ministerio de educación

Orientaciones para una navegación segura en Internet

Guía para usuarios

NTICs bolivia

Estado Plurinacional de Bolivia
Ministerio de Educación
Moromboerendañesroa Arakuarupi
Yachay Kamachiq
Yaticha Kamani

Orientaciones para una navegación segura en Internet
Guía para usuarios

Elaboración de contenidos:
Roberto Sánchez Saravia

Edición y corrección de estilo:
Claudia Dorado Sánchez

Diagramación:
Lorgia Sucso Guarachi

Diseño de portada:
Richard Cornejo Nolasco

Ilustaciones:
Pedro Condori Miranda

Supervisión:
Ministerio de Educación de Bolivia
Programa Nacional de Nuevas Tecnologías de Información y Comunicación

Germán Labraña Grundy, Coordinador del Programa

Ernesto Marconi Ripa
Henry Pers López
Virginia Ruiz Vila

Unidad de Comunicación:
Igor Centellas Rojas

Agencia Española de Cooperación Internacional para el Desarrollo, Bolivia (AECID-Bolivia)
Mariana Villarreal Careaga
Felipe Paucara Condori (consultor)

Este material fue desarrollado con el apoyo de:
Agencia Española de Cooperación Internacional para el Desarrollo, Bolivia (AECID-Bolivia)

www.educabolivia.bo Bolivia, 2009

Introducción

La Guía ***"Orientaciones para una navegación segura en Internet"*** es un material de apoyo que forma parte del curso de Ofimática Básica que oferta el Ministerio de educación dentro de una política de capacitación que busca desarrollar habilidades y destrezas en el manejo de las Nuevas Tecnologías de Información y Comunicación (NTICs) a docentes, estudiantes y miembros de la comunidad.

Esta guía ha sido elaborada para que los padres y madres de familia, así como los docentes y alumnos de las escuelas tengan pautas para evitar peligros que afecten negativamente a los niños, niñas, adolescentes y jóvenes que accederán a Internet.

La Internet es una "Red de Redes" que interconecta computadoras que comparten y difunden información y conocimiento a nivel local y mundial. Por la Red Internet permanentemente circulan cantidades increíbles de información. Esto ha dado lugar a llamar a Internet la *Autopista de la Información*. Los millones de usuarios o "Internautas" que están buscando, usando y compartiendo información son los que "navegan" por Internet en todo el Mundo, muchos de ellos son los niños, niñas, adolescentes y jóvenes que pueden no tener el suficiente criterio formado para identificar qué puede o no hacerles daño a su salud mental o física.

La información y el conocimiento que se comparte en la Red afecta la forma en que los seres humanos se comunican y también tiene repercusiones en la estructura del pensamiento para el aprendizaje, en el lenguaje, en cómo se percibe e interpreta la realidad y en la construcción cultural de las comunidades.

Internet está ocasionando un cambio en la sociedad boliviana y con los Telecentros Educativos Comunitarios en las comunidades originarias de las áreas más excluidas de nuestro país. Esto tiene una relevancia equivalente a la revolución industrial y por lo tanto supone un desafío para la educación en tanto la actualización y oportunidad de los aprendizajes deben acompañar este vertiginoso proceso.

Orientaciones para una navegación segura en Internet

Dibujo: Pedro Condori

Orientaciones para una navegación segura en Internet

Dibujo: Pedro Condori

Índice

Presentación

En el marco del Plan Nacional de Desarrollo (PND, 2006-2010) y del proyecto de Ley Avelino Siñani y Elizardo Pérez, se establece la incorporación de las Nuevas Tecnologías de Información y Comunicación al Sistema Educativo Plurinacional como política de Estado, generando espacios de igualdad y de oportunidad que posibiliten a estudiantes, docentes y miembros de la comunidad mejorar los procesos educativos.

Es así que, en la línea trazada por el Excelentísimo Presidente Constitucional Evo Morales Ayma, el Ministerio de Educación, a través del ***Programa Nacional de Nuevas Tecnologías de Información y Comunicación NTIC***, ha desarrollado condiciones para posibilitar el uso y acceso a nuevas tecnologías a través de la implementación de Telecentros Educativos Comunitarios en comunidades educativas de áreas rurales y periurbanas con mayores niveles de exclusión y marginalidad.

Para lograr que las TIC se conviertan en un factor instrumental de desarrollo socio productivo y comunitario, el Programa NTIC elaboró una estrategia de capacitación y formación que permitirá, prioritariamente a docentes y a través de ellos a los estudiantes, acceder, producir, usar y difundir información y conocimientos propios en los espacios del Telecentro.

La guía de ***Orientaciones para una navegación segura en Internet*** que el Ministerio de Educación presenta es parte del juego de materiales que apoyan el Curso de capacitación en Ofimática Básica y gestión del Telecentro Educativo Comunitario dirigido a docentes, estudiantes y miembros de la comunidad, con una estructura organizada en unidades temáticas, las mismas que incluyen objetivos, actividades prácticas, evaluaciones y contenidos.

