SEGURIDAD Y PRIVACIDAD DIGITAL

PARA LOS DEFENDORES DE LOS DERECHOS HUMANOS

FrontLine
INTERNATIONAL FOUNDATION FOR THE PROTECTION OF HUMAN RIGHTS DEFENDERS

Este libro está dedicado a todos los defensores de los derechos humanos que continúan su trabajo, difícil y honesto, también en Internet. Algunas de estas personas están en prisión debido a sus actividades en la red. Mohammed Abbou cumple una condena de 3,5 años de prisión en Túnez por publicar un artículo en Internet en el que comparaba las prisiones tunecinas con la de Abu Ghraib.

FrontLine
INTERNATIONAL FOUNDATION FOR THE PROTECTION OF HUMAN RIGHTS DEFENDERS

SEGURIDAD Y PRIVACIDAD DIGITAL

PARA LOS DEFENDORES DE LOS DERECHOS HUMANOS

Febrero de 2007

Actualización de septiembre de 2009

Escrito por Dmitri Vitaliev

Front Line agradece el apoyo financiero de Irish Aid que ha hecho posible este proyecto.
La responsabilidad por el contenido del manual es únicamente del autor y de Front Line.

Agradecimientos

Front Line y Dmitri Vitaliev desean agradecer a las siguientes personas y organizaciones su inestimable ayuda en la investigación y compilación de este libro:

■ Reporters sans frontières	www.rsf.org
■ Privacy International	www.privacyinternational.org
■ The OpenNet Initiative	www.opennetinitiative.org
■ Wikipedia	www.wikipedia.org
■ Berkman Center for Internet & Society at Harvard Law School	http://cyber.law.harvard.edu
■ International Freedom of Expression eXchange (IFEX)	www.ifex.org
■ The Association for Progressive Communications	www.apc.org
■ Peace Brigades International	www.pbi.org
■ Electronic Frontier Foundation	www.eff.org
■ Cambridge Security Programme	www.cambridge-security.net
■ Privaterra	www.privaterra.org

Rosemary Warner
Steven Murdoch
Ross Anderson
Elijah Zarwan
Julian Wolfson
Bert-Jaap Koops
Wojtek Bogusz
Mary Lawlor
Andrew Anderson

...así como a los numerosos defensores de los derechos humanos que se encuentran en países de todo el mundo—entre ellos Zimbabwe, Guatemala, China, Cuba, Túnez, Arabia Saudita, Egipto, Yemen, Kirguistán, Rusia, Bielorrusia, México, etc. —, por responder preguntas y ofrecer testimonios y pruebas que dieron lugar a la idea que subyace a este libro y su contenido.

diseño gráfico e ilustraciones Assi Kootstra

FRONT LINE

The International Foundation for the Protection of Human Rights Defenders

Los derechos humanos son garantizados por el derecho internacional, pero trabajar para asegurarse de que se efectúen y hacerse cargo de los casos de las personas cuyos derechos han sido violados puede ser una tarea peligrosa en países de todo el mundo. Los defensores de los derechos humanos son a menudo la única fuerza entre la gente común y el poder inmoderado del Estado. Son esenciales para el desarrollo de procesos e instituciones democráticos, para acabar con la impunidad y para la promoción y protección de los derechos humanos.

Los defensores de los derechos humanos suelen sufrir acoso, detención, tortura, difamación, suspensión de su empleo, negación de la libertad de circulación y dificultad para obtener el reconocimiento legal de sus asociaciones. En algunos países son asesinados o están "desaparecidos."

Front Line fue fundado en Dublín en el año 2001 con el objetivo específico de proteger a los defensores de los derechos humanos, personas que trabajan en forma no violenta a favor de todos o alguno de los derechos consagrados en la Declaración Universal de los Derechos Humanos. Front Line tiene como objetivo abordar algunas de las necesidades identificadas por los propios defensores, incluida la protección, la creación de redes, la formación y el acceso a mecanismos temáticos y de país de la ONU y otros organismos regionales.

El objetivo principal de Front Line se centra en los defensores de los derechos humanos que se encuentran en riesgo, ya sea temporal o permanente, debido al trabajo que realizan en nombre de sus conciudadanos. Front Line cuenta con un programa de pequeñas subvenciones para garantizar la seguridad de los defensores, y moviliza campañas y cabildeo en nombre de los defensores que se hallan en peligro inmediato. En situaciones de emergencia, Front Line puede facilitar reubicación temporal.

Front Line realiza investigaciones y publica informes sobre la situación de los defensores de los derechos humanos en países concretos. La organización se encarga también de elaborar materiales de recursos y de formación, en nombre de los defensores de los derechos humanos, así como de facilitar la creación de redes y el intercambio entre los defensores en diferentes partes del mundo. Los proyectos de Front Line se realizan, por lo general, en asociación con organizaciones de derechos humanos específicas de cada país.

Front Line promueve la conciencia de la Declaración Universal de los Derechos Humanos y trabaja para garantizar que los principios y normas establecidos en la "Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos" (conocida como la Declaración sobre los Defensores de los Derechos Humanos) sean conocidos, respetados y observados en todo el mundo.

Front Line tiene un Estatus Especial Consultivo del Consejo Económico y Social de las Naciones Unidas.

Para sufragar este trabajo, Front Line se basa enteramente en la generosidad de los fondos individuales e institucionales.

Front Line ha tenido la suerte, desde su lanzamiento en 2001, de recibir financiamiento de una gran diversidad de fuentes, así como donaciones de particulares.

Front Line tiene el estatus de organización benéfica (CHY NO 14029) y es independiente e imparcial.

ÍNDICE

Como sabemos, hay cosas conocidas conocidas. Hay cosas que sabemos que sabemos. También hay desconocidos conocidos. Es decir, cosas que sabemos que no sabemos. Pero también hay cosas desconocidas desconocidas, las que no sabemos que no sabemos.

Donald Rumsfeld, Secretario de Defensa de EE.UU., diciembre 2003

INTRODUCCIÓN

Los defensores de los derechos humanos usan cada vez más ordenadores e Internet en su trabajo. Aunque el acceso a la tecnología sigue siendo un gran problema en todo el mundo, los medios electrónicos de almacenamiento y transmisión de información son cada vez más comunes en las organizaciones de derechos humanos. En muchos sentidos, Internet ha mejorado el trabajo y la seguridad de los defensores: aumentó la eficacia de su misión, facilitó su acceso a la información y estimuló su comunicación con las organizaciones asociadas. Por otra parte, sin embargo, también conllevó algunos problemas y vulnerabilidades que antes no existían.

Este libro no está dirigido a un mago de los ordenadores. Sus objetivos son informar a los usuarios de ordenadores comunes y ofrecerles soluciones a los problemas de privacidad y seguridad que pueden surgir en un entorno digital moderno.

—

Escribimos documentos, dibujamos y nos comunicamos por ordenadores e Internet. Los programas para llevar a cabo estas acciones son tan sencillos que no necesitamos saber exactamente cómo funciona un ordenador, mientras funcione correctamente. Así, utilizamos una tecnología que no comprendemos totalmente; sin embargo, dependemos de ella en gran medida. Como consumidores de la era digital, queremos un producto acabado, no una lista de sus componentes.

Pero, ¿qué hacemos si las cosas van mal?, ¿cuando nuestro ordenador se estropea y aniquila años de trabajo duro?, ¿cuando nuestros correos electrónicos no llegan a los destinatarios o cuando no podemos acceder a un sitio web? ¿Cómo reaccionar ante la noticia de un virus que daña ordenadores en todo el mundo, o ante un correo electrónico recibido supuestamente de un amigo que nos pide que abramos el archivo adjunto? Las decisiones tomadas sin información conducen a malas elecciones, y la confianza ciega en la tecnología suele dar lugar a costosos errores.

—

El trabajo de los defensores y las organizaciones de derechos humanos se entrelaza con la tecnología. Ésta facilita la comunicación y nos permite almacenar y procesar grandes cantidades de información de forma barata y dentro de un espacio mínimo. Incluso permite a una organización pequeña y remota adquirir una voz global. Una conversación electrónica mantenida un par de años antes puede recordarse en cuestión de segundos, y el autor de una violación de los derechos humanos, por ejemplo, puede recibir miles de correos electrónicos y faxes furiosos de todo el mundo. En poco tiempo, los ordenadores e Internet se han convertido en partes esenciales e inseparables del trabajo en derechos humanos.

Los problemas

La abundancia de información almacenada en forma digital y la capacidad de difundirla en el mundo entero ha creado una de las industrias más grandes en

la historia humana: la industria de la información. Mueve miles de millones de dólares y genera enormes ganancias para los que controlan y operan su estructura subyacente. La capacidad de manipular, seguir y restringir la información electrónica se ha convertido en un pasatiempo, un trabajo o una política para muchas personal, empresas y departamentos gubernamentales. La guerra contra el terrorismo les ha dado carta blanca para poner en práctica la vigilancia y la censura de Internet, que antes era abierto y libre. Las justificaciones de tales actividades son profundas y con frecuencia erosionan algunos derechos humanos y libertades básicos. Algunos países incluso han introducido leyes que justifican y alientan estas prácticas para aumentar aún más la persecución y el sufrimiento de los defensores de los derechos humanos y debilitar su legítimo trabajo, reduciendo así su capacidad para proteger los derechos de otros. Decenas de defensores y periodistas se encuentran actualmente en prisión por tratar de difundir su trabajo por el mundo digital sin el conocimiento adecuado de cómo hacerlo de manera segura.

—

Hay que decir aquí que la tecnología en general todavía no ha alcanzado todos los rincones de nuestro planeta. Hay millones de personas que nunca han visto un semáforo, y mucho menos un ordenador. La enorme brecha material entre las naciones ricas y pobres también se manifiesta en el mundo de tecnología electrónica y es conocida como "**brecha digital**". Las posibilidades de llegar a la comunidad mundial de los defensores de los derechos humanos que se hallan en el lado equivocado de la brecha son muy reducidas.

—

Este libro es una introducción al mundo creciente y complejo de la seguridad electrónica. No solo va a aumentar su nivel de conocimiento y sensibilización acerca de los ordenadores e Internet, sino que también le advertirá de los distintos riesgos a los que puede exponerse en el entorno digital y le dirá cómo abordarlos.

—

El libro está escrito para los defensores de los derechos humanos, y por lo tanto, introduce las formas de prevenir la erosión de las libertades universalmente garantizadas. Junto a la teoría, ofrece posibles soluciones a algunos de los problemas de la seguridad en los ordenadores e Internet.

La seguridad como proceso

Esto no es un libro de respuestas. Imagine que acude a un experto en seguridad para que lo asesore sobre cómo reaccionar a las amenazas de la vida real y al acoso físico. Antes de darle una respuesta, es probable que el experto le haga una serie de preguntas sobre la naturaleza exacta de los riesgos y amenazas a los que se enfrenta. Lo mismo ocurre con la seguridad electrónica: no existe una solución inmediata a cada problema de seguridad en los ordenadores e Internet. Tal vez se haya percatado que los "expertos" rara vez ofrecen respuestas directas.

Este manual de seguridad es un proceso descriptivo para presentarle los muchos aspectos distintos ded funcionamiento del ordenador y de Internet (en este caso, concretamente para los defensores de los derechos humanos). El objetivo es mejorar su conocimiento y aumentar la conciencia de la seguridad electrónica y las cuestiones de privacidad digital. Este libro trata de los hechos, teorías, métodos y posibles explicaciones de la inseguridad informática y las soluciones a la misma. Le ayudará a resolver y fortalecer su propia seguridad electrónica. Esperamos que el manual también despierte el interés suficiente por los temas antes mencionados como para inspirarle a llevar a cabo su propia investigación y seguir aprendiendo.

Guía para el manual

Este manual está dividido en cuatro partes que pueden leerse en cualquier orden. El lector no requiere conocimientos especiales, aunque tener unas nociones básicas del funcionamiento del ordenador y de Internet le ayudaría. Los capítulos que contienen información de carácter más técnico están marcados "Para los *techies*".

—

La primera sección se dedica a comprender sus necesidades y vulnerabilidades de seguridad, con un enfoque no técnico al entorno digital. Le ofrece un método para identificar las amenazas que plantean situaciones concretas y, de este modo, ayudarlo a decidir las estrategias más adecuadas a la hora de aplicar las soluciones de privacidad y seguridad.

—

En la segunda sección se enumeran diferentes elementos relativos a la seguridad en los ordenadores e Internet. Se presentan al lector las operaciones informáticas y la infraestructura de Internet. Se explican en de forma detallada métodos de asegurar los datos, esquivar la censura cibernética y protegerse contra ataques maliciosos.

—

La tercera sección es un resumen de la legislación mundial para restringir y seguir el flujo de información y las comunicaciones. En ella se muestra la tendencia a la baja causada por el aumento de las restricciones a los derechos a la libertad de expresión, la privacidad y la comunicación en muchos países. Se presentan casos de defensores de los derechos humanos que actualmente se encuentran en prisión o perseguidos por su trabajo a través de Internet, como ejemplos de la forma que tienen algunos gobiernos de hacer cumplir estas leyes.

—

En la cuarta sección se ofrece a los defensores de los derechos humanos y sus organizaciones posibles escenarios para abordar los problemas de inseguridad electrónica y garantizar la continuación de su trabajo. Los escenarios se refieren a los conceptos presentados en el manual y las soluciones se basan en acciones viables.

—

Después de los estudios de casos encontrará usted los Apéndices, en los que se ofrece información detallada sobre los ordenadores e Internet, así como explicaciones más a fondo de determinados temas de seguridad. Al final del libro hay un glosario en el que se explican muchas de las palabras técnicas y desconocidas empleadas en este manual.

—

Este libro puede ser utilizado junto con el *Digital Security Toolkit* ('Juego de herramientas de seguridad digital', http://security.ngoinabox.org), una colección de herramientas y manuales de *software* gratuitos que incluye los recursos necesarios para lograr una mayor privacidad y seguridad en sus ordenadores y en Internet. El "juego de herramientas" está disponible en inglés, francés, español, ruso y árabe. Todos los programas mencionados en este manual se puede encontrarse allí o descargar gratuitamente de Internet.

Algunos de los conceptos y tecnologías descritos y explicados en este manual se han declarado ilegales en varios países del mundo. Le rogamos preste la debida atención a su legislación local y tome una decisión informada acerca de la posesión y el uso de este manual.

1.1 SEGURIDAD E INSEGURIDAD

Los ordenadores e Internet abarcan tanto la búsqueda de información como su almacenamiento e intercambio. Por lo tanto, el tema de la seguridad en el ámbito digital se refiere a la seguridad de la información. Debemos operar en un ambiente en el que nuestra información no sea robada, dañada, comprometida o restringida. Internet, en teoría, ofrece a todos la igualdad de oportunidades para acceder y difundir información. Sin embargo, como han demostrado muchos incidentes, esto no siempre es así. Los gobiernos y las empresas se dan cuenta de la importancia y el valor del control de los flujos de información y de la capacidad de decidir cuándo restringirlos. La seguridad de la información se complica aún más por la acción de personas malintencionadas que crean virus informáticos y por el "hackeo" en sistemas informáticos, a menudo sin otro motivo que causar daño.

—

La confusión se ve reforzada por la abundancia de *software*, *hardware* y dispositivos electrónicos diseñados para facilitar el almacenamiento e intercambio de información. Hoy en día, un ordenador medio contiene millones de líneas de código complejo y cientos de componentes que pueden fallar y dañar el sistema en cualquier momento. Los usuarios tienen que sumergirse en conceptos y tecnologías que parecen estar muy lejos del mundo real. La seguridad de su ordenador recae en primer lugar sobre sus hombros y requiere una cierta comprensión de cómo funcionan sus sistemas.

—

La carrera por llevarse los beneficios de Internet ha dado lugar a la aparición de numerosos servicios y agencias financieros. Ahora ya puede reservar su vuelo, comprar un libro, hacer transferencias bancarias, jugar al póquer o hacer compras y publicidad en Internet. Hemos aumentado nuestra capacidad para conseguir más cosas con mayor rapidez, pero también hemos creado una multitud de nuevos flujos de información, y con ellos, nuevos conceptos de inseguridad con los que aún no sabemos cómo tratar. Empresas de mercadotecnia están construyendo los perfiles de usuarios en Internet con la esperanza de convertir su navegación en un viaje de compras incesante. La información personal recogida por los proveedores de servicios en Internet, los gobiernos y sociedades se vende a empresas de minería de datos, cuyo objetivo es acumular la mayor cantidad de detalles posibles acerca de su vida privada y sus hábitos. Esta información se utiliza posteriormente en las encuestas, el desarrollo de productos o actualizaciones de seguridad nacional.

—

Puede parecer que nuestro mundo digital está gobernado por el caos. Nada es cierto y todo es posible. La mayoría de nosotros solo queremos seguir adelante con la escritura de nuestro documento, o el envío de correo electrónico, sin la necesidad de tener en cuenta los resultados de la inseguridad. Desafortunadamente, esto no es posible en el entorno digital. Para poder desenvolverse con seguridad y confianza en esta nueva era de las autopistas de información y las tecnologías emergentes, hay que ser plenamente conscientes de nuestro potencial y nuestras debilidades. Hay que tener los conocimientos y las habilidades para sobrevivir y evolucionar con las tendencias cambiantes.

LOS MÉTODOS Y TENDENCIAS DE VIGILANCIA, LA CENSURA Y LA AGRESIÓN ELECTRÓNICA

1.1

En el mundo moderno el derecho a la privacidad es un tema polémico. ¿Tiene alguien derecho a acceder a nuestra información privada? A raíz de los ataques del 11 de septiembre en los EE.UU., la mayoría de los gobiernos parecen pensar que deben tener la capacidad para controlar y acceder a nuestra comunicación digital. Muchos países han aplicado la legislación e introducido las tecnología necesarias para aumentar su poder de vigilancia hasta niveles nunca vistos. El proyecto **ECHELON**, por ejemplo, es un sistema de vigilancia mundial capaz de registrar y procesar comunicaciones por teléfono, Internet y satélite.

En mayo de 2001 la Comisión temporal sobre el sistema de interceptación Echelon del Parlamento Europeo (creada en julio de 2000) publicó un informe que concluía que "No hay ninguna razón para seguir dudando de la existencia de un sistema mundial de interceptación de las comunicaciones..." Según la Comisión, el sistema Echelon (al parecer, dirigido por los EE.UU. en cooperación con Gran Bretaña, Canadá, Australia y Nueva Zelanda) fue creado al comienzo de la Guerra Fría para obtener información y se ha convertido en una red de estaciones de interceptación en todo el mundo. Su objetivo principal, según el informe, es interceptar comunicaciones privadas y de carácter económico, no militares[1].

►La estación de interceptación ECHELON en Menwith Hill, Inglaterra

En Internet también se ha atacado y reprimido el derecho a la libertad de expresión e información. Como consecuencia de ello, muchos gobiernos – que no están dispuestos a conceder este tipo de libertad a sus ciudadanos y luchan para restringir este libre acceso – han obtenido la capacidad de acceso a la información desde cualquier punto de conexión a Internet en el planeta, independientemente del lugar donde se almacene esta información. Se han destinado enormes recursos en el desarrollo de unos sistemas de filtrado específicos en cada país para bloquear la información de Internet considerada inadecuada o perjudicial para las leyes del país y "la moral nacional".

En China, un sistema conocido como "el Gran Cortafuegos" dirige todas las conexiones internacionales a servidores proxy en portones oficiales, donde los funcionarios del ministerio de seguridad pública identifican a los usuarios y el contenido, definen derechos y vigilan cuidosamente el tráfico de la red, tanto de entrada como de salida del país. En una conferencia sobre la industria de seguridad celebrada en 2001 el gobierno de China anunció un ambicioso proyecto sucesor conocido como "El Escudo Dorado". En lugar de confiar únicamente en la Intranet nacional de China, separada de la Internet global por un inmenso cortafuegos, China va a incorporar ahora en la red la inteligencia de vigilancia, que le permite "ver", "oír" y "pensar". La filtración de contenidos se desplaza desde el nivel nacional a millones de dispositivos de información y de comunicación digitales situados en lugares públicos y en las casas de la gente. La tecnología que hay detrás del Escudo Dorado es increíblemente compleja y se basa en investigaciones realizadas en gran medida por las empresas de tecnología occidentales, entre las que se halla Nortel Networks, Sun Microsystems, Cisco y otras.[2]

1
Parlamento Europeo, Comisión temporal sobre el sistema de interceptación Echelon (2001): Informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON) , 18 de mayo de 2001. (2001/2098(INI)) (adoptado el 11 julio de 2001). Disponible en http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf

2
Privacy International – Informe sobre privacidad y derechos humanos de 2004 – Amenazas a la privacidad

Estos filtros socavan nuestra capacidad para sacar provecho de Internet y para cruzar fronteras geográficas en nuestra búsqueda de aprendizaje y comunicación. También incumplen varios artículos de la Declaración Universal de los Derechos Humanos que garantiza los derechos de cada persona a la privacidad y la libertad de expresión. Es significativo que estos sistemas no se hayan desarrollado hasta después de que se advirtiese el crecimiento y el potencial de Internet como intercambio global de información. No formaban parte de la idea original que había detrás del desarrollo de Internet.

—

Las técnicas de vigilancia y control han pasado de las manos del personal de inteligencia a los sistemas de *hardware* y *software* operados por empresas privadas y agencias gubernamentales. Las escuchas telefónicas y la apertura de las cartas has sido sustituidas por una tecnología que permite realizar un seguimiento de todo y de todos a la vez. La popularidad de Internet y su integración en nuestra vida diaria lo han hecho posible. Anteriormente se espiaba a personas que se consideraban peligrosas para la seguridad nacional. Hoy en día todos estamos bajo sospecha como resultado de los sistemas de vigilancia y filtrado instalados en Internet por nuestros gobiernos. La tecnología no suele distinguir entre usuarios, ya que espera a que aparezcan determinadas palabras clave en nuestro correo electrónico y búsquedas en Internet. Cuando se activa, alerta a equipos de vigilancia o bloquea nuestra comunicación.

—

El debate sobre el control de Internet y los flujos de información con la finalidad de combatir el terrorismo está fuera de los límites de este manual. Hay que decir, sin embargo, que tales prácticas han reducido la libertad de expresión, de asociación y de la privacidad en todo el mundo, en contravención directa de la Declaración Universal. Los gobiernos han instalado sistemas de control de sus ciudadanos más allá de las medidas para luchar contra el terrorismo. Son muchos los que han visto negado su acceso a información sobre los derechos humanos y las libertades de los medios de comunicación, la orientación sexual, pensamiento y movimientos políticos, por nombrar sólo unas cuantas.

> *"(...) El gobierno de Uzbekistán ordenó supuestamente a los proveedores de servicios de Internet en el país bloquear la www.neweurasia.net, que alberga una red de weblogs que abarca Asia Central y el Cáucaso. Se cree que la decisión del gobierno de bloquear todo el acceso nacional a www.neweurasia.net es la primera censura de un weblog en Asia Central (...)"*[3]

Los ataques cibernéticos y los ejemplos de ciberguerra en la vida real han aumentado el alcance de las vulnerabilidades a las que se enfrentan las organizaciones que operan los sitios web y dependen de los servicios de Internet. Los ataques digitales sufridos en infraestructuras financieras y educativas de Estonia en 2007 y en 2008 durante el conflicto entre Rusia y Georgia demostraron la necesidad de defender las fronteras digitales de un estado o una institución. El acceso a los sitios web de organizaciones de derechos humanos se ve imposibilitado por los ataques organizados de la negación distribuida del servicio (DDoS), la desfiguración de los contenidos y eliminación de datos.

LAS AMENAZAS ESPECÍFICAS A LAS QUE SE ENFRENTAN LOS DEFENSORES DE LOS DERECHOS HUMANOS

Los defensores de los derechos humanos a menudo se convierten en objetivos de la vigilancia y la censura en su propio país. Su derecho a la libertad de expre-

3
www.newseurasia.net, 6 de julio de 2006.

sión es a menudo controlado, censurado y restringido. Frecuentemente se enfrentan a graves sanciones por continuar con su trabajo. El mundo digital ha sido una bendición y una maldición para ellos. Por un lado, la velocidad de las comunicaciones los ha acercado a sus colegas de todo el mundo, y las noticias de violaciones de los derechos humanos se extienden en cuestión de minutos. La gente se moviliza vía Internet y se han promovido muchas campa?as sociales a través de la red. El aspecto negativo del uso generalizado de los ordenadores e Internet consiste en la confianza en la tecnología compleja y la creciente amenaza de la vigilancia y los ataques electrónicos. Al mismo tiempo, los defensores que se hallan en los países pobres y no tienen ordenadores o acceso a Internet se han encontrado fuera de foco y el alcance globales: otro ejemplo del desequilibrio provocado por la **brecha digital**.

—

Con los años, los defensores de los derechos humanos han aprendido a actuar en su propio entorno y han desarrollado mecanismos para su propia protección y la prevención de los ataques. Conocen los sistemas jurídicos de sus países, tienen redes de amigos y toman decisiones basadas en la sabiduría cotidiana. Sin embargo, ordenadores e Internet constituyen un nuevo mundo para descubrir y comprender. Su falta de interés o capacidad para aprender acerca de la seguridad electrónica ha dado lugar a numerosas detenciones, ataques y malentendidos en la comunidad de derechos humanos. La seguridad electrónica y privacidad digital deben convertirse no sólo en un área importante para la comprensión y la participación, sino también en un nuevo campo de batalla en la lucha por la adhesión a los principios de la Declaración Universal en todo el mundo.

—

Los correos electrónicos no llegan a su destino, la conexión a Internet es intermitente, se confiscan ordenadores y los virus destruyen años de trabajo. Estos problemas son comunes y conocidos. Otro fenómeno común es la creciente atención a las publicaciones en línea por parte de quienes ostentan el poder. Las autoridades buscan activamente sitios de noticias, blogs y foros a través de Internet, con una rápida retribución cuando descubren material “no deseado” procedente de un defensor de los derechos humanos. Tomemos el caso de Mohammed Abbou, quien cumplía una condena de 3,5 años de prisión en Túnez por publicar un artículo en línea que comparaba las prisiones tunecinas con Abu Ghraib[4]. En China decenas de periodistas se encuentran en prisión debido a sus actividades relacionadas con Internet[5].

—

Los defensores de los derechos humanos tienen que asegurar su trabajo mediante el aprendizaje sobre la tecnología y los conceptos del funcionamiento del ordenador y de Internet. Esto hará que sean más eficaces en su protección y en la de los derechos de aquellos a quienes tratan de defender.

4
Front Line - http://www.frontlinedefenders.org/news/2081

5
Reporters sans frontières – www.rsf.org, febrero de 2007

1.2 SENSIBILIZACIÓN SOBRE LA SEGURIDAD

RESUMEN

1 Pregúntese: ¿Es fácil para un intruso acceder a su oficina y espacio de trabajo?
2 Tenga en cuenta que el uso de un ordenador en un cibercafé es más inseguro que el uso de un ordenador en casa.
3 La información almacenada en su ordenador debe estar protegida por varias capas de acceso: la seguridad del ordenador en sí mismo, el cuarto en el que se encuentra y el edificio donde usted trabaja.
4 Conozca la ubicación física exacta de sus archivos de datos y cualquier duplicado archivado.
5 No use una contraseña vacía y no la revele a los demás.
6 Extreme la atención al abrir correos electrónicos y desactive la función de vista previa en su programa de correo electrónico.
7 Restrinja el acceso inmediato a su ordenador cuando no lo esté atendiendo.

En este capítulo trataremos métodos no técnicos para aumentar la seguridad de su información y comunicación. Ser consciente de sus alrededores, y por lo tanto, darse cuenta de las amenazas potenciales con que puede encontrarse es el primer paso en su plan de seguridad. También debe comprender su entorno operativo y tener un enfoque sensato con respecto al riesgo de incidentes de seguridad.

CÓMO ASEGURAR SU ENTORNO OPERATIVO

La mayoría de los incidentes de seguridad que afectan el trabajo y el sustento de los defensores de los derechos humanos están relacionados con la violencia física y la intrusión en su entorno de trabajo. Si trabaja en una oficia, lleva un portátil o utiliza únicamente los cibercafés debe ser siempre consciente de sus capacidades y limitaciones. A continuación se ofrece una lista de preguntas que debería ser capaz de responder con seguridad. En cada pregunta imagine el peor de los casos y piense cómo actuaría.

En la oficina

- ¿Es fácil para alguien de fuera acceder a su oficina sin permiso?
- ¿Se pueden romper las ventanas o forzar la puerta?
- ¿Tiene un sistema de alarma, y confía en las autoridades que responderán a la intrusión?
- ¿Tiene una “sala de espera” o área de recepción donde pueda cuestionar al visitante antes de que entre en la oficina principal?
- ¿Tiene un almacenamiento seguro (p. ej., caja fuerte) para los documentos confidenciales?
- ¿Tiene un método seguro de destrucción (p. ej., trituradora) de los documentos confidenciales?
- ¿Qué nivel de confianza le merece el personal de limpieza y qué nivel de acceso tiene este a los documentos?

- ¿Se deshace de la basura de manera que sería imposible que alguien de fuera pudiese buscar o acceder a ella? En este sentido, ¿cómo se deshace de los documentos confidenciales?
- ¿Está asegurado y tiene una estrategia en el caso de un desastre natural o robo?
- ¿Son su oficina, el personal y las pantallas de los ordenadores visibles desde el exterior de las ventanas?
- ¿Cuántas copias de llaves de su oficina existen y quién las tiene?

Área personal de trabajo

- ¿Hay alguien que pueda ver la pantalla de su ordenador mientras usted está trabajando en su escritorio?
- ¿Hay alguien en la oficina que conozca su contraseña?
- ¿Guarda información confidencial en lugares de acceso fácil en su entorno de trabajo?
- ¿Restringe el acceso inmediato a su ordenador cuando usted no se encuentra en su escritorio u oficina?
- ¿Está su ordenador o portátil bien fijado a su área de trabajo o puede moverse fácilmente?

Entorno público (p. ej., cibercafé)

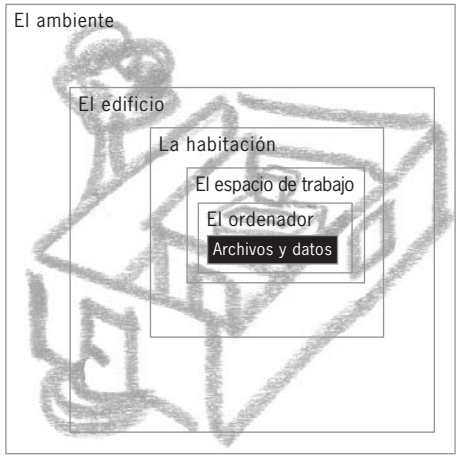
- ¿Conoce el dueño del cibercafé su nombre y otros datos personales?
- ¿Controla el dueño del cibercafé la navegación de los clientes por Internet?
- ¿Está seguro de que el ordenador que está utilizando no está a salvo de virus y espionaje?
- ¿Puede la gente que hay en el cibercafé ver lo que usted está leyendo o escribiendo en la pantalla?
- Cuando está descargando archivos de Internet ¿permanecen estos en el ordenador después de irse usted del cibercafé?
- ¿Cómo puede estar seguro?
- ¿Queda registrada la navegación por Internet en el ordenador?

Como puede observar, tendrá que ser riguroso si quiere asegurar su entorno de trabajo y su información. Algunas de estas cuestiones pueden resolverse fácilmente: por ejemplo, comprando un cable de metal para fijar su portátil al escritorio. Otras requieren la cooperación de todo el personal – por ejemplo, recibir a los visitantes en cuanto entren y preguntarles el propósito de su visita–, así como una posible inversión financiera: por ejemplo, en un seguro o una caja fuerte. La mayoría de las organizaciones de derechos humanos operan de una manera abierta, "no secreta"; sin embargo, son a menudo responsables de la confidencialidad y la seguridad de sus colegas y de otras personas involucradas en los casos que tratan (testigos, víctimas, demandantes, etc.).

—

La capacidad de mirarse a sí mismo desde un punto de vista diferente y evaluar su actual situación de seguridad le ayudará bastante para hacer algo respecto a la inseguridad.

La evaluación de la amenaza a su seguridad y la de su ordenador debe comenzar en el nivel físico del mundo real. Esta es el área en la que ya tiene experiencia y conocimientos. Tener éxito al eliminar los riesgos que plantean las preguntas anteriores le proporcionará una ventaja muy importante en la seguridad de su entorno digital.



Fíjese en este diagrama que muestra diferentes capas de seguridad en torno a la información en su ordenador.

La seguridad se basa en capas que garantizan una exhaustiva protección a través de la provisión de barreras de acceso. Debe construir las distintas capas de protección alrededor de los equipos y la información. Es necesario proteger el acceso a:

- el edificio o los locales donde se encuentran los equipos o los archivos
- el cuarto donde se almacenan los equipos o los archivos
- el entorno de trabajo y la ubicación física de su(s) ordenador(es)
- sus archivos y datos (incluso la información en papel).

La seguridad perfecta casi nunca es alcanzable. Como simples humanos, todos cometemos errores, olvidamos información importante y nos saltamos nuestras propias estrategias de seguridad debido a la pereza o falta de tiempo. Al considerar nuestra seguridad debemos emplear el sentido común. No es mi intención enseñar el sentido común a nadie, pero me gustaría presentar una lista de preguntas que yo personalmente trataría de responder a la hora de garantizar que mi trabajo dentro y fuera mi ordenador se haga de la manera menos comprometedora para mí y para la seguridad de mi información. Los capítulos que siguen le ayudarán en la aplicación de las siguientes estrategias, así que no se preocupe si al principio algunas de mis propuestas parecen demasiado exigentes.

PREGUNTAS QUE DEBE HACERSE

¿Dónde están mis datos?

En primer lugar, tenga siempre presente dónde están guardados los documentos más importantes. Podrían estar en el ordenador de la oficina, o en el portátil, o en la tarjeta de memoria USB, o incluso en un montón de discos compactos guardados en el armario en algún lugar. Es fundamental que tenga una copia de estos datos (una copia de seguridad), ya que la pérdida accidental o daños intencionados le harían retroceder varios años. También es importante garantizar la seguridad de esta copia. Si su oficina o casa está llena de muchos discos distribuidos por varios lugares no puede garantizar su seguridad.

¿Quién conoce mi contraseña?

No revele su contraseña a nadie, aunque a veces desee haberlo hecho (situaciones críticas, plazos… todos hemos experimentado esto). La presión del trabajo a menudo requiere que se dé prioridad a terminar algo y se sacrifique todo lo demás para ello. Desde una perspectiva de seguridad, esta es una práctica de riesgo. Si un intruso oye su contraseña, si la apunta y luego la pierde o se produce un accidente, puede perder el acceso a la cuenta de correo electrónico o un archivo para siempre.
Usar una contraseña en blanco es como salir de su casa, no cerrar la puerta

con llave y dejarla así toda la noche en un barrio peligroso. Tal vez no entre nadie, o tal vez sí y se lo roben todo. En Internet hay programas que buscan automáticamente "puertas no cerradas con llave" y que van a encontrar la suya bastante pronto. Hace varios años, Garry McKinnon – un pirata informático británico – logró entrar varias veces en el sistema informático del gobierno de los EE.UU. y la red del Departamento de Defensa simplemente por probar contraseñas en blanco o estándar (por ejemplo "admin" o "contraseña"). Se dice que accedió a información sobre extraterrestres y pruebas de encubrimiento. Al final fue capturado y se enfrenta a la extradición frente a los tribunales en los EE.UU.[6]

¿De quién es este ordenador?

Muchas veces tenemos que operar desde ordenadores públicos en un cibercafé o una biblioteca. A menudo resulta imposible asegurarse de que cada ordenador esté a salvo de virus, espionaje, troyanos u otros agentes dañinos. Hay que actuar con precaución con el tipo de información que elija abrir en un ordenador u otro. Trate de asegurarse de que no trabaja con información sensible que se convertirá en una responsabilidad si alguien la roba o está dañada. Recuerde que cualquier archivo abierto o leído en un ordenador público puede ser fácilmente guardado para su posterior inspección o abuso, si el equipo está configurado para ello.

Cada ordenador en Internet tiene un identificador único (volveremos a ello más adelante). Si el dueño del cibercafé apunta su nombre y la hora de la visita, no crea que su navegación por Internet es anónima: está directamente vinculada a usted.

¿Quién es?

Cada vez que reciba un correo electrónico extraño o un enlace no identificado pregúntese quién puede ser el remitente de esta información. Si alberga cualquier duda en cuanto a la legitimidad de un mensaje no haga clic en él sólo para averiguarlo: borre el mensaje de inmediato. Por desgracia, el mundo de los ordenadores ha llegado tan lejos que ni siquiera es necesario hacer doble clic sobre algo para que infectarse con un virus. Las técnicas modernas pueden hacer que el momento de abrir un correo electrónico o un navegador el ordenador puede infectarse por la nueva marca de algún programa destructivo. Por eso la precaución es su mejor amiga.

¿Quién puede acceder a mi ordenador?

Al salir de su escritorio al final del día o para ir a comer, apague el ordenador. Mientras que su ordenador está en marcha y desatendido pueden ocurrir innumerables incidentes. Al apagar el ordenador corta el suministro de energía y lo protege de los ataque de Internet. Sus contraseñas de BIOS o Windows no son eficaces si el ordenador está encendido. Algunos virus permanecen en letargo hasta la mitad de la noche y después activan el módem y marcan un número de larga distancia. La mayoría de los ordenadores tardan un par de minutos en apagarse, así que todo lo que sacrifica es un poco de tiempo mientras que gana mucho en seguridad.

—

Si está utilizando un ordenador público en un cibercafé o una biblioteca, trate de reinicializarlo después de acabar el trabajo (cuando use Windows hágalo pulsando `Inicio > Apagar > Reiniciar` y espere a que el ordenador se vuelva a cargar). Esto borrará muchos de los datos temporales generados de su sesión.

6 http://news.bbc.co.uk/2/hi/programmes/click_online/4977134.stm

¿Conozco mi entorno?

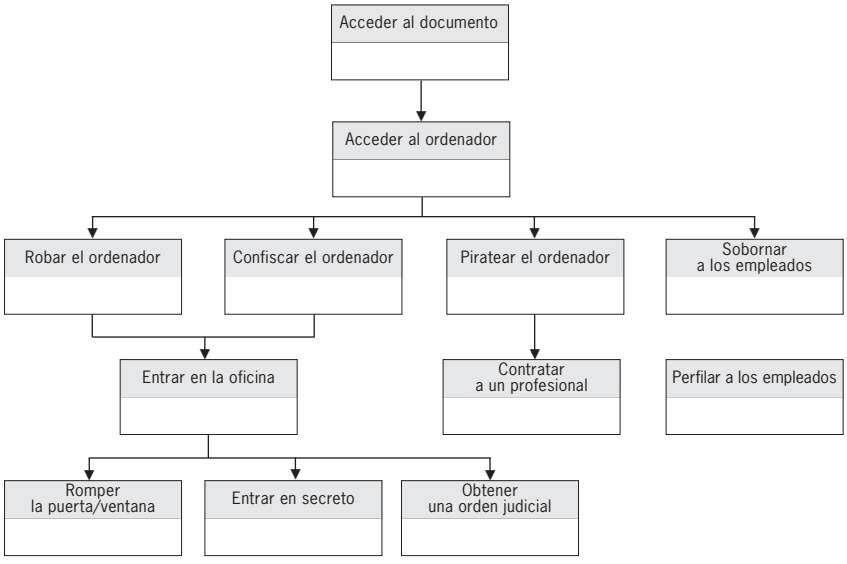
El conocimiento de su entorno es crucial para su seguridad. Debería ser consciente de los riesgos y peligros que presenta cada escenario, y de sus recursos para resolverlo. Trabajar por una seguridad electrónica debería incluir el conocimiento de la legislación local relevante, la seguridad del área de trabajo en la oficina, un círculo de confianza de amigos y colegas, los conocimientos técnicos y la conciencia de sus propias vulnerabilidades y capacidades y las de su ordenador. Para preparar una mejor política de seguridad para usted o su organización necesita construir un modelo de amenaza.

1.3 LA EVALUACIÓN DE AMENAZAS Y EL CÍRCULO DE SEGURIDAD

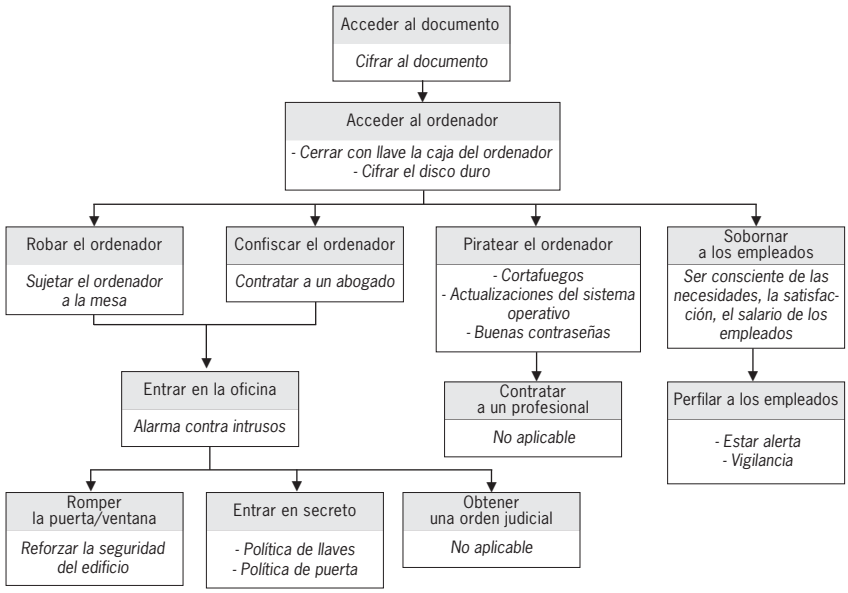
RESUMEN

1 Escriba una lista de posibles amenazas a la seguridad de su información.
2 Trate de prever y tomar las medidas necesarias para impedir que las amenazas de seguridad se hagan realidad.
3 Reaccione rápidamente a los incidentes e investigue las causas.
4 Cuando reaccione a un incidente de seguridad, suponga el peor escenario posible y tome las medidas pertinentes.
5 Considere la seguridad desde una perspectiva global. Elimine los enlaces débiles que pueda haber en su estrategia y no comprometa a la gente con quien trabaja o se comunica por ser usted descuidado con la seguridad.
6 Ponga sus conclusiones en un diagrama. Esto le permitirá a usted y a sus colegas comprender el panorama más rápidamente.
7 Concéntrese en el punto más débil de su estrategia de seguridad.

Para decidir qué medida de seguridad tomar es necesario tener una idea clara de las amenazas a las que se enfrenta, entre las que pueden hallarse amenazas de la seguridad de sí mismo, del personal, de su reputación, de la información y de la estabilidad financiera. Todos estos factores pueden verse comprometidos de un modo u otro por la inseguridad electrónica. Dado que la situación de cada persona es diferente, sólo hemos utilizado ejemplos generales para destacar la idea de modelar la amenaza.
El diagrama se escribe de arriba hacia abajo. En el nivel superior se describe qué es lo que deseamos proteger. La amenaza es la capacidad de comprometerlo. Al bajar un nivel, se hace una lista de las diferentes inseguridades que pueden producirse: las amenazas a la protección del nivel superior. El primer ejemplo muestra como modelo la amenaza de alguien que accede a un documento de su ordenador.

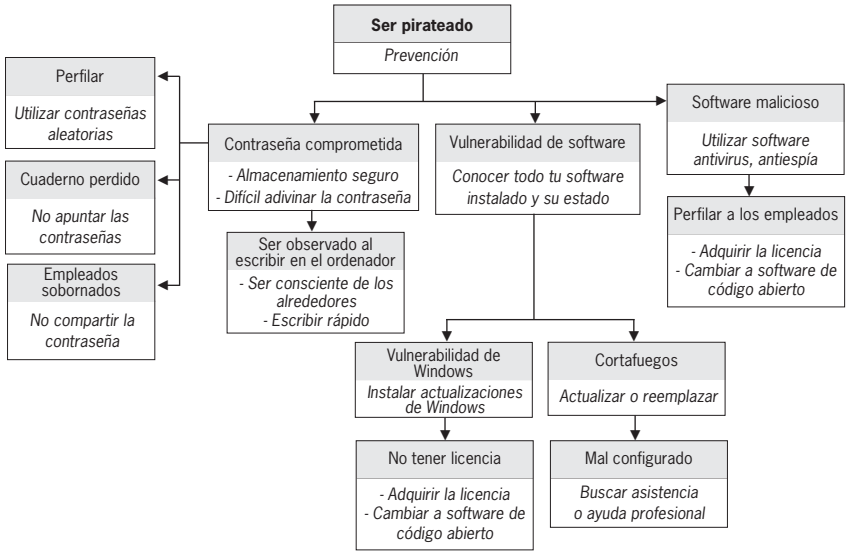


En el nivel superior, escriba la amenaza que desea evitar. En este caso, para acceder al documento, deberá tenerse acceso al primer ordenador. El acceso al ordenador puede obtenerse por robo, confiscación, piratería, soborno a uno de sus colegas, etc. Puede elegir el número de niveles que desea tener en el modelo, según le resulte útil.

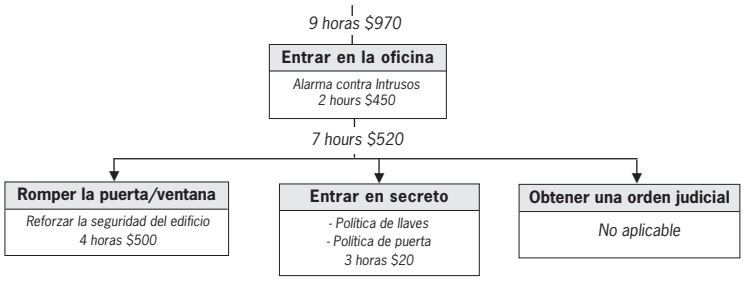


Ahora, trabajando desde abajo para arriba, llene las partes vacías del espacio de amenazas con algo que pueda eliminar o reducir esa amenaza en particular. Es posible que no pueda cambiar algunas de las amenazas (como la obtención, de la policía, de una orden judicial para entrar en su área de trabajo), pero la mayoría de ellas se puede influir. Proceda hacia arriba hasta que haya alcanzada la parte superior.

En este punto puede decidir contra cuál de las amenazas está dispuesto a defenderse y es capaz de hacerlo. Tal vez puede desarrollar e introducir ciertas políticas y salvaguardias dentro de su organización para reducir aún más el nivel de amenaza. Puede estudiar los métodos de este manual sobre cómo protegerse de la piratería y gastarse dinero en asegurar los puntos de acceso a su oficina.



También puede evaluar cada riesgo del diagrama anterior por separado. Por ejemplo, para evaluar la amenaza de piratería en su ordenador (que un intruso acceda a este) utilice el diagrama que encontrará más adelante.



Puede seguir desarrollando su modelo mediante la adición de un límite de costo o tiempo a cada espacio del árbol. Los espacios superiores contendrán los totales de todos los espacios que estén por debajo de ellos. Estos métodos le pueden ayudar a decidir la asignación de presupuestos o recursos para la prevención de una posible amenaza.

Al principio será difícil darse cuenta de todas las amenazas a las que puede estar enfrentándose, especialmente en el dominio digital. El conocimientote las mismas vendrá a base de profundizar en el estudio de las áreas específicas de la seguridad electrónica. Después de haber leído este manual su comprensión de algunas amenazas relacionadas con la tecnología debería aumentar. A continuación, será conveniente detectar las áreas sensibles de su trabajo y evaluar las amenazas a las que se enfrenta. Aunque esto pueda parecer como una planificación de decisiones racionales que se tomarían de todas formas, el proceso puede ayudar a comprender y hacer frente a numerosos factores que contribuyen a su inseguridad y evitar errores accidentales.

Prevención

A diferencia de las amenazas que se presentan en el mundo físico, las amenazas digitales a veces son difíciles de notar y, por lo tanto, de prevenir. Con los ataques electrónicos hay tendencia a comportarse de una manera más reactiva que proactiva: esta conducta resulta muchas veces ineficaz. Antes de que su ordenador sea pirateado hay que instalar un cortafuegos, y debe actualizar el limpiador del virus antes de que pierda documentos debido a una infección de virus. Para tratar de manera adecuada la posibilidad de un ataque digital, uno tiene que ser muy vigilante y paranoico. Hay que asumir el modelo de amenaza desde el principio. Hay que comprender y tratar el peor de los casos antes de que suceda. La velocidad en las operaciones informáticas y de Internet significa que las barreras de seguridad pueden ser eludidas en una fracción de segundo. Microsoft mantiene una opinión de que el 70% de los usuarios de Windows no tienen antivirus o *software* antiespionaje instalados[7]. La razón de esto no es el coste – hay varios antivirus, antiespionaje y cortafuegos gratuitos –, sino la autocomplacencia[8]. No espere hasta mañana para actualizar su sistema operativo, no espere hasta que llegue un aviso de virus para actualizar su *software* antivirus, no espere hasta que su ordenador quede confiscado o dañado antes de ejecutar las herramientas necesarias para eliminar o hacer copias de sus datos. ¡Sea proactivo!

