

# ATAQUES AL MUNDO FÍSICO DESDE EL LÓGICO

"Este documento está inspirado por el libro "Distracción" de Bruce Sterling, y por el artículo de Bruce Schneir en CryptoGram, <http://www.counterpane.com/crypto-gram0304.html#1>".

## **Autores**

---

Román Ramírez <[rramirez@chasesun.com](mailto:rramirez@chasesun.com)>  
Director General de Chase The Sun

Jesús Arnaiz <[jarnaiz@chasesun.com](mailto:jarnaiz@chasesun.com)>  
Director Técnico y Director de Operaciones de Chase The Sun

Este artículo en .RTF:

<http://www.chasesun.es/docs/logicoafisico.rtf>

[Español]

<http://www.chasesun.com/docs/logictophysic.rtf>

[English]

## **Introducción**

---

Tradicionalmente, la valoración y cuantificación de los ataques lógicos se ha realizado en función del daño lógico que estos provocan. Se habla de cifras de millones de euros o millones de dólares, siempre valorando la negación de servicio y otros factores puramente lógicos.

Pero todos estos daños lógicos tienen su repercusión en el mundo físico, y hay muchas más implicaciones y daños potenciales que todavía no se están explotando, y que probablemente en un futuro próximo, si que se explotaran.

En algunos párrafos de este artículo, parecerá que exageramos o llevamos de manera extrema temas que hoy en día no constituyen amenaza alguna, y que a simple vista, no lo serán en un futuro próximo.

El hecho es que no pretendemos inducir a la paranoia, pero si queremos evidenciar potenciales peligros que ya existen HOY, y que probablemente veremos plasmarse en casos reales en un futuro más que próximo.

## **Efectos directos y efectos laterales de un ataque lógico**

---

La propagación de un gusano (worm) como CodeRed, Nimda o Slammer, provoca en general daños en la calidad de servicio, daños a servicios críticos (como pueden ser el web y

bases de datos) y adicionalmente pérdidas de dinero por las inversiones en la reparación de los daños.

Dentro de los efectos físicos que, como resonancia, este tipo de ataques provocan, podemos contar de forma inmediata: la pérdida en horas de producción, empleados pasivos a la espera de la solución, problemas de imagen de empresa, horas a posteriori dedicadas a la solución, potenciales costes de reemplazo de hardware...

Los casos que conocemos, y que son los que marcan la pauta de nuestras valoraciones en control de daños, nos impiden observar que los ataques que estamos padeciendo hoy en día son ataques simples y poco sofisticados. El daño directo e inmediato que la mayoría de los ataques o gusanos provocan puede ser reparado en plazos rápidos, y la mayoría de las ocasiones sus efectos han quedado minimizados o restringidos a una serie de equipos en red.

Pero, ¿qué ocurre en el momento en que un ataque cualquiera afecta a un dispositivo que actúa como enlace entre el mundo lógico y el físico? El ejemplo más básico y sencillo es un ordenador que gestiona una serie de relés (interruptores controlados electrónicamente), y que dispone de una conexión de red "moderna" y permanente como puede ser DSL, WiFi o Cable.

## **Ataques físicos originados desde el mundo lógico**

---

### **Correo postal**

No vamos a detallar más el completísimo artículo de Bruce Schneier sobre ataques físicos a través del correo postal, pero si queremos hacer puntualizaciones sobre sistemas de mensajería y paquetería.

Como el propio Schneier comenta, utilizando ataques automatizados mediante programas (pueden encontrar detalles adicionales en el artículo de Simon Byers, Avi Rubin y Dave Kormann, <http://www.avirubin.com/scripted.attacks.pdf>), podemos forzar subscripciones masivas a publicaciones impresas, que pueden llegar a desbordar el buzón (físico) de cualquiera.

Imaginemos un atacante que pudiera cancelar envíos importantes y urgentes, como documentos, objetos o llegando a extremos, sangre para transfusiones u órganos para trasplantes.

Estos últimos casos, podríamos clasificarlos como difíciles, pero no imposibles, máxime teniendo en cuenta que, podemos afirmar con cierta seguridad que la mayoría de los hospitales tendrán acuerdos específicos de distribución con empresas de mensajería (especializadas en este tipo de transportes), que a fin de cuentas, también pueden ser vulnerables.