Esta capacitación permitirá desarrollar habilidades y destrezas en el uso de las herramientas para procesos educativos, aumentar la motivación e inclinación hacia el autoaprendizaje, posibilitar el acceso a bases de datos e información, desarrollar capacidades investigativas, posibilitar la sistematización del conocimiento local y aplicar nuevos métodos para el trabajo cotidiano de aula.

Les invitamos a ser parte del desafío de introducir las Nuevas Tecnologías de Información y Comunicación como instrumentos para el desarrollo del conocimiento y las capacidades de los protagonistas de la revolución educativa que estamos viviendo.

Por una revolución educativa y cultural

Lic. Roberto Aguilar Gómez
Ministro de Educación

Internet para niños, niñas y adolescentes

Dibujo: Pedro Condori

Internet para niños, niñas y adolescentes

Dibujo: Pedro Condori

Internet para niños, niñas y adolescentes

Internet es un medio de comunicación masivo. En Bolivia, de manera progresiva, está presente en las unidades educativas y en lugares públicos como los telecentros y los cafés Internet, donde la población, desde muy temprana edad, accede a ese servicio para estar comunicada y para relacionarse con otras personas, intercambiar información, divertirse y hasta producir contenidos propios utilizando cámaras digitales y creando sitios *Web* y *Blogs*, entre otros.

El desafío para los docentes y los progenitores es orientar y enseñar a los niños, a las niñas y a los adolescentes a aprovechar al máximo las ventajas que ofrece la red Internet como medio de información y de comunicación, con la finalidad de que aprendan a seleccionar páginas web confiables y a distinguir los contenidos inapropiados. En esa dirección, es importante alertarlos sobre las situaciones de riesgo, como el acoso por Internet, que podrían traer consecuencias serias en sus vidas.

Para la prevención de tales riesgos, con la participación de los docentes, de los padres y las madres de familia, y de las autoridades comunales, se deben establecer mecanismos que permitan reconocer las diversas formas de comunicación que ofrecen las TICs y las ventajas de comprender el uso de Internet como medio de expresión, de participación y de acceso a la información. Asimismo, se deben elaborar y difundir pautas de autoprotección ante situaciones de riesgo.

La red Internet merece un uso cuidadoso para la seguridad física y psicológica de los niños, de las niñas y de los adolescentes.

Código Niño, Niña y Adolescente

“Artículo 158º (Prioridad de prevención). El Estado y la sociedad en su conjunto están en la obligación de dar prioridad a la prevención de situaciones que pudieran atentar contra la integridad personal de niños, niñas o adolescentes y los derechos reconocidos en el presente Código, quedando responsables de adoptar las medidas que garanticen su desarrollo integral.”

Como en todo, en Internet existen cosas buenas y cosas malas.

¡Aprovechemos las buenas!

En la escuela, es útil para:

- encontrar información en las bibliotecas virtuales y en las bases de datos de información para hacer las tareas,
- investigar sobre diversos temas,
- conocer varios puntos de vista sobre un mismo tema y
- obtener noticias actualizadas de los medios de prensa nacionales o internacionales.

Como medio para divertirse, permite:

- jugar en línea,
- escuchar la música que se difunde en la red y
- descargar vídeos.

Como herramienta de comunicación, posibilita:

- conocer amigos o amigas de diferentes partes del país y del mundo,
- comunicarse con amigos, amigas o familiares que están en otros departamentos o en otros países,
- construir páginas web y *blogs*,
- ser parte de grupos virtuales según los gustos y los intereses de cada persona,
- divulgar información e imágenes de la propia comunidad o del barrio, y
- compartir música.

La sensibilización y la prevención ante todo

En general, es normal que los niños, las niñas y los adolescentes comiencen a buscar imágenes sobre sexo o situaciones extrañas solamente por curiosidad.

Los contenidos no adecuados y sus consiguientes riesgos en Internet son cada vez mayores. Por ello, es necesario controlar el acceso a los contenidos de la red mediante herramientas informáticas como los filtros *Web*, que están basados en listas negras de sitios inapropiados, o el software especializado para detectar contenido malicioso en textos, en imágenes, en vídeos y en sonidos.

Algunos de los contenidos maliciosos están clasificados en: i) delictivos, porque contravienen normas penales, como la pornografía infantil, el racismo y la xenofobia o la apología del terrorismo y del tráfico y la elaboración de drogas; y ii) nocivos, que si bien no están prohibidos implican consecuencias negativas, como las páginas web a favor de la anorexia, de la bulimia y de otros desórdenes de la alimentación, así como la pornografía común o la difusión de imágenes de violencia.

Por lo anterior, es necesario educar a los niños, a las niñas y a los adolescentes para que puedan disfrutar de los beneficios de Internet, haciendo énfasis en los aspectos positivos y beneficiosos, pero con la debida orientación y supervisión, a fin de conocer sus hábitos de uso, las relaciones que entablan con otras personas y la información o los contenidos a los que están expuestos.

Es importante supervisar las actividades de los niños, de las niñas y de los adolescentes cuando hacen uso de la computadora, por cuanto no pueden, por sí mismos, evaluar situaciones de riesgo que podrían generarse a partir de la visualización accidental de sitios con contenidos pornográficos, violentos o discriminatorios que los exponen a personas que hacen un mal uso de la red.