Reacción

Si la seguridad de su ordenador, contraseña o red ya ha quedado compro-

7
BBC Online
http://news.bbc.co.uk/1/hi/technology/4694224.stm

8
Véase el capítulo "Software malicioso y spam" para entender la diferencia entre virus y espionaje.

tida debe contar con lo peor y tomar las medidas necesarias. Si se ha encontrado un virus en su ordenador desconéctese de Internet. Ejecute un análisis complete de todo el sistema y ponga en cuarentena cualquier virus que se haya encontrado. Cuando ya no reciba ningún mensaje de advertencia, vuelva a conectarse a Internet para actualizar sus definiciones de antivirus y archivos del sistema operativo de Windows y haga una búsqueda por el nombre del virus para ver lo que se sabe sobre él en Internet. Puede encontrar información sobre el daño que causa el virus y la manera de erradicarlo de su sistema de forma ade-

Incidente	**Reacción primaria**	**Método** (utilizando este manual & Seguridad en un Box Toolkit)	**Seguimiento**
Ataque de virus	- desconéctese de Internet y ejecute análisis completo del sistema - actualice todas las definiciones de virus y el sistema operativo - ejecute análisis completo del sistema otra vez	- ejecute el *boot scan* del anitvirus Avast o un análisis completo del AntiVir - actualice el Avast (o AntiVir) - ejecute otro *boot scan* del Avast o análisis completo del AntiVir	- haga una búsqueda del virus en Internet - vuelva al momento de la infección - analice todas las copias de seguridad y dispositivos extraíbles - recupere la configuración afectada por el virus
Ataque de espionaje	- desconéctese de Internet y ejecute análisis completo del sistema - actualice definiciones de antiespionaje	- ejecute análisis completo del sistema con Spybot - actualice el Spybot - inmunice el ordenador contra las nuevas definiciones de espionaje	- busque "espionaje informático" en Internet - cambie todas las contraseñas del sistema y de Internet - empiece a usar el navegador Firefox u Opera (si había usado Internet Explorer)
Corrupción de documentos	- recupere el documento de la copia de seguridad - busque las carpetas temporales de documentos recientemente modificados (véase el capítulo "La seguridad de Windows")	- eche un vistazo a sus archivos anteriores de "Freebyte"' o "Abakt" - para obtener consejos sobre búsquedas en su ordenador véase el capítulo "La seguridad de Windows" - para analizar el ordenador utilice el programa Handy Recovery	- encuentre la causa del accidente del ordenador o del documento - actualice la configuración del ordenador - actualice el procedimiento de las copias de seguridad y las copias mismas
Funcionamiento lento del ordenador	- compruebe si tiene espacio suficiente en el disco duro - desinstale los programas innecesarios o instalados recientemente - en Windows (NT,2000, Me, XP) consulte el "visor de sucesos" para ver la lista de síntomas[9] - compruebe si hay virus o espías	- use "BCWipe" para eliminar los archivos temporales del ordenador - use "Registry FirstAid" para hacer un barrido y limpiar el registro de Windows	- deshabilite los servicios de Windows (consulte el *Johansson's guide*[10]) - compre más RAM - llame a un técnico
Su acceso a un sitio web está bloqueado	- averigüe si otros pueden acceder a web, pregunte a sus amigos de otro país	- véase el apéndice B ("Internet explicado" y el capítulo "Evasión de la censura y del filtrado en Internet") - instale "Mozilla Firefox" y "switchproxy" - instale "Tor" o ejecute "Torpark"	- utilice un servidor *proxy* o la red anónima - use un sitio web de traducción que pueda obtener el contenido del web
Su sitio web está bloqueado	- llame al proveedor del sitio web y consulte el bloqueo - llame al proveedor de Internet y consulte el bloqueo - cambie su web a un proveedor o nombre de dominio diferente	- véase el apéndice B ("Internet explicado" y el capítulo "Evasión de la censura y del filtrado en Internet") - use "Httrack" (OpenCD) o "SmartFTP" para reflejar su sitio web en un servidor diferente	- informe a su red de contactos sobre el bloqueo del sitio web - provea el web en varios ordenadores por duplicación. Pregunte a sus amigos y contactos si pueden reflejar su web. - consulte los motivos para bloquear su sitio web y desarrolle una estrategia de apelación o cumplimiento

Incidente	Reacción primaria	Método (utilizando este manual & Seguridad en un Box Toolkit)	Seguimiento
El correo electrónico no llega al destinatario	- envíe el correo electrónico desde una cuenta diferente (también *webmail*) - trace la ruta para el dominio del destinatario (véase el apéndice "Internet explicado"") - verifique si la dirección de correo electrónico es correcta	- véase el apéndice B ("Internet explicado")' - véase "El cifrado" en la sección de Internet del capítulo "Criptología" - use el "Soft Perfect Network Scanner" - use "Hushmail"	- limpie su ordenador de *malware* e instale o actualice el cortafuegos. - empiece a usar diferentes cuentas de correo electrónico (que ofrezcan mayor seguridad) - comuníquese a través de un medio diferente (*chat* en línea, foros web, teléfono)
Advertencia de un ataque	- haga una evaluación de la amenaza - proteja la información sensible - borre la información sensible - haga una copia de seguridad	- revise los protocolos de seguridad - use el "Eraser"' (borrador) para borrar datos - use "Truecrypt" y "Freebyte" para guardar la copia de seguridad de los datos en un lugar seguro - use "DeepBurner" para hacer la copia de seguridad de CD o DVD	- introduzca el protocolo de seguridad en la oficina - refuerce la seguridad de la oficina - garantice que haya una copia de seguridad fuera de la oficina - desarrolle un sistema para la destrucción rápida de datos en el ordenador
Recepción de correo electrónico no deseado (p. ej., SPAM)	- instale un filtro de correo no deseado o empiece a usar Thunderbird con filtro integrado - bloquee direcciones de correo electrónico - ejecute un análisis de virus y espías	- use "'Mozilla Thunderbird" y lea sobre *NGO in a Box SE* en el capítulo sobre la configuración del filtro de correo basura - use "Avast" o "AntiVir" y "Spybot"	- cambie la dirección de correo electrónico - desarrolle una política especial atención a la divulgación de información con su dirección de correo electrónico - registre otras direcciones de correo electrónico que utilice para acceder a los servicios en Internet

cuada. He aquí una guía de algunos ejemplos comunes de mal funcionamiento del ordenador y reacciones sugeridas.

Nota: Todas las herramientas y métodos que figuran en el cuadro siguiente se pueden implementar con el *Digital Security Toolkit*, que puede pedir de Front Line o encontrar en la http://security.ngoinabox.org.

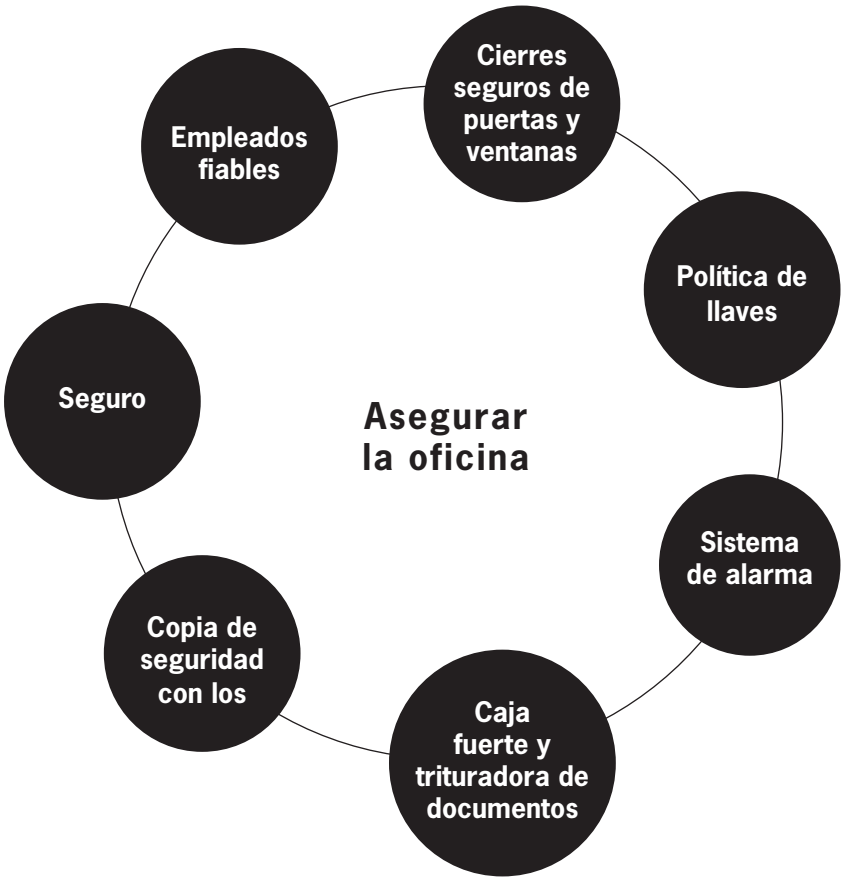
Descripción del "círculo de seguridad": seguridad compleja

Su seguridad es tan fuerte como su punto más débil. No hay mucho sentido comprar una fuerte puerta de metal para su oficina si no tiene idea de cuántas copias de llaves existen. Puede ser que, en un juicio, fracase en su defensa de una víctima de violación de los derechos humanos si los hechos no son correctos. Siempre debe evaluar el alcance completo de su situación de seguridad y estar dispuesto a percibir y tratar todos los puntos débiles, porque con frecuencia son los que destrozan el proceso de seguridad. Esto también es válido para la seguridad electrónica. Gastarse dinero en un cortafuegos caro no impedirá que el ordenador sea reciba daños físicos o que se lo roben. La aplicación de un sistema de correo electrónico cifrado no tendrá mucho efecto sobre la estrategia de comunicación de su proyecto si los otros miembros del mismo no aplican el mismo sistema. Debemos considerar nuestra seguridad desde la perspectiva de un círculo cerrado. Todos los elementos deben apoyarse unos a otros y los vínculos débiles deben ser tratados con el mayor cuidado[11]. Consideremos, por ejemplo, el proceso de establecer una oficina segura.

9
Al visor de sucesos se accede de la manera siguiente: Inicio > Configuración > Panel de control > Funciones de administración > Visor de sucesos. Esta opción sólo está disponible para los usuarios de Windows NT, 2000, XP. Esté atento a las señales de error indicadas por un signo de exclamación rojo o amarillo de advertencia.

10
http://www.markusjansson.net/

11
Existe otro enfoque para un sistema de seguridad: la defensa en profundidad. Aunque normalmente la seguridad sea tan fuerte como su vínculo más débil, debe ser diseñada, en lo posible, con protecciones independientes y redundantes, de modo que pueda fallar una sola sin que falle toda la cadena. Ejemplo: si su ordenador está infectado por un virus usted podrá recuperar los archivos perdidos de una copia de seguridad.



Probablemente puede imaginarse cómo un lapso en un área de este círculo puede conducir a un colapso de todo el sistema. Naturalmente, puede ser un poco más complicado: el sistema de alarma y la caja fuerte tendrán una combinación secreta para abrir o desactivarlos. Quien conozca esta combinación puede poner en peligro este sistema. A veces el personal "de confianza" puede ser, por desgracia, también un nombre equivocado.

—

Con todo, tener poca seguridad es mejor que no tener nada seguridad. No se deje intimidar por las situaciones difíciles explicadas en este capítulo. Sea un poco paranoico y ponga un cuidado especial con sus operaciones informáticas. Aprenda más sobre la tecnología que está utilizando y la legislación vigente en su país. Es mejor tener una contraseña larga que una corta, utilizar el **cifrado** que no utilizarlo. Pero no confíe demasiado en la seguridad electrónica sin antes ser consciente de todas las complejidades.

2.1 LA SEGURIDAD DE WINDOWS

RESUMEN

1 Actualice regularmente el sistema operativo.
2 Conozca la ubicación de los diferentes archivos y documentos que tiene en su ordenador.
3 Utilice una contraseña de BIOS para proteger el ordenador en el inicio.
4 Utilice la función de bloqueo de la pantalla o la contraseña para proteger la pantalla con el fin evitar el acceso inmediato a su ordenador.
5 No use una contraseña vacía y no la revele a los demás.
6 Tenga cuidado al instalar software nuevo o comprar un ordenador con software preinstalado. Use sólo el software que sea necesario para la función que usted desempeña y elimine todo lo demás.

Hemos hablado de la seguridad de su entorno de trabajo y la importancia de conocer el funcionamiento de su ordenador. Este capítulo presenta un aspecto más técnico. La estabilidad del sistema operativo de su ordenador es esencial para su funcionamiento. Un *software* y *hardware* diferentes podrían tener un impacto negativo sobre su funcionamiento y seguridad si usted no sabe vigilarlo y controlarlo. Su sistema operativo le ofrece la oportunidad de aumentar (o disminuir) la seguridad de su ordenador mediante varios ajustes de configuración. Es como la sede central de su ordenador. Si bien la seguridad no depende únicamente del sistema operativo, es importante conocer las vulnerabilidades y los puntos de administración críticos del mismo.

—

El sistema operativo (SO) Windows es bien conocido por sus muchas vulnerabilidades de seguridad, pero si no cambia a un sistema operativo diferente (p. ej., la distribución Ubuntu del sistema operativo Linux[12]), debería al menos ser consciente de la mejor metodología para asegurar lo que tiene. Esta sección se divide en diferentes categoría y está ordenada por las versiones del SO Windows. Cabe señalar que las versiones específicas de Windows, como XP Professional, tienen numerosas características de seguridad pero que, sin embargo, no vienen activadas por defecto: tiene que activarlas usted mismo.

La actualización

Las actualizaciones de Windows son adiciones al SO que no se incluyeron en la versión inicial. Suelen ser actualizaciones y parches para resolver las vulnerabilidades descubiertas. Las actualizaciones grandes se denominan paquetes de servicio. Microsoft ha dejado de lanzar estas actualizaciones para Windows 95, 98 y NT. Puede encontrar y descargar todas las actualizaciones de los años anteriores, pero no recibirá el apoyo continuo. Las actualizaciones y revisiones de seguridad para Windows 2000 y XP estarán disponibles al menos hasta 2011[13].

—

Si no tiene acceso a Internet es menos vulnerable a muchos de los ataques electrónicos. Pero, aun así, es recomendable que encuentre actualizaciones para su SO en el disco o CD. Siempre puede escribir una carta o un correo electrónico a Microsoft y solicitar el último paquete de servicio (tenga en cuenta que tendrá que incluir datos de las licencias de su producto original).

12 http://ubuntu.com

13 http://support.microsoft.com/gp/lifesupsps#Windows

Si está conectado a Internet, puede visitar http://update.microsoft.com y seguir el proceso descrito en el sitio web para descubrir su versión actual de Windows y las actualizaciones e instalar todas las que sean necesarias. Si tiene Windows XP el sitio web, primero, comprobará que su licencia de *software* de Windows sea válida. Aunque su conexión a Internet sea lenta y costosa, le recomiendo encarecidamente que instale estas actualizaciones. Si la conexión a Internet es un problema le sugiero instalar sólo las "Actualizaciones críticas".

—

También puede obtener todas las actualizaciones para cualquier SO en la página web del Catálogo de actualizaciones de Microsoft[14] de donde puede descargarse los archivos. Esta es una opción útil para compartir las actualizaciones de Windows entre muchos ordenadores sin tener que conectar cada uno a Internet. El Catálogo de actualizaciones de Microsoft contiene actualizaciones para todas las versiones de su SO y no comprueba la validez de la licencia de su producto.

—

Los usuarios de Windows ME, 2000 y XP que tengan una conexión permanente a Internet pueden especificar que Windows compruebe periódicamente las actualizaciones y las instale en cuanto sean publicadas. Vaya a '**Panel de control**' y seleccione "Actualizaciones automáticas" (en 2000) o "Centro de seguridad" (en XP). Elija las opciones que automáticamente descargarán e instalarán las actualizaciones.

EL BLOQUEO DE LA PANTALLA

Cada ordenador con Windows le ofrece la opción de proteger con una contraseña el acceso inmediato cuando el ordenador está encendido; podría ser mediante la activación de un bloqueo de la pantalla o una contraseña de salvapantallas.

► Bloqueo de la pantalla: **Windows NT y 2000**

Asegúrese de que su cuenta de usuario permite la contraseña.
`Presione simultáneamente las teclas CRTL + ALT + DEL.`
`Presione la tecla Enter.`

► Bloqueo de la pantalla: **Windows XP**

Opción 1: `Presione la tecla Windows (si la tiene) + L.` 

Opción 2: Debe usar el tema "Clásico" de Windows para activar la función de bloqueo de la pantalla.

`Seleccione Inicio > Configuración > Panel de control.`
`Haga doble clic en "Cuentas de usuario".`
`Haga clic en "Cambiar la forma en que los usuarios inician y cierran sesión".`
`Desmarque "Usar la pantalla de bienvenida".`

Ahora puede usar la combinación de las teclas `Ctrl + Alt + Del`.

14
http://v4.windowsupdate.microsoft.com/catalog/

Opción 3

Haga clic con el botón derecho del ratón en un espacio vacío en del escritorio.
Seleccione Nuevo > Atajo
Escriba “rundll32.exe user32.dll, LockWorkStation”.
Presione “Siguiente”.
Escriba un nombre para el icono nuevo (por ejemplo: “Bloquear ordenador”).
Presione “OK”.

De este modo, se creará un icono en el escritorio: haga doble clic en él para bloquear la pantalla del ordenador. Para desbloquearla tendrá que introducir su contraseña.

Windows 95, 98 y ME

Desafortunadamente, en estas versiones de Windows no existe una función separada del bloqueo de la pantalla, así que tendrá que crear una contraseña para salvapantallas y poner un icono o un límite de tiempo para activarla.

Salvapantallas: (todas las versiones de Windows)

En el escritorio, haga clic con el botón derecho del ratón y elija “Propiedades” del menú que aparece. Vaya a la ficha “SALVAPANTALLAS” y seleccione un salvapantallas. Marque la casilla “Proteger con contraseña” y escriba la contraseña deseada. Establezca un límite de 5 minutos. Ahora cree un atajo para activar el salvapantallas a solicitud: así no tendrá que esperar 5 minutos antes de que se ponga en marcha.

Seleccione Inicio > Buscar (archivos y carpetas).
Escriba “*.scr”.
Presione Enter.

Los resultados mostrarán todos los salvapantallas que hay en su ordenador. Elija cualquier de ellos y haga clic sobre él con el botón derecho del ratón.

Seleccione Enviar a -> Escritorio (“Crear atajo”).

Ahora puede activar el salvapantallas haciendo clic en el icono que habrá aparecido en la pantalla de su escritorio. Sin embargo, se puede hacer aún más simple:

Haga clic con el botón derecho del ratón en el icono y seleccione “Propiedades”.
Haga clic en el cuadro de texto llamado “atajo” y presione Ctrl Alt S.

Presione “OK”. Ahora, el salvapantallas se iniciará cada vez que se pulse esta combinación de teclas.
No se trata de una medida de seguridad avanzada, pero es mejor que simplemente el ordenador abierto.

14
http://v4.windowsupdate.microsoft.com/catalog/
Windows 95 users should go to http://www.microsoft.com/windows95/

BIOS

Cada ordenador tiene el **BIOS**: *Basic Input/Output System*. Su finalidad es dar a su ordenador instrucciones iniciales para empezar. El **BIOS** es un conjunto de rutinas de *software* esenciales que se ejecutan cuando se enciende el ordenador. Ponen a prueba los dispositivos de *hardware* e inician el disco duro y el sistema operativo. Las instrucciones del **BIOS** se almacenan en un lugar llamado ROM (Read Only Memory, ?memoria de solo lectura') y generalmente son invisibles para el usuario. Sin embargo, la mayoría de los ordenadores le ofrecen la opción de inspeccionar y ajustar las configuraciones del **BIOS**; entre ellas, la protección por contraseña.

El menú del BIOS

—

Para entrar en el **BIOS** del ordenador se le suele a pedir que presione una tecla determinada de su teclado en la pantalla de inicio. Suele ser la tecla F1, F2, F10 o F12, según el tipo de **BIOS** que tenga. A veces, también puede ser la tecla ESC o DEL. Algunos ordenadores saltan esta pantalla muy rápidamente y es posible que tenga que presionar el botón "Detener" de su teclado para poder leerla. Aquí solo comentaremos la configuración de la contraseña. No cambie la configuración estándar del **BIOS** si no conoce su finalidad. No todas las **BIOS** son iguales; en el suyo encontrará dos de las siguientes contraseñas o todas ellas.

—

Contraseña de inicio: Esta protegerá el **BIOS** contra el inicio sin una contraseña válida. No se cargarán dispositivos y su ordenador no se iniciará.

—

Contraseña de disco duro: Esta protegerá el **BIOS** contra el inicio y el lanzamiento del disco duro del ordenador. Esta es una opción útil para su portátil, que a menudo se queda en el modo "de espera".

—

Contraseña de supervisor (contraseña del **BIOS**): Esta es la contraseña principal que puede sobrescribir las dos anteriores. No hay que configurarla, pero si la olvida o si quiere cambiar alguna de las otras dos la necesitará.

—

La configuración de estas contraseñas impide el acceso inmediato a su ordenador, si está apagado. Se trata de un elemento de disuasión rápida de un intruso menos ambicioso. La seguridad está lejos de ser infalible, ya que hay varias formas de eliminar la contraseña de **BIOS**. Casi todas incluyen la apertura física del ordenador. Después de haber hecho esto, puede resetear **BIOS** o simplemente sacar el disco duro y ponerlo en un ordenador diferente que no tenga protección mediante contraseña del **BIOS**. Por lo tanto, si tiene un candado en su caja – bien construida y fuerte – del ordenador está, de nuevo, aumentando la seguridad de acceso a su información. Si olvida su contraseña del **BIOS** tendrá que recurrir a los métodos descritos anteriormente para restablecerla.

15
These tools can be found in the *NGO in a Box – Security edition*, and on the website http://security.ngoinabox.org

LA INSTALACIÓN DE SOFTWARE

La mayoría de los ordenadores viene con *software* preinstalado. Tenga en cuenta que esto puede ser perjudicial para la seguridad de su ordenador. Todo lo que necesita, en un principio, es el CD de Windows y el juego de herramientas *Security-in-a-Box*. Cualquier otro *software* puede encontrarlo en Internet y todo gratis[15]. El *software* preinstalado en un ordenador nuevo a menudo contiene muchas versiones de prueba de las herramientas de limpieza de virus, paquetes gráficos, etc. También puede contener programas espía (el gobierno chino está considerando una ley que requiere que todos los fabricantes y los comerciantes preinstalen un *software* de censura en todos los equipos nuevos). Si utiliza sólo herramientas de *software* recomendadas y de confianza, instale un limpiador de virus totalmente funcional y un cortafuegos: estará mucho más seguro cuando se conecte a Internet por primera vez.

Al instalar nuevo *software* investigue de antemano el productor y tome una decisión acerca de su credibilidad. No instale *software* innecesario que pueda decorar su monitor o facilitar el relleno de formularios de Internet. Por lo general, este tipo de *software* lleva muchos de los problemas descritos en este manual. No piense que un ordenador puede manejar cada programa que elija instalar. Si necesita un ordenador sólo para consultar el correo electrónico y escribir documentos lo único que le hace falta es el OpenOffice (http://openoffice.org) y Mozilla Thunderbird (http://mozillamessaging.com/thunderbird/). No instale nada más. Es así de simple.

15
Un gran recurso de diferentes programas informáticos (gratuitos y revisados) son los juegos de herramientas publicados por el Tactical Tech Collective http://tacticaltech.org/toolkits. Además, puede registrarse en http://www.socialsourcecommons.org para ver qué otras herramientas utilizan los activistas y las ONG de todo el mundo.

2.2 LA PROTECCIÓN POR CONTRASEÑA

RESUMEN

1 No se fíe en las contraseñas de Windows para proteger su información. Son fáciles de romper.
2 Cree contraseñas con 10 caracteres o más. También puede utilizar una frase corta como contraseña.
3 Es mejor apuntar las contraseñas y mantenerlas a buen recaudo que tener una corta y fácil de adivinar[16].
4 Use números, letras minúsculas, mayúsculas y símbolos en su contraseña.
5 Nunca use la misma contraseña dos veces.
6 No use contraseñas que puedan relacionarse o vincularse directamente con su vida o intereses personales.
7 No comparta sus contraseñas importantes con nadie.
8 Cambie su contraseña cada 3-6 meses.
9 Recuerde que hay muchos programas disponibles gratuitamente en Internet que pueden determinar su contraseña de Windows, el cifrado de la red inalámbrica y casi cualquier tipo de contraseña de ordenados que pueda tener.

Tener buenas contraseñas es una parte esencial del uso seguro de ordenadores y herramientas de comunicación digital. Ayudan a autenticar el acceso al servicio solicitado, ya sea una cuenta de correo electrónico, *login* de red u operaciones bancarias en línea. Una contraseña es como la llave de una puerta. Puede tener varias claves diferentes para su casa, su oficina, su coche y su caja fuerte. Ninguna de las cerraduras es igual y tiene una colección de llaves diferentes para abrirlas. Esto dificulta un robo, ya que aun cuando el ladrón encontrase una llave que abriera no podría abrir todas las otras puertas. Las cerraduras son cada vez más sofisticadas y costosas. Están hechas de muchos componentes distintos con el único propósito de impedir los robos. Lo mismo debería aplicarse a las contraseñas. Se trata de las cerraduras de las puertas por las que se accede a sus bancos de información. El advenimiento de los ordenadores ha sido testigo de que la información protegida por las contraseñas a menudo es de un valor mayor que lo que hay guardado en su armario o caja fuerte. Por lo tanto, en un sentido técnico, para proteger la información, sus contraseñas deben ser tan fuerte como la más cara de las cajas fuertes.

—

En el mundo de la seguridad digital una buena contraseña es el elemento más esencial e importante de cualquier sistema. La historia ha demostrado que el método más común para los piratas informáticos e intrusos para atacar los sistemas de información es romper contraseñas.

DESCIFRAR CONTRASEÑAS

¿Cómo se comprometen las contraseñas? Existen varios métodos de hacerlo. Uno de ellos es observar a alguien desde cierta distancia cuando escribe su contraseña. Otro es instalar un programa de espía que registra todas las pulsaciones del teclado introducidas en el ordenador y las transmite al agresor. Ambos se pueden prevenir por un comportamiento cauteloso. Asegúrese de

16
Véase el artículo del blog de Bruce Schneier
http://www.schneier.com/blog/archives/2005/06/write_down_your.html.

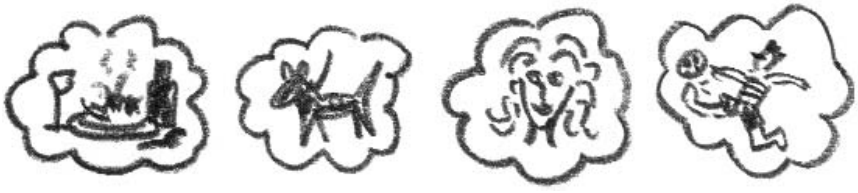
reconocer su entorno y ejecute frecuentemente programas antivirus y antiespionaje actualizados.

Perfiles de contraseñas

La creación de perfiles implica la realización de una conjetura fundamentada a partir de la recopilación de información personal y datos personales sobre la persona que posee la contraseña. En muchos casos nuestras contraseñas reflejan algo que nos resulta fácil de recordar: año de nacimiento, nombre de un familiar o un amigo, ciudad de nacimiento, equipo de fútbol favorito, etc. Los creadores de perfiles toman nota de estos y otros datos similares. Si es alguien que tiene acceso a su oficina, también puede ver los libros que tiene en su biblioteca. Sea cual sea el sistema que utilice para crear sus contraseñas se le puede excusar (¡al menos, hasta que termine de leer este capítulo!), ya que la capacidad de recordad muchas contraseñas diferentes que no tengan relación con usted y sean difíciles de memorizar es limitada. Sin embargo, adivinar la contraseña mediante la posesión de información personal sobre el usuario sigue siendo el método más habitual de comprometer un sistema y el de mayor éxito para los pirata informáticos motivados.

—

Muchos sistemas de contraseñas en Internet le ofrecen la opción de recuperar su contraseña a condición de que responda a una "pregunta secreta" previamente establecida. Por alguna razón inexplicable, estas preguntas secretas (que se establecen al crear una cuenta) siempre tienen algo que ver con el nombre de su mascota o de su primera escuela o el apellido de soltera de su madre. Eso facilita muchísimo las cosas a los creadores de perfiles. Ni siquiera tendrán que adivinar su contraseña; simplemente, responden a la pregunta secreta correctamente y reciben su contraseña en un correo electrónico. Si alguna vez se le pide crear un mecanismo de recuperación de la contraseña que consista en responder a una sencilla pregunta sobre su vida personal no lo use. Si es un requisito para finalizar el proceso de registro, simplemente escriba algo ininteligible. No se fíe del proceso de recuperación mediante una pregunta secreta para recordar una contraseña que ha olvidado.



►Contraseñas personales son fáciles de adivinar

Ingeniería social

Muchas personas han sido engañadas para revelar sus contraseñas a través de situaciones y preguntas astutamente creadas. Puede ocurrir que le llame su (supuestamente) proveedor de Internet y le diga que están mejorando sus servidores y necesitan su contraseña para asegurarse de que no pierda ningún correo electrónico en el proceso. Alguien podría hacerse pasar por un colega de otra filial de su ONG y solicitar la contraseña para acceder a la cuenta de correo electrónico común, porque la persona que la conoce está enferma y hay que enviar algo urgente. Este método se conoce como "ingeniería social". Ha habido numerosos casos de empleados que revelaron información que podía causar daño, simplemente porque fueron engañados. Para los piratas informáticos sigue siendo un método eficaz para intentar acceder a un sistema.
Nadie debería revelar ninguna información relacionada con un ordenador (sobre

19
Good advice from Steven Murdoch, a researcher in the Security Group of the University of Cambridge: is to verify the person's name and affiliation, then look up their phone number in a trustworthy directory and call them back

todo las contraseñas y códigos de acceso) por teléfono ni a alguien cuya identidad no pueda verificar[17].

Fuerza bruta

La fuerza bruta es la práctica de adivinar la contraseña mediante el uso de todo tipo de combinaciones posibles. Podría significar el uso de una versión electrónica de un diccionario para probar cada palabra contenida en él. Puede parecer una tarea larga para un ser humano, pero para un ordenador es cuestión de segundos. Si su contraseña es una palabra ortográficamente correcta de un diccionario puede verse comprometida por un ataque de fuerza bruta en cuestión de minutos.

¿Tal vez utiliza como contraseña los primeros versos de una de las de 1.000 canciones o poemas más famosos? El mundo digital es cada vez más amplio y creciente con la transferencia de la literatura y el pensamiento mundiales a Internet. Existen compilaciones electrónicas de las obras de la literatura, y también pueden usarse para romper su contraseña, de modo que debería replantearse el usar una contraseña en lenguaje natural (una frase inteligible o famosa, una combinación de palabras o una frase completa).

—

Algunos sistemas de contraseñas están protegidos contra ataques de fuerza bruta. Podemos tomar como un ejemplo un cajero automático o un teléfono móvil: a pesar de que su contraseña sea una simple combinación de cuatro dígitos el sistema se apagará después de tres intentos incorrectos.

LA CREACIÓN DE CONTRASEÑAS

Métodos mnemotécnicos

Existen diversos métodos para crear contraseñas que sean difíciles de romper y fáciles de recordar para nosotros. Un método popular es el de la mnemotécnica (un método o sistema para mejorar la memoria, como una rima o un acrónimo[18]). Tomemos una frase común:

"¿Ser o no ser? Esa es la cuestión." (*Hamlet,* Shakespeare)

La podemos convertir a "SRonSR?SIaC".

En este ejemplo, hemos sustituido las palabras con una letra que suena similar, poniendo los sustantivos y verbos en letras mayúsculas y el resto de palabras en minúsculas. O, por ejemplo:

"Soñé que todos los hombres nacían iguales." (Martin Luther King)

"SÑqtlHMsNC="

Parece que sea una contraseña relativamente aleatoria y no es tan difícil de recordar porque usted sabe el truco de cómo fue formada. Otras sugerencias son sustituir por números las letras que tengan un aspecto similar a éstos

I, i, l, t = 1; o,O = 0; s, S = 5,2) o abreviar palabras usando números, letras y signos

("No más problemas" = "No+proble+";

"Cansados por el estrés" = "Knsa2?Ls3").

17
Un buen consejo de Steven Murdoch, un investigador del Grupo de Seguridad de la Universidad de Cambridge, es que compruebe el nombre y la afiliación de la persona, después busque su número de teléfono en un directorio de confianza y le devuelva la llamada.

18
WordNet, de David Slomin y Randee Tengi.

Esto son sólo algunos ejemplos básicos; usted siempre puede crear su propio método de codificación de números y palabras. Se lo recomendamos.

Nota: Por favor, ¡no use como contraseña los ejemplos que acabamos de mostrarle!

► Captura de pantalla del programa "KeePass"

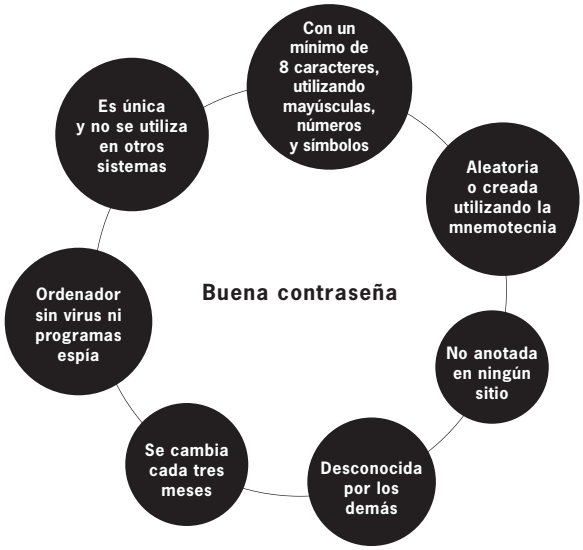
EL USO DE SOFTWARE

El siguiente paso hacia la mejora de la complejidad de su contraseña es utilizar un programa de generación de contraseñas[19]. Este programa creará una contraseña aleatoria y la guardará de forma segura. Con el programa de creación de contraseñas podrá utilizar contraseñas extremadamente complicadas y ¡nunca tendrá que recordarlas! Es la solución ideal. Estos programas suelen ser muy pequeños y pueden llevarse en un disquete o una memoria USB.

Puede agrupar sus contraseñas en categorías y copiarlas desde el programa a la pantalla utilizando el portapapeles. Las contraseñas se guardan cifradas en el programa. Por lo tanto, la única contraseña que tendrá que recordar es la del acceso al programa en sí.

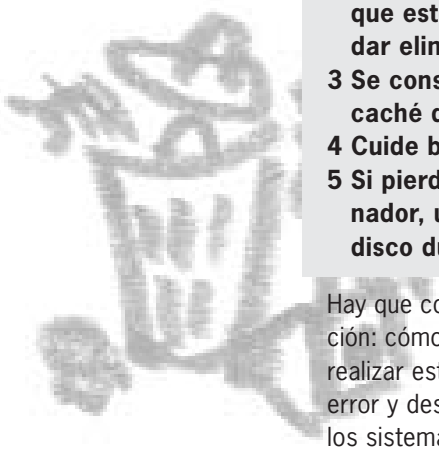
Tardará un poco en empezar a crear y guardar todas las contraseñas en un programa de este tipo, pero los beneficios en seguridad son enormemente mayores que los inconvenientes de hacerlo.

Su contraseña es a menudo la primera y más importante garantía de la seguridad de su información. Es como la puerta de su casa. El uso de una contraseña mala o no usar ninguna es como dejar la puerta abierta toda la noche. Tal vez no entre nadie o tal vez entren y le roben sus posesiones. Preste una gran atención a cómo crea sus contraseñas y dónde las guarda.



19
Véase el programa KeePass en el juego de herramientas Security-in-a-Box
http://security.ngoinabox.org/keepass_main

2.3 COPIA DE SEGURIDAD, DESTRUCCIÓN Y RECUPERACIÓN DE LA INFORMACIÓN



RESUMEN

1 Una estrategia de copias de seguridad debe incluir: el archivo de los datos, la frecuencia de la actualización del archivo, la ubicación y el almacenamiento del archivo.
2 No basta con borrar simplemente los datos de su ordenador para que estos sean irrecuperables. La información sensible deber quedar eliminada de su ordenador.
3 Se considera una buena práctica borrar los archivos temporales, el caché de Internet y el espacio libre de su ordenador.
4 Cuide bien el entorno físico de su ordenador.
5 Si pierde un documento haga una búsqueda exhaustiva de su ordenador, utilizando la función de búsqueda de Windows, y analice su disco duro con software de la recuperación de datos.

Hay que considerar dos cuestiones importantes cuando se trabaja con información: cómo duplicar la información y cómo destruirla. Los ordenadores permiten realizar estos dos procesos de forma rápida y eficiente, y son, una vez más, el error y descuido humanos las causas más comunes del mal funcionamiento de los sistemas. En este capítulo exploraremos la teoría que hay detrás del hacer réplicas de la información contenida en el ordenador, de la restauración de los datos perdidos y del borrar información innecesaria o confidencial sin la posibilidad de recuperarla. También se describirán las buenas prácticas en este ámbito.

COPIA DE SEGURIDAD

Los documentos importantes suelen duplicarse. La Declaración de Independencia estadounidense fue producida originalmente en 251 ejemplares. La gente hace fotocopias de sus pasaportes, declaraciones de impuestos y carnés de conducir. Se hacen copias de manuscritos antes de enviarlos a la editorial. Todas estas son precauciones contra la pérdida de documentos y de la información contenida en ellos. La duplicación hecha por el ordenador es un procedimiento muy fácil y rápido. Hay numerosos programas que crean copias idénticas de la base de información original y las guardan donde usted prefiera. Los tiempos en que la pérdida de su libreta de direcciones conllevaba una laboriosa búsqueda de los números de teléfono olvidados ya han pasado, y eso, como verá, es a la vez una bendición y una maldición.

—

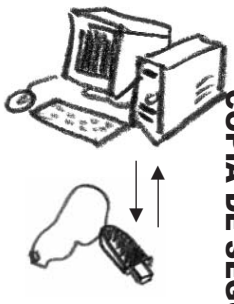
La necesidad de crear una copia de seguridad de los archivos se sustituye a menudo por la creencia que “no va a pasar nada malo”. Confiamos en que ni nosotros ni nuestro ordenador vamos a olvidar, perder o dañar la información.

—

La pérdida de información se produce a nivel micro y a nivel macro. Por un mal funcionamiento de un programa o por un virus puede perder un solo documento. Pero también puede perder todo el contenido de su ordenador por un fallo de *hardware* o por daños intencionados. Tenga siempre una estrategia de copias de seguridad para todas las situaciones.

Estrategias de copias de seguridad

Considere el tipo, la cantidad y la frecuencia de copias de seguridad de su información. Puede que prefiera llevar consigo una memoria USB con una copia de todos sus documentos. Si su equipo tiene una grabadora de discos compactos puede hacer una copia de seguridad de una gran cantidad de documentos, fotos y archivos de audio semanalmente y guardarla en un lugar aparte. Si tiene en su oficina un servidor hay que hacer copias de seguridad periódicas no sólo de los documentos que los usuarios guardan en él, sino que también de la configuración del *software* y del sistema.



Archivos de acceso frecuente

Se refiere a los documentos de trabajo a los que necesita tener acceso continuo. Estos archivos se actualizan constantemente y es necesario tener disponible la última versión.

El dispositivo más aplicable en este caso sería la memoria USB: es pequeña, no tiente partes móviles (por lo tanto, es menos propensa a sufrir daños que un disquete) y generalmente proporciona espacio de almacenamiento suficiente para un gran número de documentos. Debería sincronizar el contenido de una carpeta que tenga en el ordenador de su casa/oficina con la memoria USB[20].

► Frecuencia de las copias de seguridad: diaria.

Archivos de acceso poco frecuente

Se refiere al conjunto de la totalidad de su archivo de documentos, construido a lo largo del tiempo. Los archivos se crean y actualizan con poca frecuencia. Puede que no sea necesario conservar las últimas versiones de cada archivo, pero sigue siendo esencial tener una copia de seguridad.

-En este caso el dispositivo más eficaz para usar como copia de seguridad sería un CD-ROM regrabable (CD-RW). Le permitirá disponer de hasta 800MB de almacenamiento y sobrescribir el archivo anterior con el actual. Sólo tendrá que cuidar de uno o dos discos compactos a la vez[21].

► Frecuencia de las copias de seguridad: semanal.

PARA LOS TECHIES

ARCHIVOS DEL SISTEMA

Para evitar un largo proceso de restauración en el caso de un desplome o un mal funcionamiento del ordenador, debe hacer periódicamente una copia (imagen) de todo su ordenador. Se trata de una opción avanzada, probablemente adecuada para los administradores del sistema o quien cuide de su ordenador. Una copia de seguridad del sistema incluye todos los programas instalados (y sus licencias), el registro del sistema, **controladores de dispositivo**, etc.

Una forma de hacer esta copia de seguridad sería con una unidad de cinta. Estas unidades son bastante caras y generalmente no vienen como estándar con la compra de su ordenador. Otra opción es comprar un disco duro extraíble y hacer la copia de seguridad en él. Una copia de seguridad completa del sistema, por lo general, requiere un *software* especializado, conocido como imagen de disco. También se puede hacer utilizando la funcionalidad integrada en Windows, a la que puede acceder desde Inicio > Programas > Accesorios > Herramientas del sistema > Copia de seguridad. En caso de incendio u otro desastre, es esencial conservar la copia de seguridad del sistema en otro lugar que no sea aquel donde se encuentra el ordenador.

► Frecuencia de las copias de seguridad: mensual.

20
Para llevar a cabo la sincronización use un programa como Allwaysync (http://www.allwaysync.com).

21
Utilice el programa de copias de seguridad Cobian (http://security.ngoinabox.org/cobian_main) en combinación con un programa de grabación de discos compactos como DeepBurner Pro (http://www.deepburner.com).

Por seguridad, no cree demasiadas copias de seguridad. Si no puede sobrescribir un CD semanalmente, asegúrese de destruir adecuadamente las versiones obsoletas. De esta manera, a un agresor le resultará más difícil encontrar los archivos de copia de seguridad y usted no va a confundirse en cuanto a qué CD contiene la última copia de sus documentos.

DESTRUCCIÓN DE LA INFORMACIÓN

Es prácticamente imposible borrar por completo toda la información almacenada en su ordenador sin tener que cortar, quemar o romper el aparato en pedacitos. Puede pensar que Windows ha vaciado la "Papelera de reciclaje", pero no es cierto. Debemos tomar las precauciones necesarias para asegurarnos de que los datos que ya no queremos que estén en nuestro ordenador sean debidamente eliminados.

Entre 2000 y 2002, los investigadores Simson Garfinkel y Abhi Shelat, del MIT, compraron un gran número de discos duros de segunda mano de diferentes distribuidores a través de la subasta en línea de eBay y los examinaron para comprobar si quedaba alguna información contenida en ellos. Pudieron recuperar más de 6.000 números de tarjetas de crédito y las páginas web en caché donde se utilizaron algunas de ellas, además de partes médicos, cartas de amor e imágenes pornográficas, entre otros materiales. Parece ser que uno de los discos duros procedía de un cajero automático de Illinois.[22]

La recuperación de datos es una industria en crecimiento, y muchas empresas y organismos gubernamentales han avanzado increíblemente en lo que se refiere a rescatar datos perdidos y dañados. Otro elemento de la seguridad de nuestra información es la necesidad de que las organizaciones de derechos humanos no sólo mantengan a buen recaudo la información confidencial, sino que también la destruyan de forma adecuada. Es esta sección se examinará el proceso de eliminación permanente de la información no deseada de su ordenador.

Los problemas de la eliminación

No hay función del ordenador que pueda eliminar información. Hablando en rigor, los ordenadores sólo pueden escribir nuevos datos en el disco duro. Cuando elige la opción de "Eliminar" un archivo en Windows, simplemente, está diciendo al ordenador que ese espacio está disponible para ser sobrescrito con datos nuevos (aunque aparezca como "espacio libre"). Windows quita el icono del archivo y la referencia del nombre de su pantalla, como si el archivo ya no existiera, pero no elimina los datos reales de la unidad del disco duro. Se puede comparar con quitar la etiqueta en un archivador pero dejar aún los archivos en él. Hasta que haya sobrescrito el espacio físico exacto en el disco duro con datos nuevos, la información todavía está allí y puede verse fácilmente con la ayuda de *software* especializado.

La limpieza de datos

Aparte de desmagnetizar, quemar, someter a microondas o ingerir su dispositivo de almacenamiento digital, sólo hay un método seguro de eliminar los datos no deseados y preservar a la vez el uso del aparato en sí. Hay que sobrescribir los datos existentes con otros datos aleatorios. Este método es conocido como limpieza de datos. Puede limpiar un solo archivo, o puede limpiar el "espacio libre" en su disco duro. Con esta última opción lo que hará será encontrar todo el espacio que se encuentre actualmente sin asignación (o el espacio no utiliza-

22
Remembrance of Data Passed: A Study of Disk Sanitization Practices, publicado en IEEE Security & Privacy, ed. 1, nº 1, 2003, por SIMSON L. GARFINKEL y ABHI SHELAT, Massachusetts Institute of Technology.

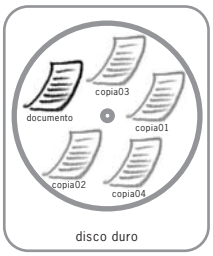
do por los archivos actuales) y sobrescribirlo con datos aleatorios. Los expertos coinciden en que para impedir la recuperación de su información se necesita al menos un pase aleatorio. El proyecto *Security-in-a-Box* ofrece la herramienta "Borrador" para limpiar la información no deseada de su ordenador[23].

—

El *software* de limpieza de datos – como, por ejemplo, el "Borrador" – puede integrarse con Windows y le permite limpiar archivos o el contenido de la "Papelera de reciclaje" con dos clics del ratón. El "Borrador" también puede limpiar todos los restos de los archivos pasados guardados en el "espacio libre" de su disco duro o dispositivo multimedia. Esta función es conocida como limpieza del espacio libre.

—

Debe ser consciente de que no son sólo sus documentos lo que debe eliminarse, sino también otros archivos utilizados por Windows y recogidos mientras usted utiliza el ordenador y navega por Internet.



►Se crean varias copias del documento cada vez que lo modifica

ARCHIVOS TEMPORALES

Esto archivos son recogidos por el ordenador mientras usted trabaja. Entre ellos se encuentran los documentos no terminados o no guardados, fotos y gráficos de Internet (también conocidos como caché) y una miríada de otros archivos que revelan sus actividades pasadas en el ordenador.

—

Imaginemos que está usted escribiendo un informe largo. Le lleva una semana de trabajo, varias horas cada día. Cada vez que pulsa "Guardar" antes de apagar el ordenador y salir de la oficina Windows crea una copia diferente de este documento y la guarda en el disco duro. Después de una semana de revisión tendrá en su disco duro varias versiones de diferentes etapas de realización. Windows no busca la ubicación física exacta del archivo original y lo sobrescribe cada vez: simplemente, pone la versión más reciente en es espacio del disco duro sin asignación. Esto puede, por supuesto, dar lugar a problemas cuando necesite borrar de su ordenador todas las huellas de este documento.

—

Debe eliminar el contenido de estas carpetas de forma periódica. Para una eliminación segura (irrecuperable) de todos los archivos temporales utilice la utilidad "CCleaner" (véase el proyecto *Security-in-a-Box*[24]).

Es muy importante eliminar los archivos temporales recogidos durante la sesión de trabajo, en especial cuando se utiliza un ordenador público, como uno en un cibercafé o una biblioteca. Puede llevar una versión portátil del programa CCleaner en su memoria USB y utilizarlo para limpiar los archivos temporales del ordenador. Véase el proyecto *Security-in-a-Box* para más información[25].

PAUTAS PARA LA LIMPIEZA DE DATOS

Si decide eliminar todas las huellas de archivos anteriores y temporales de su ordenador puede realizar los pasos siguientes, utilizando una de las utilidades de limpieza de datos contenida en el proyecto *Security-in-a-Box* u otra de su provisión.

Asegúrese de tener una copia de seguridad de todos sus documentos, archivos de licencia y registro de Windows.
Limpie las carpetas temporales que haya en su ordenador
Limpie todo el "espacio libre" que haya en su ordenador

23
http://security.ngoinabox.org/eraser_main

24
http://security.ngoinabox.org/ccleaner_main

25
http://security.ngoinabox.org/chapter_6_2

Adquiera el hábito de limpiar todos los archivos temporales antes de apagar el ordenador y siempre después de trabajar con un ordenador público.
Ejecute la limpieza del espacio libre en sus memorias USB, tarjetas de memoria de cámaras digitales y discos compactos regrabables.

PARA LOS TECHIES

Otra función de Windows que, sin saberlo usted, guarda sus documentos personales es el archivo de intercambio (también conocido como archivo de paginación). Windows utiliza el archivo de intercambio para facilitar las operaciones. Dicho de la forma más sencilla, es una parte del disco duro que se asigna Windows a sí mismo para manejar todas las operaciones que esté realizando usted. Cuando usted apaga el ordenador, el archivo de intercambio retiene toda la información que hubiera en él antes de apagarlo. Aunque utilice usted *software* de **cifrado**, sus archivos no se guardarán de forma cifrada en el archivo de intercambio. Le aconsejamos desactivar esta función (debe tener al menos 256MB de RAM en su ordenador para reemplazar la funcionalidad del archivo de intercambio) o utilizar una herramienta de limpieza para eliminar de forma segura información almacenada en el archivo de intercambio antes de apagar el equipo[26]. Para deshabilitar el archivo de intercambio en Windows 2000 y XP:

Seleccione Inicio > Configuración > **Panel de control** > Sistema.
Haga clic en "Opciones avanzadas".
Haga clic en "Rendimiento".
Haga clic en "Memoria virtual" (Opciones avanzadas > Memoria virtual para XP).
Deseleccione la opción del archivo de intercambio o póngala a "0".

Si trabaja con un portátil deshabilite la función de hibernación. Puede que tarde 30 segundos, pero va a disminuir en gran medida los riesgos de acceso a la información almacenada en su portátil.

Seleccione Inicio > Configuración > **Panel de control** > Opciones de energía.
Haga clic en "Hibernación".
Deseleccione "Habilitar hibernación".

La recuperación de la información

Los archivos que no han sido limpiados pueden ser recuperados. Algunas de las herramientas que tenemos a nuestra disposición pueden realizar búsquedas en nuestro disco duro u otros dispositivos de medios para encontrar archivos perdidos, dañados o corrompidos. Busque en Internet tecleando las palabras clave "herramientas de recuperación de datos" o instale la utilidad "*UndeletePlus*" del proyecto *Security-in-a-Box*[27].

—

Es posible que pueda aprovecharse de la incapacidad de un dispositivo digital para eliminar los datos correctamente. Por ejemplo, puede hacer una foto en su cámara digital y luego borrarla. Este método puede utilizarse para enmascarar la existencia de la foto original. Las herramientas de recuperación de datos se pueden utilizar para restaurar los datos borrados cuando sea necesario. Pero hay que tener cuidado de no sobrescribir la imagen que se necesite (tomando otro). Es necesario planificar y estudiar más esta técnica para utilizarla de forma segura.

26
Véase la herramienta de limpieza "Borrador" (Eraser, http://www.heidi.ie/eraser) o "BCWipe" (http://www.jetico.com/bcwipe.htm), que también puede encontrar en el CD NGO in a Box – Security Edition.

27
http://security.ngoinabox.org/undelete_main

Prevención

La prevención de un desplome y de una pérdida de los documentos requiere un enfoque cuidadoso de su entorno y su estabilidad. No beba, coma ni realice otras muchas funciones que podrían causar daños físicos en diferentes partes de su ordenador. Debido a la naturaleza compleja de los circuitos eléctricos, los ordenadores no reaccionan bien con el agua o campos magnéticos. Mantenga el ordenador alejado del suelo, para que los pasos pesados o saltos no lo sacudan. Asegure su ordenador contra las subidas bruscas de electricidad, ya sea con los estabilizadores y con fusibles. Puede plantearse comprar un suministro alternativo de baterías (SAI, Sistema de Alimentación Ininterrumpida; siglas en inglés: UPS). Lo mejor es preguntar a un experto en una tienda de ordenadores para que le dé una descripción más detallada de los elementos descritos y de cómo se puede evitar que su ordenador sufra daños.

