

La Seguridad y la tecnología de la información y la comunicación



(Con la colaboración de Privaterra -www.privaterra.org)

Objetivo:

Los increíbles vacíos que existen en la tecnología de la información de todo el mundo también afectan a las defensoras y los defensores de derechos humanos. El presente capítulo se centra sobre todo en la tecnología de la información (ordenadores e Internet).¹ Algunas de sus partes no tendrán interés para quienes no tengan acceso a Internet, y/o no utilicen el ordenador; estas personas necesitarían, más bien, los medios y la formación necesarias para saber usar la tecnología de la información en la defensa de los derechos humanos.

Problemas de seguridad en las comunicación y cómo evitarlos

El conocimiento es poder, y saber qué problemas de seguridad podríamos tener en nuestras comunicaciones nos da más seguridad. Trataremos los temas relacionados con el acceso ilegal a nuestras informaciones y comunicaciones, o su manipulación, para luego plantear maneras de evitarlo.

Hablar con la gente

Acceder ilegalmente a una información no es algo que se haga únicamente por Internet. Cuando tengamos que hablar de temas delicados, habrá que considerar las siguientes cuestiones:

- 1 ♦ ¿Confiamos en las personas con las que estamos hablando?
- 2 ♦ ¿Necesitan saber todo lo que les estamos contando?

¹ Capítulo basado en el trabajo de Robert Guerra, Katitza Rodríguez y Caryn Mladen de Privaterra, una ONG que da cursos y asesoramiento a las y los defensores de derechos humanos de todo el mundo sobre temas de seguridad y tecnología de la información (TI). Este texto ha sido ligeramente adaptado en algunas partes por Marie Caraj y Enrique Eguren.

- 3 ♦ ¿Estamos en un lugar seguro? Los micrófonos y demás transmisores a menudo se instalan en zonas donde la gente cree estar segura, como despachos, calles muy concurridas, dormitorios y vehículos.

Podría ser difícil contestar a la tercera pregunta porque se pueden instalar micrófonos en una habitación para grabar o transmitir todo lo que se diga en ella. Los micrófonos láser, orientados desde grandes distancias a ventanas, pueden permitir también que se escuche lo que se está diciendo en un edificio. Podemos protegernos de ellos usando cortinas gruesas o instalando doble acristalamiento en las ventanas. Algunos edificios seguros tienen dos filas de ventanas para reducir el riesgo de ser alcanzados por esos aparatos de escucha.

¿Qué podemos hacer?

▣ **Siempre partir de que nos pueden estar escuchando.** Con una actitud de sana paranoia tendremos más cuidado cuando estemos hablando de temas confidenciales.

▣ **Los equipos para detectar aparatos de escucha** funcionan, pero es posible que ese servicio sea caro y difícil de conseguir. Además, a veces quienes lo ofrecen son quienes han instalado antes esos micrófonos! Al ser contratados, o bien encuentran unos pocos micrófonos (baratos) que de hecho han puesto ahí para luego hacer que los encuentran, o, asombrosamente, no encuentran nada y nos comunican que la oficina está "limpia".

▣ **El personal de la limpieza puede constituir una amenaza real a nuestra seguridad.** Tienen acceso a nuestras oficinas cuando ya no hay nadie, y se encargan de la basura. Por razones de seguridad, todo el personal debería ser cuidadosamente investigado con asiduidad (pues sus intenciones podrían variar después de haber entrado a trabajar para nuestra organización).

▣ **Conviene cambiar a menudo la sala de reuniones.** Cuantas más habitaciones utilicemos para discutir asuntos e intercambiar información, quien nos quiera espiar tendrá que utilizar más recursos humanos y materiales.

▣ **Cuidado con los regalos que suelen llevarse encima siempre,** como un bolígrafo caro o un broche, o con los que siempre están en la oficina, como un precioso pisapapeles o un magnífico cuadro. Estos tipos de objetos han sido empleados en el pasado para escuchar conversaciones.

▣ **Partamos de que en un momento dado una parte de la información de que disponemos es ya conocida por quien nos espía.** Si cambiamos de planes o de códigos a menudo les estaríamos dando sólo fragmentos de información verdadera. También podemos considerar dar información falsa para comprobar si alguien la está usando o reaccionando a ella.

▣ Para minimizar la eficacia de los micrófonos láser, podríamos **discutir los temas delicados en un sótano o en una habitación sin ventanas.** Algunos aparatos de escucha láser son menos eficaces durante las tormentas y similares.