De igual modo, es fundamental conversar con los menores para conocer lo que hacen en Internet y para prevenirlos respecto a los peligros.

Tres son los aspectos clave para promover el uso responsable de Internet: i) el adecuado conocimiento de lo bueno y de lo malo de Internet, ii) la orientación para detectar contenidos perjudiciales y iii) la información sobre los mecanismos técnicos y legales de protección.

Tres son los aspectos clave para promover el uso responsable de Internet: i) el adecuado conocimiento de lo bueno y de lo malo de Internet, ii) la orientación para detectar contenidos perjudiciales y iii) la información sobre los mecanismos técnicos y legales de protección.

Peligros a los que están expuestos los niños, las niñas y los adolescentes

Dibujo: Pedro Condori

Peligros a los que están expuestos los niños, las niñas y los adolescentes

Dibujo: Pedro Condori

Peligros a los que están expuestos los niños, las niñas y los adolescentes

A pesar de las ventajas que ofrece Internet para facilitar las diferentes actividades de los niños, de las niñas y de los adolescentes, contribuyendo a satisfacer sus necesidades y a su desarrollo personal, el uso de la red también implica diversos riesgos que podrían derivar en desórdenes del comportamiento (como la adicción a Internet), perjudicando su normal desenvolvimiento en ambientes sociales físicos, o en la ciberdelincuencia.

Seguidamente, se describen los riesgos más comunes:

- **Exposición a contenido dañino y violento**

  Las páginas web pueden mostrar contenidos que hacen apología de la bulimia y de la anorexia, de las drogas, de la violencia, del racismo, del regionalismo, de la discriminación, de la xenofobia y del suicido, además de pornografía, terrorismo, pedofilia y actos delictivos o inmorales.

- **Violación de la intimidad personal**

  Individuos con malas intenciones intentan contactarse con niños, niñas y adolescentes para solicitarles fotografías, conocerlos personalmente o pedirles que posen frente a una cámara web. Incluso solicitan sus datos personales (nombre, dirección, teléfono y otros), con objetivos de robo y de secuestro, principalmente.

- **Imágenes indeseables**

  Las cámaras digitales y las cámaras web son otra manera de producción de pornografía que involucra a niños, a niñas, a adolescentes y a jóvenes con acceso a las nuevas tecnologías. Se usan para tomar fotografías pornográficas y difundirlas por Internet.

- **Desorden emocional**

  El material pornográfico muestra contenidos sexualmente explícitos y nocivos. Es usado por pedófilos para reducir en los menores tanto la resistencia como las inhibiciones respecto al sexo. Esas personas se ocupan de conocer a sus víctimas a través de las salas de chat, de los juegos en red, del correo electrónico, de los sitios de encuentros personales y de mensajes de texto, entre otros, para luego proponerles una relación virtual y enviarles pornografía. Posteriormente, concretan un encuentro físico personal que, por lo general, es registrado mediante fotografías y vídeos.

Cafés Internet o *Cyber* cafés

Estos lugares públicos sin control se han constituido en otros espacios donde los pedófilos captan a sus víctimas. Lamentablemente, son considerados por los docentes y los padres y las madres de familia como lugares de juego o espacios de recreación.

Recomendaciones para los docentes, los padres y las madres de familia

Dibujo: Pedro Condori

Recomendaciones para los docentes, los padres y las madres de familia

Dibujo: Pedro Condori

¡Atención docentes!

- Dialoguen abiertamente con los niños, con las niñas y con los adolescentes sobre cómo usar Internet. Hablen acerca de sus motivaciones y de sus experiencias, y propóngales ideas referidas al uso adecuado de este recurso de comunicación.
- Gestionen la instalación de software de protección, con el objetivo de evitar el acceso a sitios web no aprobados para menores de edad.
- Aprendan y familiarícense con las nuevas tecnologías y con los recursos de comunicación que los estudiantes utilizan cotidianamente.
- Generen entre los menores la conciencia necesaria sobre la veracidad de los contenidos en Internet.
- Adviertan a sus estudiantes que algunas personas cambian su identidad cuando se comunican a través del chat o del correo electrónico.
- Orienten a los niños, a las niñas y a los adolescentes para que cuando usen el chat con personas que no conocen, aunque sean "supuestos amigos", no den datos personales (dirección, teléfono, nombres de familiares o de su escuela y horarios, entre otros) o cualquier información que pueda identificarlos.
- Gánense la confianza de sus estudiantes para poder orientarlos sobre los riesgos de chatear con desconocidos y de hacer citas reales con extraños que se contactan por medio de Internet.
- Alerten a sus estudiantes sobre los riesgos de enviar fotografías con niños, niñas o adolescentes desnudos, o con poca ropa, pues se podría hacer un uso indeseado de esas imágenes.

¡Atención padres y madres de familia!