26
Also see Graham Mayor's guide on *What to do when Word crashes* http://www.gmayor.com/what_to_do_when_word_crashes.htm

27
Handy Recovery http://www.handyrecovery.com/ also available on the *NGO in a Box – Security Edition* CD; also see http://www.officerecovery.com/freeundelete/

2.4 LA CRIPTOLOGÍA

RESUMEN

1 El proceso de hacer su información inaccesible a todos salvo la persona interesada se llama cifrado. Puede cifrar un mensaje, un correo electrónico o el ordenador entero
2 Para las comunicaciones seguras se utiliza el cifrado de clave pública. Nuestro método de cifrado consiste en una clave pública y otra privada. Compartimos la clave pública con los que desean comunicarse con nosotros. Ellos nos cifran un mensaje usando nuestra clave pública.
3 La seguridad del sistema de cifrado de clave pública se basa en la validez de la clave pública que se utiliza para el cifrado, en un ordenador sin virus ni programas espía y en una buena contraseña que protega su clave privada.
4 Podemos prevenir la manipulación no autorizada de nuestro correo electrónico en ruta a su destino mediante el uso de firmas digitales.
5 El nivel de seguridad que ofrece el cifrado ha llevado a que su práctica o su teoría (enseñanza) hayan sido prohibidas en varios países.

HISTORIA

La criptología se ocupa de las técnicas lingüísticas y matemáticas para asegurar la información. El mensaje se cifra para que sea ilegible para todos salvo para el destinatario. Su larga y pintoresca historia se remonta a alrededor del siglo V aC, cuando los espartanos crearon el más antiguo método de **cifrado** conocido, utilizando dos varas de madera del mismo grosor y un trozo de papiro. El papiro se enrollaba en espiral a una de las varas y en él se escribía el mensaje longitudinalmente. Al desenrollarlo, las letras no aparecían en ningún orden comprensible. El papiro se enviaba al destinatario, que contaba con una vara idéntica para poder leer el mensaje. Otros métodos para asegurar la información frente a los intrusos son la **criptología** lingüística (p. ej., los jeroglíficos) y la estenografía, que es el proceso de ocultar la existencia del mensaje en sí.

El mensaje se escribía de forma longitudinal en el papiro enrollado alrededor de la vara, llamada escítala. La escítala utilizaba lo que hoy en día se conoce como un sistema de cifrado de transposición, por el que se cambia el orden del as letras en un mensaje[28].

—

La seguridad que proporciona la criptografía por sí sola no debe sobrestimarse. Su falibilidad es normalmente el resultado de un error humano o de un error en el procedimiento general de seguridad. El uso de la criptografía ha sido restringido por la legislación de algunos países. Matemáticos, científicos y activistas de los derechos civiles en los EE.UU. libraron una batalla de 20 años para evitar que el gobierno prohibiese el acceso del público y el uso de la **criptología** en lo que hoy se conoce como "la criptoguerra".

EL CIFRADO

El **cifrado** (y su opuesto, el descifrado) es una rama popular de la **criptología**. El **cifrado** consiste en aplicar un gran patrón matemático a un conjunto de datos y cifrarlo de forma que parezca incomprensible para todos aquellos que no conozcan el método de descifrado, también llamado "la clave".

28
El dibujo está tomado de Wikipedia.org http://en.wikipedia.org/wiki/Cryptology.

El cifrado de discos

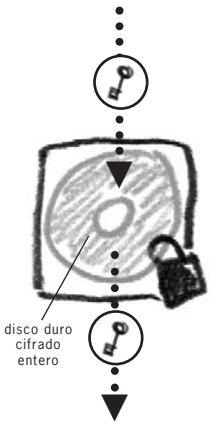
Puede utilizar el **cifrado** para proteger todo su disco duro. En esencia, cifrará cada dato almacenado en él, de modo que sólo usted pueda acceder a la información después de haber introducido la contraseña. Cada vez que se extraen los datos de su ordenador (por ejemplo, un archivo adjunto a un correo electrónico)estos se descifran automáticamente. Si le roban el ordenador la información contenida en él permanecerá inaccesible a los demás[29].

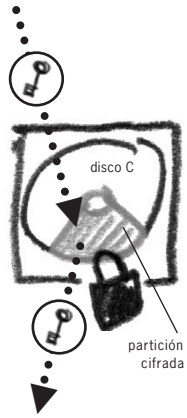
—

También puede crear en su ordenador una unidad virtual cifrada. Esta opción puede convenir a aquellos que no desean cifrar su ordenador entero, sino asignar un espacio donde almacenar información de forma segura. Si su ordenador tiene 5GB de espacio libre puede crear un contenedor cifrado y asignar 1GB de espacio para ello. Aparecerá como una nueva unidad en su ordenador (de hecho, esta unidad no es nueva y, por lo tanto, se refiere a ella como virtual). Puede configurar su programa de correo electrónico (p. ej., Thunderbird) para que almacene todos los archivos en la partición cifrada. Solamente usted, el dueño de la contraseña, podrá acceder al correo electrónico en esta partición.

—

También puede cifrar una memoria USB entera u otros dispositivos extraíbles. Esto es útil cuando viaja con todos sus documentos almacenados en su memoria USB. Hay programas, como el *True Crypt*, que también puede ejecutarse directamente desde una memoria USB, de modo que no necesitará tener el programa instalado en cada ordenador con el que desea acceder a los documentos cifrados.





El cifrado de clave pública

Los métodos tradicionales de cifrar la información que desea compartir con otra persona requerían que diese a esa persona la clave para descifrarla. Esto no era un método muy seguro, ya que podía poner en peligro su contraseña en el proceso. Para evitar este problema, los matemáticos desarrollaron el **cifrado** de clave pública (siglas en inglés: PKE). Hoy en día es el método más común de cifrar las comunicaciones (p. ej., correo electrónico).

—

Cuando utilice el cifrado de clave pública su clave se compondrá de dos partes: una pública y una privada. Juntas conforman un par de claves, las cuales están entrelazadas, de modo que lo que se cifra con una se puede descifrar con la otra. Esta es una parte esencial del cifrado de clave pública y una base para su seguridad y falibilidad.

—

Usted comparte su clave pública con quien quiera comunicarse. También puede enviarla a un servidor de claves en Internet. La clave privada se mantiene en secreto en su ordenador o en su disquete y, además, está protegida con una contraseña que sólo usted debe conocer. No comparta su clave privada con nadie. Si piensa que su contraseña ha sido comprometida (robada) tendrá que revocar su par de claves y volver a crearlas desde cero.

Cifrar y descifrar un mensaje [30]

En el sistema de cifrado de clave pública los mensajes están cifrados para enviárnoslos usando nuestra clave pública, y nosotros los desciframos con nuestra clave privada. La gente desea enviarle un mensaje cifrado obtiene su clave pública preguntándosela o buscándosela en un servidor de claves de Internet donde usted la habrá dejado anteriormente.

29
Un ejemplo de software que puede cifrar todo el disco duro, crear una partición cifrada o unidad virtual es TrueCrypt, disponible en el proyecto Security-in-a-Box (http://security.ngoinabox.org/truecrypt_main)

30
Un software que le sugerimos y con el que puede realizar el cifrado de clave pública es GPG4Win (http://www.gpg4win.org), o bien puede instalarse el programa de correo electrónico Thunderbird con la extensión Enigmail como se describe en el proyecto Security-in-a-Box (http://security.ngoinabox.org/thunderbird_usingenigmail).

Ejemplo: Me quiere enviar un mensaje cifrado. Primero, tengo que darle la copia de mi clave pública. Usted utiliza esta clave pública para cifrar el mensaje y enviarlo por correo electrónico u otro medio. Sólo yo podré descifrar el mensaje, ya que sólo yo tengo el enlace que falta: mi clave privada.

Tenga en cuenta que con "texto sin formato" nos referimos al mensaje original y con "texto cifrado" nos referimos al mensaje que ya ha sido cifrado.

Esto facilita la comunicación de mensajes cifrados sin tener que compartir una contraseña y aumenta enormemente la seguridad y la viabilidad de sus comunicaciones. El cifrado de clave pública se ha aplicado al correo electrónico, *chat*, navegación por Internet y muchos otros servicios de Internet. Su seguridad ha causado controversia con muchos gobiernos. El nivel de privacidad que ofrece la aplicación correcta de este sistema ha preocupado muchas agencias de inteligencia de vigilancia.

Seguridad de las claves

La fiabilidad del **cifrado** depende de:

- el tamaño de su par de claves (normalmente 2.048 bits de longitud);
- la capacidad de validar la clave pública del destinatario;
- la protección de su contraseña, que desbloquea la clave privada.

—

La infraestructura del cifrado de clave pública se basa en la identidad válida de la clave pública y privada. Cuando está cifrando un mensaje un mensaje destinado a mí con mi clave pública tiene que estar seguro de que esta clave me pertenece a mí. Echemos un vistazo a las propiedades del par de claves.

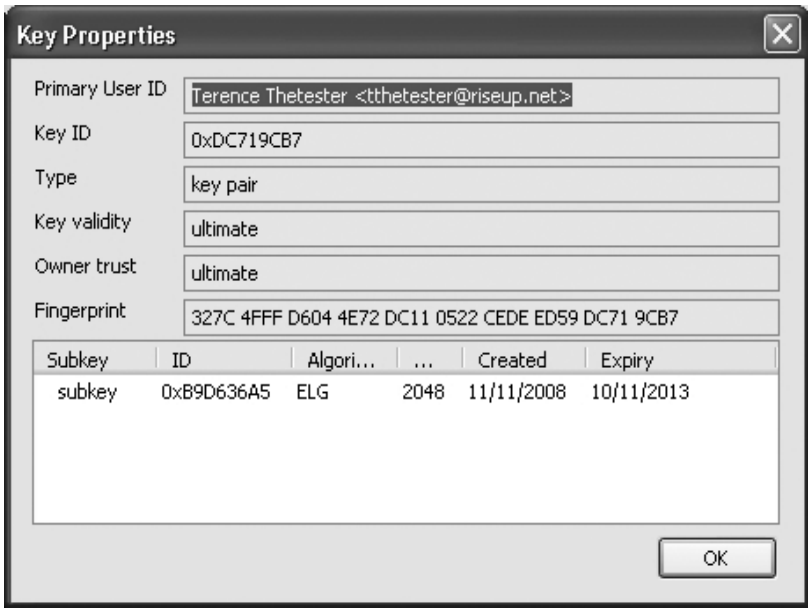
—

Un par de claves se identifica por 5 características distintas:

- Identificador del usuario: normalmente, la dirección de correo electrónico del titular de la clave. Asegúrese de que está escrita correctamente.
- Identificador de la clave: identificación única generada automáticamente por el programa de **cifrado**.
- Huella digital: (a veces denominada MD5 y SHA1. Véase el capítulo "**Cifrado** en Internet" para más detalles) se trata de un identificador único que se genera a partir de la clave pública.

29
Un ejemplo de software que puede cifrar todo el disco duro, crear una partición cifrada o unidad virtual es TrueCrypt, disponible en el proyecto Security-in-a-Box (http://security.ngoinabox.org/truecrypt_main)

- Fecha de creación: el día en que se creó el par de claves.
- Fecha de vencimiento: el día en que vence el par de claves.



►Huella digital, como se ve en el programa de administración de claves Enigmail

Pruebe y compruebe los datos anteriores antes de usar una clave pública de alguien para comunicarse con esa persona. Ya que el **cifrado** de clave pública no requiere que comparta una contraseña con el destinatario del mensaje, es importante que pueda validar la verdadera identidad de la clave pública. Las claves públicas son fáciles de crear, pero las características que las identifican también pueden ser falsificadas. Por eso debe autenticar la clave pública de la persona antes de usarla (veáse, a continuación, el apartado "Firmas digitales"). Una vez que haya comprobado que la clave pública pertenece a esa persona puede "firmarla": al hacer esto estará diciendo al programa que usted confía en la validez de la clave y desea usarla[31].

El tamaño de la clave es normalmente 2.048 bits. Este nivel de **cifrado** se considera mucho más complejo de lo que los ordenadores modernos pueden romper[32].

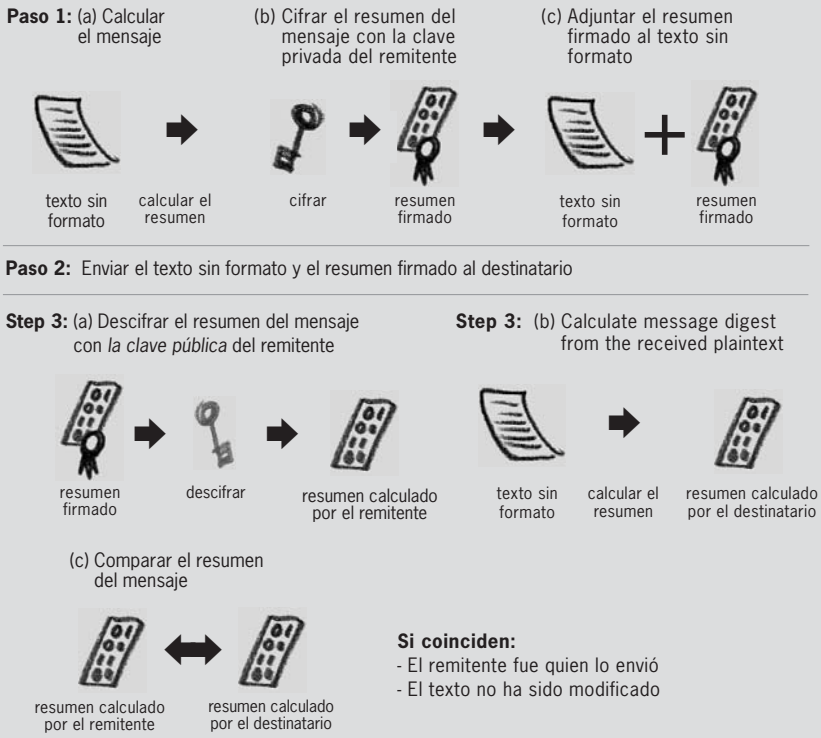
PARA LOS TECHIES

Firma digital

Es necesario que podamos verificar la autenticidad de nuestros mensajes. Esto puede hacerse mediante una firma digital, que también funciona con el cifrado de clave pública. Cuando usted firma digitalmente un mensaje está incluyendo en él un algoritmo matemático derivado de su tamaño, fecha y contenido específico. Después este resumen es cifrado con su clave privada para que el destinatario pueda verificar su validez. Una vez descifrado, el resumen original contenido en la firma se compara con el archivo recibido para confirmar si este ha sido modificado o no desde que se firmó. Es prácticamente imposible cambiar el contenido de su mensaje sin invalidar la firma.

31
Con ello también añadirá su firma a esta clave; en el caso de que la envíe a otra persona ésta verá su firma y sabrá que usted confía en la validez de esta clave.

32
En el artículo http://www.keylength.com/en/3/ encontrará la descripción de las actuales y futuras necesidades del tamaño de la clave.



►El esquema de la firma digital

Algunos programas (p. ej. GnuPG) que realizan el cifrado de clave pública pueden ser integrados con programas de correo electrónico (p. ej., GnuPG con Thunderbird utilizando la extensión "Enigmail" o con MS Outlook utilizando el conector de datos "G Data GnuPG plug-in"[33]) para hacer toda la operación más simple y rápida.

Es aconsejable que cifre todas sus comunicaciones una vez que usted y sus contactos hayan puesto en marcha el cifrado de clave pública. Esto contrarresta la posibilidad de levantar sospechas de un correo electrónico cifrado solitario que contiene información confidencial.
Para resumir, la utilización del **cifradob,** en realidad, no es tan difícil con el *software* moderno. Los principales puntos que debe recordar:

- Es necesario crear un par de claves y mantener su clave privada a buen recaudo.
- Usted cifra sus mensaje para el destinatario con la clave pública de esa persona.
- Siempre debe verificar la clave del destinatario comprobando la huella digital.

LA INSEGURIDAD DEL CIFRADO

El mayor problema con el uso del **cifrado** es que a veces da al usuario una falsa sensación de seguridad. El solo hecho de que esté utilizando el **cifrado** no significa que sus mensajes tengan que permanecer al 100% seguros. Por supuesto, es un excelente método de elevar el nivel de seguridad, pero no es infalible. El problema principal de seguridad del cifrado de clave pública es el factor humano: los errores que cometemos por negligencia o ignorancia. Menciono tres métodos de romper su privacidad del **cifrado**.

33
http://www3.gdata.de/gpg/download.html

34
http://www3.gdata.de/gpg/download.html

- **Comprometer su clave privada.** Si el agresor se las arregla para recibir una copia de la clave privada de usted, accediendo a su ordenador o de alguna otra manera, lo único que él tiene que hacer es romper la contraseña que la protege. Puede hacerlo por la fuerza bruta (usando un programa para romper contraseñas que prueba todas las combinaciones comunes y aleatorias) o por la simple observación cuando usted esté tecleando su contraseña. Otro método para robarle la contraseña sería instalar un programa conocido como "*keylogger*" accediendo a su ordenador con la ayuda de un archivo adjunto en un correo electrónico. Un programa "*keylogger*" graba todas las teclas que usted pulsa en el teclado y envía esta información a una dirección designada de Internet o de correo electrónico. De esta manera el agresor puede recibir la contraseña que usted utiliza para acceder a su clave privada, sin necesidad de acceso físico a usted o su ordenador.[34]

La solución es utilizar programas antivirus y antiespionaje y un cortafuegos, que tal vez detectarán la presencia de un programa "*keylogger*" o bien impedirán que envíe su contraseña. Tenga cuidado al escribir la contraseña y asegúrese que nadie puede ver su teclado ni la pantalla del ordenador. La mayoría de los programas de **cifrado** buenos no muestran la contraseña en la pantalla: tiene que escribirla "a ciegas".

- **Sistemas de recuperación de la clave.** Dado que el **cifrado** está hoy en día integrado en muchos dispositivos y se usa cada vez más, su marco extremamente seguro se ha convertido en un problema para muchos gobiernos y organismos que aplican la ley. Durante muchos años han estado tratando de aplicar sistemas de recuperación de claves (*key escrow*) que darían a las autoridades acceso a su clave privada. Como alternativa, los gobiernos empezaron a aprobar leyes que estipulan que una persona debe entregarles una copia de su clave privada para que la tengan guardada. Algunos programas de **cifrado** cerrados, donde el método de cifrado no ha sido probado públicamente, ofrecen una **puerta trasera** a los organismos de seguridad. Aunque esta práctica ha sido declarada ilegal en muchos países, todavía se puede encontrarse en diferentes versiones de *software* y *hardware*. La solución es utilizar productos de código abierto (como GnuPG), analizados a fondo y probados por la comunidad de Internet.

- **La validez de la clave pública y el engaño.** Como ya hemos mencionado en este capítulo, la validez de la clave pública que usted utiliza para el cifrado es fundamental para la seguridad global del cifrado de clave pública. El problema es que es fácil falsificar las claves públicas. Un descuido por parte del usuario puede dar lugar a la utilización de la clave de un adversario dando por supuesto de que en realidad pertenece a otra persona. Preste la máxima atención cuando recibe e importe claves públicas. Los pasos para verificar la validez de la clave pública se han explicado anteriormente. Aunque esto pueda retardar un poco el proceso de comunicación, estos pasos no deben ser ignorados.

Por supuesto, hay también métodos tradicionales de la intimidación y fuerza físicas que podrían utilizarse para que revele su contraseña.

—

Elija los programas de **cifrado** de los que se haya verificado públicamente que no tienen puertas traseras (como PGP, GnuPG, TrueCrypt). Entérese de las leyes

34
En 1991, el FBI lanzó una técnica llamada "Magic Lantern" (?Linterna mágica'). Según se informa, trataría de instalar un Caballo de Troya, adjunto a un correo electrónico, en su ordenador. Al activarlo, grabaría todas las teclas pulsadas por el usuario para escribir y enviaría esta información a la sede. Una justificación para esta acción fue la reacción a la creciente utilización del cifrado de clave pública. Dado que el FBI no podía leer un mensaje cifrado, trataron de robar la contraseña de la clave privada del usuario. Se dice que esta iniciativa se abandonó después de que se pusiese en duda su legitimidad en los tribunales, pero no podemos estar seguros de que, entretanto, no se haya desarrollado una variación.

locales, de si le permiten utilizar el cifrado y, en caso afirmativo, en qué nivel de complejidad (el tamaño de la clave)[35]. También debe entender que la legislación vigente en su país puede obligarle a que revele su contraseña a las autoridades. Trate de averiguar si hay garantías de la privacidad legislativa a las que pueda acogerse para evitar que esto ocurra.

35
Consulte la encuesta "Crypto Law" realizada por el Dr. Bert-Jaap Koops en http://rechten.uvt.nl/koops/cryptolaw/

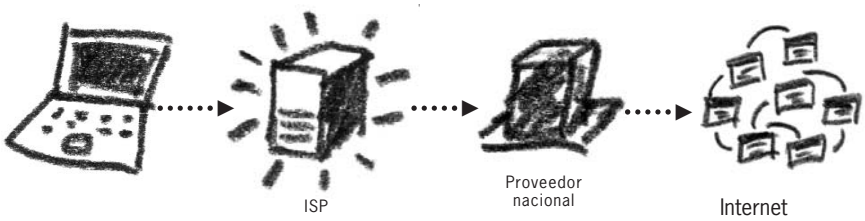
2.5 VIGILANCIA EN INTERNET

SUMARIO

1 Monitorizar tu Internet y tu actividad de correo electrónico es una tarea simple que realizan empresas y gobiernos en todo el mundo.
2 Las cookies registran tu actividad en Internet y son almacenadas en tu ordenador y los sitios web visitados.
3 El correo electrónico puede ser filtrado mediante la búsqueda de palabras y frases específicas en tu mensaje.
4 Las búsquedas en Internet y las páginas web solicitadas pueden ser filtradas al ser denegado el uso de palabras clave específicas.
5 El acceso a ciertos sitios web puede ser bloqueado para todos los usuarios de un determinado país.
6 El acceso a sitios web suele ser bloqueado de acuerdo a la dirección IP del sitio web o su nombre DNS.

Las posibilidades de vigilar y reunir inteligencia han progresado – desde monitorizar llamadas telefónicas y abrir el correo de otras personas hasta vigilar Internet. Dada la infraestructura abierta de Internet para buscar e intercambiar contenidos, la vigilancia hoy en día puede ser realizada por gobiernos, empresas, piratas informáticos y delincuentes. Establecer mecanismos que registren y monitoricen toda tu actividad en Internet es relativamente simple. Todos los sitios web registran la información sobre sus visitantes (su dirección IP y la hora de su visita), al igual que lo hace la mayoría de los proveedores de correo electrónico. Los proveedores de servicios de Internet conservan registros de toda la actividad que pasó por sus servidores. Tal "conservación de datos" se ha hecho obligatoria en muchos países. En 2006, la UE aprobó la legislación que requiere que los ISP almacenen los datos sobre el tráfico de todos sus abonados por un período de 2 años[36], aunque los estados miembros pueden decidir almacenarlos por un período de tiempo más largo. Veamos cómo puede ser monitorizada tu actividad en Internet.

MONITORIZACIÓN DE LA NAVEGACIÓN POR INTERNET



►El **ISP** puede monitorizar tu conexión de Internet

En principio, Internet es una versión más grande de una red de oficina. Está compuesto por ordenadores, conectados por cables, y asistidos por servidores, enrutadores y módems. Aunque tu mensaje en Internet puede cruzar un océano mediante un cable subterráneo, rebotar de dos satélites distintos y llegar al teléfono móvil de un usuario que se encuentra en un tren en marcha, el sistema se parece a una versión actualizada de una central telefónica. Y cuando eres un operador, un novio celoso o quieres realizar escuchas telefónicas,

36
Directiva 2006/24/CE del Parlamento Europeo y del Consejo del 15 de Marzo de 2006.

lo único que tienes que hacer es crear un auricular adicional en la línea de comunicación y podrás oír la conversación entera. Lo mismo ocurre con Internet. Cualquiera con acceso apropiado a la red puede interceptar y leer tu mensaje durante su camino alrededor del mundo.

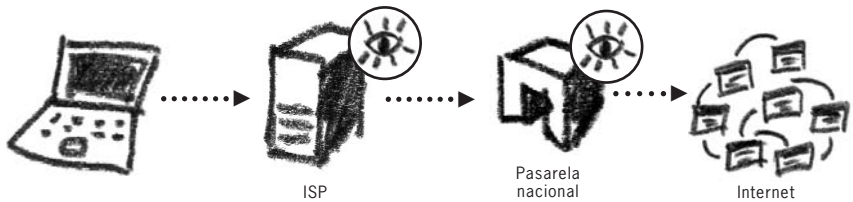
—

Mientras que interceptar un teléfono o una línea de Internet puede requerir habilidades específicas y acciones clandestinas, influir en el **ISP** es mucho más simple. Muchos países tienen sólo un **ISP** y éste suele estar bajo el control del gobierno. Países como Rusia han introducido leyes que requieren que todos los ISP instalen un ordenador específicamente para monitorizar la actividad que sus clientes desarrollan en Internet. Luego esta información se introduce directamente en las bases de datos del Servicio Federal de Seguridad de Rusia (FSB) [37].

—

Los países conectan a sus ciudadanos a Internet a través de una pasarela nacional. Todo el tráfico en Internet, por lo tanto, pasará por la pasarela nacional, y podrá ser sometido a vigilancia[38]. China ha instalado un sistema para monitorizar y restringir el tráfico en Internet en su pasarela nacional. El proyecto "Escudo Dorado" filtra y regula el acceso a Internet de toda la población de China[39].

►La monitorización de Internet en el ISP y en la pasarela nacional



A finales de los años ochenta, los EEUU, el Reino Unido, Canadá, Australia y Nueva Zelanda empezaron a desarrollar un sistema de vigilancia global que abarcaría los mayores puntos de tráfico en Internet. Los acontecimientos del 11 de septiembre en los Estados Unidos llevaron a inversiones enormes para mejorar el sistema conocido como **ECHELON**, que opera bajo la supervisión de la Agencia Nacional de Seguridad (NSA). No se sabe durante cuánto tiempo **ECHELON** conserva los datos relativos al tráfico. Puede parecer que a nivel global, es difícil analizar en tiempo real toda la comunicación telefónica y por Internet y clasificarla de manera eficaz, pero la NSA afirma tener un éxito del 90 % al hacerlo[40].

Monitorizando la actividad de sitios web

Registros de nuestra actividad en Internet se almacenan también en los sitios web que visitamos y en nuestros ordenadores personales. Muchos sitios web requieren la instalación de una cookie en nuestro ordenador. Una cookie es una pequeña cantidad de datos que almacena información específica sobre el usuario. Podría, por ejemplo, registrar el país de nuestra residencia, para que se nos presente la página del país correspondiente cuando visitemos este sitio web. Esta práctica es utilizada a menudo, por ejemplo, por sitios web de aerolíneas. La información puede incluir también los enlaces que hemos seguido para llegar a este o aquel sitio web, o incluso datos personales de nuestros propios ordenadores. Después de navegar por Internet más o menos un mes, puedes llegar a tener en tu ordenador cientos de cookies distintas. Al acceder a ellas, se puede obtener información acerca de tus intereses y afiliaciones. Una cookie en tu ordenador puede actuar como prueba de que has visitado un sitio web particular. El servicio de publicidad en Internet más grande, DoubleClick,

37
Privacy International – Informe sobre Privacidad y Derechos Humanos de 2004 – Las amenazas a la privacidad.

38
En algunos países, las conexiones vía satélite proporcionan una alternativa a la utilización del ISP local. Esto hace la vigilancia mucho más difícil de ejercer.

39
http://www.guardian.co.uk/commentisfree/2008/aug/13/china.censorship

40
Echelon Watch
http://www.nsawatch.org

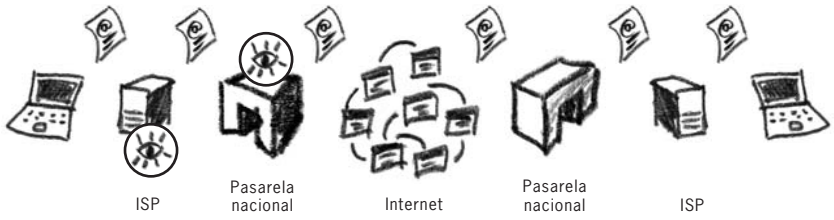
tiene acuerdos con miles de sitios web y mantiene cookies en más de 100 millones de usuarios, cada una de las cuales proporciona cientos de detalles relativos a las costumbres del usuario a la hora de navegar por Internet .

—

Es posible eliminar cookies de tu ordenador. Puedes conseguirlo mediante tu navegador de Internet o encontrándolas y eliminándolas manualmente. También es posible decirle a tu navegador que no acepte ninguna cookie. Esto puede causar que muchos sitios web no puedan abrirse en tu ordenador, pero te asegurará la protección máxima contra la infiltración de cookies. Para eliminar cookies de tu ordenador, utiliza la herramienta Ccleaner del proyecto la Caja de Herramientas de Seguridad[42].

Monitorización del correo electrónico

La comunicación por correo electrónico se basa en principios parecidos a los de la navegación por sitios web, salvo que cada mensaje tiene como destino una persona (o un grupo de personas) que también se conectan a Internet a través de su ISP.



►Monitorizando el correo electrónico en el ISP y en la pasarela nacional

Por lo tanto, un mensaje de correo electrónico pasará por tu ISP, la pasarela nacional de tu país, alrededor de Internet en sí, y luego llegará a la pasarela nacional del destinatario, y pasará por su ISP antes de, finalmente, ser leído por el destinatario. Siguiendo este esquema, nuestro mensaje de correo electrónico puede ser interceptado en todos los principales puntos de enrutamiento a lo largo de su camino. Si vives en un país con una fuerte protección legal de la privacidad, su legislación no se aplicará cuando tu correo electrónico llegue al **ISP** del destinatario que vive en un país con distintas leyes de privacidad y vigilancia. Ten en cuenta que mientras que tu correo electrónico está de camino del país A al país B, podría pasar, a lo largo de su ruta, por los enrutadores de varios países (y empresas).

—

Muchos ISP y proveedores de correo electrónico guardan una copia de todos los correos electrónicos en sus servidores. A veces, esto es beneficioso para nosotros, ya que quizás un día querremos acceder un correo electrónico que enviamos hace 3 años. Sin embargo, esto también permite a una tercera persona solicitar acceso a nuestras cuentas de correo electrónico. Anteriormente, Yahoo! entregó al gobierno chino información sobre las cuentas de cuatro activistas democráticos y académicos chinos, lo cual provocó su detención y posterior condena[43].

FILTRADO Y CENSURA DE SITIOS WEB

Aparte de monitorizar el tráfico en Internet, el gobierno y empresas de telecomunicaciones tienen la capacidad de impedir el acceso a ciertos sitios web o de controlar el resultado de una consulta en el buscador. El filtrado de acceso a la información en Internet es, en esencia, una forma de censura y supone un incumplimiento de los artículos 18, 19 y 20 de la Declaración Universal de los

41
Privacy International – Informe sobre la Privacidad y Derechos Humanos de 2004 – Las amenazas a la privacidad

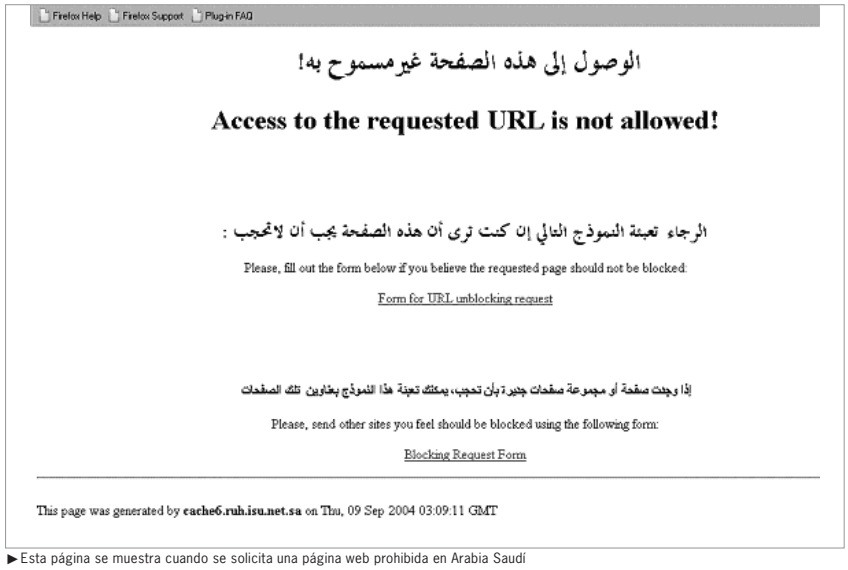
42
http://security.ngoinabox.org/ccleaner_main

43
Human Rights Watch – "Carrera hacia el fondo: Complicidad corporativa en la censura china en Internet", agosto de 2006.

Derechos Humanos (DUDH[44]) que declara que cada persona debería tener derecho a la libertad de pensamiento, religión, opinión, expresión y asociación, tanto como a "…buscar, recibir y difundir informaciones e ideas, sin limitación de fronteras, y por cualquier medio de expresión."

Censura en Internet

Muchos países prohíben a sus ciudadanos el acceso a ciertos sitios web. Estos sitios web a menudo contienen información sobre movimientos religiosos extremistas y sobre propaganda, contribuyen a la difusión de sentimientos proterroristas, o existen con el fin de exponer y distribuir imágenes de pornografía infantil. Algunos países optan por bloquear el acceso a los sitios web que critican o ponen en evidencia la política del gobierno, discuten cuestiones relacionadas con los derechos humanos o proporcionan herramientas que podrían hacer posible que se evite la práctica de la censura. La iniciativa OpenNet estudia las tendencias y tecnologías que se aplican para la censura en Internet y el filtrado de contenidos alrededor del mundo[45].



▶ Esta página se muestra cuando se solicita una página web prohibida en Arabia Saudí

El acceso a sitios web puede ser bloqueado utilizando cualquiera de los tres métodos más comunes: bloqueo de la dirección IP, modificación del sistema de nombres de dominio, o bloqueo de las URL. Dicho de otra manera, esto significa que un sitio web puede ser bloqueado de acuerdo a su dirección de Internet, nombre, o el sistema que traduce su nombre en una dirección de Internet.

—

En algunos países, la censura de sitios web existe, fundamentalmente, a petición de los propios usuarios de ordenadores – por ejemplo, de padres que bloquean el acceso a algunas categorías de sitios web en el ordenador de su hijo – o del administrador de la red. La censura de sitios web se ejerce mediante la instalación del software de filtrado de contenido en un PC individual o en la pasarela de la red.

—

La mayoría de los países que censuran sitios web por el contenido, han delegado la responsabilidad de instalar y mantener el software de censura (filtros) a los ISP. Otros, sin embargo, han elegido colocar los filtros en el nivel de la pasarela nacional. Todo el tráfico debe pasar a través de estos filtros nacionales antes de entrar en Internet propiamente dicho. China y Pakistán son ejem-

44
La Oficina del Alto Comisionado para los Derechos Humanos de las Naciones Unidas, http://www.unhchr.ch/udhr/lang/es.htm

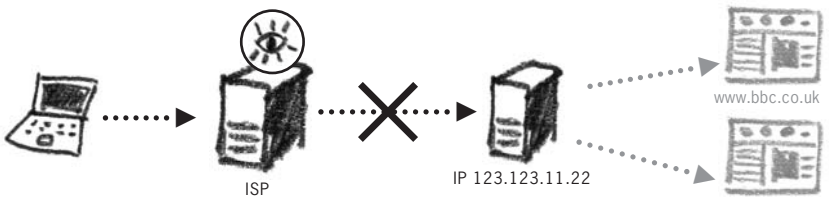
45
http://opennet.net/research

plos de países que aplican el software de filtrado, con varios objetivos y consecuencias, a ambos niveles de la infraestructura nacional de Internet[46], mientras que Australia e Irán atribuyen legislativamente la responsabilidad de censurar sitios web a los ISP.

Listas negras y modificación de DNS

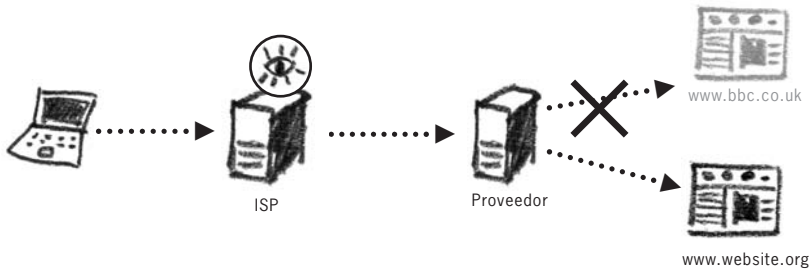
Nota: una comprensión básica de cómo funciona Internet es necesaria antes de leer las siguientes secciones. Por favor, consulta el "Apéndice B – Internet explicado".

A pesar de variar en lo que se refiere a los costes y el punto de su instalación, todos los sistemas de censura de sitios web operan sobre un principio simple. La petición de un sitio web particular enviada por parte del usuario se contrasta con una lista de las URL prohibidas. Si el sitio web solicitado figura en esta lista, la petición es denegada. De igual manera, las listas negras pueden contener direcciones IP de servidores y denegar las peticiones de esta dirección.



►Bloqueando el acceso a una dirección IP

Este método bloqueará el acceso al número IP de un sitio web. Sin embargo, un problema surge cuando se bloquean sitios web de acuerdo a su IP. A veces, estos sitios web residen en grandes servidores web que alojan varios miles de sitios web diferentes. Estos servidores sólo tienen un IP. Al ser bloqueada la dirección IP de un sitio web, también se bloquean todos los otros sitios web que se alojan en el mismo servidor web[47].



►Bloqueando el sitio web de la BBC por su URL

En el ejemplo de arriba, el filtrado existe con el fin de bloquear todas las peticiones de www.bbc.co.uk. Si el sitio web fuera registrado otra vez o replicado bajo un nombre de dominio diferente, puede volver a ser accesible.

Estas reglas se pueden aplicar por separado o juntas para crear la capacidad de filtrado y bloqueo. Algunos países cuentan con categorías predefinidas de software de filtrado y añaden nuevos sitios web en su configuración, mientras que otros emplean grandes equipos de gente para explorar Internet y catalogar lo que debería figurar en el filtro.

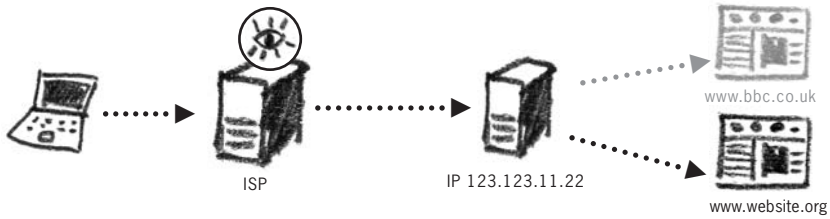
Secuestro de DNS

Este método consiste en enviar la petición de un usuario a un sitio web alterno. Cuando introduces la dirección de un sitio web que quieres visitar, eres auto-

46
Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Acceso denegado: La práctica y política del filtrado global de Internet,* (Cambridge: MIT Press), 2008.

47
"...más del 87% de nombres de dominio activos comparten sus direcciones IP con uno o más dominios adicionales, mientras que más de dos terceras partes de nombres de dominio comparten su IP con cincuenta o más dominios ..." *Ben Edelman, Web Sites Sharing IP Addresses: Prevalence and Significance,* Febrero de 2003, http://cyber.law.harvard.edu/people/edelman/ip-sharing/

máticamente redireccionado a otro sitio web. Puede que algunos usuarios ni siquiera noten la diferencia.



► Tu petición de un sitio web es automáticamente redirigida a otro sitio web

Sin embargo, esta técnica de censura se puede evitar si los usuarios especifican como su punto de referencia de DNS uno de los servidores, en lugar de las copias locales almacenadas por su ISP[48].

El 8 de septiembre de 2002, se impidió a los usuarios en China ir a la página de búsqueda en la red de Google. En cambio, fueron redirigidos a varias páginas con sede en China. La dirección en la URL decía www.google.com[49].

Filtrado por palabras clave

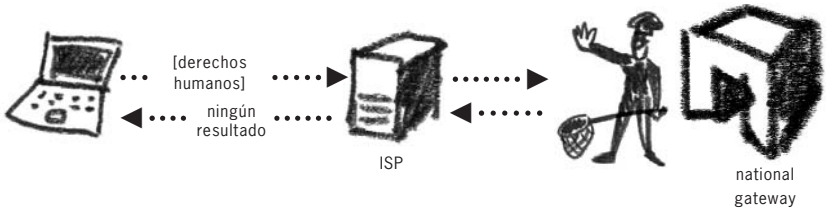
Un método de censura relativamente nuevo que, sin embargo, va ganando fuerza y cuyo uso es cada vez más generalizado es el filtrado por palabras clave. Consiste en la prohibición de ciertas palabras o frases, o en la URL o en el contenido de una página. Este sistema cuenta con una capacidad más grande para censurar sitios web y comunicaciones en Internet por el contenido, y, al mismo tiempo, permite bloquear una página concreta dentro de un sitio web y no el sitio entero. No obstante, el filtrado por palabras clave puede ser menos preciso, y probablemente impedirá el acceso tanto a sitios inofensivos como a los sitios deseados.

Un filtro de palabras clave puede ser configurado para prohibir la petición de cualquier URL que contenga la frase “derechos humanos” o “libertad de expresión”. En realidad, podría ser programado para buscar miles de palabras y frases específicas. Cada vez que se encuentra un correo electrónico o un mensa-

48
http://www.root-servers.org/

49
Análisis empírico del filtrado de Internet en China, Berkman Center for Internet & Society, Jonathan Zittrain y Benjamin Edelman, 2002.

je instantáneo que contiene la palabra clave que figura en la lista, es o bloqueado y no se le permite seguir más adelante, o registrado para investigación posterior de la identidad del remitente y del destinatario. El filtrado puede ocurrir en cualquier punto del enrutamiento del mensaje en Internet.



►Ciertas palabras en tu correo electrónico podrían activar los mecanismos del filtrado

La misma metodología se aplica para los buscadores y las herramientas de mensajería instantánea como el chat de Yahoo y Skype. Cuando introduces una consulta de búsqueda en Google, la consulta primero pasa por el ISP y una pasarela nacional antes de que obtengas la respuesta. Un sistema de filtrado podría interceptar tu búsqueda de "derechos humanos" y ofrecerte un resultado nulo o incorrecto. Más abajo hay imágenes de un resultado de búsqueda de "falundafa" (un movimiento espiritual chino prohibido) realizada en 2004 en Google.com de China.

Parece como si en Google no hubiera ninguna información sobre este tema, pero el mensaje de error en realidad proviene del software de filtrado, y no de Google en sí.[50]

El filtrado de Internet también puede explorar el contenido de sitios web a los que deseas acceder, y bloquear tu petición en caso de que el sitio web contuviera cualquiera de las palabras para la búsqueda de las cuales está programado el filtro.

50
Este método de bloqueo ha cambiado recientemente. Ahora, Google presentará su propio mensaje que indica que la consulta que introdujiste no está permitida por las autoridades locales.

2.6 EVASIÓN DE LA CENSURA Y DEL FILTRADO EN INTERNET

SUMARIO

1 La censura de sitios web puede ser evitada utilizando una variedad de herramientas y métodos de software. Éstos varían en su complejidad, fiabilidad y éxito en cuanto a evitar las prácticas de censura en un país concreto.

2 El filtrado por palabras clave puede ser evitado utilizando sistemas de evasión cifrados. Las redes de anonimato nos permiten navegar por Internet sin ningún tipo de restricciones ni rastros identificables

3 Hoy en día, existen muchas opciones de evitar la censura en Internet. Tienes que saber cómo evaluar la utilidad de cada herramienta y el método de su funcionamiento según tus necesidades y circunstancias.

Este capítulo te enseñará distintos métodos para evitar la censura en Internet y para protegerte del filtrado por palabras clave. Dicho de otra manera, te explicará cómo acceder a sitios web bloqueados, cómo ocultar ante los mecanismos de vigilancia cualquier cosa que estés leyendo o enviando en Internet, y cómo ocultar tus movimientos en Internet. Para los lectores no especializados, es recomendable leer el capítulo anterior "Vigilancia y monitorización en Internet" y también el apéndice "Internet explicado" para entender completamente esta sección.

—

Hoy en día, existen muchas herramientas y estrategias para evitar restricciones de Internet[51] . Este capítulo te familiarizará con solo algunas de ellas. Con el tiempo, estas herramientas y sitios web que te guían en su uso pueden también ser eliminadas de Internet por la censura. Para mantener tu derecho a libertad de expresión y asociación en Internet, tendrás que encontrar nuevos sitios web y herramientas que ofrecen servicios parecidos. Normalmente, esto se puede conseguir realizando búsquedas extensas en la red y comunicando con tus colegas cibernautas. El objetivo de este capítulo es hacerte consciente de servicios y estrategias existentes para que puedas utilizarlos en el futuro.

RETORNO A LA CENSURA

La censura en Internet es posible debido a los mismos cimientos del sistema de conexiones entre redes y de la red global mundial. Muchos países que prohíben a su población que acceda a sitios web lo hacen mediante la instalación de "listas negras" en sus puntos de entrada o/ y salida de la red – la pasarela. Estas listas contienen nombres de sitios web (sus URL) y a menudo la dirección IP del servidor web en el que están alojados. Las peticiones de sitios web que figuran en la lista son procesadas por la pasarela y denegadas. Este hecho es registrado y posteriormente puede dar lugar a una sanción.

Utilizando un proxy para conectarte

Las listas negras son eficaces sólo cuando un sitio web es solicitado directamente. Si pedimos que una tercera persona nos aporte el contenido de una página, entonces estas listas se hacen irrelevantes. Durante más que una

51
Por favor, consulta excelentes guías y recursos de evasión en el proyecto The Sesawe https://www.sesawe.net; 'How to bypass Internet Censorship' by FLOSS Manuals Community Members http://en.flossmanuals.net/CircumventionTools/Introduction and the 'Digital Security Toolkit' http://security.ngoinabox.org/chapter-8

década, los usuarios de servicios de Internet censurados han estado utilizando servicios online de traducción y de la caché para acceder a sitios web indirectamente. Otros han optado por anonimizadores, cuyo propósito en un principio era ocultar tu identidad ante un sitio web – y ahora es ocultar tu verdadero destino ante los filtros de censura.

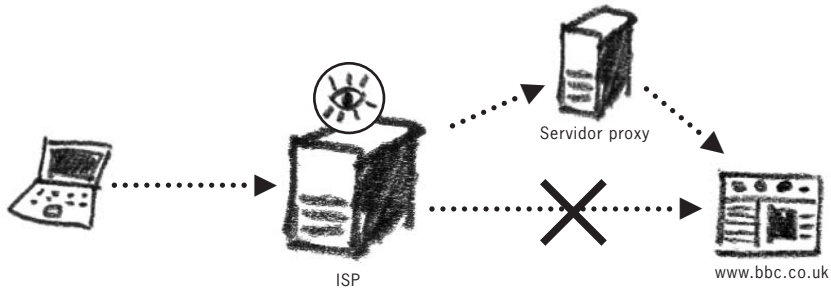
—

Si en tu país no está permitido acceder a www.bbc.co.uk, puedes pedir a otro ordenador (un proxy) que busque el sitio web por ti. Este proxy estará situado en un país diferente que no está restringido por las reglas de la censura en Internet como tu país. Para el censor, estarás simplemente accediendo a un ordenador (o sitio web) que no está presente en sus listas de filtrado.

—

Hay miles de servidores proxy de este tipo, montados de forma distinta, y su misión es la de servir de intermediario entre el ordenador de un cliente y un sitio web anfitrión.

Los servicios proxy varían en sus formas y tamaños. Es importante

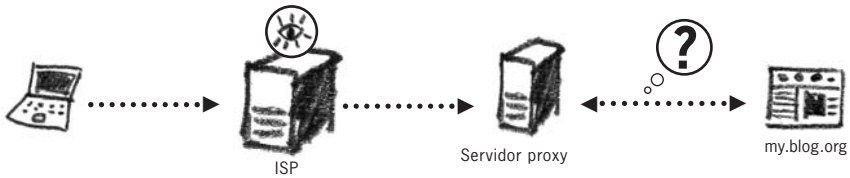


►Re-encaminando una conexión censurada a través de un servidor proxy

distinguir entre sus funciones y la seguridad proporcionada. En todo momento, ten en cuenta que no puedes controlar el método de comunicación ni la privacidad de la conexión entre tu servidor proxy elegido y el sitio web solicitado. Este capítulo se ocupa de los métodos para alcanzar un servidor proxy funcional y escapar a los mecanismos de censura de tu país.

Anonimizadores

El tipo de servidor proxy más fácil de utilizar se conoce también como anonimizador. El sistema de codificación para las operaciones de servidores proxy está incorporado en una página web, a través de la cual puedes navegar por Internet directamente. Creados originalmente para ocultar la verdadera ubicación ante el sitio web visitado, funcionan también para ocultar en Internet tu verdadero destino.



►Al utilizar anonimizadores, el sitio web visitado no conoce el origen (la verdadera dirección IP) de tu ordenador. El ISP no conoce tu verdadero destino.

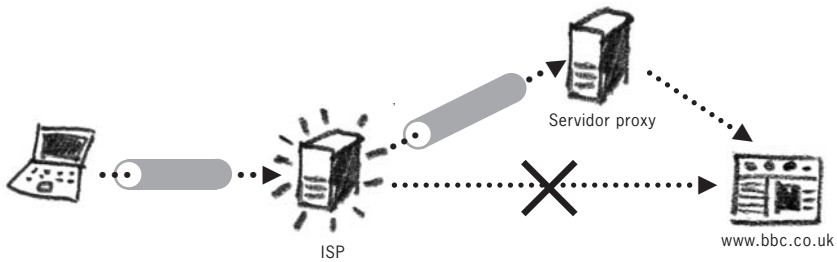
Algunos de los más conocidos anonimizadores son:

- http://www.anonymizer.com
- http://www.anonymouse.org
- http://www.the-cloak.com
- http://www.peacefire.org[52]
- http://www.stupidcensorship.com

Su popularidad, sin embargo, ha llevado a muchos países que aplican el filtrado de Internet a bloquear también el acceso a estos sitios. Ten en cuenta que si tu conexión de Internet al anonimizador está establecida sobre un canal abierto (HTTP a diferencia de HTTPS – para más explicación, véase el siguiente capítulo), los datos enviados y recibidos a través de este servicio no están protegidos de la vigilancia.

