Carta a nuestros lectores

Como ha ocurrido en diferentes profesiones, también en el periodismo el avance de la ciencia ha traído consigo el despuntar de nuevas especialidades. Una de ellas es la del periodista digital, aquel profesional con capacidad suficiente para bregar con una serie de herramientas tecnológicas que, para muchos, parecían invento de la ciencia ficción. Sobre este profesional versa el artículo de portada.

A la censura como mecanismo para coartar la libertad de comunicación y de expresión del pensamiento se une ahora aquel de los "circuitos de información", que dicen verdades a medias y decoran falsedades que terminan pasando como auténticas.

Nuevamente la humanidad se enfrenta a la trágica coyuntura de la guerra. México y Chile, como integrantes del Consejo de Seguridad de las Naciones Unidas, jugaron un papel trascendental para impedir que se la aprobara. Resulta interesante conocer cuál fue la reacción de los medios de comunicación de estos dos países, frente a la posición de sus gobiernos y la presión de los Estados Unidos.

En épocas de grandes acontecimientos el desempeño del periodismo se vuelve controversial. La opinión pública se pregunta, entre otras cosas, si el periodista se aprovecha del poder que tiene, si se convierte en peligro para la información veraz e imparcial, si abusa de las ventajas tecnológicas de los diferentes medios o, finalmente, si sigue ciegamente la política de su país aun sabiendo que es inmoral. **Chasqui** busca dar respuestas a preguntas inquietantes como estas.

En la guerra de información que existe entre gobierno y oposición en la República venezolana, resulta sumamente interesante tratar de descubrir cuál ha sido el papel que la televisión privada ha jugado en esta conflicto y, para dar un contexto más amplio a este problema, vale la pena también conocer cual es el impacto que la televisión tiene en los otros medios de comunicación, especialmente la prensa. En este número de Chasqui hablamos de estos problemas.

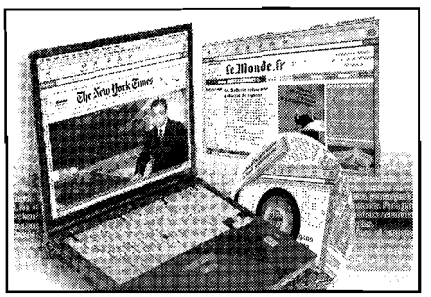
CHASQUI

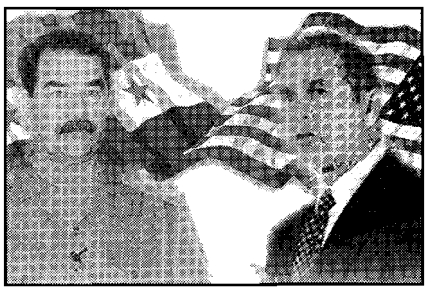
Revista Latinoamericana de Comunicación

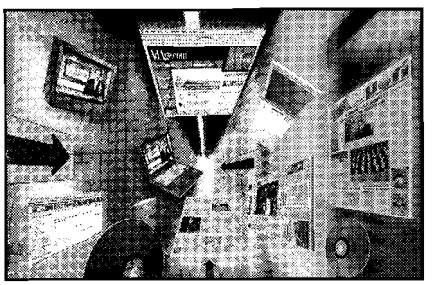
Chasqui

N° 81 Marzo 2003

Chasqui es una publicación de CIESPAL
Telf.: (593-2) 2506149 – 2544624
Fax (593-2) 2502487
e-mail: chasqui@ciespal.net
web: www.ciespal.net
www.comunica.org/chasqui
Apartado 17-01-584
Quito – Ecuador
Registro M.I.T.,S.P.I.027
ISSN 13901079







CIESPAL

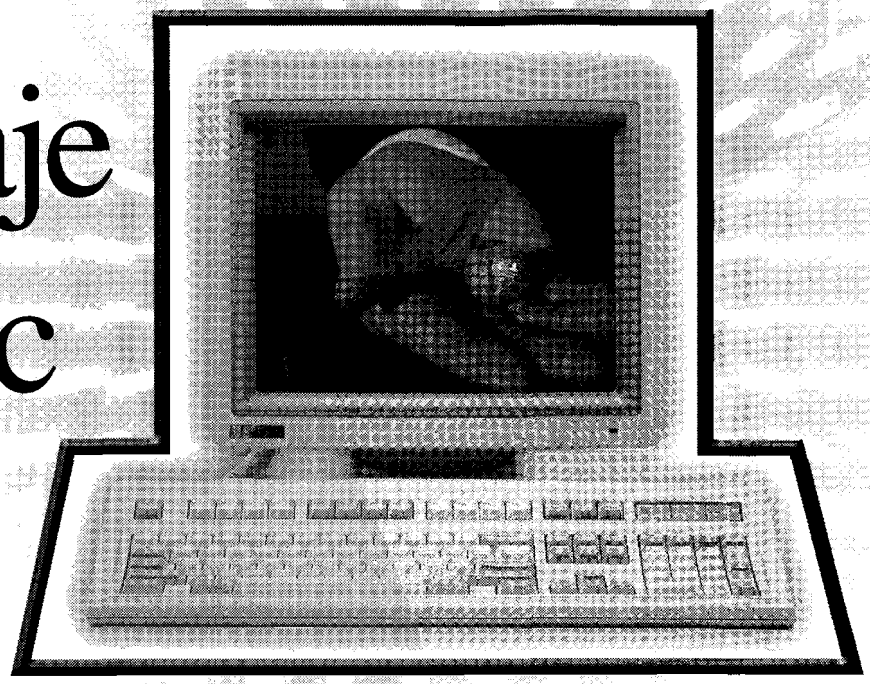
CONTENIDO

PORTADA

OPINIÓN

ENSAYOS

El blindaje de una Pc



La navegación en Internet y la consiguiente conexión a una red expone a una computadora a un sinfín de riesgos y peligros. Una PC que no sea utilizada para navegar en Internet o que no esté conectada a una red puede, incluso, ser también afectada por virus, por la utilización de disquetes contaminados que la contaminen con un virus. Para enfrentar esos problemas, la industria informática ha previsto una serie de protecciones y recaudos, de cuyo uso y utilización deben estar plenamente informados los usuarios de una PC

