

**Internet: Hackers chilenos**  
**Noviembre 2006 .**

**Dossier . 8 artículos**

**Chilenos en el “top” mundial de los hackers**  
**Genios fuera de la ley**

**Betzie Jaramillo LN. 12 de noviembre de 2006**

*Están considerados como la tercera banda de sabotadores informáticos más importantes del mundo. Byond Hackers Team estaba integrado por un estudiante universitario, un cesante y unos gemelos adolescentes que mantuvieron en jaque a los servicios de inteligencia de medio mundo. La web de la NASA fue su máspreciado sabotaje. Y jamás ganaron un peso.*



¿Peligrosos ciberterroristas o genios vanguardistas? En cualquier caso, ellos están entre los tres primeros en el ranking mundial, pero no son deportistas ni serán recibidos en La Moneda. Todo lo contrario, arriesgan a pasar cinco años en la cárcel por sus habilidades como hackers. Un autodidacta cesante, un estudiante universitario y dos gemelos adolescentes derribaron las defensas de 8.075 webs de Chile, Argentina, Bolivia, Perú, Venezuela, Israel, Palestina y Turquía, y en EEUU atacaron nada menos que a la NASA interviniendo su página web durante cuatro minutos con la imagen de un niño ensangrentado y la leyenda “no war” (no a la guerra), en protesta por los ataques israelíes al Líbano. Y cabe la posibilidad que estos países pidan su extradición. “Detenida poderosa banda de hackers”, fue el titular que recorrió el mundo, y se destacaba que eran los terceros en importancia mundial, tras un grupo asiático y otro brasileño. Esa misma semana, la prensa internacional daba noticias de otros récords nacionales, como que los estudiantes chilenos son los que más consumen marihuana y tabaco de toda América Latina, según un informe de la ONU.

La “banda” Byond Hackers Team se constituyó como equipo en 2004 y sólo en dos ocasiones se conocieron personalmente. “Nettoxic”, “SSH-2”, “Codiux” y “Phnx” eran los “nicknames”, o sobrenombres, de Leonardo Hernández, de Rancagua, 23 años, estudiante de ingeniería mecánica y jefe del grupo; Carlos Amigo, 37 años, desempleado que vive con su madre en Ñuñoa, y los gemelos de 17 años Cristóbal e Israel, estudiantes de tercero medio del Colegio Cardenal Caro, de Buin. Estos

cuatro “cerebritos” fueron hasta la madrugada del 6 de noviembre un auténtico dolor de cabeza para las ciberpolicías de medio mundo porque “hackearon” páginas webs gubernamentales, organizaron guerras virtuales con Perú y Argentina, y en Chile entraron en las webs de Mega, Ticketmaster, Movistar, Comisión del Bicentenario, Comisión de la Tortura, y en la del Ministerio de Educación colgaron un mensaje pidiendo pase escolar gratis, y así hasta llegar a más de ocho mil sitios. Su intervención del sitio oficial de la NASA los catapultó a la cima del puñado de piratas informáticos más admirados por sus pares y más perseguidos por los servicios de inteligencia.

“¡Es por hobby!”, dijo Hernández, “Nettoxic”, el líder, cuando fue detenido por la policía, y aprovechó de expresar un deseo: “Me gustaría tener un notebook”. Y es que a pesar de su capacidad y conocimientos de informática, este joven y sus “socios” jamás lucraron con sus sabotajes y todo lo han hecho con sus computadoras comunes y corrientes y sus conocimientos de autodidactas. “Ellos actuaron sólo para estimular sus respectivos egos y con afán de competencia intelectual”, reconoció el inspector Gerardo Raventós. Un desafío intelectual que, de momento, tiene a los dos mayores de edad en prisión preventiva por 90 días, y a los gemelos, en libertad hasta que se decida su discernimiento.

¿Cómo consiguieron cazarlos? Con la ayuda de los servicios de inteligencia internacionales y un trabajo minucioso de infiltración de la Brigada del Cibercrimen, que como en las mejores películas se disfrazaron de obreros, de pasajero sentado a su lado en el colectivo, de compañero de estudios, hasta que a las cinco y media de la madrugada del lunes 6 detuvieron a “Nettoxic”, hijo de un empleado de Codelco, en su casa de Villa El Teniente en Rancagua, y luego a “SSH-2” en la vivienda que compartía con su madre en la avenida Grecia con Exequiel Fernández, en la comuna de Ñuñoa, donde se ofrecía para realizar trabajos de informática para paliar los cuatro años que lleva cesante. Los gemelos “Codiux” y “Phnx”, con residencia en Buin, se presentaron voluntariamente con sus padres y volvieron a su casa después de declarar por ser menores de edad. Y ya volvieron a clases. Los cuatro son hoy verdaderos héroes para la inmensa comunidad virtual de jóvenes del mundo que considera que sus sabotajes son monumentos contemporáneos a la libertad. LND

## **Hackers, crackers, seguridad y libertad**

**Manuel Castells.** 12 de noviembre de 2006

*... El filósofo Pekka Himanen argumenta convincentemente que la cultura hacker es la matriz cultural de la era de la información, tal y como la ética protestante fue el sistema de valores que coadyuvó decisivamente al desarrollo del capitalismo....*

Los hackers y su cultura son una de las fuentes esenciales de la invención y continuo desarrollo de Internet. Los hackers no son lo que los medios de comunicación o los gobiernos dicen que son. Son, simplemente, personas con conocimientos técnicos informáticos cuya pasión es inventar programas y desarrollar formas nuevas de procesamiento de información y comunicación electrónica (Levy, 1984; Raymond, 1999). Para ellos, el valor supremo es la innovación tecnológica informática. Y, por tanto, necesitan también libertad. Libertad de acceso a los códigos fuente, libertad de acceso a la red, libertad de

comunicación con otros hackers, espíritu de colaboración y de generosidad (poner a disposición de la comunidad de hackers todo lo que se sabe, y, en reciprocidad, recibir el mismo tratamiento que cualquier colega). Algunos hackers son políticos y luchan contra el control de los gobiernos y de las corporaciones sobre la red, pero la mayoría no lo son; lo importante para ellos es la creación tecnológica. Se movilizan, fundamentalmente, para que no haya cortapisas a dicha creación. El filósofo finlandés Pekka Himanen argumenta convincentemente que la cultura hacker es la matriz cultural de la era de la información, tal y como la ética protestante fue el sistema de valores que coadyuvó decisivamente al desarrollo del capitalismo, según el análisis clásico de Max Weber.

En la era de la información, la matriz de todo desarrollo (tecnológico, económico, social) está en la innovación, en el valor supremo de la innovación que, potenciada por la revolución tecnológica informacional, incrementa exponencialmente la capacidad de generación de riqueza y de acumulación de poder. Pero innovar no es un valor obvio. Debe estar asociado a una satisfacción personal, del tipo que sea, ligado al acto de la innovación. Eso es la cultura hacker, según Himanen: el placer de crear por crear.

En los márgenes de la comunidad hacker se sitúan los crackers. Los crackers, temidos y criticados por la mayoría de hackers, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos (Haffner y Markoff, 1995). Muchos crackers pertenecen a la categoría de script kiddies, es decir, bromistas de mal gusto, muchos de ellos adolescentes, que penetran sin autorización en sistemas o crean y difunden virus informáticos para sentir su poder, para medirse con los otros, para desafiar al mundo de los adultos y para chulear con sus amigos o con sus referentes en la red. Otros crackers, más sofisticados, penetran en sistemas informáticos para desafiar personalmente a los poderes establecidos; por ejemplo, a Microsoft o las grandes empresas. Y algunos utilizan su capacidad tecnológica como forma de protesta social o política, como expresión de su crítica al orden establecido. Ellos son quienes se introducen en sistemas militares, administraciones públicas, bancos o empresas para reprocharles alguna fechoría.

En suma, en la medida en que los sistemas informáticos y las comunicaciones por Internet se han convertido en el sistema nervioso de nuestras sociedades, la interferencia con su operación a partir de una capacidad técnica de actuación en la red es un arma cada vez más poderosa, que puede ser utilizada por distintos actores y con diferentes fines. Éstas son las acciones de los crackers, que deben ser absolutamente deslindados de los hackers, a cuya constelación pertenecen, pero con quienes no se confunden.