Utilizando servicios proxy cifrados

Entre tu ordenador y el servicio proxy que has decidido utilizar se crea un túnel cifrado. Los mecanismos de vigilancia en Internet no ven la información enviada y recibida a través de este servicio, sólo que te estás conectando a él. La utilización de los servicios proxy cifrados añade privacidad a tus técnicas de evitar la censura en Internet y se recomienda en todos los casos. Sin embargo, sé consciente de los ataques de "Man-in-the-Middle" (véase el siguiente capítulo) y ten en cuenta que la información que envías y recibes no está ocultada ante el proveedor del servicio proxy en sí.



► Cifrando tu conexión sobre **SSL** al servidor proxy

Circumventores privados

Los circumventores privados son servidores proxy montados por tus amigos o compañeros en los países que no filtran los sitios web a los que deseas acceder. Es como tener tu propio portal a Internet no restringido. Su ventaja principal es que utilizan redes de confianza – un grupo de amigos o compañeros que comparten sus recursos informáticos para ayudar uno a otro. Las redes de este tipo aseguran una mayor privacidad, ya que no son conocidos en Internet público y, por lo tanto, para los mecanismos de filtrado, son difíciles de detectar y añadir a sus listas de bloqueo.

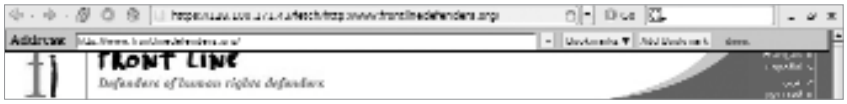
—

Un ejemplo del circumventor privado es Psiphon[53] – permite instalar el software de proxy en cualquier ordenador con Windows. Psiphon se basa en relaciones de confianza entre la gente que desea ayudar a sus amigos que viven en los países con censura en Internet. El servidor genera para sus clientes los detalles de registro, incluyendo la dirección IP del ordenador, nombres de usuarios y contraseñas apropiadas. Estos detalles luego tienen que ser enviados a tus amigos o compañeros quienes los utilizarán para conectarse a tu servidor proxy Psiphon y navegar por Internet a través de él. Aunque es muy fácil de instalar, Psiphon requiere que tengas acceso a tu módem de Internet y seas capaz de

52
Los activistas de peacefire.org suelen cambiar la dirección de sus servidores proxy CGI, debido a que en algunos países, son bloqueados. Puedes suscribirte a su lista de correo electrónico para recibir direcciones de los nuevos servidores proxy CGI. Visita http://www.peacefire.org/circumventor/

53
http://www.psiphon.ca/node/16

configurarlo para permitir conexiones (tus amigos) de Internet. La gente de Psiphon también ofrece "Managed Delivery Platform", servicio que te entregará el contenido bloqueado aunque no tengas amigos o compañeros que te ofrezcan un servicio proxy[54].



►Psiphon añade a la pantalla de tu navegador otra barra de búsqueda.

PARA LOS TECHIES

Peacefire Circumventor[55] – te permite crear tu propio servidor proxy para que puedan utilizarlo los demás. Para poder instalar y mantener este servidor, necesitarás un ordenador dedicado y una conexión a Internet con una IP estática. Es recomendable que tu servidor esté instalado en un país que no ejerce la censura en Internet. Los detalles de conexión a tu ordenador/ servidor proxy se distribuyen a usuarios que viven en los países donde existe la censura en Internet.

Redes privadas virtuales

Otra manera de evitar la censura en Internet es mediante el uso de las redes privadas virtuales (RPV). Esta denominación se refiere básicamente a una red de oficina extendida sobre Internet. Muchas organizaciones utilizan las RPV cuando quieren que sus empleados tengan acceso a unidades de red y a recursos internos, cuando no están en la oficina. Las RPV crean conexiones cifradas al servidor central, y a través de esta conexión, mandan toda la información enviada y recibida por el ordenador. Por lo tanto, si tu servidor de RPV se encuentra en un país que no aplica censura en Internet, puedes utilizar este servicio para encaminar el tráfico en Internet a través de el.

—

Your-Freedom[56] y HotSpot Shield[57] son ejemplos de servicios que te permiten acceder a su RPV para que evites la censura en Internet. Obtendrás detalles de registro y software con los que conectarte a sus servidores. Ten en cuenta que estos métodos son útiles para ocultar tu destino en Internet ante los mecanismos situados en tu propio país, sin embargo, no ante los proveedores del servicio.

REDES DE ANONIMATO

Otra posibilidad sería unirse a una de las redes de anonimato que existen en Internet. Navegar por Internet utilizando esta red ocultaría tu verdadera identidad ante cualquier ordenador o sitio web y probablemente haría cualquier filtrado y retención de datos en tu país ineficaz. Una red de este tipo es Tor (http://torproject.org), una abreviatura de "The Onion Router", con la interfaz en muchos idiomas diferentes y un enorme equipo de seguidores y contribuidores en el mundo entero. Desarrollada originariamente por el Laboratorio de Investigación Naval de los Estados Unidos para ayudar a la defensa y a los servicios de inteligencia con la navegación anónima por Internet, la red Tor actualmente está mantenida por un colectivo de especialistas en seguridad y anonimato de todo el mundo.

Tor cuenta con una gran red de servidores, administrados por voluntarios en todo el mundo. En la actualidad, hay unos mil servidores de este tipo. Cuando te unes a esta red, creas un circuito aleatorio que pasa por tres o más servido-

54
http://www.psiphon.ca/node/17

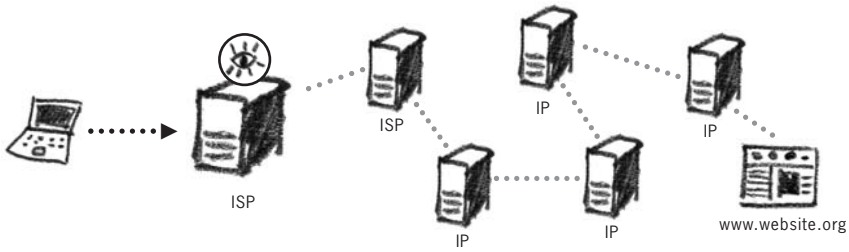
55
http://www.peacefire.org/circumventor/simple-circumventor-instructions.html

56
http://www.your-freedom.net

57
http://hotspotshield.com

res Tor y negocias un conjunto separado de claves de cifrado para cada servidor a lo largo del circuito. Esto asegura que ningún servidor en el circuito puede rastrear tu origen o tu destino final. Imagina que mandas una carta a un amigo y la envías dentro de varios sobres diferentes, cada uno de los cuales lleva una dirección distinta. La carta irá de un destinatario a otro, sin que ninguno de ellos conozca ni su origen ni su destino final, sólo la dirección de la que llegó y la dirección a la que irá. Si cualquiera de los destinatarios deseara abrir la carta, no sería capaz de leer su contenido, ya que está cifrado con una contraseña que requiere dos destinatarios (servidores) más para ser descifrada.

Cuando estás utilizando Tor, el ISP o las agencias nacionales de vigilancia no saben qué páginas estás consultando y, por lo tanto, no te pueden impedir que lo hagas. El sitio web que recibe tu consulta no sabe dónde se originó. Hay más de cien mil clientes que utilizan la red Tor para incrementar la privacidad y anonimato de su navegación por Internet.



►Haciendo anónima tu presencia en Internet con la red Tor

Puedes utilizar también la versión portátil de Tor, llamada el navegador Tor. No tiene que estar instalada en tu ordenador y se puede llevar en una memoria USB, lo que resulta útil para cibercafés y cuando utilizas ordenadores de otras personas. El navegador Tor incluye su propio navegador de Internet configurado para utilizar la red de anonimato.[58]

—

Tor es una herramienta útil para evitar la censura en Internet, pero su anonimato se convierte en una desventaja cuando quieres publicar contenidos, por ejemplo, en Wikipedia. Primero tendrás que averiguar si el sitio web deseado funcionará con Tor. Tampoco lo utilices para entrar en cuentas de correo no seguras. Tor protege tu anonimato, pero no la privacidad de tu conexión. Así como en el caso de los circumventores, el último servidor en tu ruta tendrá acceso ilimitado a tu tráfico.

UN APUNTE SOBRE LA PUBLICACIÓN ANÓNIMA EN INTERNET

Aquellos que mantienen (o contribuyen a) un **blog** o un foro de Internet deben ser conscientes de que su anonimato no estará garantizado meramente por el hecho de firmar con un seudónimo. Cada entrada del **blog** registra la dirección IP del ordenador desde la que fue enviada, y muchos ISP registran todo el tráfico que ha pasado a través de ellos. Por lo tanto, si estás publicando información sensible en un sitio web, debes tomar precauciones para no ser descubierto. A través del uso de anonimizadores y redes de anonimato, puedes ocultar tu IP origen ante un sitio web particular; mediante el uso de un proxy SSL puedes ocultar el artículo que estás descargando del ISP.
Para una guía exhaustiva de cómo publicar contenidos online, véase “Guía para bloggers y ciberdisidentes” de la página web de Reporteros Sin Fronteras. [59]

58
Puedes descargar una copia de Navegador Tor de http://torbrowser.torproject.org o encontrarlo en el kit de herramientas de la Seguridad Digital.

59
http://www.rsf.org/rubrique.php3?id_rubrique=542

RESUMEN

Las herramientas y técnicas descritas en este capítulo son útiles para la gente que vive bajo regímenes que ejercen una censura y un filtrado estrictos en Internet. Con ellas, puedes evitar algunas de estas barreras para acceder a sitios web y recuperar cierta privacidad a la hora de publicar material online. Ten en cuenta que los países que aplican la censura y el filtrado en Internet están constantemente buscando nuevos servidores proxy y herramientas de privacidad con la intención de bloquear también el acceso a ellos. En respuesta, usuarios alrededor del mundo montan cada día nuevos servidores proxy – un verdadero juego de gato y ratón.

2.7 CIFRADO EN INTERNET

SUMARIO

1 La información que envías y recibes en Internet viaja de manera abierta.
2 Algunos sitios web pueden ayudar a proteger esta información creando un túnel cifrado entre ellos y tu ordenador.
3 El túnel cifrado se crea automáticamente, es autentificado por ti y tiene rasgos distintivos para hacerte consciente de su existencia.
4 Queda una posibilidad para interceptar y vulnerar la seguridad de este sistema, mediante lo que se conoce como un ataque de "Man-in-the-Middle".
5 Tienes que validar cuidadosamente los certificados de seguridad, presentados por el sitio web que ofrece conexiones cifradas.

El **cifrado** se ha convertido en uno de los últimos recursos de privacidad en Internet. Nos permite hacer nuestros mensajes y comunicaciones ininteligibles para todos, menos la persona deseada. Una capa de **cifrado** ha sido incorporada incluso en la infraestructura de Internet para hacer posibles transacciones financieras seguras. Se llama Capa de Conexión Segura o Capa de Sockets Seguros y suele abreviarse como **SSL**. En sus inicios, se enfrentó con una fuerte oposición por parte del gobierno de los Estados Unidos. Primero, departamentos del gobierno intentaron prohibir todo el cifrado SSL de una complejidad más elevada de la que podrían descifrar, o declarar su uso ilegal. Finalmente, esta política fue abandonada gracias al esfuerzo desarrollado por parte de un colectivo de matemáticos y activistas en un período que se conoce como "Crypto Guerras".

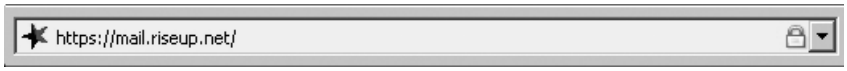
—

Hoy en día, SSL se usa ampliamente en Internet. La ventaja de utilizar SSL en servicios de correo electrónico es que la tecnología ya está incorporada en el marco de Internet, y las legislaciones nacionales que restringen el uso de cifrado prácticamente no se pueden aplicar. Si un país permite dentro de sus fronteras Internet, acepta que SSL existe y se utiliza en todas las operaciones en Internet. Algunas organizaciones pueden (y a menudo lo hacen) ofrecer servicios de correo electrónico internos protegidos por SSL. Hoy es el requisito mínimo para asegurar cierto grado de privacidad de correo electrónico y de comunicación en Internet.

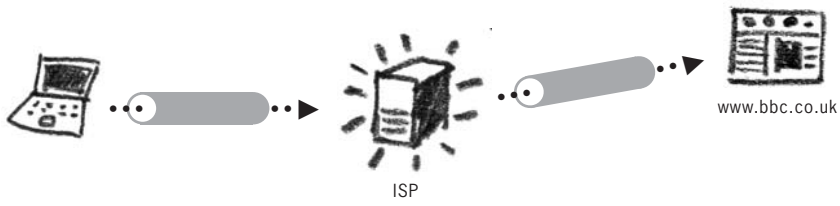
—

La existencia y funcionalidad de una conexión SSL para un sitio web concreto puede identificarse por dos rasgos distintivos:

- La dirección del sitio web empezará con https://(donde la "s" significa segura)
- Un pequeño candado aparecerá en la barra de direcciones o en la barra de herramientas inferior, dependiendo de tu navegador de Internet.



Esto significa que el sitio web que estás visitando y tu navegador de Internet han acordado un canal cifrado de comunicaciones. Para encontrar más sobre la seguridad de este método, tenemos que ver cómo funciona.



►Conectándose a un sitio web sobre **SSL**

CERTIFICADOS SSL

El sistema **SSL** basa su funcionamiento en el concepto de la Infraestructura de Clave Pública (PKI). Todos los sitios web que desean utilizar el **cifrado SSL** tienen que obtener un certificado **SSL**. Tu navegador de Internet comunica con el **servidor web** y cifra toda la información enviada entre los dos puntos. La fuerza del **cifrado** depende del certificado **SSL** del **servidor web.** El estándar de Internet en este momento es 128/256 bits, lo que es lo suficientemente fuerte para casi todos los casos.

Tu navegador de Internet (nosotros suponemos que es Internet Explorer o Mozilla Firefox) tiene incorporada una lista de Autoridades de Certificación **SSL** fiables. Si navegas a un sitio web que te presenta un certificado **SSL**, tu navegador automáticamente verificará si fue emitido por una autoridad fiable en tu lista y si todos sus detalles son correctos (es decir, no despiertan sospechas). Cada certificado contiene por lo menos lo siguiente:

- La clave pública del propietario
- El nombre o alias del propietario
- La fecha de caducidad del certificado
- El número de serie del certificado
- El nombre de la organización que emitió el certificado
- La firma digital de la organización que emitió el certificado

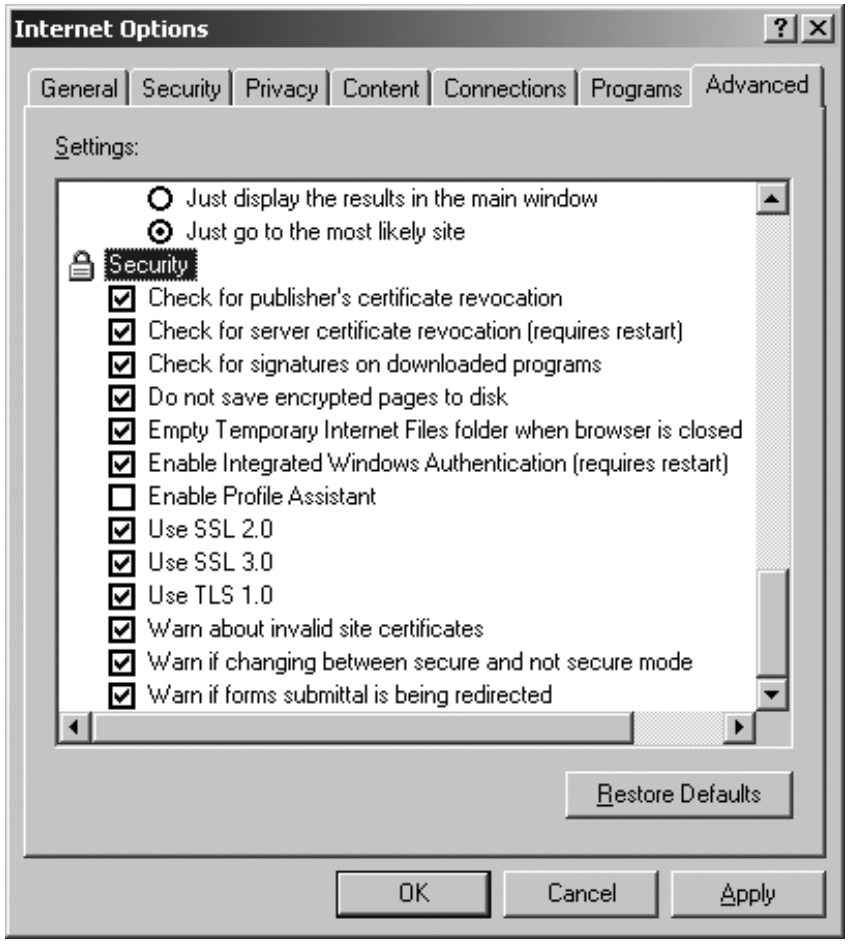
Si la autoridad que emitió el certificado no está en tu lista, o alguno de los detalles del certificado levantara sospechas respecto a su seguridad, tu navegador emitirá una advertencia y permitirá que examines el certificado.

►Advertencia del certificado de Internet Explorer

► Advertencia del certificado de Mozilla Firefox

Nota: Esto no ocurre automáticamente si estás utilizando Internet Explorer 6 o una versión anterior, en cuyo caso primero tienes que configurar esta opción en el programa.

Selecciona: `Herramientas > Opciones de Internet`
Haz clic en: `Opciones avanzadas.`

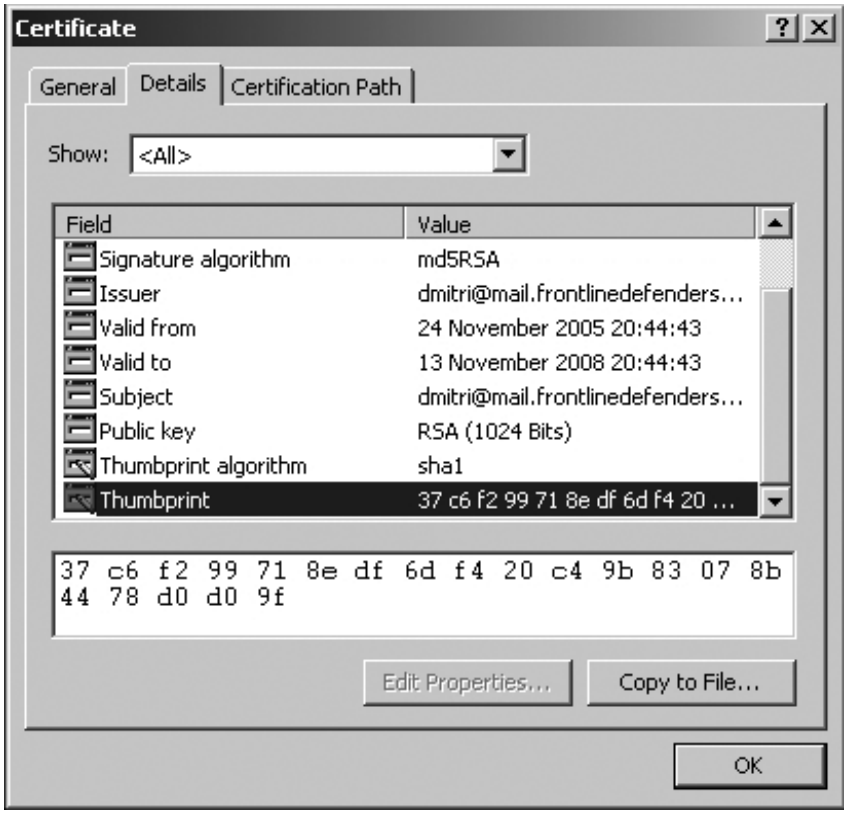


► Advanced Internet settings of Internet Explorer

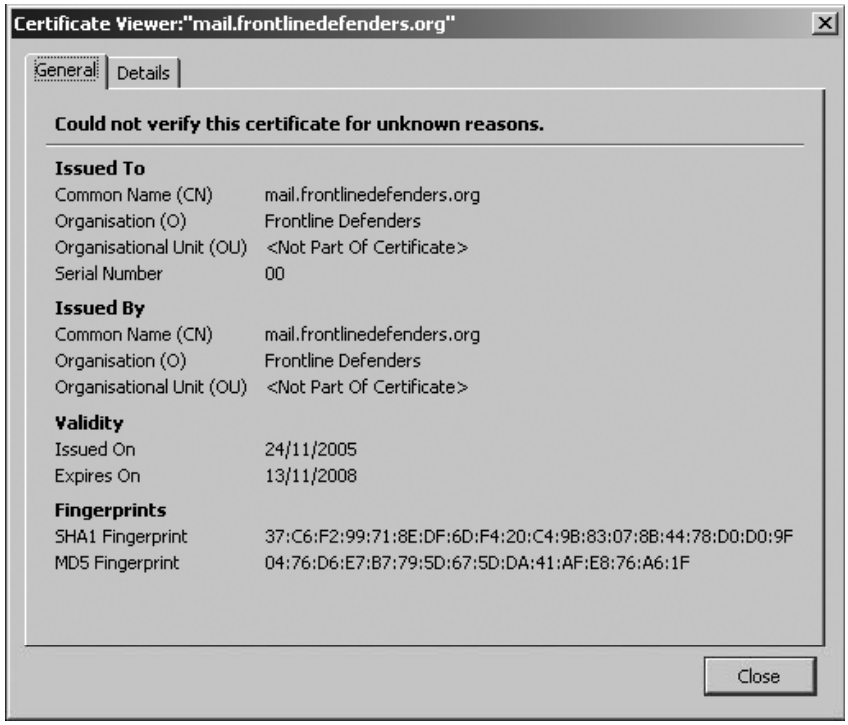
Desplaza la lista hacia abajo en la sección “Seguridad” hasta que no encuentres la entrada “Advertir sobre los certificados de sitio no válidos” y asegúrate de que esta casilla está marcada.
Los dos mensajes de advertencia se refieren al mismo problema, aunque parecen distintos en sus programas respectivos. En ambos casos, tienes la opción examinar tú mismo el mensaje y luego decidir si deseas aceptarlo o no. Si no lo aceptas, no tendrás acceso a este sitio web. Si eliges aceptarlo (“Aceptar este certificado permanentemente” en Mozilla Firefox), entonces el certificado y la autoridad que lo ha emitido serán añadidos a tu lista de confianza y **¡ya no se te pedirá que apruebes el certificado otra vez!**

Nota: Versiones diferentes de los dos navegadores pueden presentar un mensaje ligeramente modificado, aunque los principios y opciones principales se quedarán igual.

Si necesitas examinar el certificado, deberías ser consciente de las propiedades a las que hace falta prestar atención**.** El rasgo de identificación principal del certificado es su huella digital (a veces llamada MD5). Es la verificación de la huella digital la que puede identificar definitivamente que el certificado ha sido realmente creado y emitido por los propietarios del sitio web que estás visitando. Para verificar su autenticidad, tendrás que ponerte en contacto con el propietario del sitio web y comprobar con él la huella digital (por teléfono, fax, chat de Internet o en persona). Aunque este procedimiento puede resultar bastante molesto, es esencial para mantener un alto nivel de seguridad, y en la siguiente sección se explicará a qué riesgos te expones si no lo sigues.
Si la huella digital no coincide, NO aceptes la conexión. No serás capaz de acceder a este sitio web con la misma conexión de Internet, sin embargo, evitarás ser víctima de un ataque de “Man-in-the-Middle” (véase abajo).



►Información del certificado de Internet Explorer



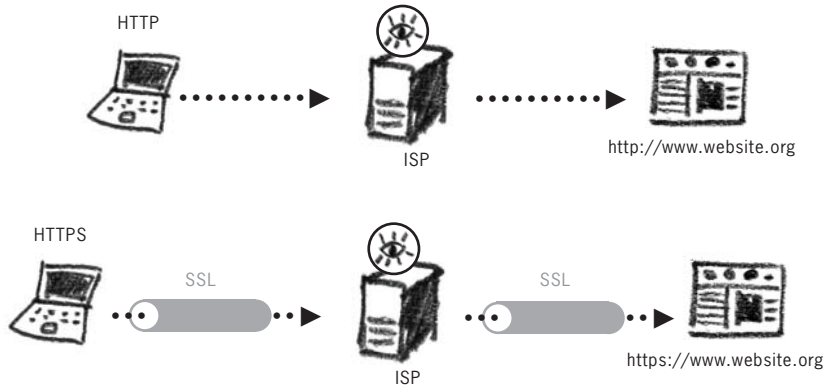
► Información del certificado de Mozilla Firefox

CORREO ELECTRÓNICO SEGURO

Las conexiones **SSL** han sido incorporadas en servicios de correo electrónico en Internet. Esto se aplica tanto al servidor web como al correo electrónico hospedado. Algunas de las cuentas de correo web que ofrecen estas medidas de seguridad gratuitamente son:

- https://mail.riseup.net
- https://bluebottle.com
- https://fastmail.fm
- https://mail.google.com (una opción en "Configuraciones" puede requerir una conexión SSL)

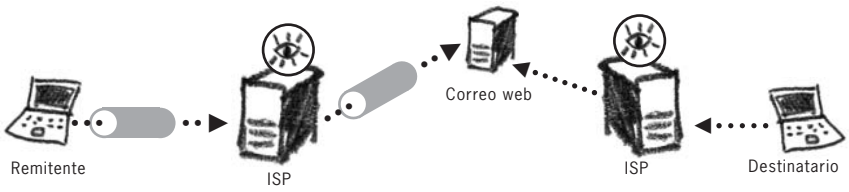
Estos servicios de correo web te permiten que entres en tu cuenta de correo electrónico y comuniques mediante ella con una conexión codificada. Aunque estos datos todavía pueden ser capturados por cualquier mecanismo de filtrado o de vigilancia, será casi imposible darles sentido o descifrarlos. Observa que las direcciones están escritas deliberadamente con "https:" al principio.



Esencialmente, esto crea un método mucho más privado de leer y escribir el correo electrónico. Utilizar una buena contraseña (véase el capítulo sobre Contraseñas), permite hacer tus comunicaciones en Internet más seguras. Registrarse con una de estas cuentas de correo electrónico no difiere en nada del registro en Yahoo o Hotmail. Observa que la mayoría de los proveedores de correo web no ofrecen a sus clientes conexiones **SSL**.

Círculo de seguridad

Por favor, ten en cuenta que los destinatarios de tu correo electrónico quizás no usan una seguridad similar cuando se conectan a su cuenta de correo web. En cuanto tu correo electrónico llega al correo web del destinatario, se somete a los estándares de seguridad de su servidor. Si el destinatario se conecta a su correo web utilizando un canal abierto (no cifrado), agentes de vigilancia del ISP o de una pasarela nacional serán capaces de examinar o leer tu mensaje entero en su totalidad.

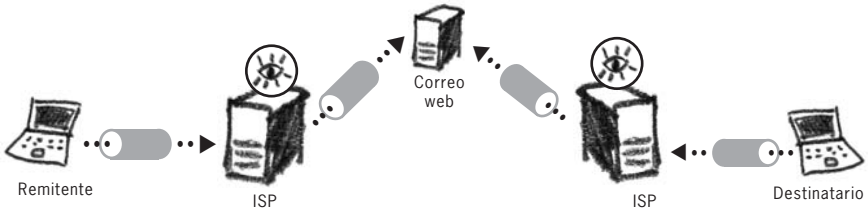


►Cifrando una parte del canal de comunicación

Para mantener en las comunicaciones por correo electrónico un nivel de privacidad más alto, ambas partes deben usar una conexión segura para su servidor de correo web, cualquiera que sea. Si tu objetivo es el de simplemente "escapar" al control del país del que estás enviando el correo electrónico, y el camino recorrido por tu correo electrónico desde el servidor de correo web del destinatario hasta el ordenador del destinatario es irrelevante, no tienes que, por supuesto, prestar atención al ejemplo de abajo. Sin embargo, mantener un circuito cerrado de comunicación siempre constituye una buena práctica de seguridad.

—

La seguridad de este método puede incrementarse si ambas partes utilizan el mismo proveedor de servicio de correo web **SSL** (RiseUp, Bluebottle). El correo electrónico, que viaja en Internet entre servidores, suele ser no cifrado y puede ser interceptado fácilmente.



►El **cifrado SSL** completo en comunicaciones por correo electrónico

En aras de la seguridad, cuando ambas partes utilizan el mismo servicio de correo web **SSL,** hay que tener en cuenta una cosa. Es el servidor de correo web en sí el que almacena y procesa todos los mensajes tuyos. Aunque tu conexión al servidor está cifrada, el correo electrónico es accesible para los que mantienen el servidor o lo piratean. Es posible que desees investigar la seguridad y fiabilidad de tu proveedor de correo web tanto como la del país donde

está localizado. Esto tiene su relevancia en el caso de países como los Estados Unidos, donde las autoridades pueden emitir una citación para confiscar el servidor y toda la información que está en él. Los servidores de correo web arriba mencionados están situados en las siguientes direcciones:

- https://mail.riseup.net – los Estados Unidos
- https://bluebottle.com – Reino Unido
- https://fastmail.fm – los Estados Unidos
- https://mail.google.com – servidores múltiples que abarcan los Estados Unidos, Australia, México, Corea del Sur y China

La capacidad de proteger tu información ante el proveedor ha sido ofrecida por un número de servicios de correo web. Éstos no sólo utilizan un canal de acceso seguro, sino que también cifran tus datos en el servidor. Sólo tú puedes acceder a tu cuenta de correo web y abrirla. El correo electrónico enviado a los destinatarios que tienen una cuenta del mismo proveedor, se puede cifrar también. Tales proveedores de correo web ofrecen un nivel más alto de seguridad de comunicación, pero suelen requerir una conexión de Internet relativamente rápida, ya que cada vez que accedes a tu cuenta, el sitio web automáticamente instala en tu ordenador un software de cifrado temporal.[60] Servicios que te permiten registrar cuentas gratuitas son:

- https://www.hushmail.com
- https://www.vaultletsoft.com
- https://www.s-mail.com

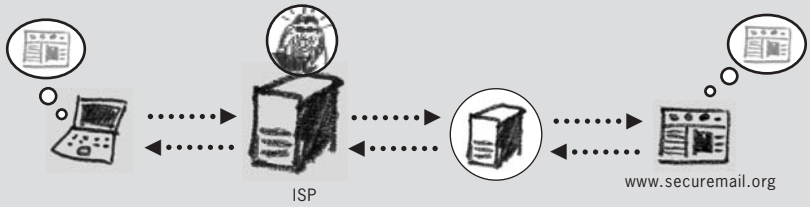
60
Tales servicios de correo web suelen requerir la presencia de la Java VM (compilador) en tu ordenador. Puedes descargarlo de http://java.com.

"MAN-IN-THE-MIDDLE"

La amenaza más grande para el modelo del Certificado **SSL** es lo que se conoce como ataque de "Man-in-the-Middle" (MITM o intermediario). Básicamente, es una intercepción de tu corriente de información de Internet – tu comunicación con un servidor web. Se puede utilizar específicamente para penetrar el por lo demás seguro modelo **SSL** explicado arriba. Primero, el adversario tiene que obtener el acceso físico a tu línea de Internet. Esto se puede hacer en el ISP, una pasarela nacional o incluso en una red local. Luego, el adversario te engañará presentando un certificado alternativo cuando intentes acceder a tu cuenta de correo web segura. Sólo que este certificado no es del proveedor de correo web, sino que pertenece al adversario. Al aceptar el certificado, entrarás en una conexión con tu sitio web a través del servidor del adversario. Cuando introduzcas tu información – detalles de registro, detalles financieros, declaraciones de testigos – el adversario los recibirá sin hacer ningún esfuerzo especial.

—

El problema es que es muy fácil hacerte aceptar un certificado que tu mismo has presentado. La gente suele hacer clic en "OK" sin leer los mensajes. Un adversario podría ser motivado a llevar a cabo un ataque MITM cuando no puede leer tu correo electrónico y otras transacciones en Internet debido a que estás operando sobre "HTTPs". Puede ver cómo accedes a tu servidor de correo web, pero no qué correo electrónico estás leyendo o escribiendo.



►Tu canal de comunicación es interceptado y transmitido a un adversario. Ambas partes tienen la impresión de que sus comunicaciones continúan de manera normal.

Cada vez que tu navegador de Internet te pide que verifiques el Certificado **SSL**, hazte dos preguntas:

- ¿Es ésta la primera vez que estoy accediendo a este sitio web desde este ordenador?
- ¿He examinado la validez del certificado apropiadamente?

Si la respuesta a la pregunta 1 es "no", entonces o no guardaste el certificado permanentemente o estás enfrentándote con un ataque de "Man-in-the-Middle". Como ya hemos mencionado, tu navegador no te pedirá que aceptes un certificado que ya has guardado antes. Si se te pide por segunda vez que aceptes un certificado de un sitio web cuyos detalles deberían estar ya en tu lista de confianza, probablemente no es el mismo sitio web.

Nota: Si estás en un cibercafé, quizás no serás capaz de verificar si la huella digital ya ha sido aceptada. Es recomendable que te apuntes la huella digital de tu sitio web cuando accedes a él desde una ubicación segura por primera vez y luego la verifiques cada vez que accedas a él desde otras ubicaciones.

Contesta la pregunta 2 examinando la huella digital del certificado y poniéndote en contacto con los propietarios del sitio web (lo mejor es hacerlo por teléfono o un correo electrónico seguro) para verificarlo. Esto puede requerir algún tiem-

po y podría ser frustrante. Desgraciadamente, así es la estructura del sistema de certificado **SSL** en Internet y la única opción que tenemos en la actualidad.

—

No hay tantos sitios web que utilizan tecnología **SSL**. Entre ellos pertenecen algunos proveedores de correo electrónico, compras online y otros servicios financieros. Quizás estarás accediendo tan sólo a 2 o 3 sitios web de este tipo. Prepárate escribiendo o llamando por teléfono a los operadores de estos sitios web y registrando sus huellas digitales **SSL**. De este modo, estarás seguro/a de su autenticidad a la hora de tener que revisar y aceptar el certificado **SSL** relativo a sus servicios.

—

Si el adversario consigue engañarte, recibirá toda la información que has introducido en el sitio web. Al conseguir interceptar una cuenta de correo electrónico, el intruso obtendrá tus detalles de registro, y será capaz de entrar en tu cuenta del correo web – un ataque común que ha causado muchas víctimas en Internet. Por lo tanto, es muy importante que entiendas el proceso de la certificación **SSL** y que sepas cómo protegerte.

2.8 ESTEGANOGRAFÍA

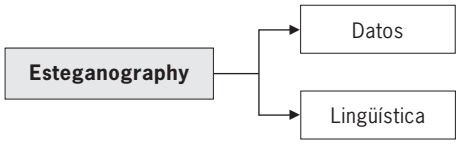
La ciencia o arte de ocultar la propia existencia de un mensaje se denomina esteganografía. Mientras que el **cifrado** oculta tu mensaje haciéndolo ilegible para el intruso, el objetivo de esteganografía es ocultar el mensaje que se comunica. Quizás has oído hablar de la tinta invisible o de escribir una carta con zumo de limón. Éstos son métodos de taquigrafía. Un ejemplo temprano de ella es el mensaje secreto que Herodes mandó desde cautividad alrededor de 440 a.C. Herodes afeitó la cabeza de su esclavo preferido, tatuó a su cuero cabelludo el texto, y esperó hasta que el pelo del esclavo volvió a crecer para ocultar de esta manera el mensaje ante los guardias. El mismo método fue utilizado por el ejército alemán tan recientemente como a principios del siglo veinte.

—

Como la legislación internacional que regula el **cifrado** complejo es cada vez más estricta, nos encontramos con el problema de mantener el derecho a la privacidad de nuestra información por medios legales. La esteganografía no intenta enfrentar un intruso con la tarea de descifrar un código complejo, sino que tiene como su objetivo eludir su atención por completo. Dado que no hay reglas específicas que definan la naturaleza exacta de un mensaje esteganográfico, es muy difícil prohibir el **cifrado** (por ejemplo, una forma de esteganografía son los mensajes subliminales). En este capítulo se presentan algunos recientes desarrollos interesantes en el campo de la esteganografía lingüística.

—

Hay dos métodos principales de esteganografía moderna. Uno es la esteganografía de datos, que supone ocultar un mensaje en una imagen, una foto, un archivo de sonido o "dentro de otros datos". El segundo es la esteganografía lingüística, es decir, utilizar la lengua para mandar un mensaje secreto – mediante el uso de símbolos, significados ambiguos, reordenación de letras y otras formas de manipulación lingüística. Debido a que la posibilidad de utilizar la esteganografía lingüística para los sistemas de ordenadores es todavía puramente teórica, nuestra discusión y ejemplos tratarán sobre las técnicas de ocultar mensajes más tradicionales.



ESTEGANOGRAFÍA LINGÜÍSTICA

La esteganografía lingüística ha ido ganando atención últimamente. En esencia, constituye casi un salto atrás a las técnicas de ocultar y cifrar mensajes asistidas por ordenador, ya que se basa en una habilidad en la que las personas todavía somos mejores que los ordenadores – el uso y la comprensión de lengua. La comprensión de palabras, su transformación en una información con sentido, la detección de humor, simbolismo y ambigüedades son todavía privilegios de la mente humana que no tienen ningún paralelo en el mundo de ordenadores. En esta sección, se explicarán algunas aplicaciones de la esteganografía lingüística que te pueden permitir eludir sistemas de vigilancia basados en tecnología moderna. Sé consciente de que la esteganografía no es una ciencia exacta, y los consejos dados en este capítulo, sobre todo sobre su aplica-

ción lingüística, deberían aplicarse con cuidado y siendo probados antes de ser utilizados en situaciones críticas o de emergencia.

—

Nuestra lengua es un código que parece incomprensible a cualquiera que no lo ha aprendido. Los ordenadores no pueden aprender idiomas, y el software de reconocimiento de voz actúa simplemente detectando diferentes frecuencias en nuestras voces y relacionándolas con los equivalentes preprogramados de letras. Por mucho que intentemos enseñar los ordenadores a entender el significado de las palabras, este tipo de inteligencia artificial (IA) todavía pertenece a un futuro lejano. Otra aplicación de la lengua que se encuentra más allá de las capacidades de los ordenadores es el reconocimiento de símbolos que los seres humanos aplicamos cuando estamos leyendo. El reconocimiento de símbolos ha sido utilizado como un método de autentificación (para comprobar que eres un ser humano, y no un robot) que se aplica cuando nos registramos para diferentes servicios online. Los usuarios tienen que introducir manualmente varios caracteres que pueden ver en la pantalla. Este sistema, llamado HIP – "Human Interactive Proof" (es decir, "Prueba Interactiva Humana") – fue diseñado para prevenir la registración automática de direcciones de correo electrónico por programas de computación que desean crear cuentas de correo electrónico para enviar spam. Los programas de este tipo son incapaces de reconocer los caracteres en una imagen. La comunidad IA sabe cuántos problemas más un ordenador no puede resolver fácilmente, simplemente porque nadie ha descubierto aún cómo incorporar en sus circuitos una *intuición*.[61]

Semagramas

Los semagramas de texto son mensajes simbólicos cifrados por medio de un texto. Mayúsculas, acentuación, una letra poco común, espacios en blanco entre palabras pueden utilizarse todos como señales de un propósito predefinido. Los mensajes subliminales también pertenecen a esta categoría. A veces son útiles cuando deseas comunicar una pequeña porción de información. Por ejemplo, podrías acordar con tus contactos que a diario, os vais a intercambiar por correo electrónico informaciones sobre el tiempo atmosférico aparentemente inofensivas. La frase "el cielo es gris" podría servir como una alerta que significa que estás en apuros y ellos deberían movilizar ayuda internacional.

Códigos abiertos

La esteganografía de código abierto oculta el mensaje en un texto legítimo de maneras que no son inmediatamente obvias para el observador. Los ordenadores y los seres humanos tienen diferentes capacidades en lo que se refiere al esteganálisis, o detección de mensajes esteganográficos (véase abajo en el subtítulo "Detección"). Los siguientes ejemplos quizás no serán aplicables a la vigilancia realizada por un esteganalista. Ellos utilizan variaciones lingüísticas del texto para engañar las formulas comunes utilizadas por filtros electrónicos y sistemas de vigilancia. Por favor, ten en cuenta que nuestras informaciones sólo se pueden considerar como consejos o sugerencias para aprovecharse de la naturaleza no inteligente de los sistemas de computación (p.ej. el software

61
Fuente: *Clasificación de técnicas de esteganografía* (Adaptado de Bauer, 2000).

de filtrado por palabras). No deberían emplearse para comunicar información importante, sino sólo para probar la efectividad del sistema de filtrado. Si sabes que ciertas palabras en tu correo electrónico no podrán llegar al destinatario, y que esta información sola no te meterá en apuros, puedes probar algunas de las variaciones abajo.

Ortografía modificada

Como los filtros electrónicos están programados para reaccionar a ciertas palabras, es imposible estar seguro de cuántas variaciones de la ortografía de una palabra se han considerado. ¡Es posible conservar el significado de una palabra con una ortografía modificada increíblemente avanzada! Una frase como "derechos humanos" podría también transmitirse como:

daareches umenos direchs hoomans dretsches humenos

y de muchas otras maneras. Mientras que esta técnica no es práctica para mensajes más largos, puedes reservarla para ciertas palabras que crees que han podido ser incluidos en los sistemas de filtrado.[62]

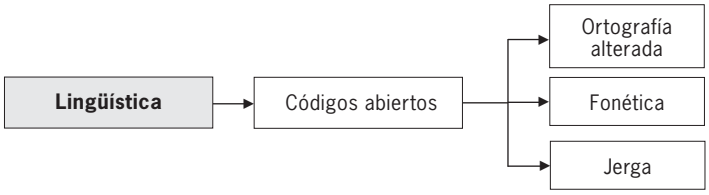
Fonética

La mayoría de los sistemas de filtrado aplicados dentro de un país se centra en palabras clave específicas de la(s) lengua(s) local(es). A veces pueden incluir palabras clave de una segunda lengua popular que se utiliza en el país o en los sitios web (inglés, francés). Otra vez, uno no puede estar seguro en cuanto a con qué precisión ha estado programado el filtrado, pero para facilitar el entendimiento y asegurar la variedad, puedes aplicar a tu mensaje la ortografía fonética. Esto puede resultar particularmente útil, si estás acostumbrado a utilizar una escritura distinta de la que se utiliza en tu país (p.ej. el alfabeto latín para los hablantes del árabe y viceversa).

Houkok Al Insan حقوق الانسان

Jerga

Utilizar en tus mensajes la jerga podría hacer su contenido parecer sin sentido a un observador exterior. Significados acordados o una terminología alternativa pueden ocultar los verdaderos contenidos del mensaje. Es aconsejable elegir palabras de tal manera que el mensaje transportado sea legible y comprensible, aunque no verdadero. Las posibilidades de utilizar la jerga son limitadas sólo por las reservas del vocabulario conocido a las partes que se están comunicando.



Códigos ocultos

Los códigos ocultos emplean un método particular o secreto para ocultar texto en un mensaje portador abierto. A veces, éstos incluyen técnicas simples de incorporar un mensaje en las palabras del portador. La ventaja de este método es que el mensaje portador puede también parecer como un comunicado relevante y posiblemente no levantará sospechas en lo que se refiere a los significados ocultados dentro de él.

62
Para tener una idea sobre las palabras clave utilizadas en el filtrado, véase los informes de la iniciativa OpenNet sobre los países que ejercen el filtrado; http://www.opennetinitiative.net/studies/

Considera el siguiente sitio que disfraza tu mensaje de manera que lo hace pasar por un spam. Si tienes una conexión de Internet, por favor, introduce el mensaje "Por favor, ayúdame" en www.spammimic.com/encode.shtml.

Dear E-Commerce professional ; This letter was specially selected to be sent to you. This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1626, Title 5 , Section 306 . THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich in 57 weeks . Have you ever noticed people are much more likely to BUY with a credit card than cash and more people than ever are surfing the web . Well, now is your chance to capitalize on this. We will help you deliver goods right to the customer's doorstep plus deliver goods right to the customer's doorstep ! You can begin at absolutely no cost to you ! But don't believe us ! Mr Anderson who resides in Arkansas tried us and says "Now I'm rich, Rich, RICH" . This offer is 100% legal ! We IMPLORE you - act now ! Sign up a friend and you'll get a discount of 30% . God Bless . Dear Cybercitizen ; Especially for you - this red-hot intelligence . We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1625; Title 2 , Section 303 . This is a ligitimate business proposal . Why work for somebody else when you can become rich in 11 weeks. Have you ever noticed society seems to be moving faster and faster and nearly every commercial on television has a .com on in it ! Well, now is your chance to capitalize on this ! WE will help YOU increase customer response by 100% plus use credit cards on your website . The best thing about our system is that it is absolutely risk free for you ! But don't believe us. Ms Anderson of Hawaii tried us and says "I was skeptical but it worked for me" ! We are licensed to operate in all states ! We BESEECH you - act now ! Sign up a friend and you get half off ! God Bless .

Nota: para descifrar este mensaje, hay que sólo copiarlo y pegarlo en www.spammimic.com/decode.shtml

En este caso, se imita un mensaje de spam para transmitir otro mensaje, ocultado dentro de su contenido. El texto de spam se deriva de una formula de palabras que es intercambiable, dependiendo de tu mensaje. Eso asegura que el spam sigue siendo legible y parece "auténtico".

—

Puedes crear tus propios mensajes que utilizaran un formato estándar de un mensaje de spam típico u otro formato, y acordar un método específico de incluir en él un texto.

Futuro

El futuro de esteganografía lingüística consistirá en desarrollar un software que cree un texto comprensible, en el que esté oculto el verdadero mensaje, empleando léxicos, ambigüedades y sustitución de palabras. Sin embargo, los expertos todavía no están seguros si los ordenadores serán capaces de crear desde cero textos con sentido y de ocultar en ellos nuestros mensajes utilizando la semántica de la lengua y la esquemática.

ESTEGANOGRAFÍA DE DATOS

La aparición de los ordenadores nos ha permitido incrustar mensajes en imágenes o archivos de sonido. Para el ojo humano, la imagen se queda igual, sin embargo, dentro de ella podría haber la información de un libro entero.[63]

63
En este capítulo, se referirá al medio en el que ocultas tu mensaje como al portador, y al mensaje en sí como al mensaje ocultado.

Los ordenadores, como quizás sabrás, funcionan con el sistema binario. Esto significa que cada letra y cada instrucción son al final reducidos a un código de "1"s y "0"s. Digamos que el binario para la letra "A" es

11101101

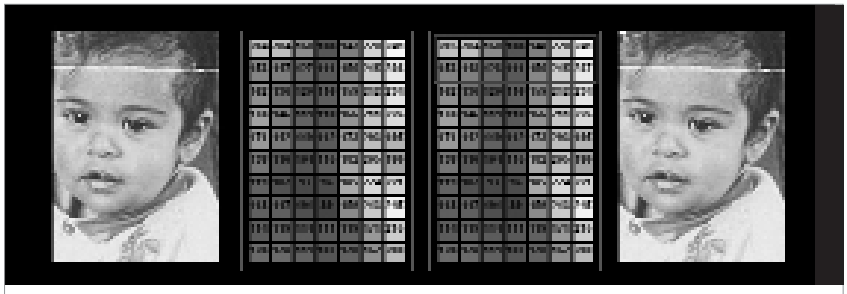
Originalmente, los arquitectos de ordenadores diseñaron este sistema de tal modo que el último "1" o "0" no tuviera ninguna influencia particular en el valor del carácter designado. Si el último número en este mensaje fuera "0" en lugar de "1", el ordenador aún así sabría que esto es una "A".

11101100

El último dígito de todos los mensajes binarios, el cual ni es significativo ni necesario, se conoce como el bit menos significativo (LSB). Un método, utilizado por el software de la esteganografía de datos, es dividir el mensaje oculto entre los LSB del portador en un patrón predeterminado. Sin embargo, esto no cambia el significado original del mensaje. Este método implica que el *mensaje oculto* no puede ser más grande que el *portador* y, en realidad, debería ser mucho más pequeño.

Ocultando en imágenes

Las imágenes digitales (las que aparecen en tu ordenador) están compuestas por píxeles – puntos diminutos de un color específico que forman juntos la imagen que tú puedes ver. Para imágenes, esteganógrafos cifran el mensaje en el LSB de un píxel. Esto significa que, para el ojo humano, el color del píxel (representado para el ordenador por su código binario) no cambia. El mensaje oculto puede retirarse de la imagen siempre que sepas: a) que en la imagen hay un mensaje, b) que utilizas el mismo programa esteganográfico para descifrarlo como el que fue utilizado para ocultarlo.



La imagen portadora	Un fragmento de la foto que representa distintos valores de los píxeles individuales.	Las dos primeras líneas de la paleta tienen incrustada la palabra "OK" en sus LSB.	La imagen esteganográfica resultante

Fuente: *Los códigos secretos*, Simon Singh.

Nota: Las imágenes esteganográficas son detectables. Al ojo humano no parecen nada diferentes, pero los ordenadores, cuando son programados para buscarlas, pueden notar las modificaciones del LSB. Por esta razón, muchos expertos en seguridad dudan de la utilidad de la esteganografía. Otros métodos, como el **cifrado**, pueden ser utilizados también para incrementar la seguridad de información. Algunos programas no sólo codificarán tu mensaje en una imagen, sino que lo cifrarán también. Así, los esteganalistas (las personas responsables de descodificar los mensajes esteganográficos) tendrían que descifrar el mensaje extraído de la imagen.

Ocultando en audio

La esteganografía se puede aplicar también a los archivos audio. Consideremos, por ejemplo, el formato MP3. Es un método de comprimir un archivo audio natural en un tamaño mucho más pequeño. Esto se consigue quitando la frecuencia audio que el oído humano no puede captar: nuestros oídos pueden oír sólo sonidos de un rango particular de frecuencia. El audio natural, sin embargo, registra un rango de frecuencias mucho más amplio, y quitar los sonidos excesivos no cambia significativamente la calidad del audio (para nuestros oídos). De esta manera son creados los archivos MP3. La esteganografía audio añade el mensaje a la frecuencia no utilizada en ellos, y – de nuevo – el oído humano es incapaz de detectar la diferencia en la calidad de sonido.

►Aquí está un diagrama de frecuencias de una transcripción audio:

►Y aquí está el mismo audio, con un mensaje oculto dentro de sus frecuencias:

Fuente: Gary C. Kessler - *An Overview of Steganography for the Computer Forensics Examiner.*

Y mientras que puedes ser capaz de detectar la diferencia al mirar este diagrama, oírla es mucho más difícil.

