



Instituto Nacional
de Tecnologías
de la Comunicación

Guías Legales

Cómo activar y configurar el control parental de los sistemas operativos

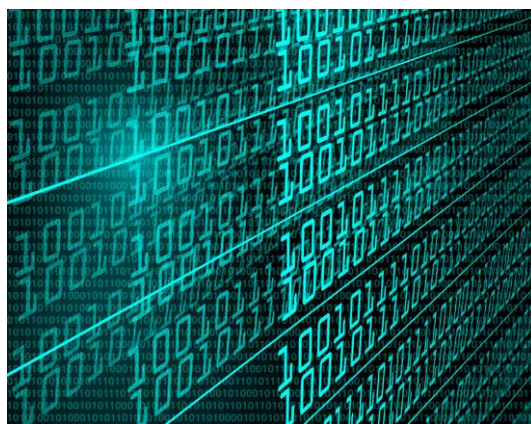


OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN
Área Jurídica de la Seguridad y las TIC

La presente guía¹ tiene por objeto ofrecer a los usuarios² información útil para conocer las pautas a seguir en la instalación y configuración de los programas de control parental que los sistemas operativos incluyen dentro de sus opciones de privacidad para mejorar la seguridad en la navegación de los menores por parte de padres, tutores y administradores de sistemas.

Aunque Internet se posiciona como una fuente amplia de información y búsqueda de recursos, en parte por la facilidad que brinda a los usuarios para localizar contenidos, crear y difundir contenidos propios y posibilitar una comunicación ágil e instantánea dentro de la Red; sin embargo, tanto los equipos como el desarrollo del software y las herramientas que ofrece Internet, no siempre son usadas de la mejor manera, pudiendo identificarse contenidos que no son beneficiosos para un correcto desarrollo de los jóvenes y menores de edad.

Al igual que en el mundo físico, padres y tutores deben conocer y hacer frente a posibles riesgos ante los que los menores se pueden encontrar en su navegación por Internet. Los principales son:



- Contenidos que pueden impactar en el desarrollo evolutivo de los menores de edad. Entre ellos: gestos obscenos, sexo explícito, erotismo, violencia, crueldad, odio, prácticas ilegales, drogadicción, etc.
- Contacto con usuarios malintencionados por medio de herramientas de mensajería instantánea, chats, foros o correo electrónico.
- Descarga de archivos (documentos, imágenes, música y videos) que se encuentren contaminados por código malicioso y que puedan hacer que nuestro ordenador se vea vulnerado permitiendo el acceso a personas que quieran obtener datos personales o privados e incluso que puedan llegar a destruir nuestros archivos personales o archivos del sistema inutilizando, de esta forma, nuestro equipo.
- El uso por parte de los menores de los datos de cuentas bancarias para realizar compras online, contratar servicios de cualquier tipo, hacer apuestas, etc.

¹ Consciente de la importancia de una navegación segura por parte de los menores en Internet, el Observatorio de la Seguridad de INTECO, publicaba en enero del año 2008 un artículo que aborda dicha materia desde el punto de vista de los contenidos y la descripción de diversas alternativas de control parental: “Los controles parentales: cómo vigilar a qué contenidos de Internet acceden nuestros hijos”. Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/Articulo_control_parental_11

² Usuarios de sistemas operativos: Windows y Mac OS X.

Para evitar este tipo de situaciones y generar seguridad y confianza entre los padres y tutores respecto de la navegación por parte de los menores a su cargo, los sistemas operativos más populares y los navegadores Web han incluido entre sus opciones de seguridad, ciertos controles parentales que restringen el acceso de los menores a contenidos que los padres o tutores consideren inadecuados para la seguridad y sensibilidad del menor.

Además las empresas de desarrollo de software y seguridad informática han creado programas específicos para detectar contenidos no aptos para los menores que previenen el acceso a los mismos y se suelen incluir dentro de sus packs de productos de seguridad, tales como antivirus o firewalls, entre otros.

