Carta a nuestros lectores

La responsabilidad periodística en la actual coyuntura, caracterizada por un mundo globalizado e intercomunicado, es el tema al que **Chasqui** dedica la portada de este número, tomando en cuenta que el fenómeno abarca, de una forma u otra, a toda la humanidad y, con mayor razón, a la actividad que cumplen los comunicadores

En la columna de opinión analizamos un programa de televisión procedente de la Argentina, que ha traspasado fronteras por obra y gracia de esa globalización y cuyo contenido ha provocado, y continúa provocando, controversias en todos los países en los que se exhibe.

La guerra contra el terrorismo, cuyo protagonista más caracterizado es el gobierno de los Estados Unidos, obliga a los comunicadores a enfrentar el tema recurrente del terrorismo, sus causas, modalidades y formas diferentes en las que se manifiesta.

A continuación, evaluamos los resultados de la Cumbre de la Sociedad de la Información, que por convocatoria de las Naciones Unidas se realizó en Suiza, y nos adentramos en una nueva forma de informar y comunicar: los weblogs o las "bitácoras" del Internet.

Hablamos de la comunicación política desde dos vertientes: el trabajo de los consultores y asesores de imagen que no pueden a un mediocre convertirlo en Dios, ni derrotar a un excelente rival, simplemente porque así lo deciden. El artículo sobre las elecciones de alcaldes en Colombia plantea una incógnita recurrente en el mundo electoral latinoamericano, que se refiere al triunfo de candidatos que la opinión pública, equivocadamente, los miró como perdedores. Humberto López despeja esta incógnita.

Poniendo fin a la trilogía sobre la nueva realidad mediática en los Estados Unidos, Leonardo Ferreira y Miguel Sarmiento ponen de manifiesto, sin duda para sorpresa de muchos, la práctica de la ética por los periodistas americanos que no concuerda con la tradición de la que siempre se han sentido orgullosos.

Por fin, en el amplio y siempre cambiante mundo de la informática, analizamos los problemas legales que enfrenta en Europa y Estados Unidos el gigante de la informática, Microsoft, por supuesto monopolio y vulnerabilidad ante el ataque de los virus.

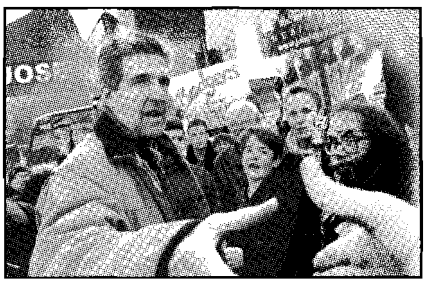
CHASQUI

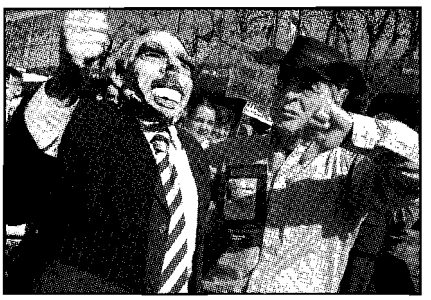
Revista Latinoamericana de Comunicación

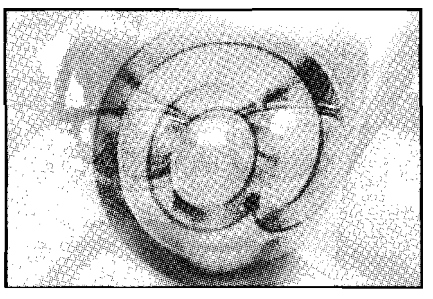
Chasqui

N° 85 Marzo 2004

Chasqui es una publicación del CIESPAL.
Miembro de la
Red Iberoamericana de Revistas de Comunicación
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