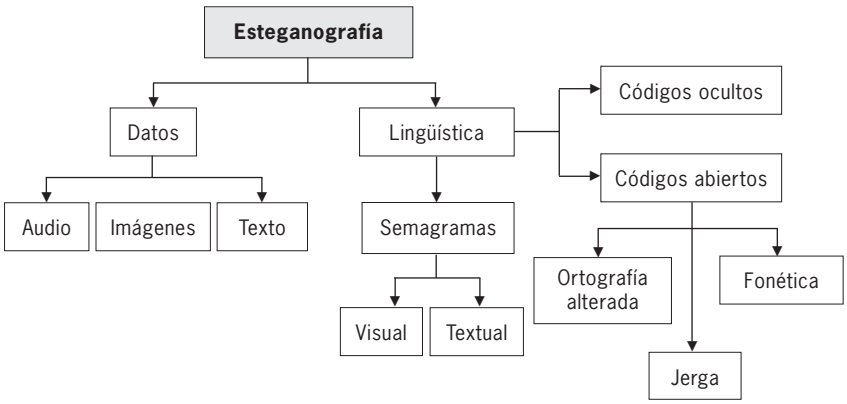
Ocultando en un texto

Los principios esteganográficos pueden ser aplicados también a archivos de texto normales. A veces, esto se hace ocultando el mensaje en los espacios en blanco entre las palabras. El mensaje está dividido a lo largo del texto entre los LSB del código binario para el espacio vacío. De nuevo, este método requiere que el texto que estás enviando sea considerablemente más largo que el mensaje que estás ocultando dentro de él. También puedes ocultar mensajes en documentos PDF y en una variedad de otros estándares, dependiendo del programa que desees utilizar.

El software de esteganografía

Existen unos cien programas distintos que realizan la esteganografía de datos, audio y texto. Cada uno utiliza su método particular de organizar tu mensaje en el archivo portador. Algunos de los más conocidos son jphide y jpseek (http://linux01.gwdg.de/~alatham/stego.html), mp3stego (http://www.petitcolas.net/fabien/steganography/mp3stego/), tanto como el producto comercial Steganos Security Suite (http://www.steganos.com). Puedes encontrar muchos más en http://www.stegoarchive.com/.

63
I will refer to the medium you hide your message in as the *carrier*, and to the message itself as the *hidden message*



DETECCIÓN

El esteganálisis es el proceso de detección de la esteganografía. Aunque desde el punto de vista técnico, para los ordenadores es fácil detectar contenido esteganográfico, tienen que ser configurados primero para buscarlos. La ventaja del uso de la esteganografía proviene del principio de "una aguja en el pajar". Cada día, millones de imágenes, archivos MP3 y documentos de texto plano son enviados en Internet. No levantan sospechas y, a diferencia de los mensajes cifrados, normalmente no son capturados para ser analizados. Cuando envías a los demás fotos de tus últimas vacaciones, puedes cifrar en ellas un mensaje esteganográfico. El hecho de compartir tu colección de música con un amigo presenta la oportunidad de incluir un mensaje corto en una de las canciones. Puedes imaginarte la imposibilidad de explorar en Internet cantidades de información enormes con el fin de buscar todo tipo de contenido esteganográfico.

—

El principio de "una aguja en el pajar" sólo funciona si hay un "pajar". Si has compartido siempre las fotos de tus vacaciones o tus canciones preferidas con tu contacto de Internet, luego la oscuridad de tu mensaje se incrementa cuando se envía simplemente una foto o una canción más. No utilices imágenes comunes o fuera de contexto. No bajes imágenes de Internet y no ocultes mensajes en ellos (el atacante podría bajar la misma imagen y comparar las dos digitalmente). En resumen, no reveles tus prácticas esteganográficas mediante una anomalía. Establece un patrón de comunicación, y utilízalo con moderación para transmitir mensajes ocultos. Para hacer tus comunicaciones seguras, no confíes sólo en la esteganografía. Si el mensaje oculto es revelado al intruso, aun así, debería ser incapaz de leer su contenido. Refuerza la seguridad de tu mensaje cifrándolo dentro de tu archivo portador.


Enviar un mensaje esteganográfico
Elegir el método de esteganografía
Elegir un programa para esconder el mensaje en un archivo portador
Comunicar al destinatario el método elegido a través de un canal diferente
Integrar el mensaje en un archivo portador, y si es posible, cifrarlo
Elegir un medio regular para transferir el archivo (correo electrónico, disco, o cargarlo a un sitio web, blog)
Seleccionar un archivo portador

2.9 SOFTWARE MALICIOSO Y SPAM

SUMARIO

1 Hay muchos tipos de software malicioso (o malware), transmitidos de un ordenador a otro de muchas maneras, que causan un daño indecible a la información.

2 Instala en tu ordenador un software antivirus y antispyware y actualízalo regularmente. Utiliza un cortafuegos y ten mucho cuidado a la hora de abrir el correo electrónico o introducir contenidos media en tu ordenador.

3 Spam es el correo electrónico no solicitado que hoy en día constituye una parte enorme de todo el tráfico en Internet y se ha convertido en un gran problema para la gente y las redes.

4 Ten cuidado con distribuir tu dirección de correo electrónico y nunca contestes o incluso abras mensajes de spam.

El software malicioso es un término que se utiliza para describir el software que perjudica tu ordenador y compromete tu seguridad y la confidencialidad de tu información. Puede dividirse en varias categorías, incluyendo los virus y spyware. Millones de ordenadores en todo el mundo han sido infectados por un virus o spyware que causan problemas enormes para la industria. Internet se ha convertido en el medio que más ampliamente se utiliza para propagar software malicioso, y siempre tenemos que estar luchando por protegernos de miles de infecciones maliciosas antiguas o nuevamente diseñadas.

—

En el Internet de hoy, un ordenador infectado con un programa malicioso puede ser utilizado por terceras personas para orquestar ataques digitales a otros sistemas. Se explota alguna debilidad en los sistemas de defensa del ordenador infectándolo con el virus particular del atacante. El virus proporciona a su diseñador el control remoto de los ordenadores, creando así lo que se conoce como una Botnet. Las Botnet luego pueden ser utilizadas para atacar un sitio web particular o los servidores de una organización o gobierno. Ataques de este tipo se denominan ataques distribuidos de denegación de servicio (DDoS), debido a que sobrecargan los servidores produciendo millones de peticiones simultáneas del servicio.

—

La popularidad de este tipo de ataques se ha generalizado durante la última década, y a menudo se llevan a cabo utilizando un gran número de ordenadores infectados. Frecuentemente, inutilizan sitios web de organizaciones de derechos humanos. Contrarrestar un ataque DDoS es muy difícil, y prevenir la infección inicial es la clave. Es demasiado tarde para ser ambivalente sobre la protección contra los virus, ya que, sin que lo sepas, tu ordenador infectado podría estar participando en un ataque DDoS contra un sitio web.

VIRUS

De modo parecido a un virus humano, los virus informáticos infectan ordenadores y dispositivos con la intención de cambiar su estabilidad, funcionamiento o integridad. Suelen ser trozos pequeños del código de software que se ejecutan en tu ordenador después de una acción específica que has llevado a cabo. También tienen la tendencia de copiarse y multiplicarse. Puedes recibir un virus

en un correo electrónico, en una tarjeta de memoria USB o simplemente navegando en un sitio web específico. A veces, es posible infectarse con un virus sólo por estar conectado a Internet.

Historia

El primer caso reconocido de virus informático que se propagó entre ordenadores fue Elk Cloner. Fue diseñado en 1982 por un estudiante de escuela secundaria de 15 años Rich Skrenta quien lo programó para los sistemas operativos de los ordenadores Apple II. Elk Cloner se propagaba infectando el sistema operativo de Apple II y transmitiéndose a los disquetes. Cuando el ordenador se arrancó desde un disquete infectado, también se arrancó automáticamente una copia del virus. Cada vez que un nuevo disquete fue introducido en el ordenador infectado, el virus se copió en él, difundiéndose así. No causó ningún daño específico al ordenador, pero fue simplemente molesto. En cada arranque nº 50, el virus mostraba por pantalla un pequeño "poema":

```
Elk Cloner: El programa con personalidad

Obtendrá todos tus discos
se meterá en tus chips
¡Sí, es Cloner!

Se pegará a ti como pegamento
cambiará también tu RAM
¡Pásalo, Elk Cloner!64
```

Gusano Morris, diseñado por Robert Tappan Morris en 1998, fue el primer ejemplar conocido de software malicioso propagado en Internet. Se estima que infectó unos 6.000 ordenadores en el mundo entero y provocó la creación de una nueva industria para contrarrestar ataques similares, presidido por el CERT (Equipo de Respuesta de Emergencias Informáticas), un instituto de investigación y centro de desarrollo de los Estados Unidos financiado con fondos federales (http://www.cert.org).

—

El virus MyDoom de 2004 infectó 1 de cada 12 correos electrónicos enviados en Internet y fue capaz de coordinar el **ataque distribuido de denegación de servicio**[65] más grande, involucrando más de 1 millón de ordenadores en todo el mundo.

VARIACIONES DEL SOFTWARE MALICIOSO

Existen numerosos tipos de software malicioso, cada uno de los cuales tiene un método específico de funcionar y distribuirse.

—

■ **Un virus** es un trozo de código informático que daña el software (y, recientemente, también el hardware) de tu PC, causando posiblemente la pérdida de datos o un mal funcionamiento del ordenador. Los virus tienen que ser ejecutados (iniciados o abiertos) por el usuario y se pueden replicar para infectar otros ordenadores.

Infección: los virus llegan como documentos adjuntos al correo electrónico, archivos cargados desde disquetes u otros medios extraíbles. Los archivos que podrían contener los virus normalmente (pero no siempre) tienen las siguientes extensiones: .exe .com .bat .vbs .php .class .jbs .scr .pif.

64
Wikipedia - http://en.wikipedia.org/wiki/Elk_Cloner

65
Véase el Glosario.

■ **Un gusano** – es parecido a un virus, pero el primero no intenta borrar o corromper la información en tu ordenador. Los gusanos suelen llegar incrustados en un mensaje de correo electrónico. Se aprovechan de la vulnerabilidad de la seguridad de los sistemas operativos y se propagan a otros ordenadores vía la red o Internet.

Infección: gusanos infectan tu ordenador en cuanto abres el mensaje de correo electrónico en el que se están escondiendo. Un ordenador infectado podría también estar enviando y recibiendo gusanos simplemente por estar conectado a Internet.

■ **Troyanos (o caballos de Troya, troyanos de puerta trasera)** son programas que se hacen pasar por software legítimo, pero, de hecho, contienen un código malicioso. No se replican pero pueden forzar a tu ordenador a que descargue un virus o ejecute una función preprogramada (como, por ejemplo, atacar otro sitio web). Los troyanos de puerta trasera pueden dar pleno acceso a tu ordenador a un intruso. Podrían permitir a un atacante acceder a tus programas o tus documentos.

Infección: troyanos se hacen pasar por programas legítimos y se activan cuando los ejecutas. A veces son los virus los que instalan troyanos en tu ordenador.

■ **Keyloggers (o registradores de teclas)** son programas maliciosos que registran tus movimientos en el ordenador y en Internet y envían esta información a un intruso. Su objetivo principal es el de minar la seguridad del ordenador y revelar información sobre el usuario con el fin de lucrarse económicamente.

Infección: los keyloggers pueden aparecer en un correo electrónico y estar incrustados en los programas que instalas. Puedes infectarte simplemente por visitar una página web incorrecta (especialmente relevante en el caso de Internet Explorer) o utilizando el software para compartir archivos. Pueden llegar en documentos adjuntos al correo electrónico o instalarse con un virus.

En el mundo de hoy, que está lleno de virus, también los teléfonos móviles pueden verse afectados por los virus, que se aprovechan de Bluetooth y de la mensajería multimedia para propagarse. Tampoco están excluidos los Blackberry, con una vulnerabilidad que permite al software malicioso convertirse en aplicaciones de confianza. Skype y MSN, iMac integrado en las cámaras de vídeo e incluso los marcapasos inalámbricos que han sido puestos en venta recientemente pueden acabar estando "bajo el control" del creador de un virus. El código malicioso se ha encontrado en imágenes en los sitios web para compartir fotos y en millones de plataformas web desprevenidas (y mal configuradas y no actualizadas) han sido "inyectadas" con un código viral. O nuestra ignorancia o su creatividad ha generado un mundo digital hostil con poco espacio para errores. Tu única esperanza es equiparte con un buen software y sentido común – para crear un castillo para tu casa digital.

—

Se requiere una política organizativa que prevenga de manera proactiva la descarga y ejecución de los virus. Una parte de ella se puede aplicar a nivel de programas, estableciendo configuraciones específicas para hacer tus programas más resistentes a los virus, y consiguiendo y utilizando software antivirus, antispyware y de cortafuegos. Hace falta buscar y actualizar activamente todo el soft-

68
If you can see the content of the email in your main program screen, you have the preview pane switched on. To disable it in Microsoft Outlook: go to the menu bar and de-select View > Preview Pane.
In Outlook Express: go to the menu bar View > Layout. In the Layout window de-select the option 'Show Preview Pane'.
In Mozilla Thunderbird go to the menu bar View > Layout and de-select 'Message Pane' or simply press F8.

ware, incluidos los programas que reparan Windows. Esto incrementará tu protección contra el software malicioso más reciente**.** Sin embargo, lo principal es enfrentarse con el software malicioso a nivel personal, siguiendo ciertas rutinas de seguridad.

Tienes que:

1 Guardar una copia de seguridad de tus documentos importantes en medios extraíbles.
2 Bloquear todos los documentos maliciosos adjuntos a tu correo electrónico en el nivel de tu servidor o tu programa.
3 No abrir nunca ningún documento adjunto a tu correo electrónico que no estás esperando y los que provienen de fuentes desconocidas, e intenta no hacer clic en ningún enlace incorporado en un mensaje de correo electrónico, sobre todo de fuentes que todavía no conozcas.
4 Realizar un escaneo de tu sistema como mínimo una vez a la semana.
5 No descargar a tu ordenador programas innecesarios. Los programas de MSN y de chat Yahoo son objetivos populares para difundir los virus. Intenta abstenerte de utilizar estos programas y el software para compartir archivos en el ordenador en el que trabajas.
6 Mantente informado/a sobre las últimas amenazas.

Si tu ordenador está infectado por un virus:

1 Desconéctalo de Internet y de cualquier red inmediatamente.
2 Cierra todo los programas y realiza un escaneo antivirus completo. Algunos programas te permiten programar un escaneo completo en el arranque que controlará todo tu ordenador al reiniciarlo. Esto es útil, dado que algunos virus se esconden en los archivos que Windows no puede controlar cuando está en funcionamiento. Borra todos los virus detectados y apúntate sus nombres. Luego vuelve a realizar el escaneo hasta que no tengas ningunas advertencias más.
3 Conéctate a Internet y obtén la última información sobre el virus concreto que has recibido. Puedes visitar www.symantec.com, www.sophos.com o www.f-secure.com para la última información sobre los virus, el daño que pueden causar y los métodos de detectarlos, prevenirlos y borrarlos. Actualiza tu sistema operativo de Windows con todos los parches necesarios.
4 Si se detecta un virus en un ordenador que reside en una red, desconecta todos los ordenadores de Internet y luego de la red. Todos los usuarios deberían dejar de trabajar, y hay que tomar los pasos de la lista de arriba para cada ordenador. Esto puede sonar como un proceso exhaustivo, pero es absolutamente necesario.

En 1999, BubbleBoy fue el primer gusano que no dependía de que el usuario abriera un documento adjunto al correo electrónico para que se infectara. En cuanto se ve el mensaje infectado de correo electrónico, el gusano se activa. Esta tendencia es seguida por muchos escritores de virus y sigue desconcertando los sistemas de seguridad más costosos mientras que está aprovechándose de la curiosidad inagotable de ver el contenido de un correo electrónico que parece sospechoso.

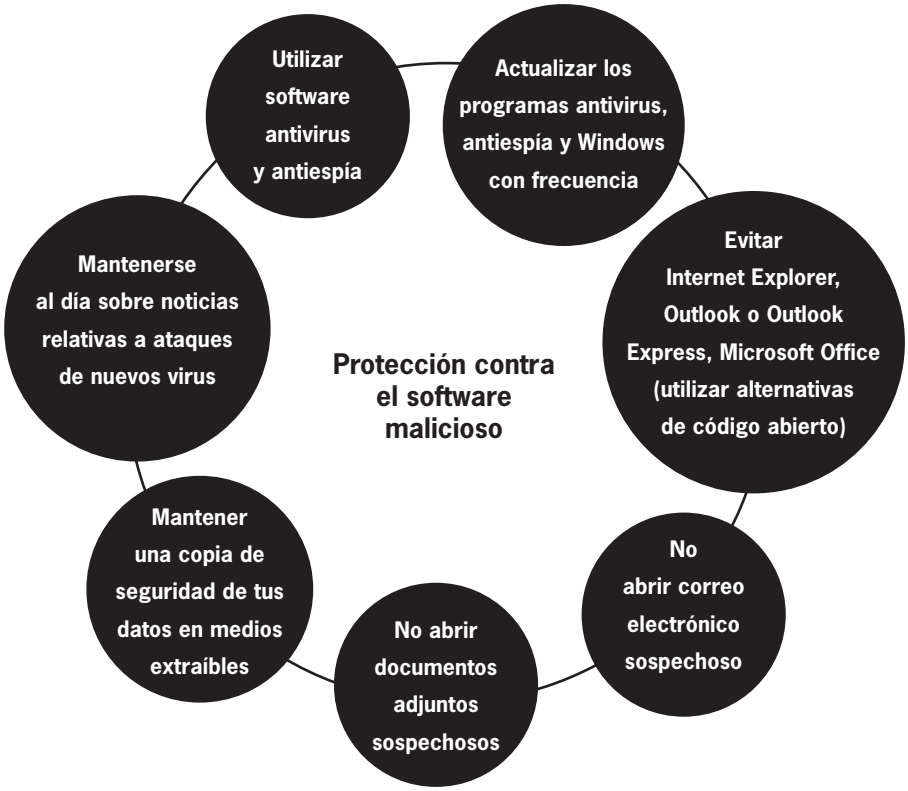
—

Apaga la opción de la vista previa del correo electrónico. Adicionalmente, elige abrir el correo electrónico solo en el formato de texto simple. Esto impedirá que el código malicioso que está escondiéndose en el correo electrónico se ejecute.

En Internet estás indefenso si no tienes instalado un software antivirus, antispyware y de cortafuegos. Éstos necesitan ser actualizados constantemente y configurados rigurosamente. No hace falta gastar ningún dinero. Empresas como Avast, Comodo y Safer Networking ofrecen un uso gratuito de su software antivirus y antispyware en casa. [66]

—

La regla más importante es ser consciente y estar alerta. Toma las precauciones requeridas, pero no dejes la existencia de los programas antivirus o antispyware darte un sentido falso de seguridad. Como se puede deducir de lo arriba mencionado, es una batalla sin acabar. Los virus se propagan no sólo por estar programados de manera ingeniosa, sino también por la falta de cuidado y la indiferencia del usuario.



SPAM

Spam es el proceso de enviar en grandes cantidades correos electrónicos no solicitados. Normalmente tienen la forma de los mensajes de publicidad o sin sentido que a menudo llenan nuestros buzones de correo electrónico. El envío de correo electrónico es una actividad encaminada a incrementar las ganancias de empresas, y cada vez más, de bandas de spam. Es un método lucrativo, dado que los costes de la distribución masiva son mínimos – mucho más bajos que en el caso del correo basura postal u otros medios de publicidad masiva. El spam constituye el 50% de toda la actividad en Internet y es un problema enorme tanto para los particulares como para las empresas. Esta sección te mostrará cómo reducir la cantidad de spam en tu buzón de correo electrónico.

—

Muchas empresas online proporcionan la lista de las direcciones de correo electrónico de sus clientes a organizaciones que se especializan en el envío de correo electrónico comercial no solicitado (spam). Otras empresas obtienen las direcciones de correo electrónico de los mensajes enviados en las listas de

66
Todo el software y manuales para su instalación pueden descargarse de la Caja de herramientas de seguridad digital, http://security.ngoinabox.org

67
Privacy International – Informe sobre la Privacidad y los Derechos Humanos de 2004 – Las amenazas a la privacidad.

direcciones, en los grupos de noticias, o de los datos relativos a la registración del nombre de dominio. En una prueba realizada por la Comisión Federal de Comercio de los EEUU, una dirección de correo electrónico, enviada en una sala de chat, empezó a recibir spam ocho minutos después de enviar un correo electrónico.[67]

Historia

El concepto de envío masivo de correo no solicitado como técnica de publicidad fue introducido por primera vez en 1994 por dos abogados de inmigración que deseaban promocionar sus servicios a través del envío masivo de correo electrónico. Sostenían que era un nuevo método viable y justificado de marketing y a sus críticos los calificaban como "radicales anticomercio". A partir de entonces, la popularidad del envío masivo de correo electrónico no solicitado creció muy rápidamente.

Previniendo el spam

Hay varios métodos de reducir la cantidad de spam que recibes, aunque posiblemente nunca serás capaz de eliminarlo por completo. Si utilizas una cuenta de correo web (como Hotmail, Gmail o Yahoo), el proveedor debería tener instalado el software de filtrado automático de spam.

—

El principal método de prevenir spam es no responder o no hacer clic en ningunos enlaces en el mensaje de spam. Aunque estés disgustado por la cantidad de spam que recibes y desees responder al mensaje con una queja o petición de que no recibas más el correo electrónico no solicitado, estás simplemente confirmando la existencia de tu dirección de correo electrónico, clasificándote como a alguien que lee el spam y reacciona a él. Nunca adquieras nada que se ofrece en los mensajes publicitarios no solicitados. Aunque sea legítimo, acabarás financiando más el mercado del envío de spam.

—

No apuntes tu dirección de correo electrónico a ninguna lista en un sitio web o servidor de listas. Si no es posible, disfrázala poniendo # o "arroba" en lugar de utilizar el símbolo @ normal. Así impedirás que arañas web capten tus direcciones de correo electrónico

usuario#frontlinedefenders #org

usuarioARROBAfrontlinedefendersPUNTOorg

Si estás enviando un correo electrónico a un grupo grande, introduce los contactos en el campo "**CCO**". Esto ocultará la existencia del correo electrónico masivo e impedirá que las personas que envían spam utilicen la lista para sus propósitos.

—

Intenta utilizar varias direcciones de correo electrónico. Uno será tu correo electrónico privado que darás sólo a los contactos de confianza. Para la registración o autentificación cuando estás en Internet puedes utilizar otras direcciones.

—

Si tu cuenta ya está enfrentándose con un masivo envío de spam y los filtros simplemente ya no funcionan, no te queda ninguna otra opción que abrirte una nueva cuenta de correo electrónico y estar más alerta.


Protección contra el spam
Instalar en tu ordenador el software de filtrado de spam
No responder, reenviar ni abrir mensajes de spam
Disfrazar tu correo electrónico si aparece en páginas web
Utilizar varias cuentas de correo electrónico, p.e. para comunicaciones privadas y para suscribirse a servicios de Internet
Utilizar el campo CCO a la hora de enviar un mensaje a un grupo de direcciones
Apagar la opción de previsualización del programa de correo electrónico
Utilizar en tu correo electrónico encabezamientos descriptivos para que no sea clasificado como spam

2.10 PERFILES E IDENTIDAD

RESUMEN

1 Tu identidad digital es una colección de tus registros de ordenador, teléfono e Internet que o están relacionados contigo o podran ser utilizados para identificarte. Comprende también la información que tú (y también tus amigos y compañeros de trabajo) compartes en sitios de redes sociales y plataformas de blogs.

2 El análisis de tu comportamineto con el fin de crear tu perfil hace ciertas suposiciones sobre tus hábitos, carácter, afiliaciones políticas o sociales, tanto como sobre los de tus amigos y compañeros de trabajo. Internet es un recurso excelente para los que desean hacer el perfil de tu identidad.

3 El anonimato es una herramienta importante para los activistas que trabajan online y utilizan tecnologías de comunicación, sin embargo, es una tarea difícil entre las nuevas tecnologías.

Este capítulo trata sobre la identidad digital y describe cómo se utilizan las nuevas tecnologías para hacer el perfil de tu personalidad, actividades y asociaciones con los demás. Aborda algunos temas sobre los que ya se ha tratado en este manual, incluyendo la vigilancia y el anonimato, e intenta señalar los riesgos e inseguridades inherentes a las tecnologías de Internet y telefonía móvil. Su objetivo es informar al lector sobre las vulnerabilidades potenciales para la privacidad y la libertad de asociación que existen en la infraestructura actual de Internet y de las telecomunicaciones, y proporcionar consejos sobre cómo regular y reducir su impacto.

—

Mientras muchos están acostumbrados a términos como Web 2.0, redes sociales, Twitter, publicación de vídeos y similares, no se presta la suficiente atención a las capacidades invasivas de la infraestructura de la red mundial que proporciona estos servicios. La tentación que suponen las comunicaciones instantáneas y el acceso a la información ofrecido por las nuevas tecnologías debe ser equilibrada con la capacidad permanente que poseen estas herramientas para penetrar en nuestras vidas privadas y recopilar registros de nuestras actividades y redes de amigos.

—

La capacidad de los servicios de inteligencia para vigilar la red va más allá de los países altamente desarrollados y que fomentan las nuevas tecnologías. La tendencia común en el comercio global de armas – países dispuestos a vender la tecnología anticuada a cualquier comprador que se la pueda permitir – se da también en las tecnologías de vigilancia y seguridad. La centralización de las bases de datos públicas y privadas, que a menudo se aprueba a pesar de las barreras legislativas y financieras en nombre de la seguridad nacional y global, tanto como el hecho de que todos nosotros adoptamos popularmente los dispositivos y servicios de comunicación hacen que se reduzca y a menudo elimine la privacidad y el anonimato de nuestra identidad – un derecho inherente y consagrado en numerosos convenios y marcos legislativos internacionales.

UNA IDENTIDAD DIGITAL

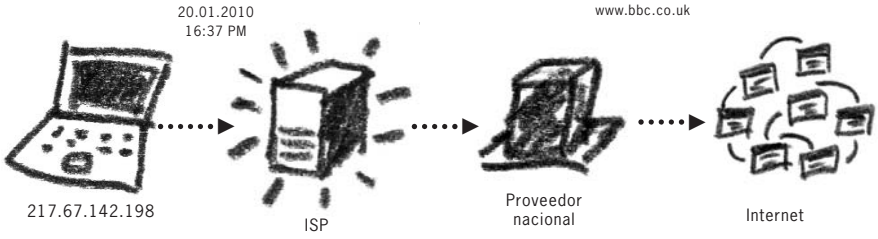
En el mundo físico, nos identifica nuestro gobierno por el pasaporte y nuestros amigos por reconocernos. Como rasgos distintivos de nuestra identidad y asociaciones sirven otros documentos e información, como por ejemplo un carnet de conducir, un número de la seguridad social o del expediente fiscal, y nuestra reputación.

—

La tecnología moderna está mucho más omnipresente y es mucho más minuciosa que el mundo al que estábamos acostumbrados. Hoy en día, se recopilan y almacenan numerosos identificadores de nuestra vida personal, hábitos, movimientos y afiliaciones sociales. El análisis de estos datos y las suposiciones relativas a nuestra vida privada y profesional se llama perfilación, y a ella nos dedicamos más adelante en este capítulo.

—

Nuestras identidades digitales pueden ser recopiladas de varias informaciones, normalmente creadas y anunciadas mediante nuestras propias actividades, o de las de nuestros amigos o compañeros de trabajo. Siempre que utilizas Internet, eres identificado por la dirección IP que ha sido asignada actualmente a tu ordenador (véase el capítulo 2.5 y el Apéndice B). En el caso de trabajar desde casa o desde tu lugar de trabajo, esta dirección IP puede ser asociada rápidamente a tu verdadera identidad – tú has registrado y adquirido el acceso a Internet de un proveedor local quien conoce tu nombre y dirección.



► El historial de tu navegación puede vincularse directamente con tu ordenador

Un principio similar se puede aplicar para las comunicaciones mediante teléfono móvil. En caso de que hayas registrado el número de teléfono bajo tu nombre, todas las llamadas hechas o recibidas por este número serán asociadas contigo. Además, la ubicación de cada teléfono móvil puede ser identificada mediante un proceso llamado triangulación – cuando varias torres de telecomunicación en el alcance de tu teléfono pueden calcular dónde estás, con un margen de error de unos pocos metros. De hecho, es cada vez más complicado. Cada teléfono móvil es identificado por un número IMEI único (…). Este número es registrado en cada una de las comunicaciones hechas con ese teléfono. El cambio de la tarjeta SIM en un teléfono que previamente ha sido vinculado con tu identidad (mediante el IMEI) posiblemente no proporcionará mucho anonimato.

—

Los teléfonos móviles de la 3ª generación – los que proporcionan el acceso a Internet y las coordenadas del GPS (Sistema de Posicionamiento Global) – revelan al proveedor del servicio tu ubicación exacta y muy a menudo, tu identidad. Se sabe que el teléfono móvil puede revelar sus coordinadas cuando el dispositivo está apagado. Los teléfonos móviles siguen comunicando con las torres de telecomunicaciones mandando una señal breve de actividad cuando están apagados[68]. Debido a esta realidad, los teléfonos móviles pueden ser encendidos remotamente por el proveedor. Una de las soluciones identificadas es extraer por completo la pila del dispositivo, inutilizando así su capacidad de propulsar cualquiera de sus funciones. También pueden ser vinculados positivamente

68
ZDNet, FBI taps cell phone mic as eavesdropping tool, Declan McCullagh, Dec 1 de 2006, http://news.zdnet.com/2100-1035_22-150467.html

con tu identidad una cuenta y dirección de correo electrónico. Esto es obvio para las cuentas registradas bajo un nombre verdadero, y es también posible para cuentas anónimas a las que se accede desde un lugar donde la dirección IP está asociada contigo.

—

El mismo principio se aplica a tus cuentas de blog y de chat de Internet, los nombres de usuario en las redes sociales, registros en foros y perfiles de juego en Internet. Como ya hemos discutido en este manual, tu Internet y proveedores de servicio móvil reúnen un registro de tus comunicaciones. Con la suficiente información, es posible hacer la identificación positiva entre tu dispositivo de comunicaciones digitales y tu verdadera identidad.

—

Los ordenadores infectados por el software malicioso pueden exponer detalles confidenciales del usuario, revelando la información sobre sus actividades a una tercera parte. Para más información sobre cómo tratar con estas amenazas, por favor, consulte al capiítulo 2.9.

Perfiles digitales

Cuando una identidad digital es positivamente (o erróneamente) vinculada con una persona concreta, el análisis del comportamiento con el fin de hacer un perfil se convierte en un problema para la privacidad. Un historial de navegación por Internet y de comunicaciones por correo electrónico pueden revelar información importante sobre una persona, sus hábitos y asociaciones con grupos y otras personas. Se pueden hacer suposiciones sobre sus puntos de vista políticos y sociales, filiación y, más importantemente, sobre sus acciones futuras.

—

La perfilación es un término que se aplica generalmente a la acción de recopilar y buscar patrones de comportamiento o los patrones que se puedan encontrar dentro de la información ya almacenada en varias bases de datos, con el fin de determinar y predecir un rasgo o acción particular de una persona o un grupo. Puede ser utilizada por las instituciones de marketing y financieras para analizar la preferencia del consumidor y su interacción con un producto o servicio. Es un método común para frustrar intenciones criminales y terroristas, ya que intenta predecir e identificar a los perpetradores antes de que sean capaces de cometer un crímen. Utilizada ampliamente en la industria del transporte aéreo, la perfilación fue introducida inicialmente para impedir que los criminales y terroristas potenciales se embarcaran en los aviones.

—

Aparte de reunir antecedentes criminales, informes de crédito, datos de empleo y médicos, la perfilación de hoy en día incluye identidades digitales recopiladas – para aumentar su efectividad y alcance. Registros del correo enviado y recibido, de las llamadas telefónicas y consultas de sitios web se almacenan y pueden ser analizados para identificar tendencias, patrones de comportamiento y asociación. Un ejemplo común es la plataforma de Google para correo electrónico y aplicaciones – que proporcionan servicios gratuitos a millones de suscriptores, financiando sus servicios mediante la publicidad basada en contenidos. El software incorporado en la infraestructura de Google explora los correo electrónicos y las comunicaciones para proporcionar publicidades “relevantes“ en la pantalla. Los clientes aceptan esta política cuando crean sus cuentas[69]. Es difícil predecir cómo reaccionará Google cuando esta información sea requerida por el gobierno de los EEUU, pero la posibilidad es suficiente para imaginarse la omnipresencia y las posibilidades de la perfilación hoy en día. De modo

69
http://mail.google.com/mail/help/intl/en/privacy.html

parecido, es aún más difícil predecir cómo la corporación actuará y cumplirá con los requisitos de los gobiernos extranjeros. Por ejemplo, en China, Google estaba dispuesto a instalar reglas de filtrado para censurar los resultados de las búsquedas realizadas por ciudadanos chinos, para cumplir con la legislación local. Varias veces al año, se reúnen las empresas principales de tecnología y el gobierno para discutir el progreso y nuevos desarrollos relativos a Internet y la vigilancia de las telecomunicaciones[70].

—

No sólo las acciones de una persona pueden revelar (o distorsionar) la información sobre su identidad, sino también lo que los demás dicen sobre ella. Un correo electrónico destinado a su buzón hace una declaración en su perfil (en el Internet de hoy) por su contenido, si ha sido recibido o todavía no. Un correo electrónico enviado a un grupo de direcciones automáticamente vincula y crea asociaciones entre esta gente, ya sean verdaderas o deseadas por cada destinatario individual. Nuestro perfil es susceptible a, y a menudo afectado por, amigos y compañeros de trabajo que se comunican con nosotros.

—

Pocos ejemplos demuestran el potencial de la perfilación tanto como el de las redes sociales. Los usuarios de estas redes cuelgan en Internet una gran cantidad de información personal, crean asociaciones entre amigos y compañeros de trabajo, revelan su ubicación, fotografías y detalles de registro, con una presión y aliciente cada vez más grandes para unirse a esta "revolución de medios". Los vendedores, gobiernos y adversarios digitales nunca lo han tenido tan fácil. La Guardia Revolucionaria de Irán pasó mucho tiempo en la plataforma de Twitter observando como se estaban planeando manifestaciones y acciones, en algunos casos haciéndose pasar por activistas e impidiendo estas actividades antes de que tuvieran lugar.[71] Puede que Twitter les haya ayudado identificar (o confirmar) las identidades de los manifestantes y activistas sociales.

—

Una vez registrada, la información es muy difícil de eliminar (para más detalles, véase el capítulo 2.3) y lo mismo ocurre también con las herramientas de las redes sociales. La página personal de Facebook de un trabajador podrá ser examinada por algunos de sus afiliados profesionales – incluso si no tiene relación con el trabajo en cuestión. Los medios patrocinados por el gobierno que deseen ridiculizar o encontrar algún tipo de "trapos sucios" sobre miembros de una ONG que defiende los derechos humanos pueden investigar no sólo la existencia de páginas personales de los empleados en redes sociales, sino también las páginas de sus amigos, y las de los amigos de sus amigos. Una vez que se encuentre una información comprometedora en alguno de estos medios, se puede extraer una historia que afecte su reputación y credibilidad.

—

La perfilación no es algo a lo que uno pueda escapar en la infraestructura técnica de hoy en día. Sin embargo, estar alerta y tener cautela puede ayudar a la gente a limitar o hasta definir la información sobre ellos que se reúne y recopila. La integración de la tecnología en la vida profesional y personal de las personas ahora supone una exposición más grande a la perfilación y una vulnerabilidad adicional para la privacidad de los usuarios.

Autenticidad y autentificación

El carácter global e impersonal de Internet conlleva que se requieren nuevos métodos para autentificar la información y los usuarios. Hasta ahora, el usuario se ha identificado en su cuenta de correo electrónico con un nombre de usuario y una contraseña. La cuenta es vinculada con su identidad y el nombre

70
http://www.issworldtraining.com/

71
http://www.boston.com / bostonglobe/editorial_opinion/oped /articles/2009/06/20/ the_repercussions_of_a_twitter_ revolution/

asociado será utilizado para autentificar los mensajes enviados a los amigos y compañeros de trabajo. Los participantes de sesiones de chat en Internet, participantes en foros y propietarios de páginas de redes sociales utilizan un nombre de usuario.

—

Como hemos discutido previamente en este manual, una gran parte del contenido que viaja por Internet está sometido a vigilancia. Además, muchos identificadores que utilizamos para autentificar a la gente en el ciberespacio pueden ser modificados. Un adversario con experiencia puede suplantar con facilidad su dirección de correo electrónico para que coincida con la tuya (véase el capítulo 2.5) y enviar mensajes en tu nombre. Examinando muy detenidamente la codificación del mensaje, uno puede descubrir la verdadera identidad del remitente, pero pocos de nosotros sabríamos cómo hacerlo (véase el Apéndice B – Correo electrónico).

—

No se puede confiar en la autenticidad de un correo electrónico si es imposible verificar al verdadero remitente. Amnistía Internacional, por ejemplo, reconoce este problema, y todas sus comunicaciones por correo electrónico llevan al final un mensaje de descargo de responsabilidad:

> *"…La comunicación por medio de Internet no es absolutamente segura, por lo que Amnistía Internacional no acepta responsabilidad legal por los contenidos de éste mensaje. Si usted no es el destinatario, se le pide no revelar ni difundir la información de este mensaje…"*

Cuando estás manteniendo un chat (en MSN o Skype), supones que la parte con la que estás conversando es la persona que alega ser, aunque sea sin tener la ventaja del reconocimiento vocal o visual para confirmarlo. Una cuenta suplantada o comprometida puede crear una vulnerabilidad peligrosa para la privacidad y seguridad de la gente que se comunica con esta cuenta de chat y confía en su credibilidad.

—

Es bastante difícil determinar la verdadera identidad del interlocutor en un chat de Internet utilizando los métodos digitales. Hay que recurrir a los medios de identificación antiguos, bien probados – revelar los detalles concertados anteriormente o personales, conocidos sólo por las personas que mantienen la conversación. Se puede tratar de una palabra o pregunta secreta compartida al iniciar un chat que asocie la cuenta o el nombre del usuario con la persona real a la que conoces.

—

La identificación en el tiempo real es más problemática en un correo electrónico. Puede que el remitente no haya incluido ningún detalle que autentifique su identidad (o bloquee la dirección del correo electrónico). Asimismo, la amenaza de intercepción de un correo electrónico o de modificación de su contenido sigue siendo una posibilidad real y constante.

—

Las firmas digitales fueron creadas como una respuesta a la inseguridad de la autentificación basada en Internet. Emplean el **cifrado** para registrar los contenidos de tu mensaje y tu identidad, asegurado por una frase de acceso fuerte. Si el mensaje es modificado, la firma digital será inválida y el destinatario será avisado sobre la invalidez del mensaje. Cuando hayas utilizado un buen sistema de **cifrado** de clave pública, tus firmas digitales serán de sumo valor para la autentificación de tu mensaje para el destinatario, o de su mensaje para ti.

Para más detalles sobre las firmas digitales como un método de autentificación, véase el capítulo 2.4 “Criptología“.

Hacia el anonimato digital

Conseguir el verdadero anonimato es una hazaña difícil en el mundo moderno de la tecnología de comunicaciones. Demasiados activistas han sido expuestos y castigados por publicar artículos bajo seudónimo, enviar mensajes de texto y hacer llamadas telefónicas uno a otro. Puede que no revelen ningún detalle para identificarse uno a otro en el contenido de sus mensajes, pero sin darse cuenta utilizan la tecnología que tiene estas funciones integradas.

—

La solución es ser consciente de cómo un dispositivo, mensaje o acción online concretos pueden ser asociados con tu verdadera identidad, y tomar las medidas necesarias. Es posible conseguir un cierto grado de anonimato registrando una dirección de correo electrónico bajo un nombre de cuenta aleatorio. Es mejor hacerlo desde un ordenador público (por ejemplo, de un cibercafé o biblioteca) donde la dirección IP no puede ser asociada contigo. Elige un servicio conocido ampliamente, como Hotmail o Gmail y una dirección de correo electrónico que no incluye un nombre u otras palabras clave fáciles de encontrar. No incluyas estos detalles en ninguna parte del mensaje e intenta tener cuidado a la hora de revelar la dirección a los demás.

—

Al navegar por sitios web, presta atención a cómo puede ser monitorizada tu actividad. Si deseas un relativo anonimato al navegar en sitios web no deseados (comoquiera que éstos sean definidos en el país), hazlo desde ordenadores públicos. Para ocultar el verdadero destino y origen de tus consultas, puedes utilizar las redes de anonimato como Tor o servidores proxy anónimos (para más detalles, véase el capítulo 2.6). Intenta no relajarte demasiado en este punto y no navegues a un sitio web “no deseado“ desde tu conexión personal de Internet “sólo una vez“. Una vez que se cree un registro de tu consulta, probablemente se quedará en los servidores del proveedor durante un largo período de tiempo.

—

En cuanto al uso de los teléfonos móviles, los nuevos dispositivos y tarjetas SIM poseen un cierto grado de anonimato. Las tarjetas SIM de prepago y los teléfonos móviles no registrados pueden hacer anónima la identidad de los interlocutores. Ten en cuenta que el grado de anonimato desciende con cada uso, y cambia de dispositivo con frecuencia. En algunos países, es también posible adquirir tarjetas SIM y teléfonos con etiquetas de identificación no registradas (o corrompidas), pero puede que esta práctica nos sea legal en todas las jurisdicciones.

—

Probablemente será demasiado tarde para hacer anónima tu identidad digital existente, ya sea en Internet o en la red de telefonía móvil. Para conseguir un medio anónimo de comunicaciones, crea nuevas cuentas y números de teléfonos móviles. Presta la atención al lugar y al método de registro, la correspondencia hecha mediante este servicio o dispositivo y su asociación con otros.

—

Mantente alerta, sé consciente y ten cuidado con tus acciones en Internet y en la red de telefonía móvil, si el anonimato es una parte esencial de tu seguridad.

Esta sección se ocupará específicamente de la legislación que mina el trabajo legítimo e importante llevado a cabo por los defensores de derechos humanos – aplicada al mundo digital y la tecnología relevante. Nos centraremos en el efecto directo e indirecto de las leyes sobre la seguridad y protección de los defensores de derechos humanos.

Con Internet ha aparecido un nuevo medio de comunicación y aprendizaje global. La mayoría de los gobiernos del mundo son conscientes de su potencial económico y social. Y mientras que algunos de ellos están muy interesados en sacar provecho del nuevo mercado global, otros tienen dudas en lo que se refiere al impacto que Internet puede tener sobre la estabilidad y supervivencia de sus regímenes gobernantes.

—

Internet cruza fronteras administrativas y geográficas con una facilidad y velocidad sin precedentes. Proporciona un método pionero de comunicación en el que la voz de una persona puede ser oída simultáneamente por todos los conectados. A diferencia de los medios tradicionales, donde la información se encuentra, raciona, edita y resume – en Internet la gente escoge lo que quiere. Los usuarios no están expuestos a propaganda política, noticias sobre famosos o resúmenes deportivos si no eligen exponerse a éstos. Los usuarios eligen lo que quieren leer, con quién quieren comunicarse y qué verdad es la verdad para ellos. No sorprenderá, por lo tanto, que esto haya causado un gran problema a los países que desean mantener las libertades políticas, sociales y religiosas de sus ciudadanos dentro del control del gobierno.

—

La infraestructura abierta de Internet sirve para promover la Declaración Universal de Derechos Humanos (DUDH), especialmente la libertad de expresión, reunión y asociación (artículo 19). En su informe para la Comisión de la ONU sobre Derechos Humanos del 29 de enero, 1999, el Relator Especial para la protección y promoción de la libertad de opinión y expresión, Abid Hussein observó que "aunque quizás único en su alcance y aplicación, Internet es, básicamente, sólo otra forma de comunicación cuya restricción y regulación violaría los derechos enunciados en la Declaración Universal de Derechos Humanos, particularmente, el artículo 19." Más adelante él argumentó:

> *"En lo que se refiere al impacto de la nueva tecnología informática sobre el derecho a la libertad de opinión y expresión el Relator Especial considera como de importancia pre-eminente que se considere bajo los mismos estándares internacionales que otros medios de comunicación y que no se tome ninguna medida que restrinja excesivamente la libertad de expresión e información; en caso de duda, la decisión debería ser a favor de la libre expresión y flujo de información. Con respecto a Internet, el Relator Especial desea reiterar que la expresión online debería guiarse por estándares internacionales y ser garantizada la misma protección como la otorgada a las otras formas de expresión."* [72]

La difusión de las Tecnologías de Comunicación en Internet (TCI) ha puesto también de relieve la cuestión de la privacidad. Como transmitimos más de nuestra información y comunicaciones por el mundo digital, nos enfrentamos con gobiernos y corporaciones que desean reunir, procesar y analizar estos datos. La información recopilada incluye los sitios web que visitamos, nuestros correos electrónicos, destinos de viajes, finanzas personales e historial médico, pertenencia a movimientos políticos o sociales, asociaciones religiosas, etc. La invasión de nuestra privacidad es ciertamente una nueva práctica, sin embar-

72
Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión para la Comisión de la ONU sobre Derechos Humanos, 29 de enero de 1999, E/CN, 4/1999/64.

go, nuestra confianza en la tecnología moderna y su infraestructura fácil de vigilar han hecho esta intrusión cada vez más habitual. Incluso la ONU ha sido víctima de este tipo de problemas. En la Primera Cumbre Mundial sobre la Sociedad de la Información (CMSI) celebrada en 2003 en Ginebra (la segunda Cumbre tuvo lugar en Túnez en 2005), todos los participantes obtuvieron tarjetas de identidad, en las cuales – sin que lo supieran los delegados – fue incorporado un chip de identificación de radiofrecuencias. El chip podía ser utilizado para registrar los movimientos y contactos de los participantes durante la Cumbre[73].

—

Los ataques del 11 de septiembre de 2001 tuvieron un efecto negativo sobre las leyes que se refieren a la privacidad, causando que los países que todavía no habían introducido (o ni siquiera discutido) la necesidad de desarrollar tecnologías de monitorización y vigilancia, las introdujeran.

> *"El período inmediato después del septiembre de 2001 fue un tiempo de miedo, cambio e incertidumbre. Las Naciones Unidas respondieron con la Resolución 1368 que apelaba a un incremento en la cooperación entre países para prevenir y eliminar el terrorismo. La OTAN invocó el Artículo 5, en el que se afirma que el ataque a cualquier país miembro de la OTAN es un ataque a toda la OTAN; las legislaciones nacionales respondieron en consecuencia. El Consejo de Europa condenó los ataques, pidió solidaridad y también una mayor cooperación en asuntos criminales. Posteriormente, la Asamblea Parlamentaria del Consejo de Europa apeló a los países a que ratificaran convenciones para combatir el terrorismo, levantaran cualquier reserva en estos acuerdos, y extendieran los poderes de los grupos de trabajo de la policía para incluir "mensajes terroristas y su descodificación."* [74]

En octubre de 2001, la Cámara de Representantes de los EEUU ratificó la Ley para Proporcionar las Herramientas Requeridas para Interceptar y Obstruir el Terrorismo (la Ley Patriótica de los Estados Unidos). Otorgó al FBI poderes para instalar en Internet una infraestructura de vigilancia, conocida como DCS-1000 (o denominada también CARNIVORE en todos los Proveedores de Servicios Internet (ISP) nacionales). En 2003, el Congreso de los EEUU eliminó para los grupos de investigación la necesidad de obtener una orden judicial para conseguir datos personales sobre usuarios de Internet y sitios web concretos[75]. Poco después, el general Ashcroft concedió al FBI la autoridad para reunir información sobre usuarios de Internet fuera de investigaciones oficiales y para iniciar la vigilancia online sobre la base de una sospecha a priori. Aprobada originalmente como una ley temporal, esta ley se aprobó de manera permanente tras los ataques terroristas en Londres en julio de 2005.

—

Tras los ataques de Bali en 2003, el gobierno australiano introdujo leyes que requerían que todos los ISP reunieran y monitorizaran voluntariamente los datos que pasaban por sus servidores, que instaran a los usuarios a que revelaran sus claves de **cifrado** y participaran en el proyecto de vigilancia **ECHELON** liderado por los EEUU. Posteriormente, el gobierno concedió a sus agencias poderes para interceptar y leer correo electrónico, SMS y mensajes del buzón de voz sin una orden judicial (como fue propuesto en el Proyecto de Ley para Interceptar Telecomunicaciones de 2002) sobre la base de que comunicaciones de este tipo, supuestamente, constituyeron "…acceso a datos "almacenados" más bien que a la información "interceptada" en tiempo real[76].

—

Colombia y Zimbabwe, entre otros, han legitimado la intercepción de comunicaciones privadas sin la necesidad de una aprobación judicial previa[77]; la India

73
http://www.washingtontimes.com/news/2003/dec/14/20031214-011754-1280r/

74
Privacy International – Informe sobre la Privacidad y Derechos Humanos de 2004 – Las amenazas a la privacidad.

75
En enero de 2005, se reveló que el FBI ya no utilizaba Carnivore, y, en cambio, había empezado a usar una aplicación de software comercial no especificada.

76
http://nocleanfeed.com/

77
Propuesto en el Proyecto de la Ley sobre la Intercepción de las Comunicaciones de 2006, publicado en Gaceta del gobierno el viernes 26 de mayo de 2006.

aprobó la Ley de Prevención del Terrorismo (POTA), que otorga a la policía amplios poderes para interceptar comunicaciones; Jordania enmendó su Código Penal para incluir el Artículo 150 que estipula el encarcelamiento de cada persona que publique de cualquier manera "…una historia, discurso o acto que ofenda la unidad nacional, incite a la gente a cometer crímenes, inculque odio entre miembros de la sociedad, instigue al sectarismo o racismo, insulte la dignidad y libertades personales de los individuos, promueva rumores inventados, incite a los demás a disturbios, sentadas, o promueva reuniones públicas que violen las leyes del país."; los Países Bajos dieron el visto bueno a una propuesta legislativa que permite a un fiscal solicitar datos sobre el tráfico de los proveedores de redes y servicios de telecomunicaciones públicas y aprobaron un decreto especial para permitir escuchas telefónicas entre abogados y sus clientes; Singapur enmendó la Ley de Abuso de Ordenadores para permitir a sus autoridades tomar acciones preventivas contra posibles piratas informáticos que se basen en "información creíble" que relacione a los sospechosos con ataques planeados contra redes de información sensible[78].