La vulnerabilidad de los sistemas informáticos plantea una contradicción creciente entre seguridad y libertad en la red. Por un lado, es obvio que el funcionamiento de la sociedad y sus instituciones y la privacidad de las personas no puede dejarse al albur de cualquier acción individual o de la intromisión de quienes tienen el poder burocrático o económico de llevarla a cabo. Por otro lado, como ocurre en la sociedad en general, con el pretexto de proteger la información en la red, se renueva el viejo reflejo de control sobre la libre comunicación.

*(\*) Extracto de lección inaugural del curso de la Universitat Oberta de Catalunya.*

-----

## **Captura de sujetos que intervinieron web de la NASA:**

### **Hacker entregó datos claves a la policía civil**

RODRIGO VERGARA V. 12 de noviembre de 2006

### **"Nettoxic" ofreció colaborar con la Brigada del Cibercrimen para convertirse en espía. Esto costó caída de su propio grupo.**

"Mekano vale callampa" y "Viva Bachelet" fueron los mensajes que quedaron en la hackeada portada de la página web de Megavisión ([www.mega.cl](http://www.mega.cl)). ¿Los autores? Cuatro personajes agrupados en un clan virtual denominado "Byond Hacker Team". Era el comienzo.

Leonardo Hernández Salas, de 23 años, "Nettoxic", era el personaje más dado a las entrevistas por las hazañas cibernéticas de la banda, y uno de los líderes junto a Carlos Patricio Amigo (37), alias "SSH-2".

Uno de sus colegas, "c0diux", el menor Cristóbal O.L.A. (17), señaló en su declaración ante la policía: "Hace tres meses aproximadamente decidimos junto a mi hermano ('phnx', Israel E.L.A. (17)) no continuar con los ataques, ya que 'Nettoxic' tenía cada vez menos cuidado con la discreción, al otorgar entrevistas y jactarse, ponía en peligro el resguardo de nuestras identidades...".

Pero "Nettoxic" iría más allá. Se ofreció como colaborador de la Brigada del Cibercrimen de Investigaciones. ¿La idea? Convertirse en espía y aportar con datos que vulneraban la seguridad nacional de otros países. Como registro de la propuesta quedan algunos correos electrónicos adjuntados a la carpeta de investigación. Entre ellos destaca uno del 14 de junio de 2006 titulado: "Quero (sic) ayudar en sus causas". Parte del texto señalaba: "Bueno soy NETTOXIC de TEAM BYOND HACKERS les escribo por las noticias y las simples vulnerabilidades que tienen los equipos gubernamentales y comerciales y bancarios chilenos (...) nosotros a veces tenemos accesos a documentos de países vecinos que es de gran utilidad para la nación...".

Es más, Hernández Salas programó una cita con una oficial de la policía en el pub "Entre Latas Light". Desde ahí, "Nettoxic" tenía nombre y rostro para los del Cibercrimen. La detención era cuestión de tiempo.

Pero faltaban dos integrantes del team. Amigo ("SSH-2") y Hernández ("Nettoxic") estaban identificados. "C0diux" y "phnx" no. Sólo siluetas en la presentación power point con que la policía mostró el caso a los fiscales a cargo y dos direcciones de e-mail: [dac0diux@gmail.com](mailto:dac0diux@gmail.com) y [byond.team@gmail.com](mailto:byond.team@gmail.com).

Estos dos correos, junto a [nettoxic@gmail.com](mailto:nettoxic@gmail.com) (Hernández) y [palestina1815@hotmail.com](mailto:palestina1815@hotmail.com) (Amigo), muchas veces quedaron como prueba de los ataques a las páginas. Con estos datos y mediante oficios a las empresas Microsoft, Terra y Telefónica se pudieron obtener direcciones IP, domicilios, fotos, rostros, pruebas, etc.

Todos fueron detenidos el pasado lunes 6 de noviembre. Era el fin. "Nettoxic" declaró a la policía sobre su grupo: "Nos dedicamos a dejar bien puesto el nombre de Chile en internet, a lo que concierne a ataques informáticos, por tal motivo teníamos que desfigurar una serie de páginas...", dice.

## MUNDIALES

SEGÚN algunas cifras que se manejan, el grupo estaría dentro de los tres primeros a nivel mundial por web hackeadas.

-----

### **Arresto de hackers genera ataques a web chilenas**

Pedro Lezaeta y Rodrigo Vergara 11 de noviembre de 2006

#### **Mensajes insertados piden liberación de "Nettoxic" y "SSH-2".**

Una decena de ataques a sitios web chilenos ha sido, hasta ahora, la respuesta de hackers por la reciente detención de dos de los suyos en la operación Byond, de Investigaciones.

En las páginas "desfasadas" o alteradas se pidió la liberación de los aprehendidos Leonardo Hernández (23), "Nettoxic", y Carlos Amigo, "SSH-2". Los autores de esta ciberguerrilla de protesta actúan bajo el nombre de Xtech Inc., parte del movimiento "Free Byond Crew".

#### **Ataque virtual por la encarcelación de Patricio Amigo, "SSH-2", y Leonardo Hernández, "Nettoxic":**

##### **Hackers apuntan a web de Investigaciones**

RODRIGO VERGARA V. 11 de noviembre de 2006

#### **Una decena de sitios han sido "bajados" de la red. Imputado llama a la calma desde la ex Penitenciaría.**

"...Es emocionante que los hackers del mundo nos apoyen (...) pienso que sería mejor mantener los ataques y protestas standby...".

Éste es parte del mensaje que Leonardo Hernández ("Nettoxic") -quien junto a Carlos Patricio Amigo ("SSH-2"), está en prisión bajo el cargo de sabotaje informático- hizo llegar desde la cárcel a un amigo.

Pero aunque el llamado es a la calma, la situación afuera es diferente. Hasta el cierre de esta edición, los ataques y desfases a sitios virtuales sumaban una decena. Y la página web de Investigaciones ([www.investigaciones.cl](http://www.investigaciones.cl)) está en la mira.

"Esto es sólo un aviso. Si los chicos (Hernández y Amigo) no salen en libertad, apuntaremos a algunos sitios especiales: gubernamentales, de las empresas que demandan y... la de los detectives", dice un miembro de la comunidad hacker, quien se reunió con "El Mercurio".

Entre las víctimas de las últimas horas se pueden contar una página en desuso de Telefónica Móvil, la sociedad Jardín Los Abedules, Criadero Chicureo y la empresa de refrigeración Doctor Cooling, entre otras.

El entrevistado adelanta que la defensa de los jóvenes detenidos apelará de la prisión preventiva. Si el pedido es rechazado, iniciarán una serie de acciones que, aparte de "botar" páginas web, incluye marchas en Santiago, México y España.

"Acá en Chile hay aproximadamente 250 personas de un poco más de 50

comunidades hacker que van a protestar", señala el joven.

Sobre si le tienen algún temor a la justicia y, en definitiva, tener el mismo destino que Hernández y Amigo, el hacker esgrime que la cárcel no es una alternativa para él.

"Yo no pondré las manos en el teclado. Serán otras comunidades de afuera. Es difícil que se pida una extradición para alguien que desde otro país atacó una página chilena", argumenta.

Así, es probable que la persona que inició los ataques hace un par de horas, quien firma como "Xtech Inc.", sea un extranjero.

En Investigaciones se informó que no es una situación que hayan abordado, porque no hay antecedentes concretos.

Los hackers chilenos habilitarán la dirección [www.br0z.org](http://www.br0z.org) para el registro de los ataques.

-----

#### **Investigación contra el cibercrimen:**

#### **Caen hackers que botaron web de la NASA**

HERNÁN ÁVALOS, FRANCISCO ÁGUILA. EM. 7 de noviembre de 2006

#### **Los cuatro integrantes del grupo fueron detenidos en allanamientos en Rancagua, Buin y Ñuñoa. Una pareja de gemelos de 17 años será llevada a discernimiento.**

Con allanamientos simultáneos en Rancagua, Ñuñoa y Buin, la Brigada contra el Cibercrimen de Investigaciones capturó ayer a cuatro hackers chilenos a quienes acusa de integrar el "Byond Team", responsable de derribar 8.075 páginas de la red internet.