- Orienten a sus hijos y a sus hijas en el uso de Internet, incluso si no tienen una computadora o no cuentan con acceso a la red en sus hogares, o en la escuela, ya que los menores podrían acceder a contenidos indebidos desde un TEC, un café Internet o cualquier otro sitio.
- Desarrollen en los niños, en las niñas y en los adolescentes la capacidad crítica necesaria para utilizar Internet, sin causarles miedo o la sensación de prohibición.

- Enseñen a sus hijos y a sus hijas a respetar a las demás personas que están en línea. Esto significa que no deben escribir, decir o responder con lenguaje ofensivo o irrespetuoso cuando se comunican en Internet.

- Establezcan con los niños, las niñas o los adolescentes ciertas reglas sobre el uso de Internet, los sitios web a los que ingresan, las personas con las que se comunican, el horario de acceso a Internet y el tipo de páginas web que pueden visitar. Reflexionen a los menores acerca de los posibles riesgos, pero también sobre la importancia de Internet como una poderosa herramienta que contiene mucha información, así como servicios útiles y provechosos. Reitérenles que la clave está en conocer y distinguir qué sirve y qué no.

- Animen a sus hijos y a sus hijas a compartir con ustedes sus experiencias en el uso de Internet, a fin de que les consulten cuando no estén seguros de algo. Disfruten de Internet con los menores.

- Expliquen a sus hijos y a sus hijas que no todo lo que está publicado en Internet, lo que reciben en su correo electrónico o lo que les dicen quienes se comunican con ellos es verdad. Los menores deben aprender a discriminar qué información es útil y cuál puede representar molestias o riesgos.

- Averigüen si los lugares que frecuentan los niños, las niñas y los adolescentes para acceder a Internet tienen algún tipo de sistema de protección o si cuentan con normas de uso de la red. Caso contrario, busquen un lugar que cumpla con esa medida.

- Expliquen a sus hijos y a sus hijas que es parte de su rol como padres y madres preocuparse y orientarlos en el uso de Internet, a fin de precautelar su bienestar físico y psicológico.

- Los adultos a cargo de menores deben aprender lo más que puedan sobre Internet, para cuidar y orientar a los niños, a las niñas y a los adolescentes al respecto. Si conocen los riesgos, pueden fijar reglas y velar por su cumplimiento.

- Si disponen de una computadora en sus hogares, ubíquenla en un ambiente compartido por toda la familia. Eviten instalarla en sectores privados o en las habitaciones de los menores.

- Instalen en la computadora algún software de protección infantil, para filtrar cualquier tipo de contenido malicioso.

Consejos prácticos para una navegación segura

Dibujo: Pedro Condori

Consejos prácticos para una navegación segura

Dibujo: Pedro Condori

Consejos prácticos para una navegación segura

Al usar el correo electrónico

- No abrir archivos adjuntos que lleguen en un correo de un remitente desconocido. Es probable, incluso, que dichos correos sean de personas conocidas, pero con archivos que generan cierta duda (nombres en inglés y modo de escribir del remitente diferente, entre otros aspectos). En general, esos archivos contienen virus.

- No abrir archivos adjuntos con extensiones .exe o .com. Tales archivos tienen un nombre y una extensión separados por un punto que indica el programa al cual pertenecen. Muchas veces, ese tipo de archivos son enviados por correo electrónico con algún tipo de virus.

- No abrir correos que anuncian alarmas de virus. Solamente se debe confiar en páginas web de empresas de seguridad conocidas.

Al usar los programas gratuitos

- Tener especial precaución cuando se descargan programas que ofertan regalos. Generalmente, las ofertas atractivas sobre productos gratuitos en Internet son un anzuelo para descargar en la computadora programas con virus, *software* espía o aplicaciones para hacer llamadas telefónicas al extranjero.

Al usar la mensajería instantánea

Distintos programas de mensajería instantánea, como *Yahoo Messenger* (www.yahoo.com), MSN *Messenger* (www.messenger.latino.msn.com) y *Skype* (www.skype.com), permiten una comunicación en tiempo real con personas en todo el mundo, por medio de mensajes de texto, de voz y de vídeo.

Esos programas funcionan sobre la base de listas de contactos que registran el sobrenombre o *nick* de cada persona. Tales listas corresponden a un registro de contactos conocidos por el usuario o de personas encontradas a través de los buscadores, por lo que es posible que cualquier usuario del mundo sea agregado, aunque usualmente se solicita primero un permiso a través de un mensaje automático.

Cuando un usuario cualquiera se contacta con niños, niñas o adolescentes y los agrega a su lista de contactos, podrá saber si éstos están conectados y enviarles mensajes instantáneos con archivos adjuntos que contengan fotografías, música, vídeos y virus, entre otros. Si ambos interlocutores disponen de micrófono, de parlantes y de cámara web en sus

computadoras, también podrán efectuar una comunicación mediante voz y/o por videoconferencia.

Si bien muchos niños, niñas y adolescentes se comunican con sus pares por medio de este servicio, también pueden contactarse con desconocidos. Por ello, es importante prestar atención a las personas que los menores tienen en su lista de contactos y orientarlos oportunamente.