¿Qué es un sistema de control parental?

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”***.

Esta aplicación toma su nombre de la finalidad de supervisión y control que los padres o tutores procuran realizar de la información a la que los menores pueden tener acceso al utilizar el ordenador.

También es habitual que la instalación de estas aplicaciones se realice en los equipos informáticos de: colegios, bibliotecas públicas y cualquier otro lugar en el que los menores puedan llevar a cabo un uso frecuente de ordenadores conectados a Internet.

Existen dos **tipos de control parental**:

- Las soluciones que vienen establecidas por defecto en los sistemas operativos³.
- Las soluciones de control parental que se ofrecen y/o comercializan por organizaciones y empresas dedicadas a la creación de éste tipo de software⁴.

³ Más información en http://www.reflejos.com/onlinepdf/20070624/20070624_Ref_p26.pdf

La diferencia entre una y otra alternativa, se encuentra en las opciones de seguridad que se establecen para cada solución. Las primeras establecen niveles de seguridad más básicos, entre las que cabe señalar el registro de las actividades de los menores para evitar que se comuniquen con personas extrañas, la generación de un registro de páginas web visitadas, las aplicaciones informáticas empleadas y la identificación de las personas con las que se ha mantenido algún tipo de comunicación. Las segundas presentan niveles de seguridad más avanzados y especializados dependiendo de cada fabricante, si bien comparten ciertos rasgos que permiten hacer una enumeración de las mismas.

Así, **las herramientas de control parental establecen**, dependiendo de las características de cada una, **las siguientes posibilidades**⁵, muchas de estas opciones se encuentran incluidas en las herramientas que crean algunas empresas de seguridad informática:

- **Control de tiempo**: brinda la opción de establecer el tiempo que los menores pueden estar conectados a Internet. La limitación se establecerá por horas o número de días a la semana. Esta posibilidad ayuda a evitar que el menor dedique un número de horas excesivo delante del ordenador y permite fijar el tiempo de conexión de los niños cuando se encuentran solos en casa.
- **Bloqueo por palabras clave**: permite bloquear páginas web que contengan palabras que presumiblemente se asocien a un contenido no apto (sexo, apuestas, drogas, casino, etc.). Sin embargo, con ésta técnica se pueden producir los denominados “falsos positivos”, es decir, cabe la posibilidad de bloquear contenidos que pueden no ser nocivos 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.
- **Registros**: permite revisar y comprobar los hábitos de navegación de los menores.
- **Bloqueo de programas**: posibilita el bloqueo de determinadas herramientas como por ejemplo: los servicios de mensajería instantánea, correo electrónico, descarga de programas, etc.
- **Listas negras de páginas web**: contienen las direcciones de los sitios web a las que se restringe el acceso. Sin embargo, esta posibilidad se ve limitada por la rapidez con la que diariamente se crean nuevos contenidos y páginas en la Red, con el consiguiente esfuerzo que conlleva la actualización de dichas listas.

⁴ En http://www.inteco.es/Seguridad/INTECOCERT/Proteccion/tiles_Gratuitos_2 puede ampliar información y enlazar a soluciones de control parental dentro de la categoría de herramientas de bloqueo.

⁵ Para ampliar información técnica visite: <http://alerta-antivirus.inteco.es/>

- Listas blancas de páginas web: se trata de listas de páginas a las que se permite el acceso por considerarlas apropiadas, únicamente se permite acceder a las páginas que se encuentren en la misma, por lo que suponen una restricción mayor ya que todo lo que no esté permitido se encuentra bloqueado.
- 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 empresas⁶.