La lista de sus víctimas incluye una veintena de gobiernos, además de organismos públicos y privados en Chile, Argentina, Perú, Venezuela, Israel, Palestina, Turquía y EE.UU., entre otros, el buscador Yahoo, incluso un sitio de la NASA, considerado como su máximo logro entre sus pares.

Su acción consistía en alterar los contenidos de las páginas web, con mensajes burlescos, nacionalistas o antibelicistas, contra las invasiones de EE.UU. a Líbano e Irak.

"Ellos actuaron sólo para estimular sus respectivos egos y con afán de competencia intelectual. No hemos encontrado intervenciones suyas con fines de lucro personal", señaló el inspector Gerardo Raventós, a cargo de la diligencia.

Aun así, podrían ser imputados de violaciones a la Ley de Delito Informático y recibir una pena de hasta seis años de prisión. (ver recuadro).

#### **Origen del team**

La investigación comenzó hace ocho meses por encargo del fiscal Carlos Gajardo, de

la fiscalía de Ñuñoa, luego que el canal de TV Mega denunciara la intervención maliciosa de su página Mega.cl.

El grupo de cuatro piratas nació en el ciberespacio a mediados del 2004, por intereses comunes en la computación, el pacifismo y la ecología. Sólo en dos ocasiones tuvieron reuniones "de cuerpo presente" y fue para conocerse y disfrutar lanzando ataques por la web, descifrar claves y vulnerar servidores.

Como líder fue individualizado Leonardo Hernández Salas, de 23 años, nickname "Nettoxic", estudiante de último año de ingeniería mecánica en Inacap de Maipú, residente de la villa El Teniente de Rancagua. "Es un joven tranquilo que vive con sus padres", señaló una vecina que salió en bata de levantarse para ver qué ocurría en el pasaje Calixto, con tanto despliegue de policías y vehículos.

Hernández involucró a su hermana, que vive en Santiago, por haber usado su computador en alguna de las operaciones pesquisadas. Pero ella carece de responsabilidad y no fue imputada. "Me gustaría tener un notebook", dijo a los detectives mientras era trasladado al cuartel central de calle General Mackenna, donde admitió su responsabilidad ante el fiscal.

Otro de los integrantes del "Byond Team" fue identificado como Carlos Patricio Amigo León, de 37 años, nickname "SSH-2", autodidacta residente en la esquina de Grecia con Exequiel Fernández, comuna de Ñuñoa, quien se gana la vida con trabajos esporádicos de informática efectuados a particulares y pequeñas empresas.

Los dos últimos son gemelos de 17 años, Cristóbal e Israel, quienes obedecen a los nicknames de "c0diux" y "phnx". Son residentes de calle Manuel Rodríguez en Buin y alumnos de 3.º medio del colegio "Cardenal Caro", de la comuna.

El inspector Raventós estimó que los cuatro tienen una personalidad "especial", pues por lo general los jóvenes de su edad destinan más tiempo al estudio, las muchachas, la diversión y el deporte, y nunca tantas horas a la computación.

"¡Es por hobby!", respondió Hernández Salas a los detectives que le exhibieron evidencias frente a su padre, empleado de la división El Teniente de Codelco. Éste se limitó a mover la cabeza, entre resignado y abatido por la situación.

Pena de 6 años de cárcel

El abogado Renato Jijena, especialista en derecho informático, señaló que los ilícitos del "Byond Team" pueden ser sancionados tanto en el lugar donde se iniciaron como en el que se consumaron. Agrega que el Código Orgánico de Tribunales de Chile otorga preeminencia al país desde donde salió el mensaje cibernético. Así, podrían ser juzgados por interceptación, interferencia o acceso computacional con el ánimo de apoderarse, usar o conocer indebidamente datos, y alteración, daño o destrucción de contenido, arriesgando penas de hasta seis años de cárcel, tres por cada delito.

## DESTINOS

"NETTOXIC" y "SSH-2" quedaron en prisión por "sabotaje informático". Los gemelos van a discernimiento.



-----  
Cómo la brigada del Cibercrimen capturó a "Nettoxic", "SSH-2", "Codiux" y "Phnx"

## **Seguimiento e infiltración: el virus troyano que desactivó a los hackers**

CARLA GALLEGOS MORAGA 7 de noviembre de 2006

*El grupo de piratas, agrupados en el Byond Hackers Team, sostuvo una "Guerra del Pacífico" con sus adversarios peruanos penetró las páginas de la NASA, entre otros web sites.*



"Son principiantes, seguro que los encuentra el Cibercrimen". Con estas palabras, y sin sospechar que estaba frente a sus propios captores, Leonardo Hernández (23), el líder hacker conocido por su alias "Nettoxic", pretendió demostrar su superioridad en asuntos informáticos.

Con un historial de más de ocho mil páginas web intervenidas y con un clan conocido a nivel mundial, el experto fue seguido durante meses por la Policía de Investigaciones, hasta que su capacidad para hacerse invisible lo traicionó.

La investigación se remonta a marzo de 2006, cuando una denuncia ingresada a la Fiscalía Oriente movilizó al prosecutor adjunto Carlos Gajardo y a un equipo especializado de la Brigada Investigadora del Cibercrimen y los puso tras los pasos del misterioso "Nettoxic".

Sin embargo, los antecedentes disponibles sobre el hacker, si bien daban cuenta de sus amplios conocimientos informáticos, no daban pista alguna acerca de su identidad.

Sólo se sabía que "Nettoxic" había avanzado por la red, que no era un "personaje" fácil de capturar y que sus ataques iban en ascendencia: de foros de jóvenes "computines", pasando por el sitio oficial de la NASA, gobiernos de diversos países con complejos sistema de seguridad informática como Estados Unidos e Israel, hasta desatar una verdadera ciberguerra contra pares peruanos y argentinos, con quienes el fuego cruzado fue la intervención de páginas gubernamentales en septiembre de 2005.

Además tenía múltiples vínculos en el extranjero.

### **¡¡Agentes en la matrix!!**

Iniciado el seguimiento de Hernández, apareció el dato de que cursaba ingeniería mecánica en Inacap y que junto a otras tres personas integraban un clan denominado Byond Hackers Team, responsable de la intervención de ocho mil 75 sitios.



Así, decididos a ubicarlos, los detectives del Cibercrimen se infiltraron en la vida de “Nettoxic”, creándose una existencia virtual para acercarse -desde el lenguaje, hasta el uso de disfraces- estar al tanto de la rutina diaria del genio informático.

Los efectivos lograron llegar a las reuniones sostenidas por hackers, colarse en sus fiestas y sostener conversaciones con los líderes, solicitando orientación para “llegar a ser como ellos”. Las respuestas siempre fueron arrogantes: “Son principiantes”, “son presa fácil para el Cibercrimen”.

En forma paralela y en la vida real, los detectives se vestían cada día de personajes distintos. Una jornada eran obreros de la construcción, en otra el pasajero que se sentaba al lado en el colectivo y en la siguiente el compañero de instituto que almorzaba en la mesa de enfrente. “Nettoxic” estaba rodeado.

Pero no sólo el líder estaba ubicado, sino también sus fieles guerreros con quienes se comunicaba por chat: Carlos Amigo alias “SSH-2”, y los gemelos de 17 años “Codiux” y “Phnx”.

El clan Byond Hackers Team es el tercero más importante a nivel mundial, antecedido por un grupo asiático y uno brasileño.

### **Sin antivirus**

Pese a sus diversas artimañas, el clan se volvió vulnerable y no hubo antivirus que lo protegiera. Esto, luego que la policía decidiera dar la madrugada de ayer el golpe final.

A eso de las 5:30 horas los carros policiales del Cibercrimen salieron en dirección a Rancagua, y en el domicilio de Calixto 01526 de la Villa El Teniente, “Nettoxic” fue el primer detenido.