También se los debe guiar para que tengan especial precaución cuando les piden información personal mediante esos servicios (nombres de familiares, direcciones, números de teléfono, números de tarjetas de crédito y contraseñas, por ejemplo), ya que personas desconocidas podrían utilizar esa información de manera inadecuada.

Otro aspecto que no debe ser descuidado está relacionado con el intercambio de programas a través de estos servicios, ya que se constituye en un foco de difusión de virus.

Pautas para compartir con los niños, las niñas y los adolescentes

- No divulgar por Internet información personal que sirva para identificarse, como nombres, direcciones, números de teléfono o contraseñas.
- Mientras se chatea, no proporcionar datos personales a personas que no se conozcan.
- No enviar fotografías sin el permiso de los padres y las madres de familia. Las fotos enviadas a sitios web no confiables o a personas desconocidas podrían ser utilizadas de modo inapropiado.
- No recibir archivos de personas desconocidas, porque podrían contener virus.
- No responder a mensajes obscenos, agresivos, de acoso sexual o de personas que no se conozcan.
- No concertar encuentros con personas que se conocen online, ya que podrían tener una identidad falsa que usan en Internet para fines que atentan contra la integridad de los niños, de las niñas y de los adolescentes.
- Remarcar que todo lo que está escrito o lo que se dice por Internet no siempre es verdad.
- Orientar sobre los contenidos o las fotografías de sitios web dudosos o de mensajes de correo electrónico, porque podría tratarse de imágenes pornográficas, violentas y agresivas, así como de algún virus.

- Si se recibe o se encuentra información que resulta dudosa o incómoda, es necesario que los menores comuniquen el hecho a los docentes o a los padres y las madres de familia.

- Verificar que los programas antivirus, *antispam* o *firewall* estén activados.

- No abrir mensajes de personas desconocidas ni mensajes de los que se desconoce el contenido.

- Tras usar el servicio de Internet desde un lugar público (telecentro, café Internet o escuela, entre otros), es importante cerrar siempre la conexión, para evitar que otra persona pueda robar la identidad virtual (nick) de los menores.

- No contribuir a la piratería distribuyendo a través de Internet materiales no autorizados (fotografías, música, imágenes, películas y otros).

Decálogo de derechos y de deberes de la infancia en Internet

1. Derecho al acceso a la información y a la tecnología, sin discriminación por motivo de sexo, de edad, de recursos económicos, de nacionalidad, de etnia y de lugar de residencia, entre otros aspectos, en especial para las niñas y los niños discapacitados.

2. Derecho a la libre expresión y asociación, y a buscar, a recibir y a difundir información e ideas de todo tipo por medio de Internet. Tales derechos sólo podrán ser restringidos para garantizar la protección de los niños y de las niñas ante información y materiales perjudiciales para su bienestar, su desarrollo y su integridad; así como el cumplimiento de las leyes, la seguridad, los derechos y la reputación de otras personas.

3. Derecho a ser consultados y a dar su opinión cuando se apliquen leyes o normas relativas a Internet que les afecten, como la restricción a contenidos, la lucha contra los abusos en red y las limitaciones de acceso al servicio, entre otras.

4. Derecho a la protección contra la explotación, el comercio ilegal, los abusos y la violencia de todo tipo a través de Internet. Los niños y las niñas también tienen derecho a utilizar Internet para protegerse de esos abusos, para dar a conocer y hacer defender sus derechos.

5. Derecho al desarrollo personal, a la educación y a todas las oportunidades de las nuevas tecnologías de la formación que aporta Internet, así como de las demás nuevas tecnologías.

6. Derecho a la intimidad de las comunicaciones por medios electrónicos. Derecho a no proporcionar datos personales por la red y a preservar su identidad y su imagen de posibles usos ilícitos.

7. Derecho al esparcimiento, al ocio, a la diversión y al juego mediante Internet y otras nuevas tecnologías. Derecho a que los juegos y las propuestas de ocio en Internet no contengan violencia gratuita ni mensajes racistas, sexistas o denigrantes y respeten los derechos y la imagen de los niños, de las niñas y de otras personas.

8. Los padres y las madres de familia tienen el derecho y la responsabilidad de orientar, educar y acordar con sus hijos y con sus hijas un uso responsable de Internet, por medio de ciertas reglas. Para ello, deben formarse sobre el uso de Internet e informarse en cuanto a sus contenidos.

9. Los gobiernos de los países desarrollados deben comprometerse a cooperar con otros países para facilitar el acceso de sus ciudadanos, en especial de los niños y de las niñas, a Internet y a otras tecnologías de la información y de la comunicación, a fin de promover su desarrollo.

10. Derecho a beneficiarse con las nuevas tecnologías para avanzar hacia un mundo más saludable, pacífico, solidario, justo y respetuoso con el medio ambiente, en el que se respeten los derechos de todos los niños y de todas las niñas.

Fuente: UNICEF.