Antivirus

Es el sistema defensivo contra virus, los denominados "troyanos" y otras amenazas por antonomasia. Un ordenador sin antivirus o con uno no actualizado, está expuesto a todo tipo de ataques cuyas consecuencias van desde la pérdida de datos vitales hasta el espionaje sobre el trabajo que el usuario realiza en su PC. Con un "troyano" (por aquello del enorme caballo de madera en el que se escondieron los invasores de la ciudad de Troya), la vida privada de un usuario de PC puede ser fisgoneada, los datos pueden ser borrados con un virus o pueden provocarse ingentes perdidas económicas.

Es imprescindible, entonces, contar con un antivirus permanentemente actualizado. Se recomienda, incluso, contar con la vigilancia simultánea de dos antivirus, teniendo en cuenta las incompatibilidades que existen entre algunas marcas y el hecho de que solo uno de ellos puede estar a cargo del monitoreo de una máquina.

Cortafuegos

La segunda línea defensiva de un ordenador doméstico es el cortafuegos o firewall.

Cuando un ordenador accede a Internet se comunica mediante unas "puertas" o puertos de conexión, que son como canales independientes que funcionan a determinadas frecuencias. Existen 65.535 de esos canales por donde los datos pueden salir o entrar en nuestro ordenador y a través de ellos, alguien puede intentar una intrusión.

El cortafuegos cierra todos los puertos que no se están utilizando mientras se navega en Internet, impidiendo cualquier conexión a través de ellos. Existen cortafuegos que pueden convertir prácticamente en invisible a un ordenador.

Por El Reporte Delta

Antispyware

Ciertos programas, mientras nos encontramos en Internet, pueden recabar y obtener información de los hábitos de navegación del usuario, para elaborar estadísticas de consumo y perfiles especializados del mismo.

Esos spyware, incluso, pueden identificar la dirección email de un usuario para enviarle el denominado tráfico "spam" o correo basura o averiguar password's y contraseñas y otros datos delicados muy personales.

Para librarnos de estos programas un ordenador debe contar con un antispyware. Existen en el mercado antivirus que también detectan y eliminan los programas spyware

Se recomienda entonces, además de utilizar un antispyware, cargar el procesador con un anonimizador que impida que nuestros datos más secretos, que están almacenados en la PC, puedan ser extraídos subrepticiamente mientras navegamos en Internet.

Encriptación

Los expertos recomiendan también hacer uso de un programa de encriptación, para codificar o encriptar los email que sean realmente vitales para la privacidad del usuario de una PC, a fin de restringir o evitar su acceso por parte de extraños.

Recuperar archivos

Pueden darse circunstancias en que por no tener instalado un antivirus o porque este no se encuentra actualizado, un usuario resulte afectado por el borrado de documentos vitales existentes en su PC.

En ese caso es preciso contar con la información necesaria sobre cómo proceder para utilizar las herramientas necesarias para recuperar gran parte de lo perdido durante un ataque.

Borrado efectivo

Otro problema para el cual se debe contar con herramientas, tiene que ver con el borrado efectivo de archivos. Debe saberse que cuando se los envía a la papelera de reciclaje y luego se la vacía, esos archivos no han desaparecido por completo sino que pueden ser recuperados.

Debe preverse esa circunstancia y también la posibilidad de que al ser desechado un disco duro, estemos enviando dentro de él información sensible que puede ser recuperada por extraños.

En cualquiera de los dos casos, en especial cuando se trate de datos sensibles, es recomendable proceder al borrado reiterativo, para lo cual existen herramientas disponibles en el mercado.

Monitorear puertos

Existen programas cuyo objetivo es realizar el monitoreo de los puertos que se abren mientras navegamos en Internet. Ello permite, por ejemplo, identificar a un "troyano" que se encuentre dentro de un ordenador y que inmediatamente después de lograrse la conexión con Internet, se prepare a enviar los datos que ha recolectado.

El programa para monitorear puertos avisará al usuario cuando el "troyano" abre su puerto para enviar información y permitirá conocer la identificación del atacante que está utilizando al "troyano", así como averiguar dónde están ubicados los servidores de las páginas web que son visitados y el tipo de conexión que utilizan con la PC del usuario

La información

Toda esta información fue obtenida a partir de un informe especial de El Reporte Delta, cuyo autor y editor, el colombiano José Camilo Daccach, lo proporciona a los interesados vía email, en la dirección http://delta.hypermart.net ó erd-subscribe@domeus.es

El documento "Blindaje de su PC" de El Reporte Delta incluye identificaciones precisas de los programas que los usuarios pueden comprar o bajar del Internet para proteger a su computadora. El Reporte DELTA es de suscripción gratuita.