### **Daños a la imagen personal y social**

Este tipo de ataques pueden afectar a las relaciones de individuos con su entorno social. Imaginemos a un ciudadano modelo que de pronto comienza a ver su correo inundado por publicaciones pornográficas de nivel extremo. En comunidades grandes, un ciudadano

cualquiera disfruta de cierto nivel de privacidad, pero en una comunidad pequeña podemos dar por descontado que el cartero es con seguridad un miembro más que puede o no hablar del contenido del correo de un individuo.

También, si nuestro buzón postal está fuera de nuestra casa, determinado tipo de paquetes son claramente identificables, y no hablemos ya de los paquetes que debemos recoger en la oficina postal.

¿Cuánto podría afectar a su imagen en la comunidad este tipo de correo o paquetes postales?

- *Subscripciones políticamente incorrectas:* Es un ejemplo inmediato, y es un caso que hemos visto a menudo; revistas de temática pornográfica remitidas falsamente a miembros relevantes de la comunidad. Conocemos particularmente casos de "bromas" que han tenido como víctima al sacerdote o la iglesia de la congregación local.
- *Compra y envío de materiales comprometidos:* En muchas ocasiones hemos escuchado casos de robos de números de tarjeta de crédito vía Internet. Con una tarjeta robada y los datos personales de una víctima, un atacante puede hacer mucho daño. Por ejemplo, comprando material sexual explícito y enviándolo a la casa de un inocente miembro de la comunidad, o incluso con ataques mas elaborados, como envíos ofensivos en nombre de otros etc.

### **Cambios en perfiles de cliente**

Cada día más entidades mejoran sus sistemas de información, para permitir al cliente gestionar o actualizar sus datos desde Internet o vía atención telefónica.

Pensemos en qué tipo de cambios podría imprimir un atacante a nuestros registros en esas entidades si fuera capaz de impersonarnos y fingir una necesidad de actualización.

En la gran mayoría de sistemas de atención telefónica nos piden datos personales que un atacante puede obtener si tiene la intención.

Por ejemplo, en muchos nos piden el número de la última factura que se nos remitió (que podría haber sido robada de nuestro buzón), o se nos pide nuestro nombre completo y número de identidad (que se puede obtener de los registros de una universidad).

- *Corrupción de la información:* Por ejemplo, reorientar nuestro correo postal a una dirección en la que nunca lo recibiríamos, o donde lo podría robar nuestro atacante, para poder utilizar nuestra identidad libremente. Cambiar nuestro número de cuenta, dando un número falso, de forma que todos los cargos que se hicieran en esta serían devueltos inmediatamente (lo que a posteriori podría provocar que nos cortaran el servicio por impago), o alteraciones en los detalles secundarios de cliente, lo que podría permitirle a un atacante poder falsificar una identificación o tarjeta (por ejemplo una tarjeta de pago de un centro comercial).
- *Desactivación de servicios:* El caso más molesto que podríamos encontrar es el de un atacante que decide dar de baja servicios que necesitamos. Por ejemplo, el

teléfono móvil, o incluso, el seguro médico. El teléfono, la conexión a Internet, suscripciones necesarias etc. todos estos servicios y muchos otros más pueden ser susceptibles de convertirse en víctimas de ataques.

### **Consumo fraudulento de recursos físicos**

Uno de los problemas que más de moda se están poniendo ahora mismo son los "Caballos de Troya" que manipulan la configuración del acceso telefónico de un usuario, para forzarle a realizar llamadas a través de número de pago con una tarificación especial.

En muchas ocasiones la víctima ni siquiera es consciente de que realiza llamadas a número con una tarificación mucho más elevada que la normal (incluso teniendo delante las facturas telefónicas).

Es de práctica común entre muchos sitios de pornografía el intentar insertar este tipo de troyanos en el sistema de una potencial víctima.

En el capítulo que dedicamos a los teléfonos móviles veremos que puede ser muy dañino un Caballo de Troya que redirige nuestras llamadas a un número con tarificación especial.

Incluso Caballos de Troya muy conocidos como Cydoor, Alexa y otros, que como principal función tienen la de capturar todos los movimientos de un usuario y aprender de sus costumbres para mostrarle publicidad personalizada, podrían llegar a convertirse en herramientas que pusieran en contacto al avatar virtual de un usuario con la persona física que lo representa en el mundo real.