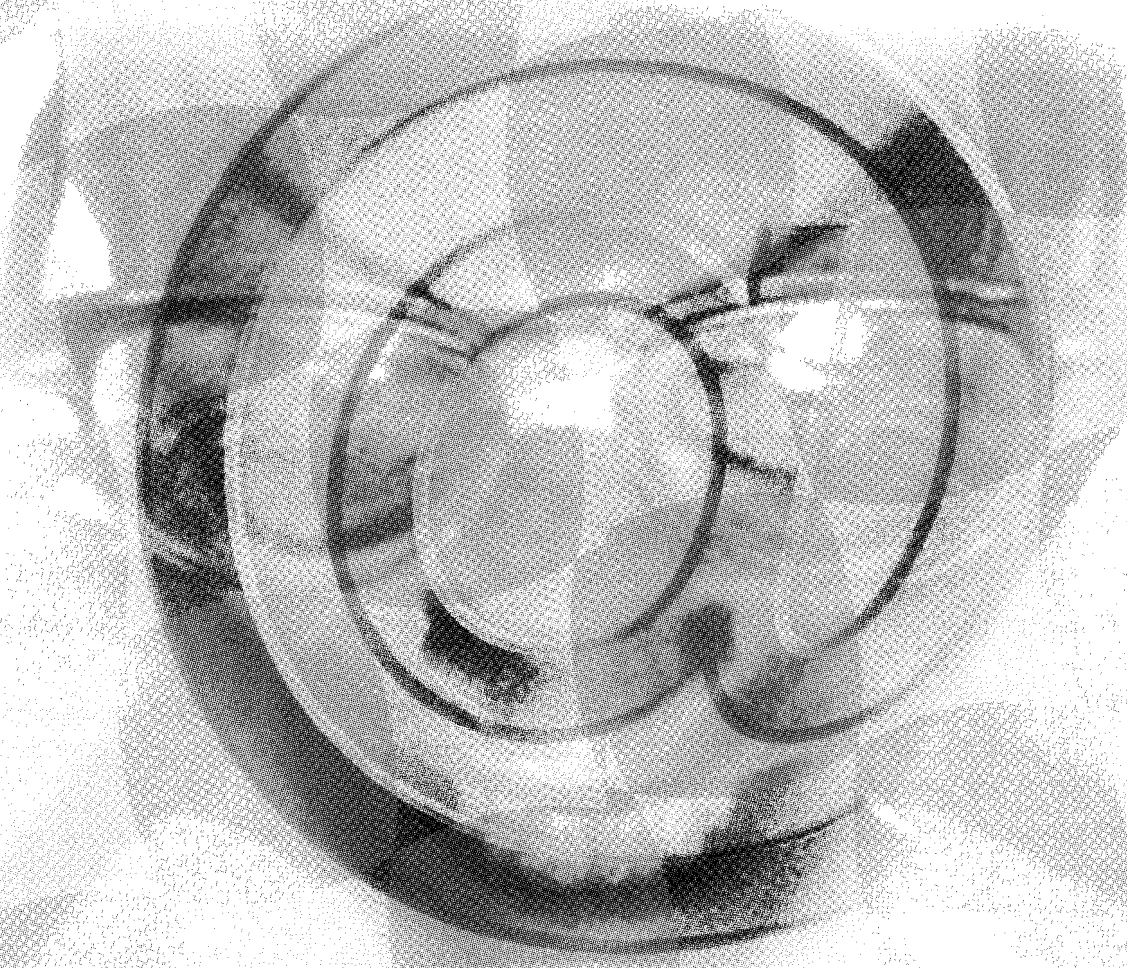




CIESPAL

CONTENIDO

CYBERTERRORISMO



historia de nunca acabar

Los ataques son terrorismo o simples bromas de desadaptados

José Camilo Daccach T.

Estar conectados a Internet es ya una necesidad cotidiana, seamos la más grande multinacional, o simplemente un habitante del mundo. Desde las soluciones más sencillas, como el envío de correo electrónico, hasta soluciones complejas de vídeo vigilancia y monitoreo, se efectúan a través de Internet y sus tecnologías.

Si bien se ha avanzado mucho en el uso de la red, también es cierto que la red inició como un proceso colaborativo entre colegas para su utilización en la investigación científica. Nunca se pensó, hace 30 años, que aparecería la Web, el protocolo *http* y demás elementos que permiten que hoy manejemos ambientes gráficos en la misma, y por lo tanto convirtiéndolo en un excelente elemento de mercadeo.

La informática siempre ha tenido un halo de lo *desconocido,* por lo que buena parte de sus usuarios sienten temor: temor de que se borren los archivos, temor a que se dañe el computadora, temor hasta de quedar en ridículo. Ahora, es el mismo temor el que nos debe proteger contra una nueva ola de ataques, catalogados por algunos como terrorismo y por otros, simples bromas de desadaptados.

Flexibilidad del ajuste

Una de las bondades de la tecnología de Internet es su flexibilidad para ajustarse rápidamente a necesidades cambiantes. Hoy se manejan todo tipo de equipos en forma remota controlados por Internet, se distribuye información, se almacenan imágenes y se maneja el comercio electrónico, a través de las mismas tecnologías. Esta *flexibilidad* y apertura, si se quiere llamar así, hacen también que haya falencias en los sistemas de seguridad de los mismos.

