clave, no permite filtrar en base a categorías de contenido. No registra la actividad web

Efectividad
Los sitios web contenidos en la lista negra son bloqueados, así como los sitios que contengan alguna de las palabras.

Seguridad
Solamente funciona en el navegador Mozilla Firefox, si el menor accede con otro navegador evitará el control.

Blocksi

Usabilidad
Instalación. Se instala a través de la herramienta de complementos de Google Chrome.

Configuración. Interfaz sencilla, fácil de utilizar y bien organizada en secciones.

Uso. Al saltar el boqueo, muestra un mensaje con la URL del sitio Web y la categoría a la que pertenece. Menos detallado es la información cuando se bloquea contenido de YouTube.

Funcionalidad
Incluye una búsqueda Safe Search. Filtrado de contenido por categorías seleccionables. Bloqueo de contenido en YouTube. Redirección a un sitio web seguro. Gestión del tiempo de acceso y uso del navegador. No registra la actividad en la web.

Efectividad
Funciona correctamente para los criterios establecidos.

Seguridad
Tiene un problema de seguridad y es que no necesita de una contraseña para ser inhabilitado.

Qustodio

Usabilidad
Instalación. Es un proceso sencillo gracias a la información que proporciona en su sitio oficial. Ofrece un tutorial de ayuda al usuario.

Configuración. El proceso de configuración es fácil. Permite editar varias opciones que cumplen con las expectativas de los usuarios y la posibilidad de personalizar el filtrado. El diseño es atractivo.

Uso. La información es muy detallada y se muestran varias estadísticas de la actividad del usuario. Muestra información sobre el tiempo que el usuario ha pasado en los sitios web. El mensaje de alerta está diseñado atractivamente y ofrece la redirección a sitios seguros.

Funcionalidad
El software ofrece varias funcionalidades. Los usuarios pueden crear varios perfiles y listas negras / blancas. Es posible personalizar el filtrado. Por otra parte, es posible bloquear y monitorear la web, correo electrónico, las redes sociales y aplicaciones streaming. Monitorización remota. El mensaje de alerta muestra una redirección a un recurso seguro.

Efectividad
Funciona correctamente sin anomalías.

Seguridad
Al estar oculta, el usuario no tiene acceso a la configuración. No es posible evitar el filtrado de ninguna manera.

K9 Web Protection

Usabilidad
Instalación. El proceso de instalación es fácil y comprensible si se siguen correctamente los pasos indicados.

Configuración. La herramienta no proporciona opciones para gestionar varios perfiles de usuario. El diseño podría mejorarse para no parecer antiguo. Es sencillo de configurar ya que viene bien estructurado en la interfaz.

Uso. La herramienta ofrece algunas opciones a realizar, cuando un sitio web ha sido bloqueado, pero estas opciones están dirigidas principalmente a los padres y no a los niños. Ofrece estadísticas de la actividad realizada en la web.

Funcionalidad
Ofrece la posibilidad de elegir entre diferentes niveles de restricción. Existen numerosas categorías de contenido para filtrar las páginas web en consecuencia. Filtrado por palabras clave. Permite establecer el modo búsqueda segura. No bloquea el acceso a aplicaciones P2P. Permite bloquear el acceso a redes sociales, pero no registra la actividad realizada. También es posible establecer restricciones de tiempo para el acceso a Internet.

Efectividad

No se han registrado errores en las pruebas realizadas.

Seguridad

El menor puede evitar el control parental accediendo al sistema en modo seguro.

5.1. Valoración final

En general, para los sistemas operativos Windows, MAC OS, IOS y Android la mejor opción para controlar la actividad de los menores en la red es la herramienta **Qustodio** por la gran funcionalidad que ofrece, cubre todas las necesidades de los usuarios, y por su seguridad, garantiza que el menor no va a eludir el filtrado.
El resto de herramientas comentadas sirven para salir de un apuro, pero el menor, tarde o temprano, terminará averiguando la manera de eludir el control parental, bien porque la funcionalidad que ofrecen es escasa, o bien porque no cumplen todas las pautas de seguridad que un sistema de control parental debe tener para ser 100% seguro.

Si el usuario decide instalar otra herramienta que no sea Qustodio, porque le basta con lo que le ofrece dicha herramienta, no es recomendable hacer uso de las extensiones para navegadores porque hay otras opciones ya comentadas que controlan las mismas áreas y además le añaden otras funcionalidades como puede ser la gestión de tiempos o la monitorización de la actividad. La mejor alternativa es hacer uso de la propia herramienta integrada en el sistema operativo, aunque no dispongan de la totalidad de funcionalidades de Qustodio pero se trata herramientas completamente seguras.

Los usuarios que hacen uso del ordenador bajo el sistema operativo Ubuntu, no disponen de una herramienta que les satisfaga todas sus necesidades. En este caso, lo mejor es combinar las herramientas, por ejemplo, Gnome Nanny y DansGuardian para obtener las mejores funcionalidades de cada herramienta (control de tiempos, filtrado por palabras clave, restricciones en el correo y aplicaciones de mensajería instantánea, …) y poder controlar a los menores con total seguridad.

6. Conclusiones

- Una vez realizada la investigación y las pruebas correspondientes de las herramientas de control parental disponibles para controlar la actividad de los menores en Internet, he comprobado que son herramientas muy útiles para que los padres no se preocupen de lo que hacen sus hijos en el ordenador cuando ellos no están delante. Estas herramientas son útiles si se configuran en los dispositivos que usan los menores para conectarse a Internet, resultando la siguiente jerarquía: los padres son administradores y los hijos son usuarios estándar (sin privilegios a modificar o violar alguna política de seguridad de restricción).