Apuntes técnicos

Dibujo: Pedro Condori

Apuntes técnicos

Dibujo: Pedro Condori

Apuntes técnicos

Dada la gran cantidad de archivos indeseados que circulan en la red, otro aspecto relacionado con la seguridad en Internet tiene que ver con medidas que permitan asegurar técnicamente el buen funcionamiento de las computadoras. En ese sentido, la protección de los equipos requiere un especial cuidado. Los principales riesgos que afectan a las computadoras al estar conectadas a Internet son los siguientes[1]:

Amenaza	Descripción
Virus	Son programas diseñados para ejercer acciones maliciosas en la computadora en la que se ejecutan. Tales acciones van desde simples mensajes hasta el borrado de la información del disco duro, así como la inutilización del sistema operativo.
Spyware *(Software* espía*)*	Son programas que generalmente se ejecutan en la computadora sin que el usuario se dé cuenta, a fin de recopilar información del disco duro sobre el comportamiento de los usuarios para formar un perfil de ellos y enviar correos indeseados con información comercial (conocidos como *Spam*) tanto al usuario de ese equipo como a los contactos de los que exista información en la computadora.
Accesos no autorizados	Estos accesos son realizados por personas conocidas como *hackers* y *crackers*, quienes ingresan a una computadora aprovechando algún "agujero" de seguridad del sistema operativo para instalar virus o *software* espía por medio de Internet.
Hoaxes (Engaños)	Se trata de correos electrónicos con información falsa que informan sobre la existencia de alguna amenaza potencial en la computadora del usuario, por lo que le solicitan ejecutar acciones preventivas como: enviar el mensaje a todos sus contactos (con el simple fin de propagar la información falsa), borrar algunos archivos utilizados por el sistema o enviar correos a una persona en particular (para luego llenarla de mensajes), entre otras. En ocasiones, esas acciones hacen que la computadora no funcione adecuadamente.
Acceso a sitios no deseados	Como Internet es de uso libre, en la red puede ser publicado cualquier tipo de contenido. Este hecho se constituye en un peligro latente para los niños, las niñas y los adolescentes, principalmente por la difusión de contenidos inadecuados como violencia, pornografía, racismo y ofensas, entre otros.

[1] Fuente: Internet segura, Fundación Chile.

Generalmente, los riesgos anteriores pueden ser contrarrestados con alguna herramienta diseñada especialmente para ese fin. A continuación, se presenta un listado de esas herramientas, haciendo hincapié en aquéllas de carácter gratuito, que cumplen su función a cabalidad, e informando acerca de las versiones comerciales, las cuales poseen un gran respaldo y trayectoria.

Herramienta	Descripción
Antivirus	Son programas que detectan y eliminan virus de las computadoras. Entre las versiones gratuitas de antivirus se pueden citar las siguientes: • NOD32 Sitio oficial: http://www.nod32-es.com • AVG Sitio oficial: http://free.grisoft.com/doc/2/lng/us/tpl/v5 • BitDefender Sitio oficial: http://www.bitdefender.com/PRODUCT... • AVAST Sitio oficial: http://www.avast.com/eng/down_home.html En cuanto a las versiones comerciales más utilizadas, éstas son: • Norton Antivirus • McAfee VirusScan • Panda Antivirus • PC-Cillin • Bit Defender
Firewalls	Son también conocidas como murallas cortafuego, porque evitan el ingreso a la computadora por medios explotados por usuarios maliciosos. Se trata de programas que bloquean el acceso desde Internet hacia el equipo, regulando el tráfico de entrada y de salida de un ordenador con conexión a Internet. Entre las versiones gratuitas de firewalls figuran las siguientes: • ZoneAlarm Sitio oficial: http://download.zonelabs.com/bin/free/es... Sitio para bajar el programa: http://zonealarm.softonic.com/ie/39034 • Jetico Personal Firewall http://jetico-personal-firewall.softonic.com/ie/32698 Entre las versiones comerciales destacan: • ZoneAlarm Pro • Norton Personal Firewall • McAfee Personal Firewall • Personal Firewall

Herramienta	Descripción
AntiSpyware	Son programas que detectan y eliminan los programas espías. Entre las versiones gratuitas tenemos las siguientes: • Spybot Search & Destroy Sitio oficial: http://www.safer-networking.org/es/index.html Sitio para bajar el programa: http://zonealarm.softonic.com/ie/20443/... • Webroot Spy Sweeper Sitio oficial: http://www.webroot.com Sitio para bajar el programa: http://www.download.com/1200-2018-5146245.html • Ad-Aware Sitio oficial: http://www.lavasoft.com Sitio para bajar el programa: http://www.download.com/3000... Entre las versiones comerciales se pueden utilizar las siguientes: • Spyware Eliminator • Spy Sweeper • SpyDoctor • Ad-Aware Pro
Filtro de contenidos	Son programas que ayudan a que los usuarios, especialmente los niños y las niñas, no ingresen a sitios web con contenido inadecuado (violencia, pornografía y otros), mediante el reconocimiento del contenido de la página web a ser visitada y el bloqueo para acceder a ella. Entre las versiones gratuitas de pueden mencionar las siguientes: • NetVeda Safety.Net 3.61 (además de filtrar contenidos es firewall) Sitio oficial: http://www.netveda.com Sitio para bajar el programa: http://www.download.com/NetVeda-Safety-Net/3000-10435_4-10382920.html?tag=lst-0-16

Herramienta	Descripción
Filtro de contenidos	Entre las versiones comerciales que destacan figuran las siguientes: • ContentProtect • NetNanny • CyberSitter • McAfee • Parental Control • Norton Parental Control

Ahora sí,
¡a seguir disfrutando de Internet!