▣ **Una grabación de ruido blanco o una canción popular** interferirá la captación del sonido, lo que es útil para el caso de los aparatos de escucha exteriores, que pueden captar una conversación a 50 metros, aproximadamente. En

otras palabras, no es sólo que puedan poner micrófonos allí donde nos reunamos: sólo la tecnología más cara es capaz de limpiar una conversación de los ruidos aleatorios del ambiente.

▣ **Los espacios amplios y abiertos pueden ser lugares buenos o malos.**

Quedar en un sitio apartado nos ayuda a darnos cuenta de si nos están siguiendo pero nos pone difícil el hacerles perder la pista porque no podemos "fundirnos en el paisaje". Los lugares bulliciosos sí nos permiten confundirnos entre la gente, pero también es cierto que se multiplica el número de personas que pueden vernos y oírnos.

▣ **Si la oficina o lugar de reunión está en una zona rural (abierta),** es bueno comprobar con alguien del grupo si se oye una conversación desde el exterior. Quedarse fuera también conviene para que tengamos vigilados a quienes no queremos que se acerquen a la reunión.

Teléfonos celulares/móviles

Cualquiera con suficiente capacidad tecnológica puede espiar una conversación telefónica, por eso debemos siempre partir de que ninguna llamada es segura. Los celulares/móviles analógicos son mucho menos seguros que los digitales, y ambos son a su vez mucho menos seguros que las líneas terrestres.

La vigilancia celular localiza nuestras llamadas además de escucharlas. Para que la llamada sea localizada, no hace falta que estemos hablando; basta con que tengamos encendido el móvil.

No debemos conservar nombres y números confidenciales en la memoria de nuestros teléfonos. Si nos lo roban, podrían usar esa información para localizar e implicar a personas que, de hecho, deseamos proteger.

Para las emergencias (y allí donde todavía sea posible), podríamos plantearnos tener dos números de teléfono de seguridad no identificados (tarjetas prepago) para establecer comunicación exclusivamente entre ellos y nunca para llamar o recibir llamadas de un número "conocido" (puesto que podría estar en una lista negra y descubrir así el nuestro). Nunca los utilizaríamos en sitios que se puedan relacionar fácilmente con nosotras o nosotros. Debemos acordarnos de sacar las tarjetas de esos móviles cuando no las estuviéramos usando, pues de lo contrario podrían ser rastreadas; además, conviene cambiarlas las dos regularmente. En cuanto a discreción en las conversaciones, hay que tener el mismo cuidado que cuando hablamos desde teléfonos más habituales.

Seguridad física de la información en la oficina

Siempre hay que cerrar la oficina con llave o cerrojo, tanto las puertas como las ventanas. Debemos usar llaves que requieran una autorización específica para hacerse una copia de ellas, y siempre habrá que saber dónde están y quién tiene las copias que se hayan hecho. Bajo ningún concepto debemos darle las llaves a terceras personas, ni siquiera al personal de mantenimiento o de la limpieza. Siempre que haya terceras personas en la oficina, deberá estar presente también alguien de nuestra total confianza. Si esto no fuera posible, tendría que ser

que al menos disponemos de una habitación de acceso restringido para guardar la información más sensible. Podríamos cerrar con llave todas las puertas de dentro de la oficina y dejar la basura fuera, en el pasillo, y sólo con los desperdicios no confidenciales.

Para material confidencial, debemos usar una trituradora que corte el papel en zig zag. Cuando sea especialmente sensible, conviene quemar las tiras de papel, desmenuzar las cenizas y luego tirarlas por el inodoro.

Medidas de seguridad básicas para ordenadores y archivos²

Cuando sea posible, cerrar con llave los ordenadores al abandonar la oficina. Las pantallas de los ordenadores nunca deben ser visibles desde las ventanas.

En todas las tomas de corriente eléctrica usaremos protección contra las sobrecargas (las variaciones en la corriente eléctrica pueden estropear los ordenadores).

Debemos guardar las copias de seguridad de la información, incluida la que esté en papel, en un lugar diferente y seguro. Para que estén bien protegidas, las guardaremos en el disco duro de un ordenador protegido con una clave encriptada, o usando cerrojos de máxima seguridad.

Para reducir el riesgo de que alguien entre en nuestro ordenador, debemos proteger el acceso a éste con una clave, y también acordarnos de apagar el ordenador cuando no vayamos a utilizarlo.

En caso de que alguien consiga entrar en nuestro ordenador, conviene tener los archivos encriptados.