En las horas posteriores los efectivos detuvieron además a Carlos Amigo (37) en su domicilio de Grecia con Exequiel Fernández en la comuna de Ñuñoa, y los gemelos ubicados en Buin, se presentaron voluntariamente a declarar, en compañía de sus padres.

A todos los involucrados se les incautaron computadores y especies relacionadas con la producción y almacenamiento de programas informáticos.

El inspector Gerardo Raventos, a cargo del procedimiento, lo calificó de exitoso y explicó que están ubicados la totalidad de los hackers de este clan.

“Las acciones de los cuatro implicados están sancionadas por la Ley 19.223 sobre delitos informáticos, y aunque aún no existen antecedentes de que se hayan efectuado robos vía Internet, por sus hechos arriesgan penas de hasta cinco años de presidio”, dijo Raventos.

### **Sabotaje informático**

Una vez que los cuatro hackers prestaron declaración, los dos adultos fueron trasladados hasta el Octavo Juzgado de Garantía para ser formalizados por diez delitos de sabotaje informático y destrucción de datos reiterados, que tiene una pena de tres años por cada antecedente estropeado, es decir una pena de 30 años. Sin embargo, el tribunal no aceptó el relato y sólo accedió a la formalización por el primer delito.

Finalizada la audiencia, los imputados fueron dejados en prisión preventiva durante los 90 días asignados a la investigación, luego que la defensa no lograra acreditar el arraigo social. Los menores quedaron a la espera de citación del Ministerio Público.

LN

## ¿Guerra del Pacífico virtual?

El 13 de septiembre de 2005 la página de la Oficina Nacional de Emergencias (Onemi) apareció hackeada o intervenida por un hacker peruano llamado “Cyberalexis”, líder del clan “Defacers”, integrado por limeños y argentinos. Los contenidos fueron alterados y en su lugar fueron puestas consignas antichilenas. La acción venía a coronar una batalla virtual seguida hacía meses.

Ese mismo día y en respuesta al ataque, el Byond Hackers Team encabezado por “Nettoxic” se apoderó del sitio del Poder Judicial peruano, asegurando en sus mensajes a toda pantalla que el pisco y el mar son chilenos. Además acusan a “Cyberalexis” de ser un Lammer.

Horas más tarde la víctima de la réplica peruana fue la página web del Ministerio de Hacienda chileno. Con un fondo negro y un mapa donde Chile aparecía con el nombre de Perú, emitiendo consignas contra los Byond.

Al día siguiente todos los hackers emprendieron retirada, a juicio compartido, porque el asunto se estaba escapando de las manos, lo que los hacía vulnerables.

---

## Ciber-glosario

**Hacker:** Experto que posee amplios conocimientos informáticos. Es capaz de crear sus propios programas de computación, y su saber lo utiliza sin razones raciales, políticas ni ideales.

**Craker:** Similar a un hacker, pero sus conocimientos son usados con fines delictivos, antimorales o incluso bélicos, como intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información, distribuir material ilegal, piratería, fabricación de virus, entre otros.

**Lammer:** Proyecto de hacker que utiliza programas creados por otros para intervenir sitios.

**Nickname:** Nombre virtual o seudónimo utilizado por los cibernautas para identificarse y resguardar sus antecedentes personales.

## Gravedad del delito aumenta cuando se dañan o alteran datos del sistema

Desde 1993 que existe en Chile una legislación que sanciona la comisión de delitos informáticos, pero existe poco conocimiento de sus disposiciones. “Tenemos tres tipos de delitos informáticos: el sabotaje, el espionaje informático y la piratería, pero que está incluida en la ley de propiedad intelectual”, explicó la abogada Lorena Donoso, directora del Centro de Estudios en Derecho Informático de la Universidad de Chile.

La profesional sostuvo que el delito de sabotaje -del que se acusó a los cuatro jóvenes ayer- es descrito como cualquier tipo de daño o alteración al sistema de tratamiento de la información y cualquier modificación a la información contenida en los sitios.

“En el fondo son delitos de daño contra las partes o componentes del sistema y los contenidos del mismo incluidas las alteraciones de éste”, precisó Donoso.

La norma también establece el delito de espionaje informático, que es el acceso no autorizado a los sistemas de tratamiento de la información, añadió.

## -¿A cuánto pueden llegar las penas que se aplican a estos delitos?

-El establecimiento de penas está elaborado en la medida que existan o no alteración de datos, es considerado más grave el delito cuando se cambian datos en los sistemas. En el caso de los tres delitos las sanciones van desde tres años un día hasta los cinco años y un día.

**-¿Cuál de estos ilícitos es sancionado con una pena mayor?**

-Las diferencias están dadas por las características del ilícito, por ejemplo, si provocas daño en el tratamiento de la información vas a estar entre el grado medio y máximo del rango estipulado.

**-¿Qué determina la ley para los menores de edad que incurren en estas faltas?**

-En el caso de los gemelos de Buin (17) que son menores, pero que bordean la mayoría de edad el endurecimiento o rebaja de las sanciones dependerá de si el tribunal los considera responsables y eso va a depender de lo que resuelva la instancia sobre si son sujetos con discernimiento o no.

**-¿Cree que la incidencia de estos delitos ha aumentado en los últimos años?**

-No diría que han aumentado pero sí que ahora se tiene un mayor conocimiento de este tipo de ilícitos. Estos temas saltan a la luz pública cada vez que hay algún hecho noticioso.

-----  
**En prisión preventiva quedaron dos de los “hackers” detenidos en la madrugada**

LN. 6 de noviembre de 2006

*El líder de la banda, Leonardo Hernández Salas (23 años), también conocido como "Nettoxic" y Carlos Patricio Amigo León, conocido con el alias de "SSh2", quedaron detenidos, luego de ser formalizados por el delito de sabotaje informático, mientras que los dos menores de edad aprehendidos fueron dejados en libertad luego de ser interrogados*



En prisión preventiva quedaron dos de los cuatro detenidos esta madrugada, acusados de hackear ocho mil páginas, entre las que se contaría la oficina aeroespacial de Estados Unidos, la NASA.

Luego de ser formalizados por el delito de sabotaje informático, el líder de la banda Leonardo Hernández Salas (23 años), también conocido como "Nettoxic" y Carlos Patricio Amigo León, conocido con el alias de "SSh2", quedaron detenidos.

En tanto, los dos menores, hasta ahora identificados sólo con sus nickname: "C0di0x" y "Phnx", detenidos en Buin, fueron puestos en libertad luego de ser interrogados.

El fiscal, Carlos Gajardo, pidió la prisión preventiva ya que aseguró que se podría probar su participación en el hackeo de 10 de las ocho mil páginas afectadas. Hernández Salas arriesga una pena de hasta cinco años de prisión, mientras que los gobiernos extranjeros donde se intervinieron sitios podrían pedir su extradición.

Los defensores de ambos imputados, los abogados Iván Santibáñez e Ignacio Osorio reclamaron por lo exagerada de la medida, alegando que la Ley de Delitos Informáticos data de 1993 por lo que estaría obsoleta.

Un amigo de los detenidos, Nassim Amer, declaró que a ellos "el ego les jugó una mala pasada tratando de mostrar lo capaces que eran" y descartó que hayan actuado buscando un interés económico o con el afán de hacer daño a las páginas intervenidas.

Además, explicó que la banda en la página de la NASA puso el rostro de un niño con esquirlas en la cara, con la leyenda de "no a la guerra" para protestar por la crisis en El Líbano.

El operativo respondió a una investigación de más de 8 meses desarrollada por los efectivos de la institución chilena a partir de antecedentes recibidos desde el exterior, en particular de servicios de inteligencia de EEUU, Israel y otros países sudamericanos.

La banda es considerada la tercera más importante del mundo, e Investigaciones indicó que entre las más importantes de las más de 8 mil intervenciones atribuidas al grupo se cuenta el hackeo de la página web de la NASA, de la Comisión de Agricultura de Chile, de sitios gubernamentales extranjeros como el del Poder Judicial de Perú, y otros en Colombia, Bolivia, Venezuela, Argentina, Estados Unidos, Turquía e Israel, además de páginas del Ministerio de Hacienda y del Pase Escolar.