Entre las **principales ventajas** que ofrecen las soluciones de control parental cabe señalar:

- El seguimiento de la actividad que los menores llevan a cabo en Internet, como por ejemplo: la participación en redes sociales o sitios web colaborativos, la utilización de sistemas de mensajería instantánea o el uso de aquellas otras herramientas o aplicaciones software que permiten establecer una relación con terceros usuarios que siendo usuarios no conocidos en el entorno del menor, pueden generar un riesgo aparente para este colectivo.
- Establecer seguimientos y registros del tiempo empleado en la navegación por Internet así como de las páginas web que son visitadas y a cuales de ellas se dedica mayor tiempo.
- Algunos sistemas de control parental cuentan además, con escritorios virtuales que permiten a los padres/tutores legales o administradores de los equipos, el acceso de forma remota al ordenador que está siendo utilizado por el menor, ofreciendo la posibilidad de realizar una vigilancia de la actividad que se esta llevando a cabo, sin necesidad de presencia física por parte de aquellos⁷.
- No permiten que los menores cambien las opciones de seguridad establecidas, sin consentimiento del administrador, padre o tutor del menor.

⁶ La Plataforma para la Selección de Contenidos de Internet (PICS), desarrollada por el World Wide Web Consortium (W3C), proporciona un medio eficiente para controlar el acceso a los contenidos. El sistema de etiquetado fue diseñado originalmente para ayudar a los padres y maestros en el control de acceso de los menores a la Red.

⁷ Este tipo de opciones solo están disponibles en algunas herramientas. La herramienta Windows Live Parental Control incluye esta funcionalidad aunque actualmente se encuentra en modo de prueba (beta) y sólo disponible en inglés. <http://www.microsoft.com/en/us/default.aspx>

Configuración de un sistema de control parental

A continuación se detallan, de modo práctico y visual, los pasos a seguir para llevar a cabo la configuración del sistema de control parental en un entorno Windows XP y en un entorno MAC OS X.

Como paso previo se señala que los parámetros que se indican a continuación deben realizarse desde la cuenta que en el equipo disponga de privilegios o permisos de administrador. En esta línea conviene recordar que las cuentas de los menores deberán ser cuentas limitadas o cuentas de invitado.

Entorno WINDOWS

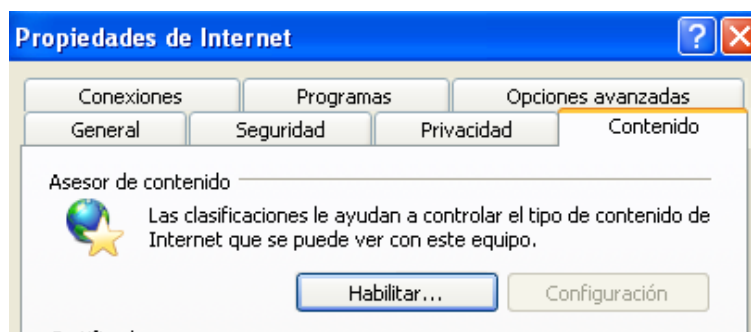
Paso 1: Propiedades de Internet

Incluir el asesor de contenidos de Windows

En el menú Herramientas de Internet Explorer o a través del Panel de Control, se hará clic en Opciones de Internet, aunque la ventana que se mostrará al usuario se denominará Propiedades de Internet en la barra de dirección.

- Haga clic en la ficha Contenido y en el botón Habilitar.