—

Éstas son sólo algunas medidas radicales para incrementar la vigilancia y recopilación de información por parte del gobierno con la excusa de aparentemente combatir el terrorismo. No incluyen las prácticas de las agencias de inteligencia que actúan fuera de la legislación existente, involucradas en practicar escuchas telefónicas ilegales, interceptar correo electrónico y robar información de ordenadores personales. En marzo de 2006, se supo que la administración Bush realizó miles de escuchas telefónicas en llamadas privadas sin permiso del Congreso. La lógica con la que se justificaba esta decisión era que los poderes del presidente y la importancia de la seguridad eran mayores que la necesidad de actuar dentro de la legislación existente[79].

—

La cuestión del abuso de poder, apoyado por cambios legislativos, es particularmente de gran actualidad en países sin un sistema judicial justo y sin organismos reguladores independientes. La mayoría de la gente se da cuenta de la necesidad de luchar contra el terrorismo, pero, de esta manera, renuncian a sus libertades personales y a su derecho a la privacidad y confidencialidad sin considerar siempre las consecuencias.

—

Para citar un comentario general sobre el derecho a la privacidad del Comité de Derechos Humanos de las Naciones Unidas, el organismo autorizado para interpretar las obligaciones de los países bajo el Pacto Internacional de Derechos Civiles y Políticos:

> "Como todas las personas viven en sociedad, la protección de la vida privada es por necesidad relativa. Sin embargo, las autoridades públicas competentes sólo deben pedir aquella información relativa a la vida privada de las personas cuyo conocimiento resulte indispensable para los intereses de la sociedad en el sentido que tienen con arreglo al Pacto. […] Incluso con respecto a las injerencias que sean conformes al Pacto, en la legislación pertinente se deben especificar con detalle las circunstancias precisas en que podrán autorizarse esas injerencias. La decisión correspondiente competerá sólo a la autoridad designada por la ley a ese efecto, que dará la autorización necesaria tras examinar cada caso en particular. […] La correspondencia debe ser entregada al destinatario sin ser interceptada ni abierta o leída de otro modo. Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones.[80]"

78
Privacy Internacional – Informe sobre la Privacidad y Derechos Humanos de 2004.

79
"NSA tiene una base de datos enorme de llamadas telefónicas de ciudadanos norteamericanos", USA Today, 11 de marzo de 2005, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm

80
Comité de Derechos Humanos de las Naciones Unidas, Observación General nº 16: El derecho al respeto a la vida privada, la familia, el domicilio y la correspondencia, y protección de la honra y la reputación (art.17), 08/04/88, para. 7 y 8.

Bangladesh, Pakistán, China, Vietnam y otros países concedieron a las agencias del gobierno amplios poderes para acceder a su discreción a todo el tráfico en Internet y por correo electrónico[81]. Corporaciones multinacionales en Internet ignoran los estándares internacionales relativos a la privacidad. Cooperan con gobiernos proporcionando información personal sobre los usuarios almacenada en sus servidores.

—

La denegación de los derechos a la privacidad y a la libertad de expresión se convirtió en una tendencia general en muchas partes del planeta. La tecnología se está utilizando para monitorizar a las personas – estén en la calle o en Internet.

81
Privacy International – Informe sobre la Privacidad y Derechos Humanos de 2004.

3.1 CENSURA DEL CONTENIDO ONLINE

PUBLICACIÓN DE MATERIALES ONLINE

Los defensores de los derechos humanos se han beneficiado de Internet, ya que les ha permitido comunicarse fácilmente con la comunidad global. Las noticias sobre violaciones de derechos humanos se publican online y pueden provocar una condena rápida desde fuera de un país o área concretos. Algunas regiones, que anteriormente estaban fuera del alcance de los medios de comunicación internacionales, ahora pueden conseguir que se oigan sus voces. Los gobiernos que intentan acallar en sus países las voces discrepantes afrontan ahora dificultades a nivel global.

—

Dado que, en realidad, no hay ninguna disposición que justifique o permita la censura del contenido dentro del marco internacional, la mayoría de los países recurre a su legislación nacional. A menudo, este razonamiento es difícil de justificar, ya que las publicaciones en Internet, a diferencia de los medios locales, están involuntariamente dirigidas a un público global y pueden publicarse en un país, pero ser accesibles en todo el mundo. En el caso de difamación *Dow Jones Media group v. Gutnick,* que tuvo lugar en Australia, Joseph Gutnick demandó ante los tribunales a la revista online canadiense *Barrons*[82] por difamación. El Tribunal Supremo de Australia confirmó la decisión del Tribunal Supremo del Estado de Victoria, que aceptó considerar el caso sobre la base de que el artículo podía ser leído también en los ordenadores situados en el estado de Victoria. En otras palabras, el lugar de publicación fue considerado con arreglo a la jurisdicción de cualquier país donde el artículo podía ser leído, no sólo donde estaba ubicada la editorial.

—

Otro caso, relativo a la censura del contenido online, empezó en 2000 y llevó al proceso *Yahoo! Inc. v. La Ligue Contre le Racisme et L'antisemitisme* en Francia y en los EEUU. El objeto del pleito fue la publicación de literatura y parafernalia nazis en un sitio web de Yahoo Groups, accesible también para los usuarios en Francia, donde la actividad de este tipo está prohibida. El tribunal francés insistió en que Yahoo tomara medidas para impedir que contenido de este tipo fuera accesible en Francia, aunque el sitio no contravenía las leyes de los Estados Unidos – donde están situados los servidores de Yahoo. Finalmente, los tribunales en los dos países fallaron contra Yahoo, desafiando la primera enmienda de la Constitución de los EEUU. Aparte de la cuestión de la propaganda nazi, este caso sentó el precedente que permitió que las leyes de un país se hicieran cumplir en otro.

—

Muchos países establecieron directrices específicas relativas a la legalidad de la publicación de información online. Por ejemplo, en **Irán** la ley *"…prohíbe y considera como un crimen publicar en Internet cualquier material que esté en conflicto con o insulte la doctrina islámica, valores de la revolución, las ideas del Imam Jomeini, la Constitución, que ponga en peligro la solidaridad nacional, infunda cinismo en el público en lo que se refiere a la legitimidad o eficiencia del gobierno, que propague una buena imagen de grupos ilegales, que revele información confidencial del estado, que promueva el vicio, haga publicidad del tabaco, acuse o insulte a los funcionarios del estado…*[83]*"*

82
(2002) 210 CLR 575.

83
"Acceso Denegado" – Un informe sobre el estatuto de Internet en Irán, Centro de Investigación y Entrenamiento de Organizaciones de Sociedad Civil de Irán, 2005.

En **Birmania**, *" los usuarios de Internet tienen prohibido publicar contenidos relacionados con la política que sean "perjudiciales" para los intereses del estado o para las políticas actuales o asuntos del gobierno.*[84]*"*

—

Tailandia y **España**, por ejemplo, prohíben cualquier acto de *lesa majestad* (ofensa a la familia real), mientras que Turquía prohíbe todo el contenido que se considera como un insulto a la nación turca o al fundador de Turquía moderna, Kemal Ataturk, tanto como referencias al genocidio armenio. Arabia Saudí prohíbe la publicación del contenido en Internet que "viole la decencia pública", "infrinja la santidad del Islam" y "cualquier cosa contraria al estado o a su sistema". Alemania y Francia activamente persiguen y cierran (o censuran el acceso a) cualquier publicación que niegue el holocausto o haga accesibles objetos de parafernalia nazi.

—

En **Egipto**, la Ley de Emergencia, que cada vez tiene más poderes, incluye una declaración acerca de la publicación de materiales, "…que piden verbalmente, por escrito, o por cualquier otro medio el incumplimiento de cualquier disposición de la constitución o de las leyes; la posesión de material escrito que requiera o favorezca estas acciones; la difusión deliberada de noticias, declaraciones, rumores falsos o maliciosos o noticias inquietantes, si su objetivo es el de alterar el orden público, provocar miedo en la gente, o causar daño al interés o bienes públicos, o el desarrollo de publicaciones que contengan cualquiera de los crímenes anteriores[85]" En 2002, los usuarios egipcios de Internet fueron advertidos sobre una serie de asuntos tabú (como las relaciones entre los coptos y los musulmanes, la publicación de ideas terroristas, la violación de derechos humanos, las críticas al presidente, a su familia y al ejército, y la promoción de versiones modernas del Islam) e informados de que hablar demasiado abiertamente sobre estos temas no sería bien visto. Varios bloggers egipcios han sido encarcelados por expresar sus opiniones en Internet.

—

Otros ejemplos de la legislación que afecta el acceso al contenido de los medios digitales incluyen:

- El Proyecto de la Ley de Enmienda sobre Servicios de Radiofusión Australianos de 1999, que establece la autoridad de la Autoridad Australiana de Medios de Comunicación y Comunicaciones (ACMA) para regular el contenido en Internet. El contenido de sitios web alojados en servidores australianos y extranjeros es clasificado por la Oficina de Clasificación de Películas y Literatura. Los servidores que alojan el contenido clasificado como prohibido pueden recibir una orden para cerrar el sitio web si están situados en Australia o el sitio web será añadido en las listas oficiales del software de filtrado en Internet.[86]
- Las Disposiciones Chinas para la Administración de los Servicios de Información de Noticias en Internet definen el contenido de noticias online como "…información, informes y comentarios sobre asuntos actuales, política, economía, asuntos militares, diplomacia, emergencias públicas y otros asuntos públicos..." El artículo 5 de esta disposición estipula que cualquier sitio web o boletín informativo que desee publicar contenido que todavía no ha aparecido en sitios web oficiales esté sujeto a la inspección y aprobación de la Oficina de Información del Consejo del Estado.[87]
- El Decreto Vietnamita sobre las Actividades Culturales y de Información somete a los que divulgan "ideología reaccionaria" incluyendo a los que revelan secretos (del partido, del estado, militares y económicos), los que niegan

84
Privacy International – Silenced 3/09/2003

85
http://www.eohr.org/PRESS/2003/3-9.HTM

86
Electronic Frontiers Australia http://www.efa.org.au/Issues/Censor/cens1.html

87
Law Info China http://www.lawinfochina.com/index.asp

logros revolucionarios, y los que no presentan sus artículos para revisión antes de su publicación a multas de hasta treinta millones de dongs (unos US$1500).[88]

- La Fundación de Vigilancia en Internet (IWF), un organismo autorregulador independiente de los ISP que fue establecido en el Reino Unido en 1996 tiene una línea directa para que los ciudadanos denuncien posibles casos de pornografía infantil ilegal. Colaborando con las autoridades competentes y de gobierno, la Fundación envía "ordenes de cierre" a sus ISP miembros aconsejando qué contenido online debería ser bloqueado para clientes.[89]
- La India requiere dentro de su acuerdo para la obtención de licencias de ISP que los ISP "…aseguren que el contenido ofensivo, obsceno, no autorizado o cualquier otro contenido, mensajes o comunicaciones que infrinjan de cualquier modo derechos de reproducción, derechos de propiedad intelectual y derecho informático internacional y doméstico o que no concuerden con las leyes de la India, no se puedan encontrar en su red, el ISP debería tomar todas las medidas necesarias para prevenirlo…"[90]

FILTRADO DE SITIOS WEB

Países en todo el mundo adoptan tecnologías de filtrado en Internet. Les permiten bloquear sitios web o el contenido específico de un sitio web para los usuarios en su territorio. Se trata de, en esencia, la censura aplicada a Internet. El filtrado ocurre en casi cada país, y suele ser determinado para categorías pre-establecidas de información. La clasificación del contenido en Internet en categorías susceptibles de ser censuradas, incluye: religión, política, pornografía, pedofilia, derechos humanos, etc.

—

Se pueden observar dos posturas respecto a la censura de información: (1) Todo lo que no está explícitamente permitido está prohibido; y (2) Todo lo que no está explícitamente prohibido está permitido. A estas dos prácticas generalmente se refiere como a la lista blanca y la lista negra respectivamente, y es esta segunda postura la que prevalece en la mayoría de infraestructuras de Internet nacionales. Cuba, Birmania y Vietnam inicialmente bloquearon para sus ciudadanos todo el contenido en Internet, permitiendo que sean accesibles sólo unos pocos sitios web[91].

—

La dificultad de mantener estas listas blancas y listas negras muchas veces ha resultado en que se delegue esta tarea a los ISP y que se los haga responsables si alguno de sus usuarios es capaz de acceder al contenido que no está autorizado en el país. Asimismo, las empresas de software comercial están involucradas en el negocio de la censura del contenido. WebSense, Content Watch y Fortinet son ejemplos de las empresas de filtrado de software, cuyos productos se utilizan en ámbitos de redes educacionales, de corporaciones y nacionales. SmartFilter, un producto de Secure Computing, clasifica por temas sus listas de las URL investigadas por la empresa, incluyendo "Aborto, Material para Adultos, Educación, Noticias y Medios de Comunicación, Ilegal o Cuestionable"[92], etc., permitiendo a sus clientes añadir sus propias direcciones de URL a las listas existentes. Sus productos son adquiridos por gobiernos e ISP que necesitan aplicar una política de censura.

—

A menudo, los países extienden regulaciones relativas a los medios de comunicación existentes para incluir publicaciones en Internet. De cualquier persona que desee crear un blog en un país concreto se puede requerir, por ejemplo, registrarse como una empresa de medios de comunicación, lo que permite que

88
OpenNet Initiative, Perfiles de Investigación, Vietnam http://opennet.net/research/profiles/vietnam

89
La Fundación de Vigilancia en Internet, http://www.iwf.org.uk/public/page.31.htm

90
Gobierno de la India, Acuerdo para la Provisión de Servicios de Internet, http://www.dot.gov.in/isp/licence_agreement.htm

91
OpenNet initiative, Informes de Países, http://opennet.net/research

92
Secure Computing, Secure Web SmartFilter http://www.securecomputing.com/index.cfm?skey=86

las leyes existentes relativas a las emisoras y medios de comunicación escritos se apliquen a la blogosfera[93]. En principio, este paso podría facilitar las consideraciones legales para controlar publicaciones online, pero un blog a menudo representa la opinión de una sola persona, no pasa por el proceso editorial y es publicado sin tener en cuenta la ubicación física de los servidores del sitio web (es decir, las leyes que regulan el contenido en un país) y las sensibilidades de los lectores. No encaja en el modelo tradicional de prensa y medios de comunicación.

—

Los estados están renunciando a los acuerdos internacionales sobre la libertad de información y expresión y están decidiendo ellos mismos qué contenidos sus ciudadanos pueden y no pueden consultar. Esto se suele hacer con el pretexto de mantener la estabilidad nacional y preservar la cultura, seguridad y el estado de derecho. Estas excusas se han utilizado ampliamente para censurar los sitios web dedicados a los asuntos de la libertad de expresión, de la política, de los medios de comunicación independientes y de los derechos humanos.

—

El 31 de diciembre de 2002, el gobierno iraní dictó el "Decreto sobre la Constitución del Comité a cargo de la determinación de sitios web no autorizados" que afirma: "Para salvaguardar la cultura islámica y nacional, el Ministerio de Información establecerá un comité que estará constituido por los representantes del Ministerio de Información, el Ministerio de Cultura y Orientación Islámica, la Radio de República Islámica de Irán, el Consejo Supremo de la Revolución Cultural, y la Organización de Propagación Islámica para determinar e informar al Ministerio de TIC sobre los criterios relativos a los sitios web no autorizados." Los sitios web revelados por el Comité al Ministerio de TIC son añadidos a la lista de los que son sometidos a la censura[94].

—

En Singapur, los sitios web son controlados y autorizados por la Singapore Broadcasting Authority (SBA) y deben acatar las directrices estrictas de la autoridad en lo que se refiere al contenido "ofensivo" que abarca desde pornografía hasta "las áreas que pueden minar la moral pública, la estabilidad política o la harmonía religiosa."[95]

—

No obstante, las intenciones del gobierno de bloquear sitios web no se publican, y las listas de sitios web bloqueados no están disponibles públicamente. Por lo tanto, algunos sitios en Internet están siendo bloqueados no porque contravienen regulaciones específicas, sino porque el gobierno considera el acceso a ellos perjudicial para la política que promociona. Un ejemplo clásico de esta metodología es China, donde los ISP y otros proveedores de comunicación están obligados a estar de acuerdo con "resistir firmemente la transmisión de la información que viola tradiciones culturales y códigos morales buenos de la nación china[96]." Por consiguiente, China ha sido capaz de utilizar la tecnología de filtrado más sofisticada del mundo, empleando a miles de personas cuyo trabajo es constantemente explorar y actualizar las listas blancas/negras de sitios web.

—

En general, no hay un consenso público sobre qué sitios web los gobiernos pueden censurar y, a menudo, no existe ningún proceso de apelación para conseguir que se quite el bloqueo de un sitio web. Esto ocasiona que la gente aplique la tecnología de evasión con el fin de evitar los sistemas de filtrado de su país. El proceso suele implicar que se solicite a un ordenador situado en un país donde Internet no está censurado tan estrictamente, que encuentre el sitio web

93
Institute for War and Peace Reporting, "Internet Hit by Media Law Change, el 30 de enero de 2007

94
Acceso Denegado – Un informe sobre el estatuto de Internet en Irán, Centro de Investigación y Entrenamiento de Organizaciones de Sociedad Civil de Irán, 2005.

95
Informe sobre la Censura en Internet – El Comité para la Protección de Periodistas de Canadá.

96
Privacy International – Informe sobre La República Popular China, 2004.

y transmita su contenido. Desde el punto de vista técnico, el usuario sólo está accediendo al ordenador de retransmisión y no al sitio web prohibido. Para citar al fundador de la Fundación Fronteras Electrónicas (EFF), John Gilmore, "Internet percibe la censura como un daño, y lo evita."

—

El filtrado de Internet no sólo dificulta el trabajo de los defensores de los derechos humanos, sino que a veces puede impedir que noticias sobre violaciones de derechos humanos lleguen a la comunidad tanto local como global. Los gobiernos pueden bloquear el acceso a los sitios web alojados en su país, paralizando de este modo la capacidad de la organización anfitriona de transmitir noticias y sus actualizaciones. O bien, pueden impedir que sus ciudadanos accedan a ciertos sitios web en Internet, restringiendo así el acceso de los defensores de derechos humanos a comunicaciones, información y su capacidad de expresar libremente su opinión.

3.2 VIGILANCIA DE COMUNICACIONES

La vigilancia de comunicaciones ha existido desde los tiempos del telégrafo. Está generalmente aceptado que la policía y los servicios de inteligencia necesitan el poder de escuchar a escondidas las conversaciones de los demás por el beneficio y seguridad de todos. Muchos delincuentes han sido detenidos gracias a las escuchas telefónicas y al registro de las grabaciones de las llamadas. También se supone que estos poderes no son concedidos arbitrariamente y que un proceso judicial rigoroso o similar tiene lugar antes de que se autoricen acciones de este tipo. La gente se resistiría y protestaría si encontrara que cada conversación telefónica que han mantenido en su vida fue grabada y almacenada.

—

Por lo tanto, es sorprendente y desafortunado que tantos países fueran capaces de introducir rápida y discretamente leyes que permiten la vigilancia y retención de comunicaciones en Internet.

En 1996, Digicom, el proveedor de servicios electrónicos más grande de Pakistán, pidió a sus clientes que firmaran acuerdos que imponían una serie de restricciones relativas al uso de Internet. Conforme a los términos de los acuerdos, se prohibía a los usuarios el uso del cifrado de datos y tenían que aceptar que sus comunicaciones podían ser monitorizadas por agencias del gobierno. Además, los usuarios de los servicios de Internet tenían que proporcionar a Digicom copias de sus tarjetas de identidad nacionales, mientras que los extranjeros tenían que presentar la copia de su pasaporte. Aquellos que no lo hicieran, se enfrentarían con la desconexión de sus servicios. [97]

Hubo rumores de que los ataques del 11 de septiembre fueron organizados en gran parte por Internet. Las autoridades en todo el mundo se otorgaron poderes adicionales para vigilar las comunicaciones de Internet que entraban y salían de sus países. El resultado de este proceso fue que se vulneraron las libertades concedidas en la época de las telecomunicaciones.

—

Como ya hemos mencionado, los sistemas de vigilancia en Internet han sido introducidos por algún tiempo a nivel nacional. El Servicio Federal de Seguridad de Rusia instaló en cada **ISP** un sistema de monitorización mediante cajas negras (el proyecto es conocido como SORM2). Además, forzaron a los ISP a pagar por el equipo de monitorización. El proyecto "Escudo Dorado" de China fue anunciado en 2001. En lugar de confiar solamente en la Intranet nacional, separada del Internet global por un cortafuegos enorme, China se está preparando para incorporar en la red un servicio de espionaje que le permitirá "ver", "oír" y "pensar."[98] Un sistema de vigilancia global conocido como **ECHELON** [99] fue lanzado conjuntamente por los EEUU, el Reino Unido, Australia, Nueva Zelanda y más tarde por Alemania después del fin de la Guerra Fría.

—

Las comunicaciones en Internet no son solamente monitorizadas, sino que también guardadas y a menudo por un período de tiempo largo. En 2005, la Unión Europea, bajo la presión del Consejo, introdujo legislación que obliga a todos los estados miembros a guardar datos relativos a Internet durante un período mínimo de dos años[100] (aunque los estados miembros pueden decidir guardarlos por períodos más largos). El Artículo 8 de la Convención Europea de

97
Informe sobre la censura en Internet - El Comité para la Protección de Periodistas de Canadá.

98
G. Walton, China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China 9 (Rights and Democracy, 2001), disponible en http://serveur.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html

99
El uso de Echelon para comunicaciones diplomáticas específicas fue puesto de relieve como consecuencia de las revelaciones hechas en 2003 por un empleado del servicio de inteligencia británico, antiguos funcionarios de las Naciones Unidas, y un antiguo ministro del gobierno británico relativas a las escuchas telefónicas realizadas por la NSA de los EEUU y la GCHQ (Central de Comunicaciones del Gobierno) británica de las comunicaciones telefónicas y conversaciones privadas del Secretario General de Naciones Unidas Kofi Annan.

100
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2005-0512+0+DOC+XML+V0//ES

Derechos Humanos garantiza el derecho de cada persona al respeto de la vida privada y de la familia. El Artículo 8 especifica que las autoridades públicas pueden interferir en este derecho sólo en circunstancias claramente definidas. En concreto, toda intromisión debe ser de acuerdo con la ley y puede ser llevada a cabo sólo para la defensa de los intereses de la seguridad nacional y de la prevención del crimen.

—

La vigilancia y retención de datos indiscriminados constituyen una amenaza para el derecho a la privacidad personal, especialmente de los defensores de los derechos humanos, que ya están sometidos a una vigilancia y monitorización especial por parte del estado. La capacidad del estado de monitorizar, registrar y almacenar las comunicaciones de los defensores de los derechos humanos supone una amenaza para su trabajo y seguridad. Las comunicaciones también pueden ser modificadas y manipuladas para desacreditar a un defensor de derechos humanos o para imponer sanciones penales. Las corporaciones de Internet que cooperan con regímenes represivos, están, por lo tanto, contribuyendo a debilitar la privacidad de individuos.

—

Cada país involucrado en la vigilancia generalizada de la actividad de sus ciudadanos en Internet debería establecer un organismo autoritativo independiente para monitorizar tanto la recopilación de los datos de este tipo como el acceso a ellos. Hay que disponer de leyes estrictas que prevengan el abuso de estos sistemas para proteger nuestra privacidad, identidad y tranquilidad.

3.3 CRIPTOGRAFÍA

Considerando las prácticas de vigilancia y monitorización de Internet, como han sido descritas en la sección anterior, es necesario que los usuarios dispongan de los medios para recuperar su privacidad online. Si la información se reúne y almacena sin consideración de su contenido o fin, uno tiene derecho a tomar medidas para hacer sus datos privados para que no estén a disposición de extraños o para que no puedan ser modificados por extraños.

—

La importancia del cifrado para proporcionar la privacidad de información y comunicación fue rápidamente aprovechada por gobiernos y sociedades civiles. La introducción de la criptografía de clave pública y varias herramientas fáciles de utilizar pusieron una herramienta increíblemente poderosa al alcance de todos. Pronto fue evidente su efectividad al neutralizar las habilidades y capacidades de las agencias del gobierno para llevar a cabo una vigilancia exitosa. Desde entonces, algunos gobiernos han estado luchando por restringir el uso público del cifrado o prohibirlo por completo.

—

El "International Survey of **Encryption** Policy" ("Estudio Internacional de la Política de Cifrado") publicado en 1999 por *Centro de Información para la Privacidad Electrónica* empezaba con la siguiente declaración: "Hoy en día, la mayoría de los países del mundo no tienen ningún control sobre el uso de la criptografía. En la gran mayoría de los países, la criptografía puede ser libremente utilizada, manufacturada, y vendida sin restricción. Esto se aplica tanto para las naciones industriales como para las en vías de desarrollo." Diez años más tarde, vemos cambios radicales en la legislación relativa al **cifrado** – como se desprende de la información recopilada por Bert-Jaap Koops para su estudio sobre las leyes del cifrado "Crypto Law Survey". Prácticamente cada país del mundo regula el uso del cifrado, la venta de productos de criptografía, su importación y exportación y a veces incluso el aprendizaje de su uso, como por ejemplo, es decretado en Kazajstán.[101]

—

La fuerza de la privacidad proporcionada por el cifrado ha llevado a su clasificación como arma militar y a su inclusión en el Tratado de Wassenaar[102]. Los Estados Unidos inicialmente exigieron un sistema de custodia de claves a nivel mundial. Primero, los gobiernos temieron la pérdida del poder de recabar información y restringieron el uso de criptografía si no eran capaces de descifrar el código. Al final, los defensores de la privacidad ganaron la batalla por no limitar el uso de criptografía para hacer la información personal segura.

—

Desgraciadamente, algunos países siguen prohibiendo el cifrado, o totalmente o mediante la persecución de sus usuarios. China, por ejemplo, aprueba el uso de los productos de cifrado que han sido desarrollados y autorizados en China[103]. Este hecho ha llevado a que la herramienta de telefonía en Internet popular Skype, que utiliza el cifrado para transmitir datos entre usuarios, sea reprogramada y comercializada en China como TomSkype.

101
http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm

102
El Tratado de Wassenaar es un acuerdo firmado por un grupo de 33 países industrializados para restringir la exportación de armas convencionales y tecnología de "doble uso" a ciertos otros países considerados como estados paria o, en algunos casos, a los que están en guerra.

103
http://rechten.uvt.nl/koops/cryptolaw/cls2.htm#prc

3.4 PERSECUCIÓN DE LOS DEFENSORES DE DERECHOS HUMANOS

Regímenes opresivos han tomado medidas estrictas contra los defensores de derechos humanos que intentan criticar a sus gobiernos y a sus funcionarios. Abajo está la lista compilada de los datos reunidos por Front Line y de otras fuentes de información sobre los defensores de derechos humanos que han sufrido la persecución y encarcelamiento debido a sus actividades en línea.

Mohammad Reza Nasab Abdullahi

Irán – El 23 de Febrero de 2005, tras un proceso a puerta cerrada celebrado sin la presencia de su abogado, fue condenado a seis meses de prisión con la posibilidad de apelación por insultar al Líder Supremo y por difundir propaganda antigubernamental. Fue encarcelado cinco días más tarde. Abdullahi, un estudiante universitario, defensor de los derechos humanos, editor de un periódico estudiantil y blogger en la ciudad de Kerman situada en el centro de Irán, cumplió seis meses en una cárcel iraní por publicar una entrada en su **blog,** Webnegar ("Estritor de Red")[104]. La entrada ofensiva, titulada "Quiero saber," fue dirigida al Líder Supremo ayatolá Alí Jamenei y criticó la supresión de "derechos y libertades civiles y personales" por el gobierno.

Arash Sigarchi

Irán – Debido a sus actividades como periodista y blogger, Arash Sigarchi ha estado en la cárcel a partir del 26 de enero de 2006, cuatro días después de ser dictada una sentencia de tres años por "insultar al Guía Supremo" y por "propaganda en contra del régimen."

Previamente, fue detenido y encarcelado durante dos meses a principios de 2005 y fue condenado a 14 años de prisión por un tribunal revolucionario por los mismos cargos en febrero de 2005. Después de pagar una fianza de 1 mil millones de riales (95 000 euros), fue puesto en libertad el 17 de marzo de 2005.

Antes de esto, fue arrestado el 27 de agosto de 2004 y detenido durante varios días por publicar online un artículo, con fotos, sobre una concentración organizada en Teherán por los parientes de prisioneros ejecutados en 1989. A partir de entonces, ha sido constantemente acosado por la policía.

El antiguo editor del diario Gylan Emroz, Sigarchi mantuvo durante tres años un blog político y cultural (www.sigarchi.com/blog) en el que a menudo criticaba el régimen. Las autoridades hicieron imposible acceder al blog dentro de Irán.

Al-Mansuri

Libia - Al-Mansuri publicó su último artículo el 10 de enero de 2005. Fue una crítica de un debate entre dos funcionarios del gobierno, uno de ellos, Shukri Ghanim, era un reformador reconocido, y el otro, Ahmed Ibrahim – un conocido partidario de la línea dura . Al-Mansuri expresó la esperanza de que al-Saddafí apoyaría al primero. El 19 de octubre de 2005, Akhbar Libia informó que un tribunal de Trípoli condenó a al-Mansouri a un año y medio en la cárcel por la posesión ilegal de un arma.

104
Disponible en
http://www.iranreform.persianblog.com

Ibrahim Lutfy, Mohamed Zaki, Ahmad Didi y Fathimath Nisreen

Las Maldivas - Ibrahim Lutfy fue detenido (junto con **Mohamed Zaki**, **Ahmad Didi** y **Fathimath Nisreen, asistente de** Lutfy) en enero de 2002 por producir *Sandhaanu*, un boletín informativo sobre las violaciones de derechos humanos y corrupción distribuido por correo electrónico. Acusados de "difamación" y de "intentar derrocar al gobierno," Lutfy, Zaki and Didi fueron condenados a cadena perpetua el 7 de julio de 2002. Lufty fue liberado en mayo de 2005 después de 3 años. Nisreen, quien tenía en el momento del proceso sólo 22 años, recibió una pena de prisión de 5 años. Fue liberado en mayo de 2005 después de 3 años de prisión.

Lutfy logró escaparse de su guardia de policía el 24 de mayo, mientras estaba en la cercana Sri Lanka por una operación de ojos. Sufría de conjuntivitis crónica, agravada por las malas condiciones en la prisión (después de muchos rechazos, las autoridades finalmente le dieron el permiso para ir a Sri Lanka y recibir el tratamiento. Pasó varios meses escondiéndose en Sri Lanka con la ayuda de una red de amigos. Luego el ACNUR le ayudó obtener el estatuto de refugiado en Suiza, donde vive en la actualidad. El policía asignado a vigilarlo durante su estancia en Sri Lanka fue encarcelado.

Didi fue ingresado en un hospital en Male en febrero de 2004 y fue puesto bajo arresto domiciliario. Tuvo problemas cardíacos graves que probablemente requerían cirugía. Zaki, cuya salud empeoró gravemente en la prisión, fue puesto también bajo arresto domiciliario. Las sentencias de los dos fueron reducidas a 15 años en 2003.

Dr Nguyen Dan Que

Vietnam - Dr Nguyen Dan Que, 61, un defensor de la libertad de expresión, liberado en 1998 después de pasar casi 20 años en la cárcel, fue detenido otra vez en su casa en Saigón el 17 de marzo de 2003. Los funcionarios no especificaron ninguna razón para su detención, pero se creía que estaba relacionada con una declaración que había publicado en línea en la que criticaba la falta de libertad de prensa en Vietnam. Estaba respondiendo a comentarios de un portavoz del ministerio de exteriores que sostenía que la libertad de información estaba garantizada en Vietnam. Aunque sufre de hipertensión arterial y una úlcera estomacal, no se le ha permitido a su familia que le visite o que se le dé la medicación que necesita. El 22 de septiembre de 2003, 12 laureados de los Premios Nobel escribieron al secretario general del Partido Comunista de Vietnam Nong Duc Manh expresando su preocupación por la salud de Que y pidiendo que le sea permitido que se le administre un tratamiento médico apropiado y visitas de la familia hasta su liberación.

Nguyen Vu Binh

Vietnam – El antiguo periodista fue condenado a siete años de prisión el 11 de diciembre de 2003 tras un proceso que duró menos de tres horas. El Tribunal Popular de Hanoi le condenó a tres años de arresto domiciliario cuando termine su sentencia. Fuentes cercanas a las autoridades vietnamitas dijeron que los cargos principales, supuestamente, están relacionadas con una carta enviada por Nguyen el 19 de julio de 2002 a la Comisión de Derechos Humanos del Congreso de los EEUU, en la que criticó la situación de los derechos humanos en su país. Aparentemente, está acusado también de estar en contacto con "disidentes subversivos" como Le Chi Quang y Pham Hong Son, los dos de los cuales están también en prisión. Además, está acusado de haber recibido 4,5 millones de dongs (unos 230 euros) "de una organización reaccionaria con sede

96
180 F. Supp. 2d 572 (D.N.J. 2001). *See generally* EPIC's Scarfo web page http://www.epic.org/crypto/scarfo.html

97
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2005-0512+0+DOC+XML+V0//EN&language=EN

en el extranjero", de haber estado involucrado en una organización anti-corrupción y de haber apelado a las autoridades vietnamitas en 2000 a establecer un partido democrático liberal. Vu Binh está también acusado de publicar en Internet mensajes de "carácter revolucionario", en particular, un ensayo titulado "reflexiones acerca de los acuerdos sobre fronteras entre China y Vietnam" en el que criticó el tratado de 1999 entre estos dos países.

Zouhair Yahyaoui

Túnez - Zouhair Yahyaoui, fundador y editor del sitio web de noticias *TUNeZINE*, fue liberado provisionalmente el 18 de noviembre de 2003 después de cumplir más de la mitad de su sentencia de 28 meses. Detenido en un publinet (cibercafé iniciado por el gobierno) de Túnez el 4 de junio de 2002, utilizó su sitio web para difundir las noticias sobre la lucha por la democracia y libertad en Túnez. Bajo el pseudónimo "Ettounsi" ("El Tunecino" en árabe), escribió muchas columnas y ensayos y fue el primero en publicar una carta abierta al presidente Ben Ali criticando la falta de integridad del sistema judicial tunecino. *TUNeZINE* fue censurado por las autoridades desde el principio. Pero sus seguidores recibieron una lista semanal de servidores proxy a través de los cuales podían acceder a él. El 10 de julio de 2002, Yahyaoui fue condenado por un tribunal de apelación a 12 meses de prisión por "publicar noticias falsas" (artículo 306-3 del código penal) y otros 16 meses por "robo mediante un uso fraudulento de un canal de comunicaciones" (artículo 84 del código de comunicaciones), lo que significó que utilizó una conexión de Internet en la publinet donde trabajaba. Fue encarcelado bajo condiciones muy duras y llevó a cabo dos huelgas de hambre a principios de 2003 para protestar contra su encarcelamiento. Fue liberado más de un año después de su encarcelamiento, en noviembre de 2003, y murió por causas naturales en marzo de 2005 a la edad de 36 años.

Mohammed Abbou

Tunéz - Mohammed Abbou es un destacado jurista defensor de derechos humanos que está en la actualidad cumpliendo su sentencia de tres años y medio de prisión por publicar en Internet declaraciones que llamaban la atención sobre los abusos de los derechos humanos en el sistema carcelario tunecino. Las declaraciones comparaban la tortura y maltrato sufridos por los prisioneros tunecinos a los que sufrieron los prisioneros en Abu Ghraib. Mohammed es un miembro del Consejo Nacional para las Libertades en Túnez, uno de muchas ONG nacionales que el gobierno tunecino rechaza a reconocer, y un ex-director de la Asociación de los Jóvenes Letrados. Como crítico tenaz de la corrupción, fue uno de los pocos abogados de Túnez dispuestos a comentar públicamente la corrupción y actuar sobre las alegaciones de corrupción en la que estaba involucrada la familia del presidente Ben Ali. Fue encarcelado en abril de 2005, tras un proceso ampliamente considerado como injusto y arbitrario por las ONG tunecinas e internacionales y está encarcelado en la prisión de El Kef, a 170 kilómetros de su casa y familia en Túnez. El 11 de marzo de 2006, para llamar atención sobre las condiciones inhumanas y degradantes en las que está detenido y sobre el acoso sufrido por los miembros de su familia cuando le visitan, Mohammed inició su segunda huelga de hambre desde su encarcelamiento.

—

Samia Abbou, esposa de Mohammed Abbou, fue objeto de un ataque brutal el 7 de diciembre de 2006. Ella y otros tres destacados defensores de los derechos humanos de Túnez fueron atacados y golpeados fuera de la prisión de El Kef, cerca de Túnez, por un grupo de unos cuarenta hombres en ropa de civil. La Libertad Nacional de Samia Abbou viajó a El Kef para visitar su marido encar-

celado con defensores de derechos humanos; Moncef Marzouki, ex-presidente del Consejo Nacional para las Libertades en Túnez (CNLT) y de la Liga Tunecina para los Derechos Humanos (LTDH); Salim Boukhdhir, un periodista conocido, y Samir Ben Amor, miembro fundador de la Asociación Internacional de Apoyo a los Presos Políticos. Según los informes, la policía detuvo el coche en el que viajaban en una serie de ocasiones durante su viaje a El Kef y estaba presente fuera de la prisión en el momento del ataque.

Habib Salih

Siria – El 29 de mayo de 2005, funcionarios de la inteligencia militar detuvieron a Habib Salih en Tartus, a unas 100 millas (130 kilómetros) al norte de Damasco (que acababa de ser liberado de una previa encarcelación – por participar en el movimiento de la sociedad civil "Primavera de Damasco"). Esta vez, fue detenido por publicar en dos sitios web una serie de cartas abiertas dirigidas a los delegados que acudieron al Congreso del Partido Ba`ath de junio de 2005 en las que describió detalladamente su experiencia en prisión. En los meses después de su liberación, también escribió artículos críticos para el periódico libanés *an-Nahar* y el sitio web prohibido http://www.elaph.com. Las autoridades le trasladaron inmediatamente a la oficina de investigaciones donde corre el riesgo de tortura. Su proceso todavía está pendiente.

Huang Qi

China – Huang es un defensor de derechos humanos que creó el sitio web de Tianwang (www.6-4tianwang.com) en junio de 1999 para publicar información sobre gente desaparecida. Gradualmente, el sitio también empezó a publicar artículos con comentarios y noticias sobre temas que no suelen ser tratados por los medios de comunicación controlados por el estado. Publicó historias sobre abusos de derechos humanos, corrupción del gobierno, y – sólo unos días antes de que Huang fuera detenido – varios artículos sobre la masacre en la Plaza de Tiananmen. Huang fue arrestado el 3 de junio de 2000 – el día antes del XI aniversario de las protestas en la Plaza de Tiananmen de 1989 – y acusado conforme bajo los artículos 103 y 105 del código penal. Fue acusado de publicar en su sitio web artículos sobre las protestas escritos por disidentes que viven en el extranjero. En una entrevista para la BBC, Huang dijo que le ordenaron a dormir en el suelo al lado del servicio durante el primer año en prisión. Rechazó la acusación de subversión e insistió en que no se le podía acusar.
Huang declaró: "Si alguien en China lucha por la democracia y libertad y es acusado de ser un participante del incidente del 4 de junio, un miembro de Falun Gong o un activista prodemocrático, seguro que voy a decir al régimen chino que yo soy uno de ellos y que estoy orgulloso de ello. No hay duda de que yo persigo la democracia y la libertad." El 4 de junio de 2005, Huang Qi fue liberado de la cárcel después de cumplir su sentencia. En 2004, Reporteros sin Fronteras le concedió el Premio "Ciberlibertades".

98
http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm

99
The Wassenaar Arrangement is an agreement by a group of 33 industrialized countries to restrict the export of conventional weapons and "dual use" technology to certain other countries considered pariah states or, in some cases, those that are at war.

4.1 CASO PRÁCTICO 1 CREANDO UNA POLÍTICA DE SEGURIDAD

Al desarrollar una política de seguridad para ti o tu organización, tienes que desarrollar también una comprensión clara de los riesgos de seguridad de tus ordenadores e información. El nivel de riesgo incrementa en proporción directa a las amenazas y a tu vulnerabilidad hacia ellas, como indica la siguiente ecuación:

RIESGO = AMENAZAS x VULNERABILIDADES

Amenazas representan la posibilidad de que alguien dañe la seguridad de tus ordenadores, información almacenada en ellos y comunicaciones en línea. Realizar una evaluación de amenazas significa analizar la probabilidad de que una amenaza particular sea puesta en práctica. Ejemplos de amenazas incluyen:

- **Un ataque de virus.**
- **Confiscación del equipo del ordenador.**
- **Bloqueo de sitios web.**

Vulnerabilidad significa el grado en que eres propenso a la pérdida, daño y sufrimiento en caso de ataque (si la amenaza es realizada) que varía con situación y tiempo. La vulnerabilidad es siempre relativa, porque toda la gente y grupos son vulnerables hasta cierto punto. A menudo, la vulnerabilidad principal en el campo de tecnología es la falta de entendimiento o un entrenamiento insuficiente. Otra vulnerabilidad proviene de confiar y depender excesivamente de una tecnología que uno no comprende por completo.

- La vulnerabilidad tiene que ver con la ubicación del ordenador. Por ejemplo, la pantalla de tu ordenador y las operaciones realizadas se pueden observar fácilmente cuando operas desde un cibercafé. Si vives en un país que sufre de sequías y cortes de electricidad, otra vulnerabilidad será el corte de electricidad (o sobrecargas de electricidad) y, por consiguiente, ordenadores e Internet inoperantes.
- Las vulnerabilidades pueden incluir también la falta de medios de comunicación, como no tener acceso al teléfono o a una conexión de Internet.
- Las vulnerabilidades también pueden estar relacionadas con el trabajo en equipo y el miedo: un defensor que recibe una amenaza puede sentir miedo, y su trabajo estará afectado por el miedo. Si no puede tratar este miedo de manera apropiada (no tiene a nadie con quien hablar, un buen equipo de colegas, etc.), es posible que cometa errores o tome malas decisiones. Esta amenaza no está relacionada directamente con el ordenador, pero podría ser de gran relevancia para la seguridad del ordenador, ya que incrementa la probabilidad de que se ponga en práctica una amenaza ya existente.

Capacidades son fuerzas y recursos a los que un grupo o un defensor pueden acceder para conseguir un grado razonable de seguridad. Como ejemplo de las capacidades podríamos mencionar el entrenamiento en cuestiones de informática y seguridad. El conocimiento del funcionamiento de los ordenadores y de Internet es una capacidad esencial para tratar con posibles inseguri-

100
Unfortunately this classification has become a strategy used by many repressive governments around the world. Internet is effectively outlawed due to its **encryption** capabilities, yet enforcement of this law is selective and could be used to pressure human rights groups.

dades. El acceso a un técnico de ordenadores fiable o a una red de personas cualificadas es un gran recurso.

- Políticas de seguridad dentro de la organización: almacenamiento de archivos eficiente, almacenamiento de copias de seguridad y de comunicaciones por Internet.
- Entrada a la oficina segura y cierres fuertes en las puertas y ventanas.
- Copias de todas las garantías del hardware y de las licencias del software (o, utilizar sólo el software de fuente abierta)

No saber lo suficiente sobre el ambiente en tu trabajo y sobre la tecnología que utilizas es una vulnerabilidad, mientras que tener este conocimiento es una capacidad. El riesgo, creado por amenazas y vulnerabilidades, puede ser reducido si los defensores tienen suficientes capacidades (cuanto más capacidades, tanto menor el riesgo).

$$\textbf{Riesgo} = \frac{\text{amenazas x vulnerabilidades}}{\text{capacidades}}$$

Así que, por ejemplo, el riesgo de perder tus documentos digitales por un ataque de virus equivale a: el riesgo de un ataque de virus, multiplicado por la vulnerabilidad de no tener instalados un virus cleaner y software de cortafuegos, y dividido por la capacidad alcanzada cuando obtuviste la Caja de Herramientas de Seguridad.

—

Desde luego, ésta no es una fórmula matemática, pero su ventaja principal radica en que te ayuda a identificar los elementos que pueden causar que surja un riesgo, y, por lo tanto, te permite eliminarlo.

ELABORANDO UN PLAN DE SEGURIDAD

Componentes del plan

Un plan de seguridad está encaminado a reducir tu riesgo. Por lo tanto, tendrá como mínimo tres objetivos, basados en tu evaluación de riesgo:

- Reducir el nivel de amenaza al que est·s sometido.
- Reducir tus vulnerabilidades.
- Reforzar tus capacidades.

Podría resultar útil que tu plan de seguridad contuviera también:

- Planes o protocolos preventivos para asegurar que el trabajo rutinario sea llevado a cabo dentro de los est·ndares de seguridad. Por ejemplo, cÛmo comunicar por correo electrÛnico con un grupo de personas sobre temas sensibles.
- Planes de emergencia para tratar con problemas especÌficos, por ejemplo, confiscaciÛn del equipo de oficina.

Responsabilidades y recursos para poner el plan en práctica

Para asegurar que el plan sea puesto en práctica, hay que integrar en las actividades de trabajo diarias unas rutinas diarias:

- Incluir una evaluaciÛn de contexto y puntos de seguridad en tu orden del dÌa.
- Registrar y analizar los incidentes de seguridad.
- Asignar responsabilidades.
- Asignar los recursos, es decir, tiempo y fondos, para la seguridad.

Elaborando el plan – cómo empezar

Si has efectuado una evaluación de riesgo para un defensor o una organización, podrías tener una larga lista de vulnerabilidades, varios tipos de amenazas y una serie de capacidades. En realidad, no puedes solucionar todo al mismo tiempo. Entonces ¿dónde empezar? Es muy fácil:

- **Elige algunas amenazas.** Prioriza las amenazas que figuran en tu lista, ya sean reales o potenciales, utilizando uno de estos criterios: La amenaza más grave – la pérdida de todos los datos del ordenador, por ejemplo; O la amenaza más probable y grave: si han sido atacadas organizaciones similares a la tuya, esto es claramente una amenaza posible para ti; O la amenaza que más corresponde a tus vulnerabilidades – porque estás más en peligro por esta amenaza específica.

- **Haz una lista de las vulnerabilidades que tienes que corresponden a las amenazas que has enumerado**. Estas vulnerabilidades deberían ser enfocadas primero, pero recuerda que no todas las vulnerabilidades corresponden a todas las amenazas. Por ejemplo, si no tienes ninguna idea de si existe una copia de seguridad de todos tus datos en el ordenador, entonces esto está relacionado directamente con perder tus datos del ordenador de manera irrecuperable.

- **Haz una lista de tus capacidades que corresponden a las amenazas que has enumerado.** Ahora est·s en la posiciÛn de intentar tratar en tu plan de seguridad las amenazas, vulnerabilidades y capacidades elegidas, y puedes estar casi seguro de que ser·s capaz de reducir tu riesgo al empezar desde el punto de partida correcto.

PONIENDO EN PRÁCTICA TU PLAN

El objetivo de este plan es asegurar que la información almacenada en tus ordenadores no se perderá, y no será robada o dañada irrecuperablemente de ninguna manera.

Amenazas	Vulnerabilidades	Capacidades
Ataque de virus	– Los empleados abren correos electrónicos sin cautela. – Nadie sabe si hay un programa antivirus en todas las máquinas y si éste está actualizado. – No existe una copia de seguridad de la información.	– Acabas de recibir una copia de '*La Caja de Herramientas de la Seguridad Digital*' de http://security.ngoinabox.org
Confiscación de ordenadores	– Acceso fácil a la oficina. – No existe una copia de seguridad. – No hay fondos para adquirir un equipo nuevo. – La información no está protegida.	– Un buen equipo de colegas quienes conocen uno a otro y cooperan muy bien. – Una buena relación con los colaboradores que aportan fondos.
Ordenadores dañados por el tiempo u otras fuerzas externas	– No hay una copia de seguridad. – No tener ningún conocimiento sobre cómo proteger la red y el equipo eléctrico.	– Una buena relación con los colaboradores que aportan fondos. – Un pariente de un empleado es electricista.

Ahora empezamos a trabajar para reducir las vulnerabilidades y, de este modo, incrementar nuestra capacidad para tratar con estas y otras amenazas que pueden surgir en el futuro. Tus soluciones y recursos pueden diferir en cada caso. Ten en cuenta que la falta de respaldo de la información es una vulnerabilidad común que causaría un gran daño si alguna de las amenazas se realizara. Abajo está la lista de medidas que podrías tomar para disminuir la vulnerabilidad (todas las herramientas y explicaciones de cómo llevar a cabo estas acciones se pueden encontrar en la *Caja de Herramientas de Seguridad)*.

Ataque de virus

- Introduce una política estricta en lo que se refiere a abrir correo electrónico desde fuentes desconocidas o a responder a spam. Simplemente, prohíbe a todo el mundo hacerlo. La gente que recibe cientos de virus y spam debería cambiar su dirección de correo electrónico.
- Instala un antivirus gratuito (p.ej. Avast) en todos los ordenadores y actualiza las definiciones de virus desde Internet. Archivos y guías de programas se pueden encontrar en la *Caja de Herramientas de Seguridad*. Asegura que cada ordenador en la oficina está utilizando un programa antivirus que funcione completamente.
- Si tu ordenador está libre de virus, haz una copia de seguridad de todos los documentos de usuario importantes. Guárdala en un soporte aparte (CD, memoria USB) y fuera de la oficina. Si sufres el ataque de un virus, por lo menos podrás recuperar tus archivos.

Confiscación de los ordenadores

- Para prevenir un robo, tienes que asegurar tus oficinas e instalaciones donde trabajas. Puertas fuertes y barras en las ventanas son esenciales (especialmente si estás situado en una planta baja), tanto como un portero electrónico u otra manera de identificación de los visitantes. Lo ideal sería que tu oficina tuviera una recepción, donde se daría la bienvenida a los visitantes antes de acceder a la sala principal.
- Deberías hacerte una copia de seguridad de toda la información y guardarla en un lugar diferente.
- Deberías tener acceso a fondos de emergencia para adquirir un nuevo equipo y para descargar en él los datos almacenados en las copias de seguridad.
- Si los ordenadores son confiscados, por lo menos los documentos que están en ellos deberían estar protegidos contra un acceso no autorizado. Utiliza el software de **cifrado** para proteger una parte de tu disco duro. Asimismo, borra toda la información innecesaria para impedir que las personas a cargo de la confiscación accedan a ella. (Véase el capítulo “Copia de seguridad, destrucción y recuperación de la información”).
- Sé consciente de quién tiene las llaves de la oficina y cuántas copias hay. Si tus ordenadores no están protegidos por el **cifrado,** o almacenas datos sensibles en papeles y ordenadores, entonces asegura que nadie puede acceder solo a tu oficina, ni siquiera los mozos de la limpieza.

Ordenadores pueden ser dañados por el tiempo u otras fuerzas externas

- Idealmente, un fontanero y un electricista deberían controlar el área de tu oficina regularmente para informar sobre su estabilidad, posibles daños sufridos por fugas de agua y la calidad del aislamiento térmico.