Lo primero que se elabora y desarrolla al montar un sistema de información es el establecimiento de funcionalidad que permita el usufructo del mismo. Los sistemas de seguridad siempre aparecen al final del proyec-

José Camilo Daccach T., colombiano, especialista en el uso estratégico de la tecnología informática, fundador de El Reporte DELTA y su respectivo portal, docente y consultor independiente. **En marzo del 2003 publicamos un informe especial para Chasqui del Reporte Delta sobre como "blindar" a una PC para que se vea afectada por virus y similares.**
Correo-e:jocada@telesat.com.co • web: www.deltaasesores.com

to, si es que terminan implementándose. Esto sucedía en un ambiente cerrado al interior de las empresas. Hoy se exige que los esquemas de seguridad también se implementen en el mismo instante que se conecte el sistema a Internet, pero la velocidad a la que avanza la tecnología convierte este proceso de seguridad en una carrera contra el tiempo, muchas veces relegada a segundos y terceros pasos a los que nunca se llega.

La informática ha tenido un halo de lo desconocido y los usuarios sienten temor

Vulnerabilidad del sistema

En la misma carrera aparecen los proveedores de las soluciones, quienes cada vez gozan de menos tiempo para probar su oferta, haciendo también los sistemas instalados vulnerables a ataques. Vulnerabilidades que son ampliamente aprovechadas por personas con fines muy distintos, como probar las fallas, o simplemente hacerse notar. Desdichadamente, la herramienta por excelencia para distribución de los males en contra de estas vulnerabilidades es el correo electrónico.

En la mentalidad de quien quiere efectuar el daño siguen los mismos objetivos que tenían los primeros productores de virus: no ser detectados y llegar al mayor número de equipos posible. Por lo tanto, el mejor vehículo para un mal masivo es, y seguirá siendo, el correo electrónico. Es muy poco lo que tiene que hacer un productor de un virus para utilizar este vehículo de distribución, y la efectividad es bastante alta. Estos mensajes de distribución, además de dañinos, se constituyen también en SPAM, o correo no deseado, y su amplia replicación hace que la saturación en la red demore el tráfico, constituyéndose en el primer problema, pero el de menor consecuencia.

Las razones para construir un virus van desde la investigación científica, pasando por la prueba de una teoría de falencia en un programa, hasta el mero interés de hacer daño. El éxito del ataque se mide por la penetración del daño y/o por el reconocimiento del mismo, por lo que siempre estarán atacadas las empresas tipo Microsoft, o un amplio número de usuarios individuales.

El MyDoom

La rivalidad comercial entre empresas no ha estado ajena a este escenario de ciberterrorismo. El último virus de ataque masivo, conocido como MyDoom, estaba dirigido expresamente a SCO, en retaliación por unas demandas que ha colocado, reclamando derechos sobre el código de Linux. Básicamente, se escribió un programa que se replica a través del correo electrónico en forma de gusano, de tal manera que cada computadora infectada enviase un ataque masivo contra el servidor de SCO. También en las últimas semanas se efectuó un ataque sobre los servidores de Microsoft, y es bien conocido que esta empresa tiene suficientes enemigos por sí sola. El ataque, en esta ocasión, también consistió en envío de solicitudes masivas a los servidores de Microsoft para que se saturaran y no pudieran atender más.

Cada empresa maneja como puede este tipo de ataques. SCO, simplemente, cambió la dirección de su servidor, por lo que el ataque no fue efectivo, pero si tuvo que efectuar serios procedimientos internos para garantizar que todos sus procesos basados en el servidor principal siguieran funcionando. Microsoft optó por otra solución: adquirir replicación de su información en servidores alrededor del mundo, de tal manera que si uno era atacado, los demás podrían suplir la necesidad de información.

Estamos hablando de empresas de alta envergadura mundial y con acceso a recursos de ese talante para poder contrarrestar estos ataques. ¿Qué puede hacer una de nuestras empresas, restringidas al máximo en su presupuesto, para contrarrestar estos ataques?

Medidas a tomar

La primera reacción es desconectarse de Internet. De seguro resuelve el problema, pero es inmediatamente descartada por lo impráctico. La segunda es asesorarse bien en materia de seguridad informática, para poder establecer un mecanismo que impida y prevenga este tipo de ataques. Lo que se debe considerar al establecer un mecanismo de seguridad es que siempre existe la posibilidad de ser vulnerada. Siempre habrá personas buscando penetrar sistemas de seguridad, por lo que su establecimiento no es un proyecto, sino un proceso de nunca acabar.

Los males básicos que se atacan por correo electrónico son el SPAM y el virus, aunque este segundo también viene por otras vías, como la navegación en páginas maliciosas; el correo sigue siendo el mayor divulgador. No podemos dejar de vista otras formas de ataque, básicamente de invasión de privacidad, como el spyware o software que se instala en los equipos sigilosamente para rastrear, registrar e informar sobre todo lo que hace su usuario.