Paso 1: Propiedades de Internet

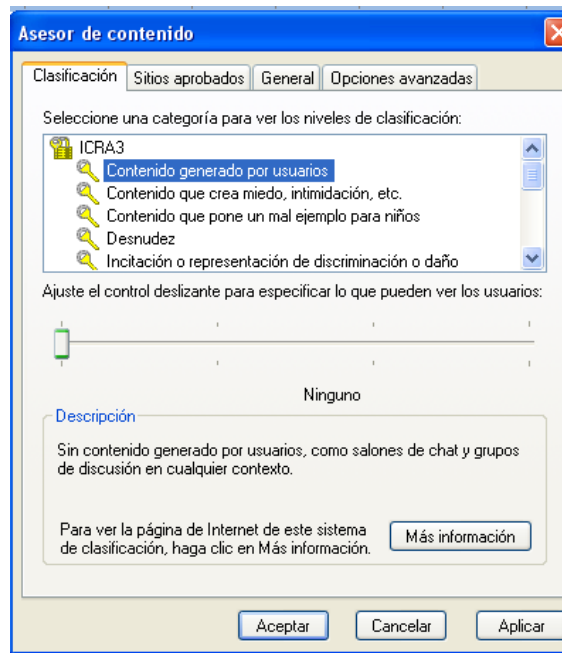


Captura de pantalla entorno Windows XP

Paso 2: asesor de Contenido (I): Clasificación

En este punto se muestra un nuevo cuadro de diálogo que establece, mediante un deslizable horizontal, distintas categorías de los diferentes niveles de clasificación del contenido y diferentes tipos de acceso:

Paso 2: Asesor de Contenido



Captura de pantalla entorno Windows XP.

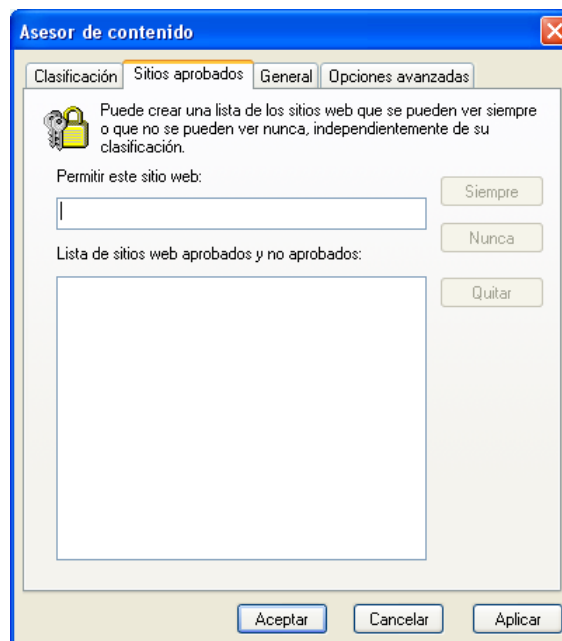
- Contenidos:
 1. Generados por los usuarios.
 2. Miedo e intimidación.
 3. Mal ejemplo para los niños.
 4. Desnudez.
 5. Incitación o presentación de discriminación o daño.
 6. Lenguaje soez.
 7. Material con contenido sexual.
 8. Representación de apuestas, alcohol, armas, drogas o tabaco.
 9. Violencia.

- Tipos de acceso:
 1. Ninguno: los contenidos bloqueados no aparecen en ningún contexto.
 2. Limitado: no aparecerán los contenidos en ningún contexto. Blasfemias o lenguaje inadecuado sólo en un contexto artístico, médico, educativo, deportivo o de noticias.
 3. Algo: los contenidos sólo serán mostrados en un contexto artístico, médico, educativo, deportivo o de noticias. Blasfemias o lenguaje inadecuado en cualquier contexto.
 4. Sin restricciones: los términos o contenidos, o lenguaje inadecuado en cualquier contexto.

Paso 3: Configuración del Asesor de Contenido (II). **Sitios aprobados**

Dentro del mismo cuadro de diálogo del asesor de contenido se deberá seleccionar la pestaña sitios aprobados, para crear una selección de páginas web de forma manual.