Dibujo: Pedro Condori

Ahora sí,
¡a seguir disfrutando de Internet!

Dibujo: Pedro Condori

Sitios para visitar

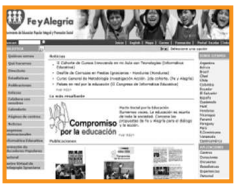
Contenidos sobre educación y salud

http://www.educabolivia.bo
Portal educativo nacional

http://www.pizarra.edu.bo
Portal educativo

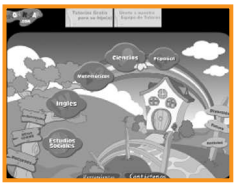
http://www.ceebolivia.net/
Comisión Episcopal de Educación

http://www.feyalegria.org/
Fe y Alegría



http://www.chicomania.com
Portal para chicos y papás

http://www.salonhogar.com
Salón Hogar



http://www.cienciaytecnologia.gob.bo
Bibliotecas virtuales de ciencia y tecnología

http://saludpublica.bvsp.org.bo/
Bibliotecas virtuales en temas de salud

http://bolivia.nutrinet.org/
Portal Nutrinet en Bolivia

http://www.ops.org.bo/
Organización Panamericana de la Salud-Bolivia

http://www.unicef.org/bolivia/
UNICEF-Bolivia

Reparticiones del Estado

http://www.presidencia.gov.bo/
Presidencia de la República

http://www.vicepresidencia.gob.bo/
Vicepresidencia de la República

http://www.bolivia.gov.bo
Portal del Gobierno de Bolivia

http://abi.bo/
Agencia Boliviana de Información

http://www.congreso.gov.bo/
Honorable Congreso Nacional

http://www.poderjudicial.gov.bo/
Poder Judicial de Bolivia

http://www.cne.org.bo/
Corte Nacional Electoral

www.defensor.gov.bo/
Defensor del Pueblo

http://www.facilita.bo
Portal país

Informática

http://softwarelibre.org.bo/comunidad/weblog/
Comunidad de *software* libre-Bolivia

http://www.icq.icq.com
ICQ (chat)

http://messenger.latino.msn.com
Messenger (chat)

Glosario

Actualizar: Instalar la versión nueva de un programa computacional que ya se posee.

AntiSpyware: Programas que detectan, eliminan y previenen la instalación de programas espía.

Antivirus: Programas cuya función es detectar y eliminar virus informáticos, al igual que programas maliciosos.

Aplicaciones: *Software* o programas especializados en actividades específicas. Existen aplicaciones para: escribir texto, realizar cálculos, organizar archivos de datos, hacer correr juegos y utilizar los servicios de Internet, entre otras acciones.

Attachments: Archivos computacionales que se envían adjuntos a un mensaje de correo electrónico.

Autentificación: Certificación de que un usuario efectivamente es quien dice ser. Se realiza mediante la solicitud del nombre de usuario y de la clave.

Bajar (*Download*): Acción de copiar un archivo computacional (puede ser un programa o un documento) desde un servidor en Internet a la computadora personal.

***Blogs* fotográficos:** Galería de imágenes fotográficas publicadas regularmente en Internet por uno o más autores. Usualmente, se trata de fotografías personales.

Bloqueo de ventanas emergentes (*Pop-ups*): El término *Pop-ups* se refiere a una ventana que aparece sobre otra ventana. El bloqueo de estos elementos consiste en impedir su despliegue.

Buscadores: Páginas en Internet que permiten a un usuario encontrar otras páginas o documentos que contengan una determinada palabra o un conjunto de palabras.

Cargar: Trasladar la información desde un servidor a la memoria de trabajo de la computadora o a la memoria RAM, para visualizarla en la ventana del navegador.

Chat: Conversación en tiempo real a través de Internet. Ésta también puede incluir el intercambio de sonidos (voz) y de imágenes (vídeo).

Cliente: Computadora y programa computacional que solicita servicios a otra computadora en Internet, llamado servidor.

Comunidad *Online*: Agrupación de usuarios de Internet que comparten intereses comunes.

Correo electrónico (*E-mail*): Servicio virtual que permite a los usuarios enviar y recibir mensajes. Con los mensajes, también se pueden enviar archivos de fotos y documentos.

Diarios *Online* (*Blogs*): Un *weblog*, también conocido como *blog* o bitácora, es un sitio web actualizado con cierta frecuencia por uno o por varios autores con textos y/o artículos que se presentan como una recopilación cronológica. Generalmente, los *weblogs* son publicados en un estilo personal e informal.

Documentos: Archivos computacionales que contienen información (al contrario de instrucciones). Pueden ser textos, imágenes, sonidos y vídeos, entre otros.

***Emoticons*:** Símbolos que representan rostros expresando una emoción o un estado de ánimo. Son utilizados en las herramientas de comunicación de Internet.