Todos los cables eléctricos sueltos deberían desecharse y las conexiones defectuosas deberían ser reparadas. Esto puede ser costoso, pero es necesario, debido a que los ordenadores son extremadamente delicados y no pueden sobrevivir daños por agua o fuego.

- Deberías hacer una copia de seguridad de toda la información y guardarla en un lugar diferente.
- Puedes adquirir para tus ordenadores una batería del Sistema de Alimentación Ininterrumpida (UPS) para impedir que se apaguen inesperadamente en caso de corte de electricidad. Los enchufes de potencia o tableros de alimentación deberían tener protectores contra sobrecargas en la red eléctrica. En las regiones que sufren cortes de electricidad durante meses enteros, se debería de considerar el uso de un generador propulsado por gasolina u otras fuentes de energía.

Es difícil introducir políticas de seguridad sin minar algún aspecto de la productividad de tu oficina. Prestar atención a la seguridad suele requerir mucho tiempo y concentración. Un descuido, fechas límite y personal insuficiente son los enemigos de una buena seguridad. Por lo tanto, es necesario que las reglas sean acordadas e interiorizadas por todos. Su introducción debería incluir a todo el mundo y los directores de las organizaciones deben asumir el liderazgo y dar un buen ejemplo. Una buena seguridad también requiere que seas proactivo y que te des cuenta de las amenazas y encuentres maneras de tratarlas antes de que ocurran.

4.2 CASO PRÁCTICO 2 CANALES DE COMUNICACIÓN

RESUMEN

La ONG global "Derechos Humanos para Todos" (Sede Central) con sede en Europa ha solicitado que una de sus ramas internacionales (la Agencia) lleva a cabo una investigación sobre casos de tortura sufrida a manos del gobierno local. El país elegido "N" es conocido por utilizar la tortura contra los prisioneros y especialmente contra los defensores de los derechos humanos. La Agencia está situada en la capital de "N" y emplea varias personas cualificadas con muchos años de experiencia trabajando en situaciones difíciles. Pueden recopilar la información necesaria para el informe sobre la tortura, pero temen que el gobierno no se detenga ante nada para impedirles que lo hagan. "N" tiene una política muy estricta en lo que se refiere a controlar la información y asegurar que en el exterior se sepa lo menos posible sobre sus actividades internas. Los defensores de los derechos humanos necesitan establecer un canal seguro de comunicación con la Agencia y asegurar que el proyecto continúe hasta su finalización o cuanto más tiempo posible. Hay un entendimiento de que la seguridad es de suma importancia en este caso y han asignado para la Oficina un presupuesto de 5.000 USD especialmente para este asunto. El proyecto tiene que ser sometido a una revisión de sus métodos de recabar y transmitir la información, tanto como de crear una política de seguridad para que la aplique todo el personal.

—

Se decide que todo el personal recibirá entrenamiento sobre la seguridad de información por parte de un experto local y realizará su propio estudio e investigación sobre los asuntos de seguridad en Internet. Casos prácticos, informes de testigos y otra información sobre casos de tortura que el personal descubra, serán almacenados por escrito y en formato electrónico. Los corresponsales comunicarán sus hallazgos al traer los apuntes que han tomado durante su misión, y enviando a diario informes desde un cibercafé. En otras palabras, toda la información será duplicada en formato físico y electrónico.

—

La oficina dispone de un apartamento alquilado en el centro de la ciudad. Allí hay dos ordenadores con conexión de Internet. El personal conoce bien a los vecinos y disfruta de su apoyo. Anteriormente, alguien ha entrado ilegalmente en la oficina, aunque no se llevó nada importante.

AMENAZAS

Para llegar a entender qué elementos la Oficina necesitará para asegurar este proyecto, primero deciden hacerse una lista de todas las amenazas que puedan afrontar. Las instalaciones donde este proyecto se lleva a cabo son compartidas por la Sede Central, la oficina de la Agencia y los trabajadores de campo. Cada uno se enfrenta con sus propias amenazas particulares, que tienen que ser solucionadas por separado. Asimismo, las amenazas en sí se dividen en las que afectan a la oficina, a la información y a la seguridad de comunicación[105].

105
Hay un elemento adicional de la seguridad del personal, pero éste está mejor descrito en el "Manual de Protección para los Defensores de Derechos Humanos" escrito por Peace Brigades, http://www.frontlinedefenders.org/es/manuals/protection

SEDE CENTRAL

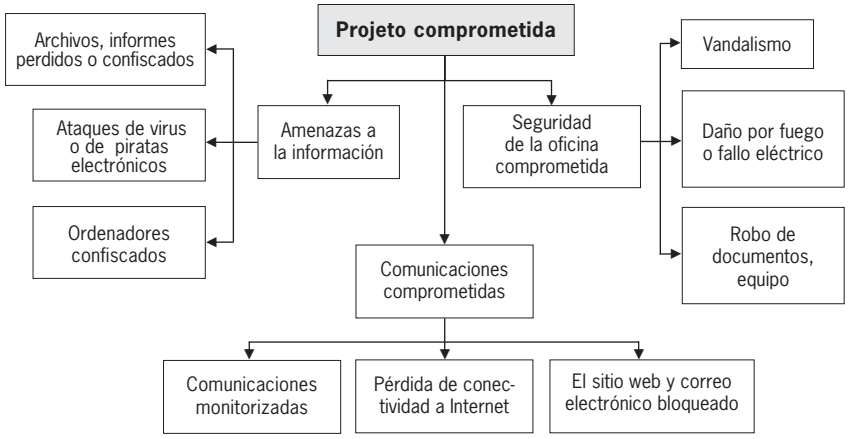
Amenazas en la oficina: mínimas.
Amenazas para su información: Los informes se podrían perder debido al daño causado por un virus o por la piratería informática.
Amenazas para la comunicación: El canal de comunicación con la Agencia podría ser interrumpido, o los informes podrían ser suplantados (falsificados por intrusiones maliciosas).

La Agencia

Amenazas en la oficina: Vandalismo contra su equipo, robo, cortes de electricidad, fuego.
Amenazas para su información: Los ordenadores son confiscados, los son datos alterados por ataques de virus o piratas informáticos.
Amenazas a la comunicación: Internet en la oficina es desconectado, los correos electrónicos no se envían o no llegan, el sitio web y la dirección de correo electrónico de la Sede Central son bloqueados, las comunicaciones son monitorizadas.

Trabajadores de campo

Amenazas para su información: los informes se pierden o son confiscados.
Amenazas para su comunicación: los trabajadores de campo no pueden acceder a un cibercafé, el acceso al sitio web de la Agencia o de la Sede Central está bloqueado dentro de N.



SOLUCIONES

Comunicación

La comunicación entre los diferentes agentes en este proyecto es esencial para su supervivencia. Por lo tanto, los participantes crean varios estándares y métodos de establecer o continuar esta comunicación.

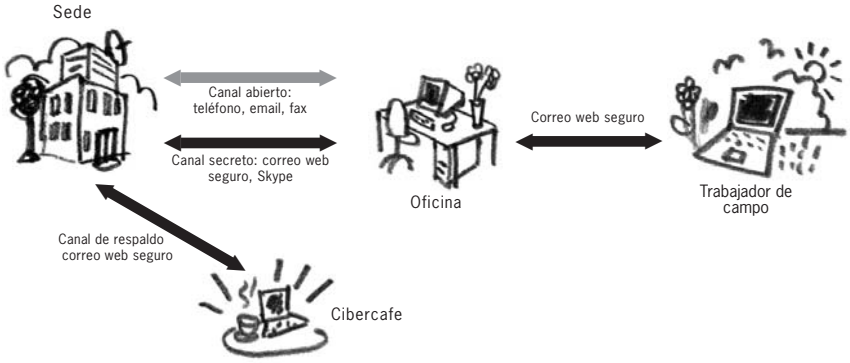
—

Se establecen tres canales distintos de comunicación con la Sede Central. Hay un **canal abierto**, donde la información es transmitida de forma insegura – por teléfono, correos o correo electrónico regular. Es importante tener un canal abierto para que los organismos de monitorización puedan estar satisfechos al tener el acceso a comunicaciones del proyecto. La información enviada por el canal abierto no es sensible e incluiría datos organizativos y administrativos típicos.

Un **canal privado** proporcionará comunicaciones sensibles y seguras. Se utilizará para intercambiar información sobre los casos, los informes de testigos y la estrategia organizativa. Se opta por usar una solución de correo web segura y Pidgin con OTR plugin para la mensajería instantánea[106]. No se transmitirá ninguna información sensible por teléfono, fax o correo electrónico no seguro. El canal privado no se utilizará regularmente para no atraer demasiada atención.

—

Los canales arriba mencionados requieren una conexión de Internet para la comunicación. Se acuerda que la Sede Central no sufrirá cortes en la conexión a Internet y se crea un **canal de respaldo de información** para la Agencia y sus trabajadores de campo, por si Internet deja de funcionar o es desconectado. El canal de respaldo de la información incluirá que los trabajadores de la Agencia utilicen un cibercafé cercano. Usarán versiones portátiles del software necesario, que se puede obtener de la *Caja de Herramientas de Seguridad* y las llevarán encima en una memoria USB. El propietario del cibercafé les ha asegurado que no hay ningún virus en sus ordenadores. De todas maneras, el personal utilizará los ordenadores públicos con cuidado.



► Esquema gráfico de las comunicaciones de la Agencia

Información

Todos los datos registrados y recabados por el personal se guardarán en papel y electrónicamente. Esto requerirá medidas de seguridad necesarias para garantizar que los datos no se pierdan y que no sean robados o dañados. Será muy importante crear y mantener un procedimiento de respaldo de información que sobrevivirá los posibles ataques. Asimismo, el medio del respaldo de información tendrá que ser seguro, dado que llevará una copia adicional de los documentos sensibles.

Para asegurar que no se pierda ningún informe de campo antes de que sea transmitido a la Agencia, se adquirirá un portátil. Los trabajadores de campo apuntarán la información en papel y la duplicarán en el portátil. Comunicarán a diario (o lo más frecuentemente posible) esta información a la Agencia desde un cibercafé.

Oficina

La seguridad de la oficina supondrá una política estricta para el personal, reforzar los puntos de entrada al edificio y un mantenimiento general para asegurar que las posibilidades de que un ordenador deje de funcionar sean reducidas. Los documentos físicos necesitarán ser guardados en una caja fuerte, y el papel gastado tendrá que ser destruido apropiadamente. Hay que tomar en cuenta que los ordenadores u otro equipo de oficina podrían ser dañados o confiscados, así que se mantiene un fondo de reserva para permitir a la organización comprar un nuevo equipo y terminar su trabajo en caso de que esto ocurriera.

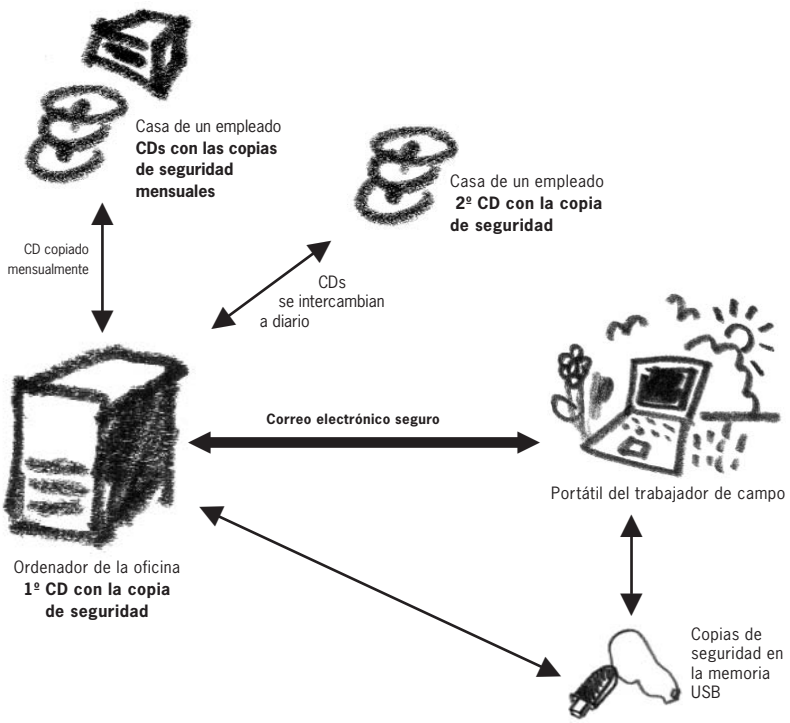
106
Puedes encontrar Pidgin y OTR plugin en la Caja de Herramientas de la Seguridad Digital.

RESPUESTAS DETALLADAS A LAS AMENAZAS

Después de desarrollar una idea general de cómo actuar cuando se enfrentan con posibles disrupciones de su trabajo, el personal intenta contrarrestar todas las amenazas individuales enumeradas en el diagrama. Los empleados reciben un entrenamiento sobre seguridad y llevan a cabo su propia investigación de la seguridad electrónica en Internet.

Amenazas para la información

- **Archivos, informes perdidos o confiscados:** Para prevenir la pérdida de datos, se hace regularmente una copia de seguridad de la información en los ordenadores y los portátiles. Se adquiere un disco compacto regrabable (CD-RW) por 200 USD y se instala en uno de los ordenadores. El respaldo de información se realiza utilizando el software Cobian Backup disponible en la *Caja de Herramientas de Seguridad* y los archivos se graban en el CD con el programa DeepBurner[107]. Un día sí y otro no se hace una copia de seguridad de todos los documentos de usuario, se graba en un CD y se traslada fuera del sitio. La persona encargada por mantener esta copia de seguridad alterna dos CDs, uno de los cuales está siempre en la oficina y el otro – en su casa. A final de cada mes, se hace una copia de seguridad adicional, la cual se da a otra persona para que la guarde en casa. De esta manera, en caso de que se estropearan o fueran dañados los ordenadores de la oficina y el sistema de respaldo de información diario fuera inutilizado (lo que es bastante difícil de orquestar), habrá un tercer nivel del respaldo de información del mes pasado. En el caso de los trabajadores de campo, el respaldo de información se realiza en una memoria USB. Esta memoria contiene una copia de todos los documentos recientes, creados por los reporteros desde que visitaron la oficina la pasada vez. Si el portátil se pierde o es confiscado, los documentos por lo menos podrán ser devueltos a la oficina.



► Capas múltiples del respaldo de datos

107 Http://www.deepburner.com

- **Ataques de virus o piratería informática:** Para prevenir la pérdida de datos causada por un ataque de virus o piratería informática, la Agencia instala en todos los ordenadores y portátiles el software antivirus Avast4. El software es gratuito para las organizaciones sin ánimo de lucro y se actualiza automáticamente cuando el ordenador se conecta a Internet. También se instala Spybot para contrarrestar otro software malicioso y el cortafuegos Comodo para impedir a los piratas informáticos que accedan a los ordenadores. Todo el software y explicaciones correspondientes se pueden encontrar en la *Caja de Herramientas de Seguridad*. En lo que se refiere a los virus, se introduce una política estricta, que garantice que nadie abra mensajes de correo electrónico que puedan levantar sospechas ni utilice un disquete externo en un ordenador sin escanearlo primero con el software antivirus.
- **Confiscación de ordenadores:** Si los ordenadores son confiscados, la organización debe tener medios para continuar con sus acciones. Será necesario adquirir nuevos ordenadores, y en el presupuesto tiene que haber dinero para este caso. Incluso sólo un ordenador será suficiente si las circunstancias lo exigen. El personal encuentra a un vendedor de ordenadores al por menor que les venderá un ordenador nuevo por 1000 USD. No hace falta decir que se necesitará una copia de seguridad de los archivos y documentos para que la organización vuelva a ser operativa y pueda continuar con el proyecto.
- **Robo de documentos, equipo:** Se introduce una política principal estricta y sólo aquellos que necesitan disponer de las llaves de la oficina obtienen su copia. No se puede hacer ninguna copia adicional sin un acuerdo general. Todos los ordenadores están apagados durante la noche y se adquiere una caja fuerte para los archivos por 300 USD. Todos los CDs, disquetes y papeles que llevan información sensible se guardan en la caja fuerte. Se toman medidas para asegurar que ninguna persona no autorizada pueda entrar en la oficina. Las ventanas están en la planta baja y, por lo tanto, estarán protegidas con barras de metal. También se refuerza la puerta y se instala una mirilla. Se acuerda con una empresa local que haga los dos servicios por 500 USD.
- **Pérdida de conectividad a Internet:** Es posible que Internet sea inutilizado para el uso de la Agencia. Esto se podría deber a la presión sobre el **Proveedor de Servicio de Internet** o a un mal funcionamiento de la red. Como estrategia de respaldo de información, el personal decide utilizar un cibercafé. Por si la interrupción de la conexión a Internet en la oficina fuera a largo plazo, se reservan 500 USD como fondo de emergencia para utilizar el cibercafé. Se usará una tarjeta de memoria de USB para transmitir archivos entre la oficina y el cibercafé.
- **Comunicaciones monitorizadas:** Si la infraestructura de vigilancia de N es suficientemente avanzada, estarán monitorizando los correos electrónicos que entran y salen del país. La Agencia sospecha que su correo electrónico es lo suficientemente sensible para justificar su monitorización y empieza a utilizar un servicio de correo web **SSL** seguro. Registran dos cuentas en https://mail.riseup.net[108] y utilizan una para comunicarse con la Sede Central y una para los trabajadores de campo. Toda la información se transmite a diario a la Sede Central por correo electrónico. Dado que la conexión al cliente de correo web es sobre **SSL** (HTTPs), está cifrada. El personal de la Sede Central investiga la posibilidad de los ataques "Man-in-the-Middle" y cuidadosamente examina los certificados presentados por el sitio web.
- **Sitio web y correo electrónico bloqueados:** Si el gobierno decide bloquear el acceso de Internet al sitio web de la Sede Central y al correo web RiseUP, hay que encontrar una alternativa. Los empleados de la Sede Central pueden

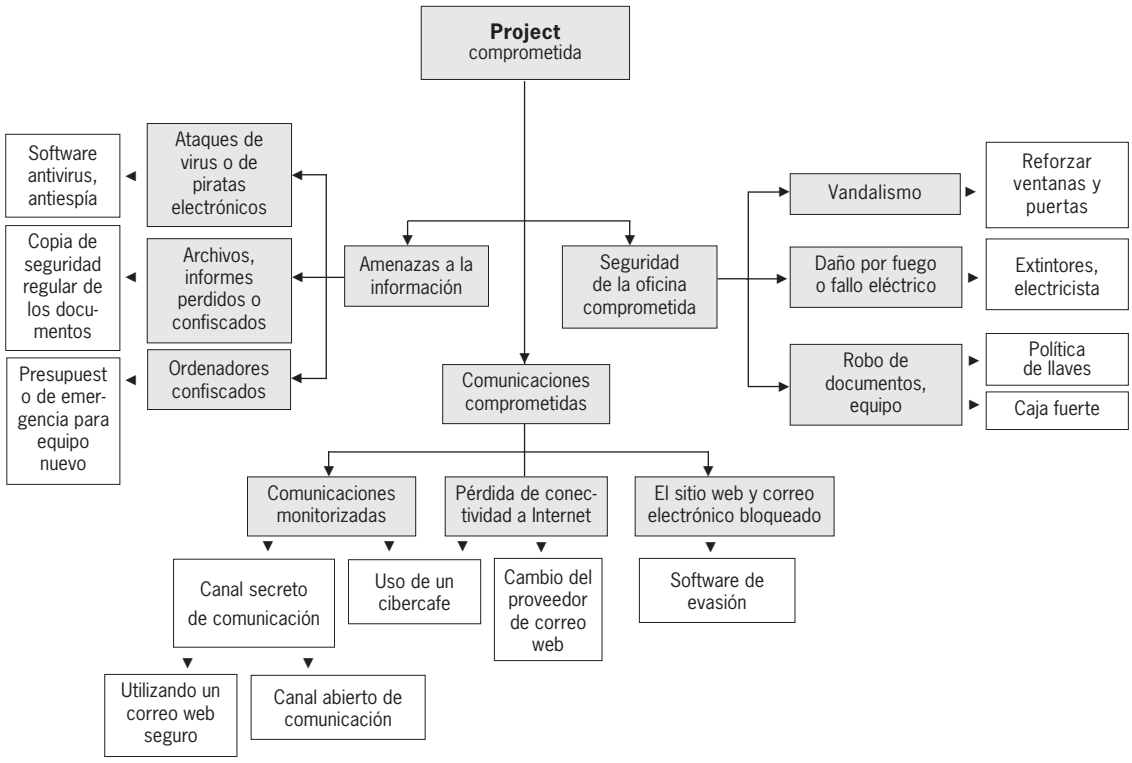
108
Otras posibilidades de correo web seguro incluyen https://www.bluebottle.com y https://www.fastmail.fm

encontrar otros proveedores de correo web seguro o emplear una serie de métodos de evasión para evitar estos bloqueos. Se decide pedir a la Sede Central que instale la herramienta Psiphon en sus PC en casa. Las direcciones IP relevantes y los detalles de registro se envían a la Sede Central. Estos pasos proporcionan una manera segura de evitar los bloqueos del gobierno y proporcionar el acceso a los servidores de la Sede Central.

- **Técnico informático:** Un técnico informático de confianza visitará la oficina dos veces al mes para efectuar una revisión general y estará de guardia para situaciones de emergencia. La tarifa será 1000 USD por 6 meses.

Presupuesto

Barras en las ventanas y el refuerzo de la puerta	500 USD
Regrabadora de CD y 10CDs	200 USD
Caja fuerte	300 USD
2 tarjetas de memoria USB	100 USD
Portátil	1.000 USD
Técnico informático	1.000 USD
Total	**3.100 USD**
Dinero de emergencia: 1000 para PC, 500 para cibercafé	1.500 USD
Presupuesto Total	**4.600 USD**



4.3 CASO PRÁCTICO 3 ASEGURANDO Y ARCHIVANDO DATOS

RESUMEN

Una ONG de derechos humanos, con sede en un país en vías de desarrollo, proporciona asistencia legal gratuita a las víctimas de violaciones de derechos humanos. Llevan cinco años reuniendo casos y asistiendo a los habitantes de la ciudad. Recientemente, empezaron a trabajar en la elaboración de un texto para su entrega ante el tribunal de derechos humanos regional sobre un caso especialmente complicado y sensible de brutalidad policial. La semana pasada, recibieron dos amenazas de una persona desconocida – una por teléfono que exigía que dejaran de trabajar en este caso inmediatamente y otro – expresado por un policía local. Él dijo que el material que estaban recopilando se consideraba peligroso para los intereses de la seguridad nacional y podría ser confiscado en cualquier momento. Los abogados de la ONG están convencidos de que esto no es verdad y que es simplemente un método de intimidación. Están seguros de que el caso entra dentro del derecho nacional y acuerdos internacionales. La ONG desea continuar con este caso hasta su final y ha solicitado una pequeña subvención del financiador que les ayude incrementar la seguridad de la información recopilada.

—

La oficina está situada en un edificio bien protegido, con acceso fácil a una calle concurrida. La ONG tiene una reputación sólida dentro de la comunidad local y círculos oficiales. A los vecinos siempre les gusta asistir y mantener los ojos abiertos para los intrusos. Durante los cinco años de su funcionamiento, la seguridad de su oficina no ha sido puesta en peligro, el personal tiene confianza en su ubicación y ha establecido políticas estrictas relativas a las llaves de la oficina y las visitas de los clientes. Sin embargo, los cambios recientes en la administración local preocupan a la ONG, ya que temen que la policía obtenga el permiso para hacer una redada en su oficina y confiscar los documentos relacionados con el caso. Están preparados a desafiar cualquier acción de este tipo ante un tribunal, pero les preocupa que el contenido del material confiscado podría poner en peligro la seguridad de muchas personas. Deciden asegurar la información reunida contra esta posibilidad. También se ha decidido proteger toda la información relativa a sus casos que han reunido desde su establecimiento.

—

La oficina tiene un ordenador y el personal dispone de pocas capacidades técnicas. El ordenador tiene conexión a Internet a través de un módem de acceso telefónico y la oficina adquiere tarjetas de Internet con detalles de conexión temporal. Este ordenador dejó de funcionar debidamente hace mucho tiempo, ya que está lleno de virus. Los armarios en la oficina están llenos de documentos relativos a los casos en los que la ONG trabajó en el pasado. La subvención del colaborador se elevó a 1500 USD.

Amenazas y vulnerabilidades

El personal de la ONG se ha dado cuenta de que la amenaza principal con la que se enfrentan es que se ponga en peligro el texto que están preparando para el tribunal en caso de que la policía confiscara el material relativo a este caso. Esto podría posiblemente poner en peligro a sus clientes y testigos. Esta amenaza puede ser realizada mediante:

1 la confiscación de todos los documentos con un orden judicial.
2 la confiscación ilegal de los documentos por la fuerza.

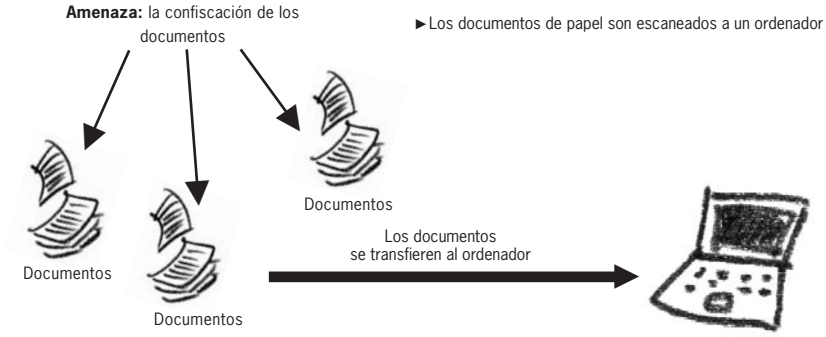
En cualquiera de los dos casos, el resultado será el mismo y hay que proteger la información contra ambas eventualidades. La ONG no sólo tiene que proteger la información, sino que asegurar también que los detalles acerca del caso se queden en su posesión para que el trabajo pueda continuar. La ONG hace una lista de sus vulnerabilidades para comprender mejor qué áreas necesitan más atención.

- **Los apuntes de los casos de violaciones que existen sólo en papel no están protegidos.**
- **El ordenador no funciona por los virus.**
- **El software sin licencia puede ser utilizado como un pretexto para confiscar los ordenadores.**
- **Los archivos almacenados en los ordenadores no están protegidos contra los piratas informáticos.**
- **No hay ningún sistema de respaldo de información para los documentos en caso de que sean confiscados o se pierdan.**

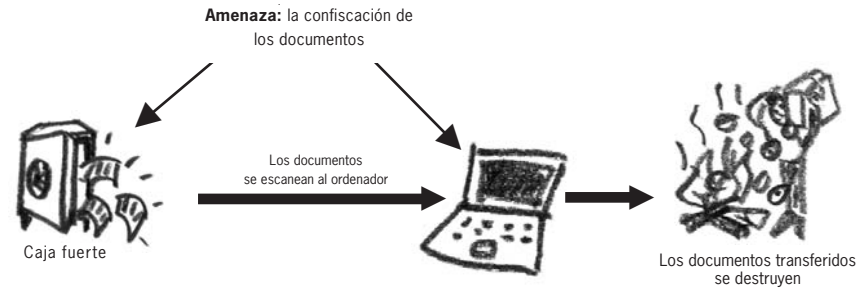
SOLUCIONES

Acceso a la información

Se decide eliminar el riesgo que supone la información que existe sólo en papel, transfiriéndola en el ordenador. Luego, los casos en el papel se destruirán y todos los datos se almacenarán eléctricamente, con la posibilidad de imprimir el documento deseado cuando sea requerido.



Hay que almacenar en un sitio seguro también la información guardada actualmente en papel, mientras que se está pasando en el ordenador. Por esta razón, se adquirirá una caja fuerte en la que se guardarán todos los documentos importantes antes de su computerización tras la cual serán destruidos (el personal decide que el método más seguro de hacerlo será quemándolos).



►Los documentos de papel redundantes se destruyen

Ordenadores

El personal de la ONG decide que su ordenador actual es demasiado viejo y podría ser incapaz de procesar la gran cantidad de información que habrá que almacenar. Tras buscar en Internet y hablar con sus amigos, se dan cuenta de que es posible comprar un disco duro extraíble con una gran capacidad de almacenamiento. Básicamente, es un disco duro que puede llevarse encima y enchufar en cualquier ordenador.

—

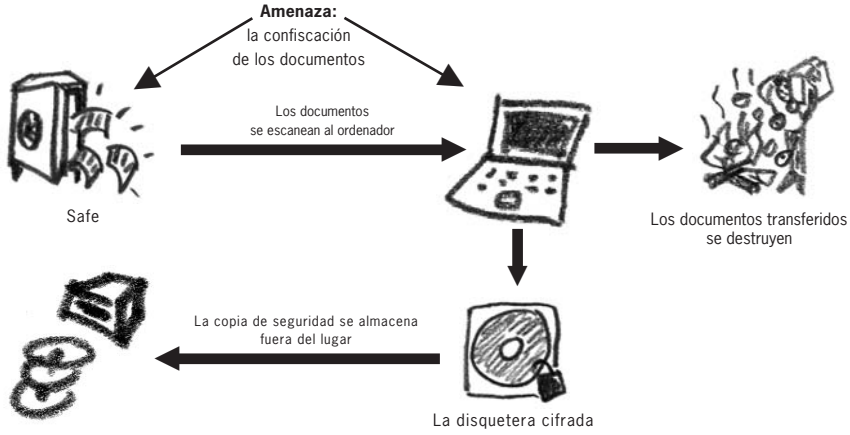
Para proteger los datos almacenados en el ordenador, se le recomienda al personal que utilice el **cifrado**. Aunque nadie sabe muy bien cómo se cifra, el personal obtendrá una copia de la *Caja de Herramientas de Seguridad*. Parece que el programa TrueCrypt será capaz de cifrar todo el disco duro de manera que nadie sea capaz de acceder a él sin conocer la contraseña. Deciden cifrar el disco duro extraíble utilizando TrueCrypt. Si el disco duro extraíble es confiscado, los datos que lleva se quedarán cifrados.

—

Ya que toda la información es centralizada, es esencial que se cree un sistema de respaldo de información, por si el disco duro extraíble es dañado o confiscado. El soporte de respaldo será una grabadora de DVD. Al final de cada día, se hará una copia de seguridad del disco duro extraíble en un DVD y se llevará fuera del sitio. Dado que la información en el disco duro está cifrada, se quedará cifrada en los DVDs.

—

La transferencia de los documentos en papel a los archivos electrónicos se realiza con un escáner. Se estima que una persona que trabaja con un ordenador y un escáner puede digitalizar 100 páginas al día. En ese caso, el trabajo se puede llevar a cabo en dos semanas.



►Los documentos electrónicos son protegidos contra su pérdida a través de la creación de un mecanismo de respaldo de información

Software

La ONG decide adquirir una copia de Microsoft Windows XP Home Edition. La adquisición está justificada por la necesidad de garantizar que todo el software propietario en sus ordenadores esté correctamente autorizado. En lugar de utilizar una versión pirateada de Microsoft Office, consiguen una copia del OpenDisk[109] y deciden utilizar Open Office y el programa GIMP para escanear los archivos. Todo el software necesario: antivirus, de cortafuegos, del **cifrado** y de grabado de DVD se puede encontrar en *La Caja de Herramientas de la Seguridad*, completamente gratuito y de código abierto. Por lo tanto, la ONG no tendrá problemas por utilizar software obtenido de manera ilegal.

109
http://www.theopendisc.com/

RESPUESTAS DETALLADAS A LAS AMENAZAS

- **Hardware:** Se envía a un empleado a la ciudad más cercana para adquirir un escáner, un disco duro extraíble y una grabadora de DVD extraíble. Éstos están disponibles en la mayoría de las tiendas de informática. El equipo adquirido es de una marca acreditada y cara. Un escáner A4 cuesta 150 USD, el precio del disco duro extraíble con capacidad de 100 gigabytes asciende a 250 USD y la grabadora de DVDs extraíble cuesta 250 USD también.

- **Software:** En la tienda de ordenadores**,** se encuentra también una copia de Microsoft Windows XP Home Edition por 96 USD. El empleado de la ONG pregunta si la tienda podría proporcionar un técnico para instalar todo el hardware y software. Hay un técnico disponible que hará el trabajo por 100 USD. Se encarga la *Caja de Herramientas de Seguridad* en el sitio web http://orders.ngoinabox.org. La *Caja* contiene también el OpenDiscCD.

El técnico informático instala una nueva copia de Windows XP y borra todos los datos anteriores. Esto es aconsejable para deshacerse de todos los virus y fallos técnicos que había en el ordenador. Instala también la grabadora de DVD, el escáner y el disco duro extraíble. Luego instala el siguiente software:

Software	Objetivo	Fuente
Open Office	Procesamiento de textos, hojas de cálculo, presentaciones, base de datos (plenamente compatible con los documentos de Microsoft Office)	OpenDisc
GIMP	Editar imágenes y escanear	OpenDisc
Avast 4	Antivirus	Caja de Herramientas de Seguridad
Comodo (Internet computer)	Cortafuegos	Caja de Herramientas de Seguridad
TrueCrypt (data computer)	Cifrar el disco	Caja de Herramientas de Seguridad
DeepBurner (data computer)	Software de grabado de DVD	Caja de Herramientas de Seguridad

- **Cifrado**: El programa TrueCrypt cifrará el disco duro extraíble de tal manera que se pueda copiar fácilmente en un DVD al final de cada día. El personal crea una carpeta de TrueCrypt en el disco duro extraíble, de 4 gigabytes (que complementa la cantidad de espacio de almacenamiento de un DVD). La partición cifrada está protegida con una contraseña, conocida sólo por el personal encargado. La misma contraseña será necesaria para abrir esta partición desde el DVD. Se elige una contraseña que contiene 12 caracteres y consta tanto de letras como números. No se apunta en ninguna parte y la memorizan todos los que requieren el acceso.
- **Copias de seguridad:** Al final de cada día, la partición desmontada, ahora un archivo, se copia en el DVD. Es mejor regrabar la versión previa del archivo (para eso, habrá que adquirir una regrabadora de DVD y discos de DVD regrabables).

El DVD con la copia de seguridad se guarda fuera de la oficina – en casa de uno de los empleados. A finales de cada semana, se hace una copia de seguridad separada y se guarda en una ubicación no revelada. Esto es una medida adicional del respaldo de información, por si el disco duro extraíble y las copias de seguridad diarias sean confiscadas.

PRESUPUESTO

■ Escáner A4	150 USD
■ Disco duro extraíble	250 USD
■ Grabadora de DVD+RW extraíble	250 USD
■ 10 discos de DVD regrabables	50 USD
■ Microsoft Windows XP	96 USD
■ Servicios informáticos	100 USD
■ Caja fuerte	300 USD
	Total: 1.145 USD

En el presupuesto, se asigna más dinero, por si se necesita adquirir una nueva impresora o discos DVD adicionales.

—

La ventaja de este sistema es la seguridad incrementada de todos los documentos reunidos por la ONG. Después del período principal de digitalización de los documentos de papel, no habrá ningún dato que sea fácilmente accesible a un intruso. Todo el conjunto de documentos será fácil de transmitir entre ordenadores. Incluso si todo el equipo es confiscado o se daña, el personal sólo necesitará el disco de DVD con la copia de seguridad y otro ordenador con el programa TrueCrypt instalado. Por supuesto, ¡alguien tiene que conocer la contraseña!

4.4 CASO PRÁCTICO 4 CORREO ELECTRÓNICO SEGURO Y BLOGS

RESUMEN

Una periodista independiente informa sobre violaciones de los derechos humanos en su país. Tiene un portátil con el que trabaja desde casa y que a menudo lleva consigo cuando trabaja. Escribe principalmente para publicaciones extranjeras y utiliza un pseudónimo, dado que es peligroso publicar información de este tipo en su país, donde los medios de comunicación son estrictamente censurados y se sabe que el gobierno tiene la capacidad para rastrear periodistas online. Ella también tiene un **blog** donde son publicados todos sus artículos.

—

Es cada vez más difícil para ella seguir trabajando. Sus artículos no llegan a su destino, el acceso a su sitio de **blog** ha sido bloqueado y teme poner en peligro a la gente a la que entrevista y menciona en sus informes. Teme que su correo electrónico esté monitorizado. En un caso, le escribió un editor sorprendido por el contenido de su reciente artículo. Al releerlo, se da cuenta de que el artículo ha sido alterado por alguien después de que lo envió desde su buzón de correo electrónico al periódico.

AMENAZAS

Antes de decidir que medidas tomar, ella hace una lista de todas las amenazas actuales con las que se enfrenta:

- **No puede mandar sus artículos por correo electrónico.**
- **No puede acceder a su blog y actualizarlo.**
- **Su identidad ficticia podría ser puesta en peligro.**
- **Sus artículos, almacenados en su portátil, son accesibles para los intrusos.**
- **Los virus o los piratas informáticos podrían dañar los artículos en su portátil.**

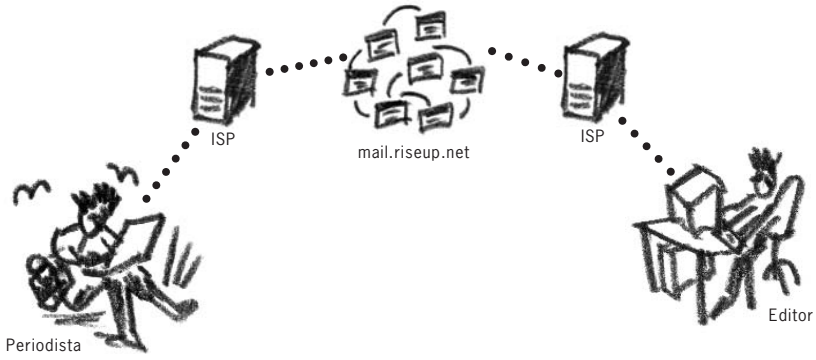
SOLUCIONES

Correo electrónico seguro

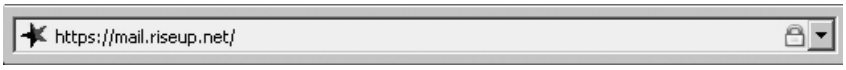
Como primera prioridad, decide asegurar su buzón de correo electrónico, de manera que sus mensajes no podrían ser leídos ni alterados por un intruso. Escribe a security@ngoinabox.org y pide los códigos de acceso necesarios para registrar una nueva cuenta de correo electrónico con RiseUp. Ésta es una cuenta de correo electrónico de correo web a la que se puede acceder sólo cuando está en Internet. El correo web funciona sobre **SSL** y, por lo tanto, es cifrado entre el ordenador y el servidor de correo web. Además, pide a sus destinatarios que registren también una cuenta gratuita en https://mail.riseup.net, para que sus artículos puedan llegarles sólo a través de túneles de Internet cifrados. Decide confiar en que la gente de RiseUp no pondrá en peligro ni accederá a su correo electrónico.

—

Esto parece ser un método simple y efectivo de tratar con los problemas de los periodistas. Siempre que la barra de direcciones del navegador de Internet a través del cual ella accede a su cuenta de correo electrónico empiece con "https:", la periodista sabrá que sus comunicaciones son seguras.



►Comunicacioens seguras con cuentas de correo electrónico Riseup.net sobre SSL

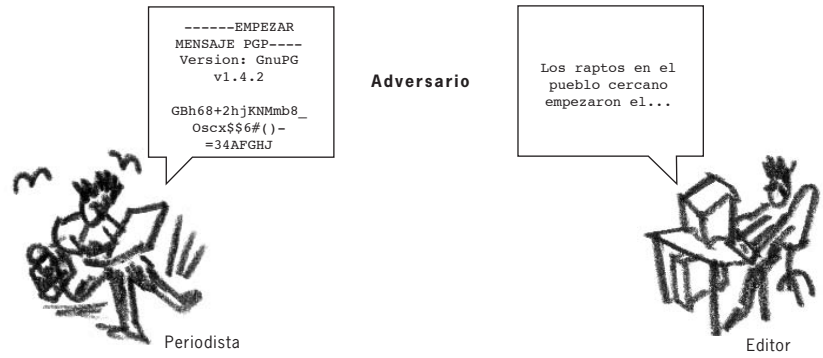


Como otra precaución, escribe a RiseUp pidiéndoles que le envíen la huella digital de su certificado **SSL**. La remiten a su sitio web dónde está su huella digital. La medida que ella está tomando en este caso es para prevenir un ataque "Man-in-the-Middle", con el que el adversario intercepta la línea de comunicación a https://mail.riseup.net e intenta engañar al usuario para que crea que ha llegado al sitio web deseado. Se presenta un certificado **SSL** y, una vez que el usuario lo acepte, la conexión es redirigida al sitio web del adversario. Sin embargo, una inspección del certificado **SSL** revelará si difiere del original o no.[110]

MD5 Fingerprint	68:82:D8:DC:E1:BF:D0:ED:E0:2F:4C:CA:46:B5:D1:AC

Asegurando la información

Aunque ha conseguido asegurar el buzón de su correo electrónico, le gustaría hacer los artículos que envía ininteligibles para todos menos para el destinatario. Lo quiere hacer por si pierde la contraseña de su correo electrónico o si ésta ha sido puesta en peligro. También sirve como una buena medida preventiva contra los ataques "Man-in-the-Middle". Instala en su portátil el programa de correo electrónico Thunderbird y lo configura para leer su cuenta de RiseUp. Añade a Thunderbird la extensión Enigmail y sigue las instrucciones de la *Caja de Herramientas de la Seguridad* para crear un par de claves que utilizará para cifrar sus artículos con la clave pública del editor.[111] Todas las partes que desean comunicarse uno con otro de manera segura utilizando el sistema de **cifrado** de clave pública tendrán que instalar en sus ordenadores el software apropiado e intercambiar uno con otro sus claves públicas.[112]



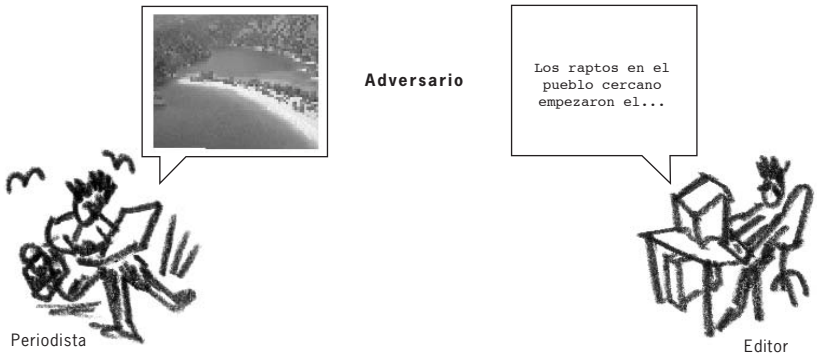
►Utilizando el **cifrado** para asegurar los mensajes enviados

110
Para más información, véase el capítulo "Cifrado en Internet".

111
http://security.ngoinabox.org/thunderbird_main.html

112
Para más información, véase el capítulo "La criptología". Para descargar el programa GnuPG, visita http://www.gnupg.org o lo puedes encontrar en la Caja de Herramientas de Seguridad.

En algunos casos, el uso del **cifrado** podría alertar al organismo que realiza la monitorización. La periodista no sabe si el **cifrado** es legal en su país ni si no atraerá a ella mucha más atención no deseada. Decide emplear un método alternativo que no parecerá enigmático en seguida, y, por lo tanto, sospechoso. Utilizando un programa de esteganografía, puede incrustar su artículo en una foto y cargarla a un sitio web que no llame la atención. Siempre y cuando acuerde primero con los editores dónde y cuándo buscar la imagen/ el artículo, con este método podrá evitar muchos sistemas de vigilancia. La periodista debería aplicarlo manteniendo una frecuencia regular de la misma actividad (cargar fotos a Internet) que no debería parecer irregular en su patrón de actividad normal.[113]



►Utilizando la esteganografía para ocultar la presencia de un mensaje en tus comunicaciones

Correo electrónico anónimo

Otra manera de contrarrestar el bloqueo de correo electrónico y la censura radica en utilizar una serie de servicios de correo web gratuitos populares. Yahoo, Hotmail, Gmail y otros tienen millones de usuarios registrados. Es posible crear una cuenta completamente nueva cada vez que desees enviar un correo electrónico. Los detalles de registro pueden ser aleatorios y, al ser mandado desde un espacio público (p.ej. un cibercafé), el correo electrónico debería ser muy difícil de rastrear.

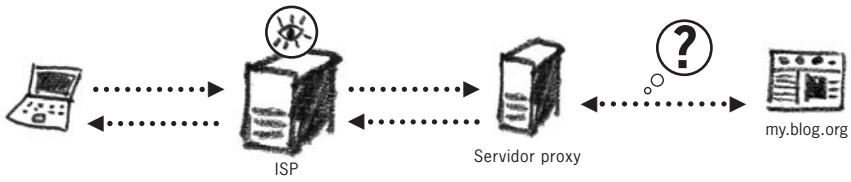
—

Es posible que los servicios de correo electrónico seguro (como RiseUp) ya estén bloqueados o serán bloqueados después de ser utilizados frecuentemente. Sólo unos cuantos países bloquean el acceso a los grandes sistemas de correo electrónico gratuito, como Yahoo. Sin embargo, estos proveedores globales han cooperado en el pasado con algunos gobiernos (p.ej. con el gobierno chino) al proporcionarles el acceso a las cuentas de correo electrónico de sus usuarios. En caso de que la periodista decidiera utilizar un proveedor de correo web grande, su uso debe ser limitado a acceder a su servicio desde un cibercafé u otro espacio público, donde no se registran sus detalles y no se puede rastrearla mediante la dirección IP desde la cual fue enviado el correo electrónico. La periodista también se puede crear cuentas utilizando un pseudónimo, acordado con su editor.

Evitando los bloqueos de sitios web

Para acceder al sitio de su **blog,** la periodista necesitará distintos métodos para evitar el bloqueo de Internet en su país. La elección de herramientas dependerá de la práctica del bloqueo aplicada por el gobierno. Por ejemplo, debería registrarse para recibir noticias sobre los últimos anonimizadores de Peacefire[114] o pedir a un amigo que viva en un país que no censura Internet crear un Psiphon (para más explicaciones, véase el Capítulo 2.6) para su uso.

114
http://peacefire.org/



►Con un servidor proxy anónimo, el sitio web deseado no sabrá dónde está ubicado de verdad tu ordenador

Como alternativa, instala en una memoria USB el navegador Tor[115] para que pueda trabajar sin absolutamente ningunas restricciones causadas por el bloqueo. Tor hará sus solicitudes de sitios web anónimas y penetrará la mayoría de los sistemas nacionales de censura.

—

Muchas veces, resulta más fácil y práctico pedir a un amigo de otro país cargar tus artículos en tu **blog**. Los artículos pueden transmitirse por correo electrónico seguro.

Protegiendo la identidad

En este momento, la periodista no desea que su identidad sea vinculada con su pseudónimo. Por esto, tiene mucho cuidado para no poner su verdadero nombre en los correos electrónicos ni en los artículos que envía por Internet. Tampoco utiliza su cuenta de correo electrónico **ISP**, ya que está directamente relacionada con ella. Utiliza sólo la conexión a Internet de su casa para acceder a una cuenta de correo web seguro o lo hace junto con otra herramienta de anonimato a la hora de actualizar su **blog**.

—

En su ciudad, algunos de los cibercafés han empezado a registrar los nombres de sus usuarios y la hora de su acceso. La periodista evita estos cafés, debido a que la actividad en Internet y de correo electrónico puede rastrearse a la dirección IP del ordenador y finalmente a ella.

—

Al utilizar un ordenador de un cibercafé, tiene mucho cuidado para no permitir al navegador recordar sus contraseñas y la historia de su navegación. Al principio de su sesión, pasa un par de minutos configurando el navegador de Internet de manera que sea más seguro, y al final, elimina del ordenador toda la información guardada.[116]

Asegurando el portátil

Todos los artículos son escritos y almacenados en su portátil. Tiene que asegurarse contra su pérdida, una entrada no autorizada y daños por virus y spyware. Establece una contraseña **BIOS** para prevenir el acceso inmediato a su ordenador e instala un programa antivirus, antispyware y de cortafuegos gratuito de la *Caja de Herramientas de Seguridad*. Actualiza su software de Windows en cuanto estén disponibles nuevos parches. Como su portátil tiene una grabadora de CDs, compra unos discos virgen y crea una copia de seguridad de sus documentos.

Contraseñas

Su portátil, **BIOS**, cuentas de correo electrónico, blogs, etc. requieren cada uno una contraseña. Estas contraseñas son fundamentales para su seguridad, ya que incluso el sistema más avanzado es sólo tan bueno como la contraseña que lo protege. Dado que es imposible memorizar todas las contraseñas,

115
http://security.ngoinabox.org/tor_portable

116
Véase, por favor, el capítulo sobre las configuraciones de programa de Internet

utiliza un programa KeePass[117] para almacenarlas para ella. Tiene una copia del programa y el archivo con las contraseñas en su portátil y en memorias USB. Para incrementar la seguridad de sus contraseñas, el programa KeePass las crea para ella.

En resumidas cuentas, dispone de distintos trucos y métodos que puede utilizar a su discreción. Al principio, puede parecer que son laboriosos y requieren mucho tiempo, pero ella sabe que su seguridad es primordial. Quizás bastará con un portátil y una dirección de correo electrónico seguros para que pueda continuar con su trabajo. Como algunos métodos de protección se hacen obsoletos o no están disponibles, puede elegir soluciones diferentes. Internet es un espacio vasto con muchas posibilidades tanto de vigilancia como de anonimato.

117
http://security.ngoinabox.org/keepass_main

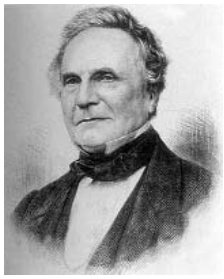
APÉNDICE A
ORDENADORES EXPLICADOS

A

Tomemos en consideración un aparato futuro de uso individual que es una especie de archivo privado mecanizado y biblioteca. Como necesita un nombre, y por establecer uno al azar, podríamos denominarlo "memex". Un memex es un aparato en el que una persona almacena todos sus libros, archivos y comunicaciones, y que está mecanizado de modo que puede consultarse con una gran velocidad y flexibilidad. En realidad, constituye un suplemento ampliado e íntimo de su memoria.

El memex consiste en un escritorio que, si bien puede ser manejado a distancia, constituye primariamente el lugar de trabajo de la persona que accede a él. En su plano superior hay varias pantallas translúcidas inclinadas sobre las cuales se puede proyectar el material para ser consultado. También dispone de un teclado y de un conjunto de botones y palancas. Por lo demás, su aspecto se asemeja al de cualquier otra mesa de despacho.