Imaginen un Caballo de Troya que tras aprender los hábitos y costumbres del usuario, se encargara de enviarle publicidad postal personalizada y adaptada a sus gustos.

O peor, que este tipo de sistemas capturaran sus datos postales de, por ejemplo, la configuración de su programa de correo electrónico, y la distribuyeran entre ávidos anunciantes de productos pornográficos.

### **Maquinaria y hardware vulnerable**

- *Equipos informáticos:* Pienso que no hay duda de que los sistemas informáticos son vulnerables a ataques lógicos. Hasta la fecha se han observado ataques de todo tipo, clasificados principalmente en tres grandes grupos; ataques de negación de servicio, intrusiones (donde se puede producir o no manipulación), y robo de información. Pero el futuro próximo nos traerá amenazas voraces y tangibles, como nuevos gusanos (worms) con capacidades de inteligencia artificial, que, por poner un ejemplo, sabrían como adaptarse a diferentes plataformas, con capacidad de aprender nuevas técnicas de asalto, con capacidad de generar su propia "prole" de nuevos gusanos con limitadas (o no) capacidades de ataque. Un ejemplo que se nos ocurre, es el de un gusano que mantenga una conexión permanente con un sistema remoto, el cual le dota de una actualizada base de datos de todos los nuevos agujeros o ataques 0d ("zero Day"), de forma que este gusano modificaría su patrón de comportamiento cada cierto tiempo. Incluso este mismo gusano, podría incorporar su propio compilador que le permitiría generar sus propios binarios, que "nacerían" con alteraciones que les harían indetectables para las herramientas de

antivirus o los IDS. Un ejemplo de compilador en menos de un megabyte es TinyC, <http://fabrice.bellard.free.fr/tcc/>. Incluso con el propio Tiny C, se podrían crear gusanos capaces de interpretar código fuente en C, de forma que sin necesidad de compilar sus capacidades podrían ser infinitas. Debemos estar preparados para los verdaderos casos de ataques polimórficos y mutables, ya que las nuevas aplicaciones de software, y por ende, los gusanos, cada vez tienen más capacidades genéticas.

- *Teléfonos móviles, PDAs y redes PAN:* Hoy en día prácticamente todo el mundo tiene un teléfono móvil, tanto en el ámbito profesional como en el personal, en grupos de edad avanzada como en grupos de jóvenes y menores de edad, la mayor parte de las personas lo llevan veinticuatro horas al día, y de hecho, en occidente, hay más teléfonos móviles que ordenadores. Ni que decir tiene que el auge de las redes PAN (Personal Area Network, red de área personal), van a abrir muchas puertas de ataque al "espacio vital" de un usuario. Actualmente, mediante la tecnología de Blue Tooth, cualquier usuario puede construir su "burbuja de tecnología personal", quedando envuelto por una red de comunicaciones que enlaza todos los dispositivos electrónicos, creando un campo de posibilidades (y de posibles vulnerabilidades) enorme. Las posibilidades que un teléfono móvil o un PDA brindan hoy en día son abrumadoras, desde la posibilidad de localización geográfica vía GPS (o directamente, a través de la posición relativa a las celdas de cobertura GSM), llamadas internacionales, agenda, libreta de direcciones integrada, posibilidades de grabación de audio y video, posibilidades de hacer y procesar fotografías, y muchas otras más... Si, además, tenemos en cuenta que están comenzando a aparecer dispositivos como relojes con conexión móvil, como el "Spot" de Microsoft, y que la mayor parte de estos nuevos dispositivos, probablemente, terminarán utilizando las posibilidades avanzadas de las conexiones GPRS y UMTS, debemos plantearnos el futuro de estos dispositivos y sus efectos sobre nosotros en caso de sufrir un incidente de seguridad. Las opciones de los SMS y MMS (mensajes cortos multimedia) pueden permitir efectos tan curiosos como la negación de servicio de un teléfono a través de avalanchas de mensajes. Posiblemente asistiremos a una nueva generación de abusos y ataques a través de estas opciones multimedia y MMS. El abuso de la localización geográfica podría ocurrir en casos desde secuestradores y maníacos acechando a una persona, hasta empresas que registran, ya no donde compra la gente en la red, si no en que tiendas entra (recordemos la película de Tom Cruise, "Minority Report", <http://us.imdb.com/Title?0181689>), cuándo se detiene para tomar un helado, qué días toma café y con quien (cruzando los registros de cada persona), cuándo y con quién se relacionan determinados individuos, incluso pasando por "jefes" que comprueban cuando sus empleados salen o entran de la oficina, se levantan del escritorio, van al cuarto de baño, etc. Los márgenes de error en la localización geográfica van desde las tres a los diez metros, hoy en día. Incluso, la mayor parte de los operadores de teléfonos móviles incluso dan servicios que permiten a un usuario averiguar el momento en que otro usuario enciende o apaga su teléfono móvil, con el consiguiente efecto que tiene sobre la privacidad de este último. Las especiales opciones multimedia, como pueden ser la grabadora de vídeo, sonido y cámara de fotos, pueden convertirse en herramientas "espías" de un posible atacante, que a través de un Caballo de Troya que pudiera infectar el PDA o teléfono, podría activar remotamente el micrófono, la cámara de fotos o la grabadora de vídeo, convirtiendo la privacidad de un usuario en un concepto susceptible de ser verificado. El teléfono móvil y el PDA hoy en día son el primer computador que el ser humano transporta constantemente, prácticamente pegado a su piel (en algunos casos, aprovechando el propio cuerpo humano, para, por ejemplo, transmitir una