Encriptación: Proceso mediante el cual cierta información es cifrada de modo que el resultado sea ilegible para otros, a menos que se conozcan los datos necesarios para su interpretación.

Favoritos: Marcas de página que almacenan automáticamente una dirección de Internet, con el objetivo de facilitar el regreso a dicha página sin tener que recordar o escribir la dirección exacta.

Filtro de contenido: *Software* o programa que permite restringir el acceso a determinados contenidos de páginas web que el usuario define.

***Firewall* o cortafuegos:** Elemento de *hardware* (parte física del equipo) o de *software* (programa computacional) utilizado para restringir el acceso de un usuario conocido o desconocido a un sitio o a un servicio de Internet.

Foros de mensajes: También son conocidos como foros de opinión o foros de discusión. Usualmente, son soportados por una aplicación o por página web.

***Freeware*:** *Software* gratuito, es decir, que puede ser copiado de manera gratuita.

***Hackers* y *crackers*:** Los *hackers* (del inglés *hack*, recortar) son expertos en una o en varias ramas relacionadas con la computación y con las telecomunicaciones, entre ellas:

la programación, las redes de comunicación y los sistemas operativos. En ocasiones, un *hacker* busca romper las vallas de seguridad de los sistemas informáticos, sin un afán dañino. Los *crackers* (del inglés *crack*, romper) usan ese conocimiento experto con fines maliciosos, antimorales o incluso bélicos, como la intrusión a redes, el acceso ilegal a sistemas gubernamentales, el robo de información y crímenes informáticos, como la distribución de material ilegal o moralmente inaceptable y la creación de virus, entre otros.

Hoaxes (Del inglés *hoax*, engaño): Mensaje de correo electrónico con contenido falso o engañoso, normalmente distribuido en cadena.

Internet: Es una red de redes a escala mundial, que une a miles de millones de computadoras y de personas. Para lograr la comunicación, Internet utiliza un protocolo de comunicación único: TCP/IP.

***Link*:** Enlace entre páginas web. Se trata de sectores de la página web (textos o imágenes) vinculados a otras páginas, de manera que al hacer clic sobre ellos se ingresa a una nueva página de Internet relacionada con la primera.

Lista de contactos: Listado de personas con sus direcciones de correo electrónico.

Lista de interés: Servicio de Internet que permite intercambiar mensajes de correo electrónico sobre un tema determinado, con un grupo definido de personas.

Mensajería instantánea: Servicio de Internet que permite enviar y recibir mensajes de texto instantáneos entre usuarios conectados a Internet.

Multimedia: Sistema que integra textos, imágenes fijas o en movimiento y sonidos en un único formato de presentación. Se trata de una combinación de varios medios con sonidos, gráficos, animación y vídeo.

Navegador web: Conocido también como web *browser*, es una aplicación (*software*/programa) que permite al usuario acceder a páginas web.

Página web: Documento o conjunto de documentos a los que se puede acceder a través de Internet usando un navegador. Usualmente, están en un formato o lenguaje llamado HTML. Además, pueden incluir textos, imágenes, animaciones y vídeos, entre otros recursos.

***Password* (palabra o clave de acceso):** Código secreto conocido sólo por el usuario al que pertenece. Se utiliza para proteger la privacidad de la información.

Portal: Lugar o sitio en Internet que agrupa un gran número de servicios. Puede incorporar múltiples páginas web.

Respaldar: Guardar una copia de la información almacenada en el computador en otro soporte o en otro equipo, por ejemplo, en un disquete, en un disco compacto de sólo lectura (CD-ROM) y en una memoria *flash* (*pendrive* o *flash memory*), entre otros dispositivos.

Servidor: Computadora y programa computacional que brinda los servicios solicitados por otra computadora denominada cliente.

***Shareware*:** Tipo de *software* o programa que puede ser utilizado de modo gratuito por un periodo determinado o que posee limitaciones funcionales para su uso.

Sistema operativo: Conjunto de *software* o programas destinados a permitir la comunicación entre el usuario y la computadora. Comienza a trabajar cuando se enciende el equipo y administra los componentes de éste (pantalla, teclado y mouse, entre otros).

***Software*:** Programas con los que trabaja una computadora, entre ellos, el procesador de textos, la hoja de cálculo y el navegador. Permiten la interacción de un usuario con el equipo.

***Spam*:** Mensajes electrónicos (habitualmente de tipo comercial) no solicitados y distribuidos masivamente.

***Spyware*:** "Programa espía" que recopila información sobre un usuario o una organización, sin su consentimiento.

Utilitarios: Pequeños programas que sirven para un trabajo determinado, por ejemplo, reproducir música en la computadora.

Videoconferencia: Servicio multimedia (audio y vídeo) que permite a varios usuarios mantener una conversación a distancia en tiempo real.

Virus: Programa que puede infectar otros programas modificándolos para incluir una copia de sí mismo.

Con el apoyo de:

EMBAJADA DE ESPAÑA EN BOLIVIA

aecid
Agencia Española de Cooperación Internacional para el Desarrollo