-----

Entrevista con Víctor Carceler

**"Un hacker hace su trabajo con entusiasmo porque su motivación básica es aprender, divertirse, comunicar sus logros y conseguir reconocimiento social"**  
**Salvador López Arnal.** El viejo topo. Diciembre 2004

La delegada responsable de Microsoft en España ha declarado que su compañía tiene un plan, un plan sobre (o contra) el movimiento del software libre. Dice que han hecho trabajar a sus empleados de la sede central con los programas elaborados desde ese movimiento para (de)mostrarles sus inconvenientes y desventajas. La poderosa multinacional quiere probar, sin posible respuesta, que los postulados del movimiento son quiméricos (simple herencia sesentaoychista) y que los productos que salen de ese entorno no tienen un valor informático potente. Más allá de Windows, el caos y el sinsentido. Para hablar del movimiento del software libre hemos conversado con Víctor Carceler, ingeniero técnico en telecomunicaciones y profesor del ciclo formativo de grado superior de Administración de Sistemas Informáticos (ASI) en el IES Puig Castellar de Santa Coloma de Gramenet (Barcelona).

\*\*\*

*Si te parece podríamos iniciar la conversación precisando algunos términos. ¿Qué debemos entender por software libre? ¿Qué le diferencia del software propietario? ¿Es equivalente a software gratuito?*

Lo que se entiende por software libre tiene diferentes matices según quien esté utilizando el término. En cualquier caso, el concepto de software libre está relacionado con la libertad que tiene el usuario sobre el software para poder estudiarlo, adaptarlo, utilizarlo y, si fuese el caso, redistribuirlo.

En inglés se utiliza el término 'free software' con el mismo significado de software libre, no con el de gratuito que podría desprenderse del ambiguo término 'free'. Si el software se ha obtenido de manera gratuita o no es una cuestión básicamente comercial. De una u otra manera el usuario ha de contar con las mismas libertades.

Mi definición favorita de software libre es la de la 'Free Software Foundation' (en adelante FSF) que, como principal impulsor del proyecto GNU (que se inició en 1984 con el objetivo de conseguir un sistema operativo compatible con Unix que fuera software libre), ha contribuido de manera definitiva a la divulgación y aclaración del concepto. Puede consultarse esta definición en:

<http://www.fsf.org/philosophy/free-sw.es.html>

En la Wikipedia (una enciclopedia de contenido libre que se consulta y escribe desde cualquier navegador web) también se puede encontrar una entrada sobre el software libre. En este caso se matiza que el concepto se aplica tanto a determinado tipo de software como al movimiento que lo promueve. Puede verse esta definición en: [http://es.wikipedia.org/wiki/Software\\_libre](http://es.wikipedia.org/wiki/Software_libre)

La diferencia entre el software libre y el propietario es, pues, precisamente la libertad. Con el software propietario el usuario no la tiene. En general, no puede verificar lo que realmente está haciendo, o va a hacer, el software que ha adquirido, no puede adaptarlo a sus necesidades, se le imponen unas condiciones de uso y, desde luego, tampoco puede redistribuirlo.

Estas condiciones con frecuencia llevan a situaciones en las que el legítimo usuario de un producto encuentra un error y legalmente no está autorizado a corregirlo, o bien puede suceder que ese mismo usuario, que tiene guardados todos sus datos/obra en un formato que no controla, dependa de que determinado fabricante siga considerando que le conviene incluir soporte para dicho formato en sus productos.

*¿Pero entonces, si el fabricante considerara lo contrario, el usuario perdería su trabajo, todos sus archivos quedarían inutilizados?*

Si en el futuro no pudiese utilizar un software que entendiera el formato en el que originalmente se guardó la información, seguiría teniendo sus archivos pero no tendría manera de acceder a esta información. Su trabajo, en definitiva, se perdería.

*Desde instancias dirigentes de grandes multinacionales de la informática (léase, por ejemplo, Microsoft) se suele señalar que el movimiento por el software libre es un movimiento bienintencionado pero ineficaz. No es posible conseguir grandes cosas, buenos programas, con los procedimientos postulados por el movimiento. ¿Qué procedimientos son esos? ¿Crees que tiene alguna punta de veracidad esta crítica?*

Tratándose de Microsoft, sinceramente creo que se trata de una campaña de desprestigio hacia el software libre. Que el movimiento del software libre es muy eficaz se puede demostrar fácilmente con hechos. Algunas piezas de ingeniería que hacen que Internet funcione tal y como la conocemos son el servicio DNS...

*¿DNS? ¿Qué significan estas siglas?*

Domain Name System. Es el servicio de nombres de dominio que se encarga de mantener la relación entre nombres como [www.google.es](http://www.google.es) y la IP del servidor. La IP del servidor es la dirección de los ordenadores, de Google en este caso, pero para los humanos es más fácil recordar [www.google.es](http://www.google.es) que una serie de números.

*De acuerdo. Prosigue, si te parece.*

Citaba el servicio DNS y, además, están el correo electrónico y los servidores Web. Pues bien, el servidor DNS más ampliamente utilizado es Bind; el servidor de correo electrónico es Sendmail y el servidor Web por excelencia es Apache. Los tres servidores de reconocida calidad son software libre.

Pero hay más. Sin duda el producto de software libre que más eco social está obteniendo es GNU/Linux. GNU/Linux es un completo sistema operativo libre que actualmente se puede ejecutar tanto en dispositivos embebidos (móviles, agendas electrónicas) como en ordenadores domésticos (de diferentes arquitecturas) y en superordenadores. GNU/Linux ha mantenido un ritmo evolutivo vertiginoso. La colaboración permite partir de los desarrollos existentes para dar un paso más. Si además, al dar ese paso, el nuevo software mejor adaptado a determinada situación vuelve a estar disponible para toda la comunidad se produce una realimentación que acelera enormemente el proceso.

El mecanismo no es nuevo. Es exactamente el mismo que utiliza la comunidad científica al discutir sobre matemáticas, física o medicina. Todos podemos experimentar y publicar. Las buenas ideas son adoptadas por la comunidad y éstas no se guardan y no e deben guardar en secreto. No hay ni debe haber ocultación de información. Esto es lo contrario del espíritu científico verdadero.

*Luego, por tanto, las personas que colaboran en los proyectos son científicos o ingenieros informáticos. ¿Su trabajo es, entonces, trabajo voluntario, no remunerado?*

No tiene por qué ser trabajo sin retribuir. Es posible que una parte del software libre se desarrolle de manera voluntaria o por resolver problemas personales, pero también es perfectamente posible que dicho trabajo sea remunerado. Una empresa puede pagar a sus colaboradores por desarrollar determinado producto.

*Desde instancias similares a los que antes me he referido, suele también apuntarse que los programas del software libre son muy complicados de manejar, es decir, que el usuario sin conocimientos de informática se pierde en ellos, que están escritos pensando en los especialistas. Buenos, de acuerdo, pero para pocos. ¿Es el caso?*

*¿Hay que ser un informático profesional o poseer muchos conocimientos informáticos para manejar productos del free software? ¿Es más fácil el Word que el Writer, que el OpenOffice, por ejemplo?*

No hay ninguna razón para que el software libre sea más complicado de utilizar o requiera una mayor formación que el software propietario.

Ahora bien, tradicionalmente muchos de los desarrollos del software libre han nacido en ámbitos académicos o técnicos para dar respuesta a problemas concretos de ingeniería, investigación y áreas similares. En estos casos se trata de software específico que está dirigido a usuarios expertos en un determinado campo y, consiguientemente, no es justo comparar la facilidad de uso de estas herramientas con el software de propósito general.

Pero, además, actualmente el software libre cuenta con un gran abanico de herramientas enfocadas al usuario final. Hay multitud de distribuciones de GNU/Linux que compiten entre ellas por conseguir la instalación y un uso más sencillo. Hoy en día, instalar una distribución de GNU/Linux como Mandrake, Suse, Ubuntu u otras no plantea ningún problema, de hecho consiste en contestar siguiente, siguiente, siguiente... durante el proceso de instalación y se termina con un SO plenamente operativo.