- Antes de realizar el proyecto, desconocía la existencia de este tipo de herramientas y es ahora cuando valoro la actuación de los desarrolladores de este tipo de software, pues, como se ha explicado al principio de la memoria, existen multitud de peligros cuando se navega por Internet. No lleva mucho tiempo instalar y configurar las herramientas, y evitan la aparición de material pornográfico, software malicioso o problemas relacionados con el acoso cibernético.

- No existe una herramienta 100% eficaz y 100% segura que garantice que los menores estén exentos de este tipo de problemas, pero es conveniente la configuración de alguna de ellas para reducir los niveles de riesgo.

- A mi juicio, no podemos confiar únicamente en la activación de las diversas herramientas u opciones enumeradas, sin detenernos y reservar algunos momentos para intentar explicarles a los menores el funcionamiento del entorno web, en su doble vertiente: por un lado, la vertiente que nos trae beneficios y aporta conocimiento casi instantáneo permitiendo una comunicación e intercambio de información sin precedente, y por otro lado, la vertiente “maléfica”, que puede ir en contra de nuestra integridad personal o profesional, o causar daños tanto a nivel virtual, como en nuestra vida real.

- Muchos de los padres no conocen la existencia de este tipo de herramientas, o simplemente no tienen conocimiento de lo que sus hijos realizan en la red, mientras ellos no están en casa.

- El uso de herramientas de control parental no está destinado únicamente al control de menores, también puede utilizarse en empresas que deseen que sus trabajadores accedan exclusivamente a determinados sitios relacionados con la actividad empresarial o para evitar que personas con escasos conocimientos informáticos instalen aplicaciones o accedan a sitios con software malicioso.

7. Bibliografía y referencias

[1] Monsoriu Flor, M. *Cómo Controlar lo que hacen tus hijos con el ordenador: Técnicas de hacker para padres*. Madrid: Creaciones Copyright, 2007.

[2] Mifsud, E. y Márquez, P. *El buen uso de Internet.* Valencia: Generalitat Valenciana, 2007.

[3] Montero Ayala, R. *Cómo proteger el ordenador de intrusos, virus, espías y spam con programas gratuitos y fáciles de utilizar: Protección ante Internet.* Madrid: Creaciones Copyright, 2007.

[4] García Jiménez, A. Beltrán Orenes, P. Pérez Pais, M. *"La investigación sobre los usos y riesgos de Internet en menores y jóvenes. Estado de la cuestión en España y proyección iberoamericana"*, CONFIBERCOM, 2007.

[5] Catalina García, B. López de Ayala López, MC. García Jiménez, A. "Los riesgos de los adolescentes en Internet: los menores como actores y víctimas de los peligros de Internet". Revista Latina de Comunicación Social, 69, pp. 462 a 485, 2014.

[6] Garmendia, M. [et. al.]. "*Riesgos y seguridad en Internet: los menores españoles en el contexto europeo". 2011*.

[7] García Vitoria, E. "*Redes sociales y control parental*", Dirección General de la Policía y la Guardia Civil, 2011.

[8] INTECO, "Los controles parentales: cómo vigilar a qué contenidos de Internet acceden nuestros hijos". [online]. España: Instituto Nacional de Tecnologías de la Comunicación, 2009. Disponible en: https://www.incibe.es/

[9] INTECO, "Guía práctica sobre cómo activar y configurar el control parental de los sistemas operativos". [online]. España: Instituto Nacional de Tecnologías de la Comunicación, 2009. Disponible en: https://www.incibe.es/

[10] INTECO, "Guía sobre ciberbullying y grooming". [online]. España: Instituto Nacional de Tecnologías de la Comunicación, 2009. Disponible en: https://www.incibe.es/

[11] INTECO, "Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles". [online]. España: Instituto Nacional de Tecnologías de la Comunicación, 2009. Disponible en: https://www.incibe.es/

[12] Rodríguez Álvarez, C. "Control parental en el uso de Internet y del ordenador". [online]. España: Aventuratec, 2011. Disponible en: http://aventuratec.blogspot.com/

[13] Peter, M. Kent, K. Nusbaum, J. "Guide to Malware Incident Prevention and Handling". United States: National Institute of Standards and Technology, 2005.

[14] Control Parental.
http://geekland.eu/conceptos-herramientas-control-parental/.
https://www.segu-kids.org/padres/control-parental.html.

[16] SafeSurf.
http://www.safesurf.com/.

[17] Herramientas control parental.
http://www.sipbench.eu/

[18] Control parental Windows 8.
http://www.xatakawindows.com/bienvenidoawindows8/control-parental-en-windows-8-como-activarlo-y-configurarlo.

[19] Control parental Windows 10.
https://support.microsoft.com/es-es/help/12413/microsoft-account-set-up-family-features.

[20] Control parental MAC OS X
https://support.apple.com/kb/PH14414?locale=es_ES&viewlocale=es_ES

[21] Gnome Nanny.
http://projects.gnome.org/nanny/.

[22] Dansguardian.
http://dansguardian.org/.

[23] TimePKR.
http://www.webupd8.org/2014/09/install-timekpr-parental-control-app-in.html.

[24] OpenDns.
http://www.opendns.com/.

[25] Blocksi.
http://www.blocksi.net/.

[26] Procon Latte.
http://www3.gobiernodecanarias.org/medusa/contenidosdigitales/FormacionTIC/cdtic2014/01ns/322_procon_latte_para_firefox.html.

[27] Qustodio.
https://www.qustodio.com/es/?x.

[28] K9 Web Protection.
http://www1.k9webprotection.com/.

8. Índice de Ilustraciones

9. Índice de Tablas