Paso 3: Selección de páginas web prohibidas (Lista Negra)



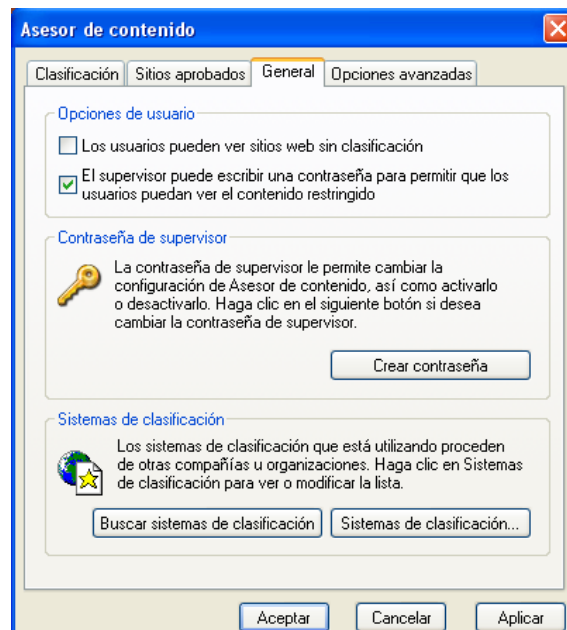
Captura de pantalla entorno Windows XP.

Se irán incluyendo las direcciones URL de las páginas que se desee bloquear por considerarlas contraproducentes o no oportunas para los menores que utilicen el equipo. Finalmente se mostrará el listado de páginas que han sido prohibidas. Este listado podrá actualizarse según se estime conveniente.

Paso 4: Configuración del Asesor de Contenido (III). **General**

El asesor de contenido incluye una pestaña general donde se establecen las cuestiones básicas de utilización de esta herramienta, contraseñas e importaciones de sistemas.

Paso 4: Pestaña General



Captura de pantalla entorno Windows XP.

- A la hora de establecer la contraseña en un sistema de control parental conviene seguir las reglas básicas de creación segura de contraseñas⁸. Entre ellas:
 - Longitud recomendable 8 dígitos.
 - Alfanuméricas.
 - reutilización indistinta de letras mayúsculas y minúsculas.
 - Renovación de la contraseña por periodos de tiempo no superiores a 60 días.
- También otra forma de configuración del control parental es la importación de un sistema de clasificación. Normalmente son los sistemas tipos realizados por el

⁸ Más información en el artículo "Recomendaciones para la creación y uso de contraseñas seguras" del Observatorio de la Seguridad de INTECO. Disponible en: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/recomendaciones_creacion_uso_contraseñas

Family Online Safety Institute⁹, que establecen que tipo de páginas o contenidos han de ser limitados. Entre las principales ventajas de estos sistemas cabe señalar su constante actualización.

Entorno Mac OS X

La solución de control parental que incorpora este sistema operativo aunque es más amplia que la expuesta anteriormente para el entorno Windows, ya que incluye la configuración de las limitaciones de las cuentas de usuario no administrador, sin embargo, pierde algunas funcionalidades.

Paso 1: Menú Inicio/Menú preferencias del sistema dentro del menú inicio. **Menú Inicio**

Paso 1: Menú Inicio



Captura de pantalla entorno Mac OS X.

Paso 2: Preferencias del Sistema

Dentro del cuadro de diálogo de preferencias del sistema se debe crear una cuenta de usuario para el menor que, en ningún caso, dispondrá de privilegios de administrador, ya que en caso contrario, no se podrá instalar la solución de control parental.

Paso 2: Preferencias del Sistema



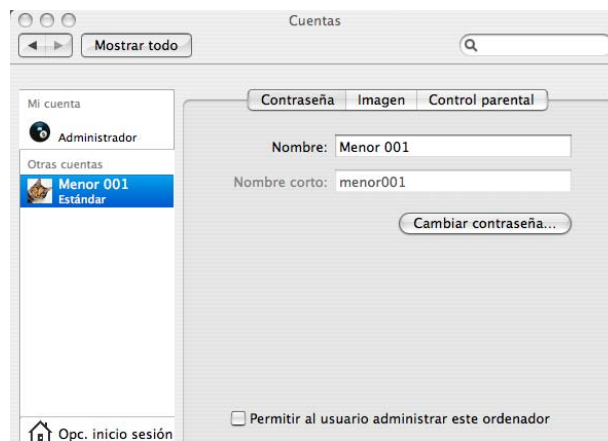
Captura de pantalla entorno Mac OS X.