La facilidad de uso de las distribuciones de GNU/Linux modernas es tremenda. Un usuario final encontrará todas las herramientas para navegar por la web, leer el correo, escribir textos, trabajar con hojas de cálculo o con programas de dibujo, y con muchas aplicaciones más totalmente a punto para ser utilizadas. Hay que recordar que en el campo del software privativo, el usuario tras la instalación del Sistema Operativo, se encuentra desnudo y sin ayuda: tiene un Sistema Operativo carente de aplicaciones de ofimática, de desarrollo, de manipulación de gráficos y un largo etc. Todas esas aplicaciones las debe adquirir como productos independientes.

Además, hay que resaltar que la naturaleza cooperativa del software libre implica algunas ventajas. Por ejemplo, los programas se traducen a muchas lenguas. Es verdad que nada impide al software propietario hacer lo mismo, pero muchas veces Microsoft ha argumentado por ejemplo, que traducir sus productos al catalán no resulta rentable. Y ha publicado la traducción para determinados productos después de que la Generalitat de Catalunya pagase a Microsoft por la adaptación de esos productos al catalán. Esto es así, no es tan sólo una posibilidad.

El problema con frecuencia es que estas traducciones llegan tarde, cuando ya existen versiones nuevas del software en el mercado, que por supuesto han salido sin ser adaptadas al gallego, al catalán, al vasco o al danés, pongamos por caso.

El software libre permite a todos participar en su desarrollo, de manera que si, por ejemplo, la Generalitat catalana, el gobierno holandés o la presidencia peruana deciden que es interesante contar con OpenOffice en catalán, en holandés o en el español de Perú, los mismos técnicos de la administración pueden aportar la localización al proyecto general.

Actualmente OpenOffice.org cuenta con 33 idiomas nativos -soportados en el proyecto principal, hay adaptaciones fuera del proyecto principal para otras



lenguas- que van desde el árabe al vietnamita incluyendo el catalán, el castellano y el euskera entre otros.

*Desde el movimiento del software libre se critica en ocasiones la mala calidad y el espíritu estrictamente comercial de muchos de los productos vendidos por empresas del sector informático privatista que se presentan como el no va más de la última (y supuestamente imprescindible) innovación científico-tecnológica ¿Podrías darnos algunos ejemplos de ello?*

En el software privativo es fundamental el marketing del producto, y algunas veces estos aspectos comerciales pueden tener mayor prioridad que los aspectos funcionales. Al fin y al cabo, se trata de vender cajas cerradas que no pueden desmontarse para ver qué contienen.

Pueden citarse diversos casos en los que la propaganda ha enviado mensajes contradictorios. Por ejemplo, mientras Microsoft comercializaba Windows NT, que es un sistema operativo destinado a servidores, argumentaba que las cuotas de disco eran una característica innecesaria, tal vez porque Windows NT no contaba con soporte para las cuotas. En cambio, en la siguiente versión de su producto, Windows 2000, finalmente se incluyeron esas cuotas de disco. En ese momento, Microsoft argumentó, en contra de lo dicho anteriormente, que se trataba de *una característica fundamental*. La verdad es que en un servidor las cuotas de disco son necesarias ahora, en los tiempos de Windows NT y también antes.

*Luego, por tanto, si no te sigo mal, se han dado conscientemente informaciones falsas o como mínimo inexactas.*

Microsoft tiene mucho cuidado en sus declaraciones. Las cuotas de disco no eran necesarias, según ellos, aunque otros sistemas operativos las soportaban. Pero, mientras defendían esto públicamente, trabajaban para incluirlas en su próxima versión del mismo producto.

Otro ejemplo de informaciones tendenciosas es cuando Microsoft llama 'característica técnica no documentada' a las vulnerabilidades que se descubren en sus productos. La función del eufemismo es obvia.

Probablemente la mayor evidencia de que los aspectos relacionados con el marketing tienen una prioridad más alta que los aspectos técnicos se encuentra en el campo de la seguridad. Cualquier usuario de Windows está acostumbrado a la existencia de software antivirus, que le protegen de virus con diferentes nombres pero que, básicamente, siempre han hecho lo mismo: llegar por correo electrónico y reenviarse a todas las direcciones guardadas en su agenda. El usuario ha llegado a aceptar como un mal menor, la existencia de estos virus, programas maliciosos y otra fauna, cuando en realidad debería haber montado en cólera por las deficiencias de su software y exigir responsabilidades.

Los medios de comunicación hablan de virus y gusanos de Internet, cuando, si fueran más cuidadosos, en el 99% de los casos deberían hablar de fallos, deficiencias y vulnerabilidades de determinados sistemas operativos o programas.

Los sistemas operativos y productos libres puede que no sean perfectos. Puede que contengan algunos errores de implementación, pero estos errores se corrigen rápidamente en cuanto se descubren. Además, durante el desarrollo de estos

productos, la seguridad y la eficiencia son aspectos de la máxima prioridad. Y en ningún caso, una vulnerabilidad en un producto software se utiliza para decir al cliente 'Este fallo no existe en nuestra nueva versión. ¡Cómprala!', como con frecuencia se hace en el mundo del software privativo, en el que dejar de dar soporte a una versión obliga a los usuarios a adquirir la próxima versión del mismo producto.

Curiosamente cuando compraron la primera versión, la propaganda decía que era maravillosa, pero el contrato licencia del usuario final -que, desde luego, nadie lee- probablemente advertía de que si el software no cumplía con su función anunciada el fabricante carecía de responsabilidad.

*Has dado razones que explican el interés de la comunidad científica informática en el movimiento del software libre, pero acaso el movimiento tenga interés también para el ciudadano no especializado en ese ámbito. ¿Es así? ¿Podrías exponer brevemente los beneficios ciudadanos del software libre?*

Gracias al software libre un ciudadano puede disponer de un potente y moderno Sistema Operativo como GNU/Linux, FreeBSD u otros, en los que se pueden ejecutar toneladas de software libre que prácticamente cubren cualquier necesidad que pueda tener el usuario final. Gracias al software libre, un ciudadano que utiliza GNU/Linux no se debe preocupar por ficheros infectados adjuntos en mensajes de correo electrónico, puede acceder de manera continua a actualizaciones y a nuevas versiones del software y puede contar con un sistema a medida que se le ajusta como un guante. Con GNU/Linux un usuario cuenta con la posibilidad de escoger qué distribución utiliza y qué software instala.

Igualmente, gracias al software libre un ciudadano puede utilizar con libertad herramientas como el navegador Mozilla, el software de seguridad GPG, el de ofimática OpenOffice.org o el programa de gráficos Gimp, por apuntar cuatro aplicaciones entre la multitud de posibilidades. Cuando el usuario utiliza una herramienta que es software libre, puede estar razonablemente seguro de que la herramienta no incluye características indeseadas como *spyware*, *puertas traseras* o publicidad. Da igual que el usuario no sea capaz de leer y entender el código fuente de la aplicación. Como el código está disponible, otros lo leerán y expondrán todos los trucos sucios que pueda incluir.

El software libre, por su propia naturaleza, en la que el código fuente está disponible para que cualquiera lo revise y adapte, cuenta, en mi opinión, con las siguientes características: 1. Es seguro. 2. Es eficiente. 3. Resuelve los problemas de los usuarios, en lugar de condicionar a estos a trabajar del modo que desea el fabricante. 4. Impide abusos de poder en los que el fabricante impone su política de precios. 5. Fomenta el desarrollo tecnológico y divulga el conocimiento.