Existe en el mercado amplia protección contra virus y spam, y sin embargo todavía estos ataques son exitosos, básicamente porque los usuarios están desprevenidos, inconscientes, o realmente desinteresados en lo que les pueda pasar. Es claro que así debería ser, el usuario simplemente debería poder utilizar la tecnología, sin tener que preocuparse por mucho más, pero así como quien conduce un vehículo debe conocer los principios básicos de mecánica, o por lo menos saber cambiar una llanta pinchada, el usuario de las tecnologías de Internet deberá ser también responsable de las medidas de seguridad que están a su alcance.

Protección de los servidores

La protección no solo compete al usuario final, sino también a las empresas que prestan servicios de conexión a la Internet. El mayor daño que se efectúa con un virus o mensajes no deseados es la pérdida de productividad. Si se puede lograr que los mensajes infectados o los no solicitados no lleguen siquiera al usuario final, estaríamos reduciendo en un alto grado el riesgo de pérdida de productividad.

Los proveedores de servicios de Internet han desarrollado soluciones que permiten llegar a este tipo de controles. En el caso de los virus, basta con colocar un servidor antivirus al recibo del correo para probar todos los mensajes, y no recibir ninguno que esté infectado. Sin embargo, el establecimiento de este esquema implica el pago de cifras, en algunos casos astronómicas, a las empresas que producen los programas antivirus.

Otra de las dificultades aparentes es la velocidad de reacción que pueda tener el proveedor del programa de antivirus para producir las vacunas contra los

El éxito del ataque de los virus se mide por la penetración del daño que causan

ataques que van surgiendo. Dado que los ataques, por diseño, son sigilosos, se hace más difícil detectarlos antes de una propagación extensa.

También existen soluciones para el control del SPAM y sus diferentes variantes. El correo electrónico se ha convertido en una herramienta de mercadeo que bien utilizada genera frutos espectaculares. Estas prácticas tienen sus características de buen uso, sin embargo, algunos aduciendo ignorancia, y otros simplemente abusando del medio, efectúan barrido de SPAM tratando de vender sus productos.

El correo no deseado

El remedio para el correo no deseado es precisamente la utilización de programas AntiSPAM. Se utilizan herramientas de *lectura y calificación* de los mensajes recibidos para tratar de determinar si son SPAM o no. Se utiliza la técnica heurística y algunas de las características que se buscan son la cantidad de enlaces, imágenes, y/o formato en HTML que se presente en el mensaje. Estos factores que se van midiendo emiten un puntaje y con base en este puntaje se califica un mensaje como SPAM o no. La incidencia, sin embargo, en estas características, puede ocasionar que un mensaje válido sea calificado como SPAM y rechazado. Esto se conoce como falsos positivos, y pueden ocasionar pérdidas si, por ejemplo, es un pedido que se efectúa a una empresa.

La alternativa es guardar los mensajes en un buzón de *posible SPAM,* para que el destinatario pueda revisar y tomar la decisión de sí es o no SPAM, e ir lustrando el programa que toma la decisión, mediante la utilización de *listas blancas* sobre qué mensajes puede dejar pasar sin problema. La complejidad de estos sistemas radica en la intervención alta del usuario del programa en la estructuración del mismo para que sea efectivo.

Una advertencia

Por otra parte, no protege contra ataques de spam conocidos como ataques de directorio, donde se envía correo indiscriminado a cualquier combinación de letras al mismo dominio. Por ejemplo, se envían correos a a@dominio.com, b@dominio.com, aa@dominio.com y así sucesivamente, llegando a construir millares de mensajes dirigidos al mismo sistema de correo, lo que lleva a su colapso. Para este tipo de ataques no sirve la estrategia de leer el correo y determinar si lo es o no, sino mas bien programas que están constantemente monitoreando la actividad de los servidores y de los puertos de entrada, y determinando qué se puede constituir en un comportamiento sospechoso.

El e-mail es una herramienta de mercadeo que genera frutos espectaculares

En los Estados Unidos se aprobó, recientemente, una ley conocida como la Can Spam Act, que pretende castigar a quienes efectúen SPAM; sin embargo, se duda de su efectividad, en especial cuando la Internet no tiene fronteras. Bill Gates, propietario de Microsoft, también anunció una *eliminación* del SPAM en dos años, e inclusive se ha hablado de cobrar por el envío de mensajes, cobro que aminoraría el envío de correo indiscriminado.

Es claro que no nos podemos desconectar de Internet, pero también es claro que tenemos algunas herramientas a nuestra disposición para la protección. Se deberá establecer un equipo conformado por los usuarios y los prestadores de servicios, enfilados contra estos males. Existen aplicaciones tanto para los equipos de los usuarios, como para los administradores de redes en las empresas y los proveedores de servicios de Internet, que utilizadas en conjunto permiten hoy en día establecer un esquema de protección, aunque no infalible, por lo menos bastante sólido.