⁹ Más información en el sitio web Family Online Safety Institute: <http://www.icra.org/support/contentadvisor/setupv03/>

Paso 3: Creación de Cuentas de Usuario

Se procederá a seleccionar la cuenta de usuario del menor. No se debe marcar la opción denominada “Permitir al usuario administrar este ordenador” ya que se le otorgarían privilegios de administrador que no permitirían utilizar un programa de control parental.

Paso 3: Creación de Cuentas de Usuario



Captura de pantalla entorno Mac OS X.

Paso 4: Control Parental

Creada la cuenta se selecciona la pestaña denominada control parental para poder realizar las limitaciones que se consideren necesarias, seleccionando una a una las cinco categorías que muestra la imagen para su posterior configuración.

Paso 4: Control Parental

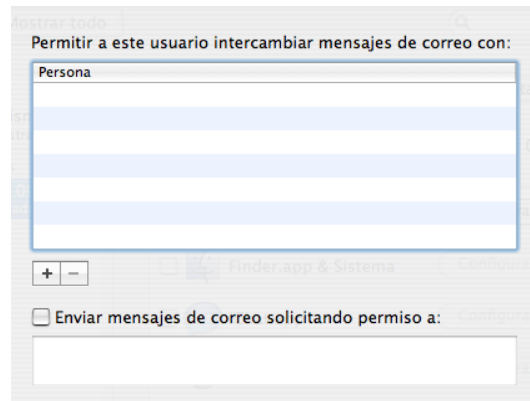


Captura de pantalla entorno Mac OS X.

Selección de e-mails

La aplicación de correo electrónico establece las cuentas de correo con las que se permite el intercambio de mensajes, así como la posibilidad de solicitar autorización al administrador del equipo para poder enviarlos a terceros no autorizados.

Selección de e-mails



Captura de pantalla entorno Mac OS X.

Finder

Esta aplicación limita el uso de los programas informáticos y acciones que el menor puede utilizar. También en esta categoría se muestran las opciones para los servicios de mensajería instantánea.

Finder

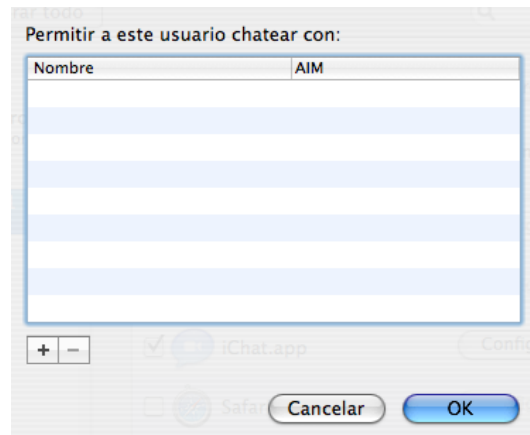


Captura de pantalla entorno Mac OS X.

iChat

Es una herramienta de mensajería instantánea incluida dentro del propio entorno Mac OS X. Con ella se podrán limitar los usuarios con los que puede interactuar.

iChat



Captura de pantalla entorno Mac OS X.

Safari

Después de incluirlo como limitado hay que cambiar de usuario y abrir la cuenta del menor. Se iniciará una sesión en el navegador Safari para limitar el tipo de páginas a que se quiere Acceder.

- En primer lugar, se inicia desde la cuenta de usuario del menor una sesión desde el *navegador Safari*.

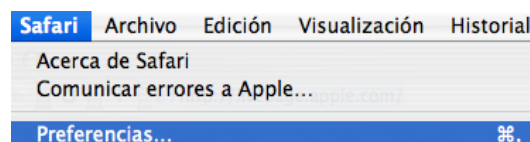
Safari



Captura de pantalla entorno Mac OS X.

- *Menú Safari:* Del menú del navegador Safari se despliega la pestaña preferencias.