*Martin Michlmayr, director del proyecto Debian, uno de los distribuidores de software libre, señalaba (auto)críticamente que una de las, digamos, no virtudes de este movimiento, de este software era la lentitud de sus innovaciones. Seguros, muy seguros, pero poco modernos. ¿Estaréis de acuerdo con esta crítica?*

Debian es una gran distribución de GNU/Linux que cuenta con unas reglas bien establecidas desde hace tiempo para determinar qué piezas de software se incluyen. Uno de los objetivos de Debian es la estabilidad. Esta es incompatible con utilizar versiones que no han sido probada exhaustivamente, por ello, en la versión estable

de Debian -existe otra de desarrollo-, tal vez no se incluyan las últimas versiones de los programas seleccionados. Pero esto, si acaso, es una característica específica de Debian, no del software libre, que es tremendamente creativo e innovador.

*¿Existe alguna relación entre el movimiento del software libre y el copyleft?*

El *copyleft* es el instrumento que se utiliza para traspasar junto con el software, su código fuente y las libertades para estudiarlo, utilizarlo, adaptarlo y redistribuirlo, asegurándose de este modo que todos lo podrán utilizar pero que, en ningún momento, alguien pueda secuestrarlo, para su beneficio exclusivo, realizando muchos o pocos cambios y convirtiéndolo en software privativo.

El copyleft es el instrumento que utiliza habitualmente la FSF para publicar el software del proyecto GNU. Sin copyleft, el software también puede ser libre; por ejemplo, el software de dominio público, pero nada impide que alguien realice software privativo a partir de él.

*¿Pero esto no sería contradictorio con uno de los postulados básicos del movimiento?*

Hay muchas personas que así lo entienden, y por eso defienden licencias tipo BSD u otras que dan total libertad sobre el código, incluso permiten hacer a partir de él software privativo. Pero el copyleft no tiene por objetivo restringir las libertades, sino más bien incentivar el desarrollo de software libre y asegurarse de que en el futuro nadie lo capturará para su uso exclusivo y excluyente. El copyleft es el medio legal para asegurarse de que quien utiliza una pieza de software libre y la modifica, o adapta de alguna manera, no recorte sus libertades fundamentales.

En ocasiones el copyleft levanta polémica. Por ejemplo, Microsoft ha declarado que la licencia GPL -la licencia que utiliza el proyecto GNU de la FSF- es una licencia vírica porque infecta. Es decir, cualquiera puede partir de software GPL para desarrollar un nuevo software. Pero este elemento derivado del original debe seguir siendo GPL. Ese es el tipo de “infección” al que se refiere Microsoft: no se pueden tomar desarrollos GPL y tras alguna modificación venderlos como desarrollos cerrados.

Evidentemente el copyleft no es un virus sino una defensa y una especie de contrato social. Muchas veces la industria se ahorra costosos gastos de desarrollo al utilizar software GPL. Por ejemplo, Cisco, un conocido fabricante de equipos de comunicación, utiliza el núcleo Linux en algunos de sus equipos con más éxito de ventas. Cisco se ha ahorrado las incontables horas de desarrollo que hay detrás del núcleo Linux, pero, a cambio, la comunidad recibe las modificaciones que Cisco hace al núcleo Linux para que se pueda ejecutar en sus productos. Si el copyleft no protegiese a Linux, Cisco lo podría haber utilizado sin devolver nada. Eso es lo que puede ocurrir al utilizar licencias que no incluyen en copyleft. Por ejemplo, hay diferentes sistemas operativos libres que descenden de Unix BSD. Al ser excelentes piezas de software y al utilizar una licencia sin copyleft, en muchas ocasiones las empresas han tomado el código para su beneficio sin retornar nada a cambio. Este es el tipo de software libre que Microsoft no considera vírico: un software que le ahorra costes de desarrollo y puede utilizar dentro de sus productos sin, además, dar crédito de ello.

*Pero Microsoft no debe ser la única empresa a la que le gusta tomar sin devolver nada a cambio. ¿Qué tal se porta Apple?*

Apple vende un sistema operativo muy bonito que se llama MacOS X. Pues bien, MacOS X está basado en software libre. El núcleo del sistema se llama Darwin, y es una implementación de un núcleo BSD. El navegador Safari, utiliza mucho código de Konqueror, un gran navegador muy utilizado en GNU/Linux. Pero esta semana he leído, aunque no pueda confirmarlo con toda seguridad, que Apple ha incluido una cláusula en los contratos con sus desarrolladores que les impide colaborar con proyectos de software libre en su tiempo libre. Es escandaloso. Algunas veces empresas como Apple mantienen posturas antagónicas, en ocasiones colaboran con el software libre y en ocasiones lo consideran un adversario.

*¿Qué papel juegan Richard Stallman y Linus Torvalds en el movimiento?*

Son dos grandes hackers. Richard Stallman lanzó en 1984 el proyecto GNU que pretende desarrollar todo un sistema operativo y sus aplicaciones como software libre bajo la licencia GPL, que está protegida por el copyleft. Stallman desarrolló diferentes piezas de software y aún mantiene un famoso editor de textos que se llama Emacs. Pero la razón por la que más se le conoce es por su energía en divulgar la idea de software libre que promueve la FSF.

Linus Torvalds inició el desarrollo de un núcleo tipo Unix que se pudiese ejecutar en ordenadores domésticos de bajo coste. El proyecto pronto despertó un gran interés y personas de diferentes puntos del planeta, que no se conocían físicamente, comenzaron a colaborar. En 1991 nació el núcleo Linux.

Para tener un sistema operativo completo se necesita un núcleo y un montón de aplicaciones y servicios. Si bien el proyecto GNU contaba con un gran número de aplicaciones, tenía algún problema con su propio núcleo. Por otro lado, una de las motivaciones para desarrollar Linux fue poder ejecutar software GNU, así que pronto se completó el sistema operativo libre conocido como GNU/Linux y que combina las dos piezas fundamentales.

Actualmente, Stallman defiende el software libre como presidente de la FSF y Torvalds coordina el desarrollo del kernel Linux.

*¿Kernel Linux? ¿Qué es el kernel?*

El Kernel es el núcleo del sistema operativo, la parte que se encarga de trabajar a bajo nivel comunicándose con el hardware, creando y manejando procesos, haciendo operaciones básicas que el resto del sistema operativo necesita para poder funcionar.

*Hablabas, al referirte a Stallman y Torvalds, de grandes hackers. Pero, ¿un hacker no es un “pirata”, aunque sea del ámbito de la informática? ¿Cuál es la filosofía de un hacker? ¿Destruirlo todo, arrasar con todo lo instituido?*

Los medios de comunicación hablan de hackers cuando se produce cualquier tipo de ataque o acto ilegal. En realidad deberían hablar de crackers. Un hacker es una persona apasionada por un determinado tema. En este caso, por temas tecnológicos. Un hacker hace su trabajo con entusiasmo porque su motivación básica es aprender, divertirse, comunicar sus logros y conseguir reconocimiento social.

*Podríamos hablar entonces de hackers de la pintura, de la filosofía o de la matemática.*

Efectivamente. Usando de forma correcta esta terminología la respuesta es afirmativa. Picasso fue un hacker de la pintura, Gauss lo fue en el ámbito de la matemática.

*Uno de los mayores escándalos del mundo actual es el abismo creciente entre algunos sectores minoritarios de países enriquecidos y multitudes excluidas de ciudadanos empobrecidos. Las nuevas tecnologías no parecen disminuir las distancias. ¿El movimiento del software libre se plantea llegar de alguna manera a estas numerosas capas sociales marginadas de todo avance tecnológico?*

Aunque ya he comentado que el software libre no tiene que ser gratuito forzosamente, es evidente que en la práctica, gracias a la libertad de poderlo redistribuir, es posible adquirirlo a muy bajo coste o sin coste. Esta es la razón por la que cualquier persona puede disponer de este software sin necesidad de contar con grandes ingresos.

Tal vez el software libre no se pueda comer, evitando así el hambre, pero gracias a él todo el mundo -insisto, todos los ciudadanos del mundo sin exclusión- puede contar con herramientas de desarrollo y herramientas con las que estudiar y trabajar, sin quedarse atado a determinadas condiciones de uso del fabricante que o bien limitan el provecho que se puede sacar del software o bien determinan la dependencia del usuario.