Si nos roban el ordenador o queda destruido, podremos recuperar toda la información que contenía si hemos desarrollado la costumbre de hacer una copia de seguridad a diario. Habrá que recordar que las copias de seguridad encriptadas las tenemos que guardar fuera de la oficina en un lugar seguro.

También podemos usar un servidor externo para hacer una copia de la información usando Internet. Esto nos permite recuperarlo todo en caso de que nos quedemos sin el ordenador.

Los archivos que borremos no podrán recuperarse si usamos para destruirlos la utilidad para borrar archivos PGP Wipe o similares, en vez de enviarlos a la papelera de reciclaje del ordenador.

Nuestro ordenador podría estar programado para enviar fuera nuestros archivos, o bien dejarnos sin ellos, haciéndonos más vulnerables. Para evitar esta situación, conviene comprar el ordenador de una fuente segura. A continuación, reformatearemos el disco duro y sólo entonces procederemos a instalar el software que queramos. No debemos dejar que cualquiera manipule nuestro ordenador: sólo técnicos informáticos de nuestra confianza, y siempre estaremos presentes cuando nos lo estén arreglando.

² Para información más pormenorizada sobre seguridad informática, escribir a info@frontlinedefenders.org (Front Line) o a info@privaterra.org (Privaterra)

Deberíamos desenchufar el módem o la conexión telefónica del ordenador, o la conexión física a Internet, cuando no estemos usándolo. Así, ningún programa podrá intentar acceder a nuestro ordenador de noche. Siempre tenemos que desenchufar el ordenador cuando nos marchemos. Además, se puede instalar un software que desactiva el acceso al cabo de un tiempo (que determinaremos previamente) sin usarse el ordenador. Esto hace que la máquina no sea vulnerable cuando hacemos un descanso o vamos a hacer unas copias.

En nuestros Favoritos, podemos activar las extensiones de archivo para saber qué tipo de archivo vamos a abrir antes de abrirlo. Si creemos que vamos a abrir un archivo de texto y luego resulta que es un archivo ejecutable podríamos estar activando un virus. En el Explorador de Internet, ir al menú de Herramientas y elegir Opciones de carpeta. Hacer clic en la pestaña Ver y comprobar que NO está marcada la opción Ocultar las extensiones de archivo para tipos de archivo conocidos

Problemas de seguridad con Internet

Nuestros correos electrónicos no van directamente de nuestro ordenador al de quienes escribimos. Pasan por varios nodos y dejan un rastro de información que **puede ser seguido desde cualquier punto del recorrido** (ino sólo en nuestro país!).

Al escribir un correo, podrían estar espiándonos por encima del hombro, sobre todo en un ciber café. Si nuestro ordenador está en red, cualquier persona que se encuentre en la oficina podría leerlo. La persona a cargo de la administración del sistema también puede acceder a los correos de todo el mundo.

Nuestro proveedor de servicios de Internet (el servidor; ISP en inglés) tiene acceso a todos nuestros correos. Si alguien tiene la capacidad para presionarle, nuestro servidor podría enviarle una copia de todo lo que pidiera, o impedir que correos que hubiéramos enviado lleguen a su destino.

Los correos, al viajar por Internet, pasan por cientos de terceras partes nada seguras. Los hackers pueden acceder a todos los correos cuando éstos se dirigen a su destino. Debemos recordar que el servidor de quienes van a recibir nuestros correos también puede ser vulnerable, así como sus redes u oficinas.

Medidas de seguridad básicas para Internet

Los virus y similares, como los troyanos, pueden venir de cualquier sitio, porque incluso personas amigas pueden estar difundiéndolos sin saberlo. Es fundamental instalar un buen programa antivirus y activar las actualizaciones automáticas que se producen cuando nos conectamos a Internet. Siempre se están creando y descubriendo nuevos virus: en la Virus Information Library (biblioteca de información sobre virus), www.vil.nai.com, podemos encontrar información sobre los últimos parches de protección.

Los virus son programas simples diseñados para reproducirse y pueden ser malignos o no. Los troyanos son programas diseñados para proporcionarle a una tercera parte (¡a cualquiera!) acceso a tu ordenador. Se suelen difundir por correo electrónico, por lo que es importante usar el correo adecuadamente (ver abajo).

Un buen cortafuegos (firewall) nos ayuda a ser invisibles ante los hackers y nos protege de los intrusos que pretenden entrar en nuestro sistema. También nos garantiza que sólo las aplicaciones autorizadas se conecten a Internet desde nuestro ordenador y evita que programas como los troyanos envíen información fuera o abran agujeros por los que cualquier hacker podría entrar.