Vannevar Bush – Grupo Conjunto de Investigación y Desarrollo Científico, 1945



Charles Babbage (1791 – 1871)

HISTORIA

La teoría y las matemáticas necesarias para crear ordenadores tienen sus raíces hace siglos. El sistema binario de aritmética (que utiliza "1" y "0" para llevar a cabo todas las ecuaciones aritméticas) fue inventado por Gottfried Wilhelm von Leibniz (1646 – 1716), a quien se le atribuye también ser, junto con Isaac Newton, el inventor del cálculo infinitesimal. Charles Babbage es probablemente el investigador más ampliamente reconocido de la primera época de la computación. Él fue el creador de las máquinas diferenciales y analíticas. Las máquinas analíticas utilizaban tarjetas perforadas para registrar cualquier operación numérica, para que el cálculo anterior pueda guardarse y posteriormente introducirse en el ordenador. Babbage describe cinco componentes lógicos de la máquina – el almacén, el molino, el control, la entrada y la salida (en términos modernos: disco duro, unidad central de procesamiento (CPU), software, teclado/ ratón y monitor). [118]

1991 Reconstruction of the Difference Engine by the London Science Museum

George Scheutz oyó hablar por primera vez sobre la máquina diferencial de Babbage en 1833, y, con su hijo Edvard, intentó construir una versión más pequeña. Antes de 1853, habían construido un dispositivo que podía procesar números de 15 dígitos y calcular diferencias de cuarto orden. Su máquina ganó la medalla de oro en la feria mundial de París de 1855, y, más tarde, la vendieron a Dudley Observatory de Albany, Nueva York, que lo utilizaba para calcular la órbita de Marte. Uno de los primeros usuarios comerciales de los ordenadores mecánicos fue la Oficina del Censo de los EEUU, la que tabuló los datos para el censo de 1890 con la ayuda de un equipo de tarjetas perforadas, diseñado por Herman Hollerith. En 1911, la empresa de Hollerith se fusionó con un competidor para crear una corporación que llegaría a ser International Business Machines (IBM) en 1924.

118
http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians

El IBM 5150, que salió al mercado en 1981

LA ACTUALIDAD

El primer ordenador moderno fue llamado "Simon" y fue montado por un par de estudiantes de la Universidad de Columbia. Inútil como máquina de procesamiento, sirvió de inspiración para otros modelos. El primer y más popular PC asequible comercialmente fue el IBM 5150, que salió al mercado en 1981.

—

Nadie sabe exactamente cuántos ordenadores se utilizan hoy. Según un comunicado de prensa de la empresa de investigación y consultoría en tecnologías de información Gartner Dataquest[119] de 2002, "… se han vendido un mil millones de ordenadores personales en el mundo entero". Este número excluye agendas electrónicas, teléfonos móviles, consolas de videojuegos, y muchos otros dispositivos que han llegado a formar parte de nuestra vida cotidiana. Hoy en día, los ordenadores operan los coches y semáforos, tanto como aviones e informes sobre el tiempo atmosférico. Generan y almacenan música, corrigen la ortografía de nuestros documentos y preparan nuestra comida. Lo que hace sesenta años sonaba como ciencia ficción hoy se ha convertido en la realidad cotidiana.

—

Los ordenadores han ido haciéndose cada vez más pequeños (al funcionar cada vez más rápido y almacenar cada vez más información). En la actualidad, los PC corrientes son capaces de realizar mil millones de operaciones por segundo y guardar tantos datos como cualquier biblioteca local.

CÓMO FUNCIONAN LOS ORDENADORES

Abajo está una descripción (y diagramas) de los componentes principales de un ordenador.

- **Unidad de potencia** – suministra y regula la corriente eléctrica del ordenador. Los portátiles tienen también suministros de energía de reserva.

- **CPU** – Unidad central de procesamiento. Realiza las operaciones del ordenador. Éstas son sucesiones de numerosas operaciones lógicas y matemáticas llevadas a cabo a gran velocidad. Una CPU se calienta a una alta temperatura y tiene que ser refrigerada por un ventilador.

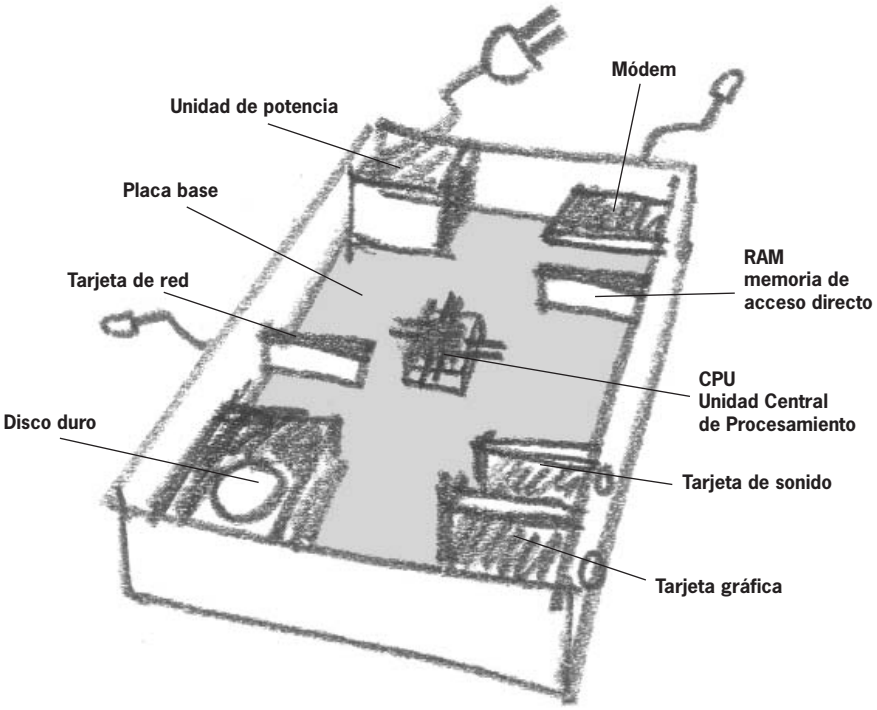
- **Disco duro** – Éste es el lugar donde se almacenan todos los datos de tu ordenador. Suele ser un disco magnético rotativo. Siendo sensible a campos magnéticos, el disco duro requiere una caja protectora.

- **RAM** – memoria de acceso directo. Esto es una unidad de almacenamiento temporal para los datos que utilizas actualmente. Cuando abres un programa (p.ej. un procesador de textos), el ordenador copia el programa desde el disco duro a la memoria RAM. Cuando escribes un documento, se almacena también en la memoria RAM. Al optar por "Guardar" el documento lo guardas en el disco duro.

- **Placa base** – Una parte integral grande del ordenador que permite a todos los dispositivos comunicarse entre sí.

- **Tarjeta gráfica** – responsable de la visualización de la información en el monitor.

119
Gartner declara que "en 2005, se vendieron 285 millones de PCs y portátiles en el mundo entero. Antes de 2008, se debería alcanzar el nivel de 2 mil millones.", fuentes http://news.bbc.co.uk/2/hi/science/nature/2077986.stm y http://www.dailytimes.com.pk/default.asp?page=2006%5C01%5C23%5Cstory_23-1-2006_pg6_1



- **Tarjeta de sonido** – Responsable de la entrada y salida del sonido en el ordenador.

- **Tarjeta de red** – Responsable de conectarte a una red. Puedes conectarte a Internet, siempre que la red en la que estás tenga acceso a Internet.

- **Módem** – Conecta tu ordenador a una línea telefónica analógica. Sus variantes incluyen ADSL y módems digitales. Se pueden utilizar para conectar tu ordenador a Internet.

- **Monitor** – Visualiza la información del ordenador en una pantalla.

- **Teclado y ratón** – Te permiten introducir datos en el ordenador.

Véamos ahora cómo funcionan algunas operaciones del ordenador:

1 Abres un programa de procesamiento de textos y escribes un documento
CPU ► encuentra el programa en el disco duro y lo copia a la memoria RAM ► la tarjeta gráfica visualiza el programa en el monitor ► escribes una página y eliges "guardar" el documento ► el documento se copia del RAM al disco duro.

2 Ves tu correo electrónico e imprimes un mensaje de correo electrónico
CPU ► encuentra el programa de navegación por Internet en el disco duro y lo copia a la memoria RAM ► el módem conecta tu ordenador a www.riseup.net ► introduces tu contraseña ► el correo electrónico se visualiza en el monitor ► el correo electrónico se copia en la memoria RAM ► eliges "Imprimir" ► la placa base comunica con la impresora ► el documento se imprime.

Nota: tu correo electrónico ha sido copiado a tu ordenador, aunque no pediste que se guardara. Ahora tienes una copia en la memoria RAM. Ésta es la manera estándar de cómo funcionan los ordenadores, y hace falta tomarla en cuenta al evaluar la seguridad del ordenador (véase también los capítulos sobre la seguridad de Windows y "Copia de seguridad, destrucción y recuperación de la información").

En el mundo de los ordenadores, todo gira alrededor de su velocidad y capacidad. Aquí está una guía aproximada de cómo se miden:
Supongamos que el carácter "A" requiere 1 byte de la capacidad de almacenamiento.

```
8 bits = 1 byte (B)
1024 bytes = 1 kilobyte (kB)
1024 kilobytes = 1 megabyte (MB)
1024 megabytes = 1 gigabytes (GB)
1024 gigabytes = 1 terabytes (TB)
```

Nota: la unidad de medida de 1024 se debe a que es un factor de 2, necesario para un sistema digital.

Supongamos que una operación del ordenador por segundo se denomina un *hertz*.

```
1000 hertz = 1 kilohertz (kHz)
1000 kilohertz = 1 megahertz (MHz)
1000 megahertz = 1 gigahertz (GHz)
```

Así que, un ordenador con la velocidad descrita como 1,3 GHz/s realiza 1,300,000,000 operaciones por segundo. Lo que es mucho más rápido que "Simon".

SISTEMAS OPERATIVOS

Todos los ordenadores requieren instrucciones para que funcionen. La fuente principal de estas instrucciones, y el puente que conecta todas las partes del ordenador, programas y nosotros – los usuarios – es un sistema operativo (SO; OS en inglés). Probablemente conocerás Windows, que es el programa operativo más popular y es producido por Microsoft. Su popularidad es el resultado de interfaces gráficas fáciles de entender, contratos exitosos con fabricantes de ordenadores y estrategias de marketing agresivas.

—

Se han producido numerosas versiones de Windows. Cuando compras un ordenador nuevo, es probable que ya tenga instalado Windows. El Windows SO no es gratuito y tienes que tener una licencia válida. Sin embargo, éste no es el caso de todos los ordenadores: pueden tener una versión "pirateada" ilegal de Windows. Muchos entusiastas y técnicos informáticos desprecian Windows por sus estrategias de marketing, programación defectuosa y monopolio del mercado. Algunos de ellos intentan descubrir vulnerabilidades de los sistemas operativos y o alertan a Microsoft para crear un parche o escriben virus, aprovechándose de los defectos y alterando los datos en los ordenadores que han sido infectados.

—

Hay muchas alternativas a Windows OS. Por ejemplo, el ordenador Apple utiliza su propio SU. También existe Linux, un sistema operativo gratuito que se ha hecho muy popular debido a su distribución en Internet. Linux fue escrito por mucha gente diferente que no es empleada por ninguna empresa. Como pro-

ducto de participación voluntaria masiva, se ofrece gratuitamente. Muchas versiones diferentes (incluidas las versiones en distintos idiomas) de Linux han salido al mercado, y la mayoría de ellas son gratuitas. La más popular y quizás la más fácil de utilizar es Ubuntu[120].

SOFTWARE – PROPIETARIO VS FOSS

Un software se considera como propiedad intelectual de su creador (como un libro o guión de una película). La licencia para su uso se vende junto con el código del ordenador. La práctica de piratear el software, es decir, de descodificar el código de la licencia o simplemente utilizar el software sin tener una licencia válida, está muy extendida en todo el mundo. Muchos gobiernos han aprobado leyes que protegen software bajo una la ley de propiedad intelectual. Las personas y organizaciones atrapadas utilizando un software pirateado se enfrentan con sanciones severas. Se imponen sanciones estrictas a las personas y organizaciones capturadas al utilizar software pirateado.

—

No todos los programas conllevan estas restricciones de licencias debidas a la necesidad de obtener la licencia. Así como tú puedes dedicar voluntariamente tu tiempo y capacidades a un fin sin ánimo de lucro o benéfico, algunos programadores crean y luego distribuyen su software gratuitamente. Ese software a menudo ha sido escrito utilizando el código abierto, lo que significa que el código de programación está abierto para inspección, modificación y mejora. Voluntarios traducen este software a sus propios idiomas y los ofrecen para su distribución gratuita. Este tipo de software se denomina FOSS – software libre y de código abierto. En el mercado puedes encontrar casi todos sus tipos.

—

Una suite de Microsoft Office con licencia te costará entre 200-500 USD[121] por copia, mientras que OpenOffice (disponible en www.openoffice.org) es distribuido gratuitamente. Los dos son muy similares en sus operaciones y funcionalidad: crean los mismos tipos de documentos. Se ha planteado la cuestión de la interoperabilidad entre la versión '95 y las versiones anteriores de Microsoft Office y Open Office. La solución es que tu oficina y los compañeros con los que comunicas cambien por completo uno de los productos. Puede que esto no sea una tarea fácil, pero si la legalidad de tu software te importa, deberías considerar dejar de utilizar los productos de Microsoft o si no, comprar sus licencias.

—

El software libre y de código abierto (FOSS) te liberará de los problemas de piratería del software propietario (o privativo o de código cerrado). Aunque el FOSS quizás no es tan fácil de utilizar (en lo que se refiere a su instalación, orientación intuitiva y gráficos), dado que no te proporciona tanta ayuda con el programa y un apoyo tan grande como el software pagado, tiene una gran comunidad de usuarios, quienes crearon varios foros para contestar las preguntas más comunes y responderán a cualquier nueva consulta que envíes. En esencia, en la comunidad de código abierto encontrarás una red de apoyo más receptiva y con respuestas más detalladas que las ofrecidas por el número de apoyo técnico costoso y constantemente ocupado para la última versión de Microsoft Windows.[122]

120
www.ubuntu.com

121
Al realizar búsquedas en Internet en septiembre de 2006, se encontraron precios diferentes.

122
Para más información, véase la Fundación para el Software Libre http://www.fsf.org y La Open Source Initiative http://www.opensource.org/

APÉNDICE B
INTERNET EXPLICADO


Illustration 49: Robert Kahn

HISTORIA

La idea de interconectar ordenadores situados en distintas ubicaciones geográficas surgió después de la Segunda Guerra Mundial. Mientras los ordenadores todavía se estaban empezando a desarrollar, el concepto existía sólo en las mentes de los futurólogos y filósofos. El lanzamiento del Sputnik por la Unión Soviética impulsó al gobierno de los EEUU a invertir fuertemente en la investigación y desarrollo. A finales de los años sesenta fue establecida la Agencia de Proyectos de Investigación Avanzada (ARPA), y antes de 1969 cuatro ordenadores fueron conectados al ARPANET. En 1972, Robert Kahn realizó una demostración exitosa de ARPANET en la Conferencia Internacional de Comunicación entre Ordenadores y presentó una nueva aplicación de ARPANET – el correo electrónico. La red ARPANET fue el antepasado de Internet tal y como lo conocemos hoy.

En 1977, ARPANET conectó 111 ordenadores, y antes de 1985 la red alcanzó Europa y Australia. Internet se hacía global y desmilitarizado. En 1983 fue introducida la versión 4 del protocolo TCP/IP – un protocolo con el que cualquier ordenador del mundo, independientemente de su marca o modelo, podía comunicar con cualquier otro en la misma red. Este gran avance técnico se considera como el nacimiento de Internet. Robert Kahn desarrolló el Protocolo de Control de Transmisión/Protocolo de Internet atendiendo a cuatro principios básicos:

- **Conectividad de red**. Cualquier red podría conectarse a otra red.
- **Distribución**. No habría ningún control o administración central de la red.
- **Eliminación de errores**. Los paquetes perdidos serían retransmitidos.
- **Diseño de caja negra**. No habría que hacer ningún cambio interno en una red para conectarla a otras redes.

TCP/IPv4 sigue siendo el protocolo común del Internet de hoy en día. Hasta ahora, su estructura ha garantizado que ninguna persona o empresa concreta dirija Internet, y que todos los que se conecten a Internet tengan un acceso no restringido a su contenido (sobre la censura y el filtrado en Internet hemos hablado antes).

LA WORLD WIDE WEB ("RED GLOBAL MUNDIAL" O LA TELARAÑA MUNDIAL)

Actualmente, la manera más popular de utilizar Internet es mediante la World Wide Web (WWW). Internet en sí es la conexión de los ordenadores con las redes de ordenadores, mientras que la WWW es una plataforma específica que sirve para que estos ordenadores puedan comunicarse en ella. El concepto y la tecnología de la WWW fueron desarrollados por Tim Berners Lee y Robert Cailliau en el laboratorio de física nuclear *Conseil Européen pour la Recherche Nucleaire (CERN)* y hechos públicos en1991. Los rasgos principales de la WWW son:

- **enlaces** – (hipervínculos) que conectan una página web con otra
- **comunicación** – HTTP (protocolo de transferencia de hipertexto) – una lengua electrónica hablada por ordenadores en Internet.

112
Different prices found by searching the Internet in September 2006

113
For more info see the Free Software Foundation http://www.fsf.org and the Open Source Initiative http://www.opensource.org/

- **páginas web** – HTML (lenguaje de marcas de hipertexto) – utilizado/as para diseñar páginas web e interaccionar con otros mediante enlaces. Otros lenguajes populares para escribir sitios web son PHP y JavaScript.
- **direcciones** – URL (localizador universal de recursos) – un sistema de direccionamiento para referirse a páginas web y otra información en Internet.

Juntos, constituyen los pilares del Internet que utilizamos hoy en día. La comunicación entre sitios web es realizada a través de protocolos TCP/IP.

INTERNET HOY EN DÍA

Según un estudio estadístico sobre Internet, en enero de 2006 había más de mil millones de usuarios de Internet. Esto parece una cifra increíble, al tomar en cuenta que nadie conocía Internet en 1990. Para mucha gente, se ha convertido en el método principal de almacenamiento e intercambio de información.

—

Un ejemplo reciente significativo del poder de Internet es Wikipedia.org – una enciclopedia online, con artículos escritos y editados por la comunidad en Internet. En los 5 años transcurridos desde su fundación, Wikipedia.org editó más de un millón y medio de artículos en inglés y, como mínimo, cien mil en diez otros idiomas. Su popularidad llevó a una evaluación independiente de la exactitud de su información, en comparación con la Enciclopedia Británica. Los resultados revelaron que las dos enciclopedias eran una casi tan precisa como la otra.[123]

INFRAESTRUCTURA BÁSICA

Internet es la red distribuida más avanzada. Esto significa que no tiene ninguna base ni servidor central. Aún así, aplica estándares en la manera de la que funciona (llamados protocolos) y a las organizaciones que desarrollan estos estándares. El Internet de hoy dispone para su funcionamiento de 3 capas principales. Primero, existe una infraestructura de telecomunicaciones. Una colección de cables de teléfono, fibras ópticas, microondas y satélites que todos juntos trabajan para garantizar que el tráfico en Internet llegue a cada rincón del mundo. La segunda capa son estándares y servicios técnicos. Está compuesta por distintos protocolos que dirigen el tráfico por la infraestructura y permiten que visitemos páginas web y enviemos correo electrónico. Es en esta capa dónde nos podemos conectar a Internet. La última capa: el contenido y aplicaciones – es la capa en la que operan todas las páginas web y servicios de Internet. Uno de los puntos fuertes de Internet es que cada una de estas capas opera de manera independiente[124].

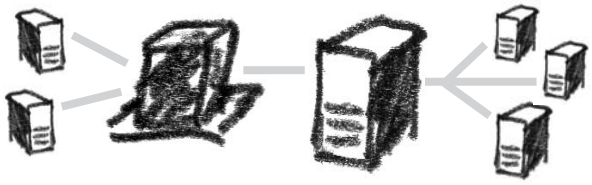
—

Veamos cómo funciona Internet desde el punto de vista del usuario. Primero, tenemos que conectarnos a Internet. Esto se puede hacer creando una cuenta con un **Proveedor de Servicios de Internet (ISP)**, quien, por su parte, adquiere su propio acceso de un proveedor nacional. Los proveedores nacionales reciben su conexión de una de las empresas multinacionales que mantienen la columna vertebral de Internet. La columna vertebral es una estructura de gran potencia y de gran amplitud de banda, con conexiones globales a través de cables submarinos y satélites, que permite las comunicaciones entre países y continentes. Conocida también como Tier 1 (nivel 1), Tier1, es administrada por empresas como MCI, AT&T, Cable Wireless y France Telecom.

123
http://news.bbc.co.uk/2/hi/technology/4530930.stm

124
La Gobernanza de Internet – La cesta de las infraestructuras y la estandarización.

Estándares del contenido y aplicación



Estándares técnicos (TCP, IP, DNS, etc.)

Infraestructura de telecomunicaciones

Cuando te conectas a Internet, a tu ordenador se le asigna una dirección IP. Como una dirección postal, la dirección IP identifica únicamente a este ordenador en Internet. Dependiendo de tu **Proveedor de Servicios de Internet**, se te pueden asignar distintas direcciones IP en distintos momentos de conexión. Todos los sitios web y servidores web tienen una dirección IP.

www.frontlinedefenders.org es, de hecho, 217.67.142.198

Sin embargo, cuando queremos visitar un sitio web, no solicitamos ver 217.67.142.198, sino que introducimos www.frontlinedefenders.org. Hay un método para traducir los números IP a nombres en lenguaje común. Se llama el Sistema de Nombres de Dominio (DNS), y en Internet hay ordenadores dedicados cuya función es realizar estas traducciones. Por lo tanto, no tenemos que preocuparnos por memorizar combinaciones de números complejas, sino que sólo tenemos que recordar las descripciones lingüísticas del nombre del sitio web.

—

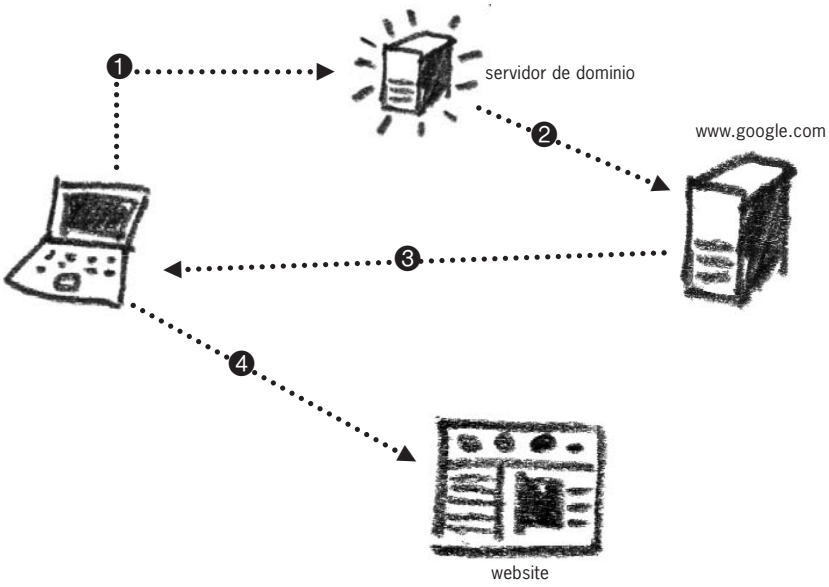
El DNS depende de los servidores raíz. Éstos son, básicamente, varios ordenadores escogidos que mantienen una lista de los nombres de sitios web más importantes, otros son operados por las agencias de gobierno de los EEUU y sus identificadores relevantes (.COM .ORG .NET .GOV, etc.). Algunos de estos servidores raíz son de propiedad privada, otros son operados por las agencias del gobierno de los EEUU. Actualmente, la mayoría de estos servidores están

114
http://news.bbc.co.uk/2/hi/technology/4530930.stm

115
Internet Governance – The infrastructure and standardisation basket

situados en la costa este de los EEUU. La estructura DNS es administrada por la Corporación de Internet para los Nombres y Números Asignados, que opera bajo la jurisdicción del Ministerio del Comercio. De hecho, algunos de los actores principales (los que poseen y gestionan los servidores raíz), como Verisign (una empresa privada norteamericana), tienen el poder de veto en este organismo gobernante – esto se ha convertido en una cuestión controvertida para los que temen que los EEUU ejerzan demasiado control sobre Internet.

Para poder consultar una página web desde tu ordenador, tienes que solicitarla introduciendo el nombre de su sitio web en el URL. Internet luego encuentra la dirección IP del sitio web consultando al DNS. Finalmente, hace falta encontrar un camino desde tu ordenador hasta el sitio web deseado. Este camino podría pasar por países, océanos y espacio; podría medir miles de millas y podría pasar por numerosos ordenadores. ¿Cómo sabe por dónde ir cuando hay cientos de millones de sitios web diferentes? La tarea de dirigir tu mensaje al sitio web (y hacia atrás) es realizada por los enrutadores, y el proceso se conoce como encaminamiento (o enrutamiento). Estos enrutadores pueden ser manipulados para registrar o redirigir sus paquetes o para bloquear el acceso a ciertos sitios web.



► Ejemplo de cómo tu mensaje viaja en Internet cuando busca una página web a través de Google

1. Escribes www.google.com. El ordenador busca en el servidor DNS la dirección IP de Google
2. El servidor DNS te dirige a www.google.com
3. Introduces tu consulta de búsqueda y Google te dará los resultados
4. Eres dirigido a la página deseada (nota: es posible que tu ordenador encuentre la dirección IP de esta página web otra vez a través del servidor DNS)

Cada ordenador o enrutador, por los que pasas para llegar a tu destino, se llama un salto. La cantidad de saltos es la cantidad de ordenadores/ enrutadores con los que tu mensaje entra en contacto durante su camino. Abajo está el camino que sigue mi ordenador en Internet para llegar a www.google.com. Puedes ver que mi solicitud pasa por 13 ordenadores (saltos) como mínimo para llegar a su destino.

traceroute www.l.google.com (**66.249.93.99**), 64 saltos max, paquetes de 40 byte

1 217.67.143.157 (217.67.143.157) 74.53 ms 30.910 ms 49.643 ms

2 217.67.140.61 (217.67.140.61) 29.780 ms 28.60 ms 29.628 ms

3 217.67.131.10 (217.67.131.10) 49.987 ms 29.872 ms 29.615 ms

4 217.67.131.6 (217.67.131.6) 40.267 ms 34.815 ms 40.219 ms

5 85.91.0.61 (85.91.0.61) 41.237 ms 39.192 ms 38.831 ms

6 208.50.25.109 (208.50.25.109) 31.452 ms 115.234 ms 37.396 ms

7 so0-0-0-2488M.ar3.LON2.gblx.net (67.17.71.25) 89.496 ms 44.303 ms 46.455 ms

8 ldn-b1-pos2-0.telia.net (213.248.100.1) 47.497 ms 44.190 ms 45.240 ms

9 google-104716-ldn-b1.c.telia.net (213.248.74.194) 52.678 ms 89.984 ms 61.543 ms

10 72.14.238.246 (72.14.238.246) 69.863 ms 72.14.238.242 (72.14.238.242) 59.778 ms 72.14.238.246 (72.14.238.246) 75.364 ms

11 216.239.43.91 (216.239.43.91) 65.671 ms 61.264 ms 53.603 ms

12 72.14.232.141 (72.14.232.141) 55.727 ms 54.204 ms 216.239.43.88 (216.239.43.88) 54.456 ms

13 64.233.175.246 (64.233.175.246) 72.265 ms 53.48 ms 55.586 ms

14 **66.249.93.99** (66.249.93.99) 54.490 ms 113.495 ms 66.249.94.46 (66.249.94.46) 57.798 ms

trace complete

Si has utilizado Internet alguna vez, sabes que, a pesar de su estructura aparentemente compleja, es muy fácil de manejar. Esta simplicidad se debe a su arquitectura estable, como hemos explicado arriba. Nos permite localizar rápidamente lo que necesitamos en el océano de información electrónica. Los servidores DNS y enrutadores son los responsables de coordinar este proceso. Si alguien puede controlar o influir en su funcionamiento, nuestro uso de Internet será dañado o restringido.

CORREO ELECTRÓNICO

El correo electrónico consiste en redactar mensajes electrónicos y enviarlos por Internet. Cualquier persona puede registrar una cuenta de correo electrónico en Internet, o recibir una de su **ISP**, y estos anfitriones se convertirán en sus proveedores de correo electrónico. Cada cuenta de correo electrónico tiene una dirección única (dmitri@email.com) donde el nombre del usuario está separado de la dirección del proveedor por una "@".

El correo electrónico se envía por Internet siguiendo los mismos principios de DNS y encaminamiento. Primero, se encuentra al proveedor del correo web por su nombre de dominio (p.ej. email.com), luego se consulta al proveedor sobre la existencia de una cuenta de usuario particular (p.ej. dmitri). Si la información es correcta, el correo electrónico se entrega. En caso contrario, el correo electrónico se nos devuelve (o rebota) con un mensaje de error.

Cada correo electrónico que envías o recibes contiene la siguiente información:

- el nombre registrado para la cuenta de correo electrónico (e.g. dmitri vitaliev).
- la dirección de correo electrónico.
- el número IP del ordenador de origen o del proveedor de correo electrónico.
- el camino seguido por el correo electrónico a su destino.
- la fecha de cuándo el correo electrónico fue enviado y recibido.

Esta información se almacena en las cabeceras de los mensajes de correo electrónico y suele tener la siguiente forma:

```
Received: from hotmail.com (bay17-f12.bay17.hotmail.com [64.4.43.62])
by mail2.frontlinedefenders.org (Postfix) with ESMTP id 5AB164F
for <dmitri@frontlinedefenders.org>; Thu, 20 Jan 2005 14:44:06 +0000 (GMT)
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
         Thu, 20 Jan 2005 06:44:04 -0800
Received: from 217.67.142.198 by by17fd.bay17.hotmail.msn.com with HTTP;
        Thu, 20 Jan 2005 14:43:58 GMT
Message-ID: <BAY17-F12DBF0F22EC08A06194JKDB9810@phx.gbl>
From: "Dmitri Vitaliev" <dmitri@hotmail.com>
To: dmitri@frontlinedefenders.org
Date: Thu, 20 Jan 2005 15:43:58 +0100
Content-Type: text/plain; format=flowed
X-Originating-IP: [217.67.142.198]
X-Originating-Email: [dmitri@hotmail.com]
X-Sender: dmitri@hotmail.com
```

Este ejemplo muestra el encabezado de un mensaje del correo electrónico enviado de dmitri@hotmail.com a dmitri@frontlinedefenders.org. Puedes ver la IP de los servidores de Hotmail (64.4.43.62) y la IP del ordenador del que fue enviado el correo electrónico (217.67.142.198).
Todo nuestro correo electrónico y tráfico en Internet es identificado y registrado por la IP del destino/ origen y la hora de ser enviado/ recibido. Esta información se utiliza para autentificar nuestro mensaje y su entrega. A veces, se utiliza también para monitorizar y restringir nuestras actividades en Internet. La estructura básica de Internet, descrita arriba, es bastante favorable para las actividades de vigilancia y censura, simplemente debido a que sus creadores no tuvieron en cuenta el tema de la seguridad.

SITIOS WEB

Un sitio web es una colección de páginas escritas en HTML (y otros lenguajes adaptables a Internet). Un sitio web tiene que residir en un **servidor web,** al que se refiere también como a un **anfitrión**. El anfitrión proporciona una dirección IP para el sitio web, y también tienes que registrar para él un nombre DNS único, p.ej. www.mywebsite.com. Un sitio web podría compartir su dirección IP con muchos otros que residan en el mismo anfitrión, sin embargo, todos tendrán nombres DNS únicos.

—

A fines de estabilidad y seguridad, algunos sitios web son replicados al ser copiados a distintos anfitriones, a menudo en países diferentes. Si tu sitio web primario deja de funcionar o es bloqueado el acceso a él, su réplica ocupa su lugar.

Voz sobre IP (VoIP)

Voz sobre IP es un nombre técnico para las "Comunicaciones basadas en Internet". En lugar de utilizar la red de centrales telefónicas, puedes mantener una conversación de voz en Internet. Es un método de comunicación cada vez más popular, dado que después de los costes de configuración iniciales, no pagas las tarifas de larga distancia, ya que la ubicación geográfica es irrelevante para Internet. Skype es probablemente el programa más conocido (con unos

100 millones de usuarios) que utilizan esta tecnología hoy en día[125]. VoIP se ha convertido en el rival principal de las empresas de telecomunicaciones tradicionales y se ha enfrentado con una dura oposición en los países que intentan mantener el monopolio de las telecomunicaciones.

Blogs

Éste quizás sea el uso de Internet más influyente de hoy en día. En esencia, un diario online o una columna de opinión, puede ser creado por quien lo desee en cualquiera de los múltiples anfitriones gratuitos de **blog**. No tienes que montar un **servidor web**, ni costear gasto alguno. A veces, la estructura de la página web ya está diseñada a propósito, y todo lo que tienes que hacer es rellenarla con tu contenido. Los blogs proporcionan una oportunidad para expresar tu opinión sobre cualquier tema que elijas.

—

En marcado contraste con los medios de comunicación tradicionales que esperan que los consumidores simplemente digieran la información presentada en ellos, la publicación online es la opción más cercana disponible a una voz global. Es una recopilación de todos los artículos, opiniones y **blogs** (actualmente hay unos 50 millones de blogs) sobre cada tema existente. Lleva una información completamente no editada que sólo expresa la opinión de su editor.

—

El "periodismo ciudadano" es un término que se aplica a los que informan sobre las noticias, eventos y cambios en sus países mediante un **blog**. A menudo, es la única fuente de noticias "verdaderas" de un país. El "periodismo ciudadano" se ha convertido en un arma potente en la lucha por la libertad de expresión, y, por lo tanto, es fuertemente monitorizado y reprimido por regímenes opresivos.

Redes sociales

Este término se refiere a la capacidad presentada por Internet y una variedad de aplicaciones nuevas para crear y mantener las redes de amigos y compañeros. Las herramientas te permiten permanecer en contacto uno con otro a través de varios métodos, incluyendo la mensajería instantánea, fotos e intercambio de vídeos, tanto como el envío de mensajes de texto. Las redes sociales son responsables por el hecho de que muchas causas sociales se presentan y promueven en Internet, y también por las relaciones entre personas que viven en diferentes partes del mundo. Sin embargo, tienen muchas desventajas y peligros inherentes de los que los usuarios tienen que ser conscientes. La información privada sobre la gente se lleva online y al dominio público. Las relaciones entre las redes de activistas son expuestas, y pueden ser fácilmente explotadas por un adversario determinado. Los usuarios sacrifican de buena gana la información privada, que es muchas veces imposible de eliminar de Internet más tarde.

125
Puedes descargar Skype de http://www.skype.com o véase el CD de la Caja de Herramientas de Seguridad. Ha habido muchos debates relativos a la seguridad de las comunicaciones de Skype. Aunque Skype utiliza el cifrado para asegurar chats instantáneos y transferencias de archivos, el código de su programa está cerrado y la seguridad no puede ser verificada por expertos externos. Véase el trabajo escrito por Simon Garfinkel sobre la seguridad de Skype, http://www.tacticaltech.org/files/tacticaltech/Skype_Security.pdf

APÉNDICE C ¿CÓMO DE LARGA DEBERÍA SER MI CONTRASEÑA?

Veamos cuánto tiempo tardaría un programa de ordenador en adivinar tu contraseña. Suponiendo que tu contraseña esté compuesta sólo por minúsculas, calcularemos el número máximo de las posibilidades que el intruso tiene que revisar.

Longitud de a contraseña	**3**	**5**	**7**	**9**
Cálculo	*26 x 26 x 26*	*26 x 26 x 26 x 26 x 26*	*26 x 26 x 26 x 26 x 26 x 26 x 26*	*26 x 26 x 26 x 26 x 26 x 26 x 26 x 26 x 26*
Numero de posibilidades	*17,576*	*11,881,376*	*8,031,810,176*	*54,295,503,678,976*

Ahora, añadamos a nuestra contraseña dígitos y mayúsculas. Esto incrementa las variaciones de cada carácter a 62 posibilidades distintas.

Longitud de a contraseña	**3**	**5**	**7**	**9**
Cálculo	*62 x 62 x 62*	*62 x 62 x 62 x 62 x 62*	*62 x 62 x 62 x 62 x 62 x 62 x 62*	*62 x 62 x 62 x 62 x 62 x 62 x 62 x 62 x 62*
Numero de posibilidades	*238,328*	*916,132,832*	*3,521,614,606,208*	*13,537,086,546,263,552*

Cómo puedes ver, las probabilidades incrementan dramáticamente cuando añades las variaciones de los caracteres de la contraseña y cuando aumentas su longitud. Pero ¿cómo de rápido los ordenadores pueden descifrar estas contraseñas? Supondremos que un ordenador (PC) moderno procesa 100.000 posibilidades de una contraseña por segundo. La tabla de abajo indica las longitudes de contraseñas desde 3 hasta 12 caracteres. Las cifras en la parte de arriba – 26, 36, 52, 68, 94 – indican el número de caracteres que forman las contraseñas (si suponemos que se utiliza el alfabeto inglés). 26 es la cantidad de minúsculas, 36 son letras y digitos, 52 son mayúsculas y minúsculas, 68 son mayúsculas y minúsculas con dígitos, símbolos y puntuación.

	26	**36**	**52**	**68**
3	0.18 segundos	0.47 segundos	1.41 segundos	3.14 segundos
4	4.57 segundos	16.8 segundos	1.22 minutos	3.56 minutos
5	1.98 minutos	10.1 minutos	1.06 horas	4.04 horas
6	51.5 minutos	6.05 horas	13.7 dias	2.26 meses
7	22.3 horas	9.07 dias	3.91 meses	2.13 años
8	24.2 dias	10.7 meses	17.0 años	1.45 siglos
9	1.72 años	32.2 años	8.82 siglos	9.86 milenios
10	44.8 años	1.16 milenios	45.8 milenios	670 milenios
11	11.6 siglos	41.7 milenios	2,384 milenios	45,582 milenios
12	30.3 milenios	1,503 milenios	123,946 milenios	3,099,562 milenios

Basándose en estas cifras, uno puede suponer que incluso una contraseña arbitraria de 8 minúsculas y dígitos será suficiente en su complejidad. Si tu contraseña principal hasta ahora ha sido sólo de 5 caracteres, es posible que ya haya sido comprometida, o es probable que sea comprometida si surge la necesidad. **Nota:** las cifras mencionadas arriba se aplican sólo a las contraseñas arbitrarias. La perfilación y ataques de diccionario son diferentes, ya que trabajan sólo contra las contraseñas del "mundo real".

116
You can download Skype from http://www.skype.com or see *the NGO in a Box – Security Edition* CD. There have been many debates as to the security of Skype communications. Even though Skype uses **encryption** to secure instant chats and file transfers, their program code is closed and the security cannot be verified by external experts. See the paper written by Simon Garfinkel on Skype security http://www.tacticaltech.org/files/tacticaltech/Skype_Security.pdf

GLOSARIO

Acceso DSL – se refiere a la tecnología de las comunicaciones de datos que permite una transmisión de datos sobre un par de cobre más rápida que la que puede proporcionar un módem convencional. La abreviatura DSL significa Línea de abonado digital ("Digital Subscriber Line") (con variantes de ADSL - asimétrica y SDSL – simétrica).

Ataque de denegación de servicio (DOS) – Un ataque de denegación de servicio (DOS) se realiza mediante intentos repetidos de un ordenador de conectarse a un sitio web. El objetivo del ataque es sobrecargar el servidor web al hacer millones de solicitudes iguales en el tiempo más corto posible. Un ataque distribuido de denegación de servicio incluye ordenadores especialmente preprogramados para atacar un sitio web particular.

BIOS – significa **El Sistema Básico de Entrada/ Salida ("Basic Input/ Output System"**). Esta denominación se refiere al código del software utilizado por un ordenador cuando se pone en funcionamiento por primera vez. La función primaria de **BIOS** es preparar la máquina de manera que otros programas de software almacenados en varios soportes (como, por ejemplo, discos duros, disquetes y CDs) puedan cargar, ejecutar y asumir el control sobre el ordenador.

Blog – un sitio web donde las entradas se hacen siguiendo el estilo de un diario y se publican en orden cronológico inverso. Los blogs a menudo proporcionan comentarios o noticias sobre un tema particular, como comida, política o noticias locales; algunos funcionan como diarios personales online. Un **blog** típico combina textos, imágenes y enlaces de otros blogs, páginas web y otros medios de comunicación relacionados con este tema. Los buscadores de **blog** más populares incluyen www.wordpress.com, www.livejournal.com, www.blogspot.com.
Muchos periodistas y defensores de derechos humanos utilizan blogs para comunicar información vital, no disponible de otra manera en los medios de comunicación dominantes a la comunidad en Internet. Esto ha sido etiquetado "periodismo ciudadano" – un método cada vez más popular de obtener información veraz sobre un evento o un país.

Brecha digital – una diferencia entre los que tienen un acceso regular y efectivo a las tecnologías digitales y los que no lo tienen. La brecha digital está relacionada con la inclusión social y la igualdad de oportunidades. Se ve como un problema político y social y cobra cada vez más un interés general, ya que las naciones industrializadas dependen cada vez más de las tecnologías digitales.

Capa de Conexión Segura o Capa de Sockets Seguros (SSL) – un protocolo criptográfico que proporciona comunicaciones seguras en Internet para el correo electrónico, envío de fax en Internet y otros tipos de transferencias de datos.

CCO – Copia de Carbón Oculta. Se refiere a la práctica de enviar mensajes a destinatarios múltiples de manera que los que los reciben no pueden ver la lista completa de los destinatarios.

Hay varios razones por los que utilizar esta función:

- Para enviar una copia de tu correspondencia a un tercero (por ejemplo, a un colega) cuando no quieres que el destinatario sepa que lo estás haciendo (o cuando no quieres que el destinatario conozca la dirección de correo electrónico de la tercera parte).
- Cuando envías un correo electrónico a destinatarios múltiples, puedes ocultar sus direcciones de correo electrónico de uno para otro/ de uno y otro/ ante uno y otro. Ésta es una medida antispam sensible, ya que ayuda a evitar que se compile una lista larga de las direcciones de correo electrónico disponible a todos los destinatarios (lo que es lo que pasa si pones las direcciones de cada uno en el campo Para: o CC:). Por este motivo, a menudo merece la pena utilizar el campo **CCO:** para las listas de correo electrónico. Algunos virus copian las direcciones de correo electrónico de la carpeta de cache de los usuarios o de la lista de contactos, y listas largas de CC (Copia de Carbón) pueden favorecer a la propagación de virus no deseados - un motivo más para utilizar **CCO.**

Certificado SSL – es generado para cada sitio web que desea funcionar sobre SSL. Sirve como un identificador único que comprueba la autenticidad del sitio web y proporciona la información necesaria para un canal cifrado entre el anfitrión y el cliente.

Ciber-disidente(s) - una persona o varias personas que se oponen activamente a la estructura política establecida y expresa(n) sus opiniones políticas a través del medio de Internet.

Cifrado – el proceso de ocultar información para hacerla inteligible sin un conocimiento especial.

Controlador de dispositivo – código de ordenadores que permite que un hardware específico funcione en tu ordenador.

Cortafuegos – un equipo de hardware y/ o software que funciona en las redes de ordenadores para prevenir comunicaciones prohibidas por la política de seguridad.

Criptanálisis (sta) – estudios de los métodos de obtener el significado de una información cifrada, sin acceso a información secreta. Un criptanalista es una persona que lleva a cabo estudios de este tipo.

Criptografía – el estudio de patrones de codificación matemáticos, lingüísticos y otros, y sus historias.

Criptografía de clave pública (cifrado) – una forma de criptografía que generalmente permite a los usuarios llevar a cabo comunicaciones seguras sin tener un acceso previo a una clave secreta compartida. Esto se realiza al utilizar un par de claves criptográficas, designadas **clave pública** y **clave privada**, que están relacionadas matemáticamente.

ECHELON – el nombre para describir una red altamente secreta de inteligencia de señales y de análisis utilizada en todo el mundo y mantenida por la comunidad UKUSA (conocida también como la “alianza anglosajona”). Sobre ECHE-

LON han informado varias fuentes, incluido el Parlamento Europeo. Según algunas fuentes, ECHELON puede capturar comunicaciones por radio y satélite, llamadas de teléfono, faxes y correos electrónicos y otras corrientes de datos en casi todo el mundo. Incluye un análisis automatizado por ordenador y clasificación del material interceptado.

Eliminación de archivos – el proceso de sobrescribir un archivo, a veces archivos múltiples, para asegurar que toda la información sea borrada. Eliminar un archivo es similar a triturar un documento en una trituradora de papel.

Evasión – en este libro, la evasión se refiere a los métodos de evitar bloqueos de sitios web en Internet. Esto se consigue mediante el uso de la tecnología que "sortea" el obstáculo dado.

ISP – véase el **Proveedor de Servicios de Internet**

Estándares abiertos del cifrado – métodos o algoritmos del cifrado el código de los cuales está abierto al público general para la revisión y mejora. Éstos se consideran como el tipo más seguro de algoritmos de cifrado probados independientemente. Los algoritmos del cifrado cerrado pueden tener serios defectos (inadvertidos por sus creadores), o "puertas traseras" especialmente diseñadas que podrían dejar filtrar toda tu información a una tercera parte.

Panel de Control – una función de Microsoft Windows que te da el acceso para modificar las configuraciones del sistema de tu ordenador, incluyendo la gestión del usuario, las opciones de potencia, el acceso a la red, los controladores del sistema, y muchas más.

Partición (partición de disco) – creación de divisiones lógicas en un disco duro. Permite la creación de varios sistemas de archivos en un solo disco duro y tiene muchos beneficios: facilitar la configuración de un arranque dual (por ejemplo, para arrancar Microsoft Windows y Linux), compartir particiones de intercambio entre múltiples distribuciones Linux, y proteger o aislar los archivos.

PKE – véase Criptografía de clave pública

Proveedor de Servicios de Internet (ISP) – un negocio u organización que ofrece a los usuarios el acceso a Internet y a los servicios relacionados. En el pasado, los ISP fueron gestionados por las empresas de telefonía. Hoy en día, los ISP pueden ser iniciados por casi cualquier persona. Proporcionan servicios como tránsito por Internet, registro del nombre de dominio y alojamiento de sitios web, conexión por línea conmutada o DSL, acceso por línea dedicada y coemplazamiento (el servicio de mantener tu propio servidor en las instalaciones del ISP).

Puerta trasera – en un sistema de ordenadores, un método de evitar la autentificación normal o asegurar un acceso remoto a un ordenador, mientras que se intenta permanecer oculto ante una inspección ocasional.

Registro del sistema – una lista de todas las aplicaciones de software, dispositivos de hardware y configuraciones del sistema en tu ordenador. Cada componente y programa instalado de tu ordenador tiene que tener una entrada en

el registro. Esto se suele producir automáticamente. A veces, cuando se desinstala un programa, no elimina su entrada del registro, lo que podría suponer un problema de seguridad. Los virus a menudo atacan y corrompen el registro y podrían dañar la funcionalidad de tu sistema. Se conoce también como "registro" o "registro de Windows".

Servidor proxy – un ordenador que permite a los clientes hacer conexiones indirectas de red a otros servicios de la red (sitios web).

SORM-2 – (*Sistema Operativno-Rozysknykh Meropriyatii*, literalmente "Sistema de Medidas Operativas de Inteligencia") – una ley rusa, actualizada en 1988, que permite al FSB (Servicio Federal de Seguridad) monitorizar comunicaciones en Internet.

SSL – véase **Capa de Conexión Segura o Capa de Sockets Seguros**

Servidor web – Un ordenador que aloja uno o más sitios web. También anfitrión de sitio web, anfitrión.

UNA PROPUESTA DE CARTA DE DERECHOS EN INTERNET

1 El derecho a acceder a la infraestructura de Internet sin consideración del lugar donde vivas.

2 El derecho al conocimiento y habilidades que permiten utilizar Internet y adaptarlo de manera que puedas satisfacer tus necesidades.

3 El derecho a un software gratuito y de código abierto.

4 El derecho a la igualdad de acceso para hombres y mujeres.

5 El derecho a acceder y a crear contenido que sea cultural y lingüísticamente diverso.

6 El derecho a la libertad de expresión.

7 El derecho a protestar online.

8 El derecho al acceso a conocimientos.

9 El derecho a la libertad de información.

10 El derecho a acceder a la información financiada con fondos públicos.

11 El derecho a estar libre de vigilancia

12 El derecho a utilizar el cifrado.

13 El derecho a que exista una gestión democrática multilateral de Internet.

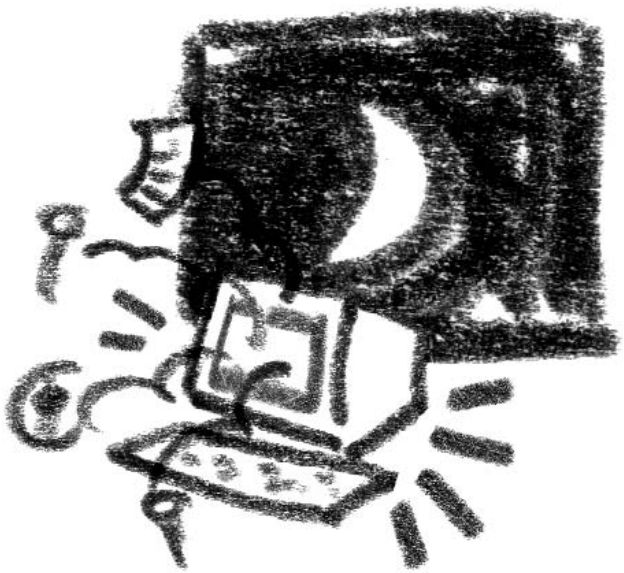
14 El derecho a la transparencia y accesibilidad del organismo legislativo de Internet.

15 El derecho a un Internet descentralizado, colaborativo e interoperativo.

16 El derecho a la protección de derechos, conciencia y educación.

17 El derecho a recurso cuando son violados tus derechos.

(Para el texto entero, por favor, consulta el original en el sitio web de la Asociación para las Comunicaciones Progresivas http://rights.apc.org/charter.shtml)



SEGURIDAD Y PRIVACIDAD DIGITAL

PARA LOS DEFENSORES DE LOS DERECHOS HUMANOS

81 Main Street
Blackrock
Co Dublin
Ireland
Tel: +353 (0)1 212 3750
Fax: +353 (0)1 212 1001
E-mail: info@frontlinedefenders.org
www.frontlinedefenders.org

security.ngoinabox.org