Gracias al software libre, en cualquier centro educativo del planeta que cuente con algún ordenador, se pueden utilizar las mismas herramientas avanzadas. Así, tanto en Helsinki, en Barcelona como en Nueva Delhi, se puede utilizar el compilador GCC, el programa de gráficos Gimp o el software ofimático OpenOffice.

El software libre no puede acabar con todas las desigualdades de un plumazo, pero en cuanto al uso de los recursos de software es una herramienta con un gran poder de divulgación y de equiparación.

*¿Hay alguna experiencia de interés en el uso institucional del software libre? ¿Qué ventajas, si existen, ha reportado? ¿Podrías darnos algún ejemplo?*

Hay muchas experiencias de uso del software libre en el ámbito institucional. Alemania, Reino Unido y Suecia promueven el uso del software libre en su Administración. Países como Brasil, Venezuela o China también tienen importantes experiencias en el uso del software libre.

Las razones para pasar a utilizar software libre pueden ser muy diferentes. Una administración puede buscar independencia tecnológica de otras potencias, puede buscar el modo de ofrecer un mejor servicio a sus ciudadanos, puede pretender reducir el coste de los sistemas de información o puede asegurarse de que la inversión en sistemas de información generará riqueza y desarrollo locales.

De todos modos, no hay que irse muy lejos para ver experiencias en el uso institucional del software libre. En España, por ejemplo, distintas administraciones autonómicas (Andalucía, Extremadura y Valencia, entre otras) han utilizado con éxito software libre en su Administración. El caso de Extremadura es

probablemente la punta de lanza en España. La Junta de Extremadura ha desarrollado una distribución de GNU/Linux específicamente adaptada a las necesidades de la administración extremeña. Esta distribución se utiliza en diferentes ámbitos: educación, sanidad... Los resultados han sido tremendamente positivos. Una evidencia es que en Extremadura, gracias a los ahorros en costes de licencias, se cuenta con un ordenador por cada dos alumnos en los centros educativos públicos. Otra evidencia es que gracias a Linex, se está potenciando en gran medida la industria tecnológica en Extremadura, donde se realizan desarrollos que tienen eco internacional.

Así, pues, gracias al software libre, la Administración de Extremadura puede ofrecer a sus ciudadanos un mejor servicio al utilizar herramientas en las que priman el rendimiento y la seguridad por encima de aspectos de marketing. Además, de resultados de utilizar software libre, la Administración puede auditar el funcionamiento interno del software utilizado, adaptarlo a sus necesidades y asegurarse de que la información de sus ciudadanos, se guarda en formatos abiertos a los que se podrá tener acceso en el futuro sin ningún problema.

Conviene resaltar que Microsoft considera que el uso del software libre en la Administración Pública atenta contra la libre competencia, y que tras la presentación de Linex en 2002, Microsoft dedicó una partida de sus productos para Extremadura como una donación para las áreas más deprimidas de España. Evidentemente, Microsoft tiene mucho interés en que no se extiendan los casos de uso de software libre en la administración pública y para eso utiliza los medios que tiene a su alcance.

*Juntamente con otros compañeros de trabajo, tú has organizado en Santa Coloma de Gramenet, una población del extrarradio barcelonés, una red ciudadana denominada XEILL (Xarxa Educativa i Lliure, red educativa y libre). ¿Podrías explicarnos en qué consiste este proyecto?*

La XEiLL es un proyecto educativo en el que se pretende estudiar las posibilidades de los medios tecnológicos aplicados a la docencia.

La XEiLL es una red telemática, educativa y de libre acceso. Es una experiencia en la que participan los alumnos de ciclos formativos de familias relacionadas con las tecnologías de la información. En la red están integrados diferentes centros educativos que participan voluntariamente en el proyecto. La red la montan, administran y mantienen alumnos de formación profesional y en ella participan centros educativos de primaria o secundaria.

Para los alumnos de ciclos, la red es una fuente de motivación y de experiencia real. Para los centros educativos que participan, la red es una herramienta más que tienen a su disposición para realizar distintas actividades didácticas.

Una característica fundamental de la XEiLL es que utiliza la tecnología inalámbrica WiFi (un conjunto de estándares para redes inalámbricas), de modo que simplemente acercándose a un centro educativo que mantiene un nodo de la XEiLL se puede conectar con dicha red.

Es una red de acceso libre en cuanto no hay ningún control administrativo para conectar con ella. Cualquiera puede acercarse a un centro educativo, conectar con la XEiLL y acceder a los recursos que ofrece. Precisamente, este acceso sin trabas

es ideal para alcanzar los objetivos del proyecto, entre los que se incluyen: 1. La divulgación de las nuevas tecnologías. 2. Fomentar la colaboración entre los centros educativos. 3. Acercar los centros educativos a su entorno social 4. Evitar situaciones de exclusión social en cuanto a recursos tecnológicos.

Finalmente, quiero comentar que aunque para conectar con la XEiLL se puede utilizar cualquier Sistema Operativo (sea este privativo o libre), toda la infraestructura de la red y todos sus servicios están basados en software libre.

*Dos preguntas más para finalizar. Te ruego brevedad. Microsoft ha informado que ha llegado a un acuerdo con los gobiernos de treinta países amigos (incluyendo, entre ellos ,a China y España) a los que va a abrir el código de sus productos o parte de él. Luego, por tanto, la "gran empresa " también practica el software abierto". Eso sí, a sus amigos, sólo a sus amigos.*

Esta opción que ha tomado Microsoft se debe a que no puede competir en igualdad de condiciones con al software libre y a que distintas Administraciones han mostrado claramente su interés por este software. Microsoft deja ver parte de su código, para que las administraciones o organismos amigos, puedan verificar su contenido. Pero lo que Microsoft no deja es modificar ese software ni adaptarlo ni por supuesto redistribuirlo. Tampoco deja ver el código completo del producto. Por tanto, es más un movimiento de publicidad que otra cosa. En la práctica no se puede asegurar que el software que se ejecuta cuando se compra el producto y el código fuente que Microsoft muestra tengan algo en común a no ser que este código fuente se compile y se comparen los binarios obtenidos con el producto original. En las condiciones del acuerdo propuesto por Microsoft, eso no se puede hacer. Además, quien tenga acceso a parte del código, se compromete a no desarrollar productos que pudieran ser competencia de Microsoft. Las limitaciones son evidentes, y su filosofía también.

*Por otra parte, ha corrido estos días la noticia de la vulnerabilidad de los ficheros JPEG y la posibilidad de perder el control del ordenador al navegar con Internet Explorer.*

Debido a un error de programación en el código que maneja las imágenes JPEG, algunos programas como Internet Explorer y Outlook pueden comprometer el ordenador del usuario que visualiza esta imágenes.

Simplemente se trata de una vulnerabilidad en el software de Microsoft, tal vez sea especialmente llamativa por lo evidente del fallo. Pero lo importante es mostrar que no hay nada perfecto, así que si el código está expuesto para que todo el mundo lo pueda revisar, como en el caso del software libre, entonces todos podremos estar más tranquilos.

*Nota: Una versión de esta entrevista apareció en la revista El Viejo Topo, nº 200, diciembre de 2004.*





Información disponible en el sitio ARCHIVO CHILE, Web del Centro Estudios “Miguel Enríquez”, CEME:

<http://www.archivochile.com>

Si tienes documentación o información relacionada con este tema u otros del sitio, agradecemos la envíes para publicarla. (Documentos, testimonios, discursos, declaraciones, tesis, relatos caídos, información prensa, actividades de organizaciones sociales, fotos, afiches, grabaciones, etc.)

Envía a: [archivochileceme@yahoo.com](mailto:archivochileceme@yahoo.com)

**NOTA:** El portal del CEME es un archivo histórico, social y político básicamente de Chile. No persigue ningún fin de lucro. La versión electrónica de documentos se provee únicamente con fines de información y preferentemente educativo culturales. Cualquier reproducción destinada a otros fines deberá obtener los permisos que correspondan, porque los documentos incluidos en el portal son de propiedad intelectual de sus autores o editores. Los contenidos de cada fuente, son de responsabilidad de sus respectivos autores.

© CEME web productions 2003 -2006