Un sistema de key logger (registrador de teclas) puede rastrear todas las pulsaciones que hagamos en el teclado. Estos programas se propagan o bien porque alguien los instala en nuestro ordenador cuando no estamos, o bien por un virus o un troyano que haya atacado nuestro sistema desde Internet. Los key loggers averiguan cuáles han sido las teclas que hemos pulsado e informan de nuestras actividades, normalmente a través de Internet. Se combaten usando la protección de una clave, utilizando el correo electrónico de forma segura, instalando un programa antivirus, y usando un programa de teclado virtual para escribir nuestra clave con el ratón (aunque ya existen key loggers que descifran esto también). Se desactivan cuando desconectamos el acceso a Internet de nuestro ordenador físicamente (normalmente, desenchufando la conexión telefónica).

Una dirección de correo electrónico puede ser imitada (spoofing, o suplantación de identidad) o utilizada por alguien que no es quien la tiene de verdad. Esto se hace consiguiendo el acceso al ordenador y contraseña de la víctima, entrando como hacker en el servidor, o utilizando una dirección que se parece a la de esa persona, por ejemplo, cambiando una letra "l" por un número "1". La mayoría de la gente no notará la diferencia. Para combatir el spoofing, debemos titular los correos, para que quede claro que son nuestros, y podemos hacer también alguna pregunta que sólo el auténtico o la auténtica propietaria de ese correo sabría contestar. Ante cualquier petición sospechosa de información, debemos utilizar alguna otra forma de comunicación para comprobar que es fidedigna.

Cuando naveguemos por Internet, si queremos que nuestras visitas sean privadas, tendremos que no aceptar las cookies del sitio visitado o borrar nuestro caché después de usar Internet. En el Explorador de Internet, ir a Herramientas, después a Opciones. En el Navegador de Netscape, ir a Editar, después a Preferencias. En cualquier de estos menús, borraremos entonces toda nuestra historia, las cookies que podamos tener y vaciaremos nuestro caché. Debemos acordarnos de eliminar también nuestros favoritos. Los navegadores también guardan informes de los sitios que visitamos en los archivos caché, por lo que tendremos que averiguar qué archivos hay que borrar en nuestro sistema.

Conviene actualizar a todos los navegadores web a una versión más reciente que les permita funcionar con una encriptación de 128-bits. Esto nos ayudará a salvaguardar cualquier información que queramos transmitir de forma segura a través de la web, incluidas las contraseñas y demás datos confidenciales que usamos para rellenar formularios. Debemos de instalar los últimos parches de seguridad para todo el software que usemos, en especial de Microsoft Office, Microsoft Internet Explorer y Netscape.

No debemos utilizar un ordenador que contenga información sensible para navegar por sitios que no es esencial que visitemos.

Medidas de seguridad básicas con el correo electrónico

A continuación presentamos unas rutinas de seguridad para cuando usemos el correo electrónico y que todos y todas deberíamos asumir, tanto nosotros como nuestras relaciones personales y profesionales. Podríamos decirle a nuestros contactos que hemos decidido no abrir correos que no sigan estas pautas mínimas de seguridad.

- 1 ♦ NUNCA abrir un correo de alguien que no conozcamos.
- 2 ♦ NUNCA reenviar un correo de alguien que no conozcamos, incluso si éste nos ha sido a su vez reenviado por alguien que conocemos. También esos correos que circulan con "mensajes positivos" pueden contener virus. Al reenviarlos, podemos estar infectando los ordenadores de todo el mundo. Si alguno nos parece muy bueno y deseamos que más gente lo lea, tendríamos que abrir un nuevo correo y copiar el mensaje, mecanografiándolo. Si no podemos perder el tiempo en eso, no será tan importante...
- 3 ♦ NUNCA descargar o abrir un documento adjunto a no ser que sepamos lo que contiene y que es seguro. Debemos desactivar la opción del programa de correo electrónico que hace las descargas automáticas. Muchos virus y troyanos se propagan como "gusanos" y los gusanos modernos a menudo resultan haber sido enviados por alguien que conocemos. Los gusanos replicantes escanean nuestro listín de direcciones, en especial si usamos el Microsoft Outlook o el Outlook Express, y luego se envían solos disfrazados de adjuntos normales procedentes de nuestros contactos. Si usamos el programa PGP al firmar nuestros correos, tanto en los que van con adjunto como en los que no, podríamos ayudar a quienes reciben nuestros correos a tener menos dudas respecto a si el adjunto está libre de virus (el PGP es un software que encripta la información. Ver nota a pie de página abajo, en "La encriptación: preguntas y respuestas").
- 4 ♦ No escribamos los correos con HTML, MIME o texto enriquecido (.rtf; rich text): sólo con el texto, "texto sin formato". Los correos de texto enriquecido pueden contener programas que podrían facilitar el acceso a nuestros archivos del ordenador o que lo estropeen.
- 5 ♦ Si estamos usando el Outlook o el Outlook Express, conviene desactivar la opción de pantalla Mostrar panel de vista previa que está en el menú Ver - Diseño.
- 6 ♦ Encriptemos los correos siempre que nos sea posible. Un correo no encriptado es como una postal, puede ser leído por cualquiera. Un correo encriptado es como una carta en un sobre y dentro de una caja fuerte.
- 7 ♦ Es importante poner títulos con sentido a los mensajes para que quien los reciba sepa que han sido enviados intencionadamente. Podemos comentar con nuestros contactos que debemos usar la línea del asunto del mensaje para así poder reconocer rápidamente que el mensaje procede de tal o cual persona. Cuando no la reconozcamos, es posible que estemos recibiendo un correo del spoofing o que un troyano haya enviado un