tarjeta de presentación, <http://www.almaden.ibm.com/cs/user/pan/pan.html>) y de forma completamente voluntaria, personalizándolo y convirtiéndolo en una extensión del propio ser. En muchos casos, forma parte de su identidad. ¿Cuáles son las consecuencias de padecer una "intrusión" en nuestro teléfono móvil? La pérdida de nuestras claves privadas de pago, posiblemente, puede ser una de las más graves, y pensemos, que si hay personas que interpretan el móvil como una extensión de su propio ser, es posible que depositen todo el peso de su confianza sobre este dispositivo, que en última instancia, es como cualquier otro "ordenador", y adolece de los mismos problemas de seguridad. ¿Cuál podría ser el coste económico de ser infectados por un Caballo de Troya que fuerce a nuestro teléfono móvil a lanzar todas las llamadas a través de un número especial internacional o de pago? ¿Podría un atacante utilizar nuestro teléfono móvil como punto de salto intermedio para realizar llamadas ocultando el verdadero origen de estas?

- *Electrodomésticos*: Hoy en día la domótica es una disciplina de uso común (ya en los años 80-90 hubo una explosión del interés general por la automatización de procesos en las casas). Hoy en día, podemos encontrar desde lavadoras y neveras que pueden ser gestionadas por Internet (observen los modelos de Siemens o de Ariston Digital), hasta complejos sistemas de televisión como pueden ser canales vía satélite o equipos como TiVO. Un ataque que afectara a los sistemas informáticos de una casa, podría provocar efectos graves sobre el funcionamiento de estos dispositivos. Recordemos las vulnerabilidades encontradas en los gestores de SNMP (CERT, <http://www.cert.org/advisories/CA-2002-03.html>), e imaginemos un ataque contra el gestor de uno de estos dispositivos caseros, provocando un mal funcionamiento y entre otros posibles efectos, el desague de una lavadora, la descongelación de un frigorífico o como efecto más espectacular, la proyección de pornografía (y/o publicidad) a través de TiVO (podría ser trivial modificar la configuración de las preferencias de un usuario de un servicio como TiVO teniendo acceso privilegiado a su dispositivo). ¿Qué otros dispositivos vamos a ver "conectados" en el futuro? ¿Hornos? ¿Calefacción? ¿sistemas de ventilación? ¿Maquinaria médica especializada?
- *Impresoras y Faxes*: En los 90 se puso de moda un ataque sencillo contra los dispositivos de Fax, que consistía en utilizar una hoja de papel negro, que una vez introducida en el Fax, quedaba convertida en una tira de papel infinito pegando con cinta los dos extremos del papel, de forma que cuando se enviaba ese Fax, el destinatario gastaba toda su tinta. Este era un ataque sencillo y destructivo, ya que provocaba una "negación de servicio" del Fax, y obviamente un gasto en el reemplazo del cartucho de tinta. Actualmente, muchas pequeñas empresas cuentan con dispositivos de Fax e Impresora integrados, y en muchas ocasiones integrados en un pequeño Modem que simula la oficina completa (por ejemplo, integrada en un portátil). ¿Cómo de seguros o cómo de vulnerables son estas completas soluciones de oficina portátil? Quizás habilitando nuestro simulador de Fax estamos abriendo la puerta a potenciales ataques remotos.
- *Sistemas de video-vigilancia y cámaras*: En grandes ciudades como Londres, París y Madrid, existen áreas urbanas controladas por sistemas de Circuito Cerrado de Televisión (CCTV). Por motivos de seguridad o protección, se controlan zonas y calles a través de complejas estructuras de cámaras y paneles de control. También, podemos encontrar cámaras de vigilancia en la mayoría de los cajeros automáticos, que, cada cierto tiempo toman imágenes de lo que tienen frente a ellos (que no tiene que ser por fuerza una persona justo delante de este). Muchos fabricantes (por