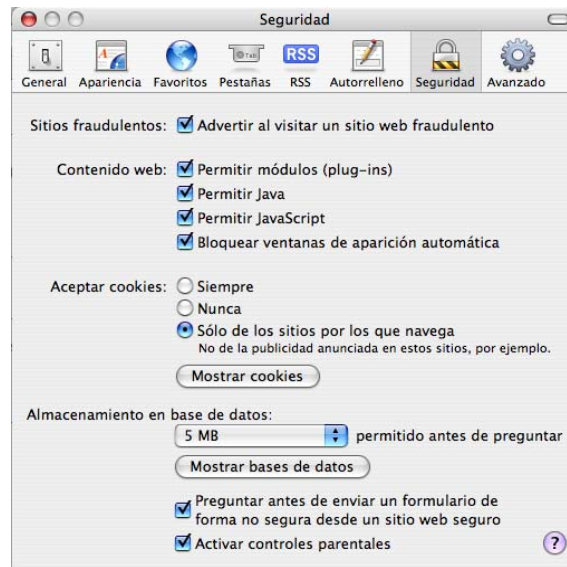
Menú Safari



Captura de pantalla entorno Mac OS X.

- *Preferencias de Seguridad:* en esta ventana se establece la utilización del control parental.

Preferencias de Seguridad



Captura de pantalla entorno Mac OS X.

Dictionary

En el cuadro de diálogo de esta categoría se limita el acceso a contenidos que contengan las palabras que se desean restringir.

Dictionary



Captura de pantalla entorno Mac OS X

Recomendaciones

Los programas de control parental se constituyen en una alternativa válida desde el punto de vista de la seguridad de los menores en su navegación a través de Internet, al tiempo que proporcionan confianza a padres y tutores.

Éstos deberán analizar los niveles de seguridad que se desean implementar tanto en los equipos como respecto de las personas que van a tener acceso a los mismos. Complemento de esta medida, cabe señalar las siguientes recomendaciones:

- Informar a los menores sobre la posible existencia de riesgos y contenidos no adecuados en la Red.
- Acompañar al menor durante la navegación, cuando sea posible, sin invadir su intimidad, de forma que perciba la existencia de un apoyo continuado por parte de padres y tutores, de forma que en el caso de que durante la navegación identifique una conducta que incómoda o sospechosa pueda informar de ello con confianza.
- Informar al menor de las posibles consecuencias que puede conllevar el hecho de facilitar información personal (nombre, dirección, teléfono, contraseñas, fotografías, etc.) en plataformas o servicios no confiables.
- Establecer tiempos de conexión del menor a Internet y a los servicios de la Sociedad de la Información para propiciar el complemento con otras actividades.
- Utilizar herramientas de control parental que le ayudan en el filtrado de los contenidos accesibles por los menores.
- Crear una cuenta de usuario limitado para el acceso del menor al sistema.

Enlaces de interés

Descarga de útiles:

- INTECO:

http://www.inteco.es/Seguridad/INTECOCERT/Proteccion/tiles_Graticos_2

- CyberPatrol

<http://www.cyberpatrol.com/>

- Barra de herramientas para el explorador de Internet:

<http://www.parentalcontrolbar.org/>

- Safe Eyes

<http://www.internetsafety.com/>

- Apple Leopard Parental Controls

<http://www.apple.com/>

- Windows Parental Controls

<http://www.microsoft.com/spain/protect/products/family/onecarefamilysafety.msp>

- IMSafer (control de conversaciones)

<http://www.imsafer.com/>

Asociaciones:

- Ciber-centro amigo de la Infancia:

<http://www.cibercentroamigo.com/>

- Ciberfamilias:

<http://www.ciberfamilias.com>

- Internetsegur@:

<http://www.igua.net>

- Protégeles:

<http://www.protegeles.com>

- Asociación de Madres y Padres Internautas:

<http://www.aempi.com/>

- Chavales:

<http://chaval.red.es>