ejemplo Axis, 3Com, Cisco...) disponen de dispositivos WiFi que de una forma u otra habilitan a una cámara la posibilidad de emitir sus imágenes a través de ondas (con el consiguiente riesgo de interferencia o captura). Imaginemos un potencial atacante que ganara acceso a estos sistemas de CCTV, y los aprovechara en su beneficio, para por ejemplo controlar los movimientos de ciudadanos particulares o de importantes representantes políticos (la serie "24horas", protagonizada por Kiefer Sutherland, muestra el uso fraudulento y criminal que se le puede dar a las cámaras en un sistema de CCTV). Otras obras de ficción, como la película "Acosada" (de Sharon Stone), muestran como el uso de los sistemas de vigilancia de un edificio da poder infinito al "voyeur", que atentamente vigila los movimientos de todos sus vecinos. O en la serie de televisión "CSI" podemos encontrar un episodio en el que, un asesino, vigila a sus víctimas instalando sistemas de cámaras gracias a su acceso "privilegiado" como instalador del cable ("CSI", episodio 42). Imaginen lo vulnerables que nos encontraríamos si grupos criminales organizados pudieran acceder a los sistemas de vigilancia de nuestras casas, de nuestras empresas o de nuestras calles. La combinación de accesos a múltiples sistemas de CCTV, podría ayudar a grupos criminales a planificar el ataque a furgones blindados, transportes militares, o el seguimiento de víctimas.

- *Maquinaria controlada por ordenador:* Hay cientos de dispositivos que dependen de un controlador por ordenador, o que de alguna manera envían información a algún tipo de gestor informatizado. En entornos empresariales los sistemas SAP/R3 y la tecnología de MRP, parten del control de cada punto de la cadena de producción, de forma que podemos afirmar que, prácticamente, cada paso está gestionado por el sistema informático. Muchas industrias mantienen plantas de montaje o proceso a través de complejos robots, cuya gestión se realiza desde ordenadores, e incluso, muchas de las infraestructuras básicas que dan servicio a los ciudadanos dependen de la informática (sistemas de agua, electricidad, tratamiento de residuos...). Un ataque lógico que pudiera afectar a este tipo de infraestructuras podría ser catastrófico. Pueden encontrar un interesante documento sobre daños a las infraestructuras básicas en la página web de eEye Digital Security, <http://www.eeye.com/html/Research/Papers/DS20020724.html>, por Marc Maiffret. Potenciales víctimas de ataques en sistemas de maquinarias:
  - Semáforos: pensemos en las implicaciones de un ataque que pudiera afectar al control de tráfico, semáforos, carteles electrónicos... El riesgo potencial es inmenso.
  - Ascensores: en grandes edificios y rascacielos, el control de ascensores depende de un ordenador central. El acceso a este ordenador puede mantener a todo el edificio marginado del acceso a los ascensores.
  - Incendios: el sistema de incendios suele estar conectado a la gestión informática. Si un atacante pudiera activarlo de manera remota, ¿Cuánto dinero se perdería por daños ocasionados a través del agua o espuma de los antiincendios?
  - Sistemas industriales en la empresa: muchas industrias dependen del sistema informático para la gestión de la cadena de producción (redes de Petri por ejemplo). ¿Cuáles podrían ser los efectos de un ataque a los sistemas informáticos?
  - Sistemas industriales de servicio ciudadano: control de residuos, sistemas de agua, producción eléctrica, distribución de combustible, recicladores de aire en el Metro, etc.

- Otros: añadan a la lista todos aquellos sistemas que se les ocurran.

### **Traslación de la responsabilidad criminal**

Tradicionalmente esto se hace mediante técnicas de "IPspoofing" o de "rebote" en equipos informáticos ajenos. Lo que el atacante intenta es que la dirección origen de los ataques que lanza contra un sistema remoto no sea la suya, de forma que utiliza rebotes sobre otros sistemas (proxy por ejemplo) o técnicas avanzadas que le permiten esconder su dirección.

Pero, ¿y si el atacante lo que quiere es esconder su personalidad ciudadana? En Internet tenemos múltiples bases de datos que registran información sobre ciudadanos, entre ellas registros en universidades, censos, periódicos con noticias que involucren a un ciudadano...

Un criminal podría querer utilizar otra identidad para hacer compras vía Internet, para registrar un domicilio alternativo (y recoger compras fraudulentas a nombre de la víctima) o por muchos otros motivos.

Dentro de este tipo de intenciones, podemos incluir los ejemplos antes citados que incluyen el uso de tarjetas de crédito robadas, que pueden llevar a construir una personalidad simulada simplemente "pagando", y lo que es peor, pueden permitir a un potencial atacante "clonar" la identidad completa de algún otro ciudadano.

En EEUU y otros países, no existen el documento nacional de identidad, lo que hace que cualquiera con medios e interés, puede llegar a "crear" un documento falso (un carnet de conducir por ejemplo) accediendo simplemente a la partida de nacimiento de otro ciudadano (muchas veces se hace utilizando datos de ciudadanos muertos, o de niños muertos al nacer).

### **Inducción al crimen vía métodos lógicos**

En el libro "Distracción", de Bruce Sterling, viene una "técnica" de inducción criminal, realizada a través de las redes.

La idea es conseguir que una serie de asesinos potenciales (psicópatas por ejemplo), sientan la necesidad de actuar criminalmente contra una víctima. Esta técnica se realiza partiendo de una gran base de datos de personas con tendencias homicidas, a las que se bombardearía con información constante sobre la víctima a la que se quiere dañar.

Aunque es una teoría propia de una novela, no debemos olvidar que hay cientos de especulaciones sobre figuras tales como los "durmientes", los "asesinos Manchú" y entre otros, sobre el libro "El guardián entre el centeno" de J.D. Salinger, ISBN: 8420634093. Durante años se ha relacionado este libro con los asesinatos de John Lennon (Mark David Chapman), el intento a Ronald Reagan (John Hinckley) y otros.

En la CIA durante mucho tiempo se hicieron experimentos en control mental, como los proyectos BLUEBIRD y ARTICHOKE (que en el futuro se conocería como MKULTRA) demostraron.

En la película "Conspiracy Theory" de Mel Gibson, encontramos referencias directas al libro "El guardián entre el centeno" como un activador de asesinos.

¿Es posible inducir a cometer un crimen a personas predispuestas para ello? Esta es una pregunta compleja de responder, y debería ser analizada por especialistas.

Lo que es claro, es que a ninguno de nosotros nos dejaría tranquilo saber que alguien puede estar enviando, activamente, información nuestra a una lista de asesinos reconocidos o potenciales.

### **Notas y referencias**

---

- [1] "Distracción" - Bruce Sterling, ISBN: 84-8421-280-7
- [2] "Automated Denial-of-Service Attack Using the U.S. Post Office" - Bruce Schneier, <http://www.counterpane.com/crypto-gram-0304.html#1>
- [3] "El guardián entre el centeno" - J.D. Salinger, ISBN: 84-2063-409-3
- [4] "Tiny C", <http://fabrice.bellard.free.fr/tcc/>
- [5] Proyecto MKULTRA, <http://www.medals.org.uk/unosir/archives/mkultra.htm>
- [6] Chase The Sun, <http://www.chasesun.com>
- [7] eEye Digital Security, <http://www.eeye.com>
- [8] "CHO's Testimony on the Nation's Infrastructure Systems for a Congressional Subcommittee Hearing", por Marc Maiffret, <http://www.eeye.com/html/Research/Papers/DS20020724.html>
- [9] "PAN FACT SHEET", por Thomas Zimmerman, <http://www.almaden.ibm.com/cs/user/pan/pan.html>

Madrid, 18 de Abril de 2003