programa infectado a toda la lista de correos, incluida nuestra propia dirección. Atención: en los correos encriptados no debemos añadir en el título palabras que desvelen información sensible! Recordemos que la línea del asunto del mensaje no va encriptada nunca y que por tanto puede identificar la naturaleza del correo que hayamos encriptado, lo que nos haría más vulnerables a un ataque. Hoy en día existen muchos programas de espionaje que automáticamente escanean y copian mensajes con títulos como "interesante", "informe", "confidencial", "privado" y descriptores similares, que anuncian que el mensaje puede ser interesante.

8 ♦ NUNCA debemos enviar un mensaje a un grupo numeroso usando la línea del "Para" (destinatario/a(s)) o "CC" (con copia a). Cuando deseemos enviar algo a mucha gente, en la línea de "Para" copiaremos nuestra propia dirección y añadiremos las direcciones de los demás en la línea "CCO" (copia oculta a). (Para acceder a CCO es necesario ir a "Herramientas" y luego hacer clic en "Seleccionar destinatarios".) Esto no se hace sólo por cuestión de seguridad: es una cuestión de respeto a la privacidad: darle a otras personas la dirección de correo de alguien que no nos han autorizado a hacer tal cosa se considera una falta de educación, una falta de respeto y algo que nos puede dar un disgusto y poner en peligro.

9 ♦ NUNCA responder al spam, ni siquiera para pedir que nos borren de una lista. Los servidores de spam envían correos a listas interminables de direcciones y nunca saben cuáles están en uso. Cuando respondemos, el servidor nos reconoce como dirección válida y esto suele implicar que a partir de ese momento nos freirán a spam.

10 ♦ Si es posible, conviene tener un ordenador diferente, no conectado a ningún otro, para la recepción de correos y que no contenga archivos con datos.

11 ♦ Asimismo, podemos usar también dos direcciones sólo para nuestras comunicaciones internas (como con los dos números de teléfono para emergencias, y siguiendo las mismas reglas); o bien, una sola dirección que pueden consultar las personas de más confianza de la organización: los correos no tendrán que viajar varias veces (a varias personas) y sin embargo serán leídos por varias personas. Conviene recordar que cuantas más personas usen esa dirección, menos segura será. Es recomendable cambiar la dirección de vez en cuando.

La encriptación: preguntas y respuestas

A continuación respondemos a una lista de preguntas frecuentes. Podéis formular cualquier duda en la ONG Privaterra (www.privaterra.org).

P: ¿Qué es 'encriptar'?

R: Encriptar significa crear un código secreto para unos datos, para que nadie salvo quien deba recibir el mensaje pueda descifrarlo. Con tiempo y capacidad informática, todos los mensajes encriptados pueden descifrarse, pero hace falta

eso mismo: mucho tiempo y muchos recursos. Explicado de manera sencilla, encriptar es una forma de proteger nuestros archivos y correos de ojos que espían. Se traducen nuestros archivos a un código (un montón de números y letras aparentemente combinados al azar) que no tiene sentido para quien lo ve. Para encriptar un archivo, tenemos que "cerrarlo con llave", lo que se hace usando una clave. Para encriptar un mensaje podemos usar la criptografía asimétrica o de clave pública, que es la que usa dos claves, una pública y otra privada. Se cifra el mensaje con la clave pública pero sólo podrá descifrarlo la persona a la que va dirigido, que utilizará su clave privada.

P: ¿Por qué deberían encriptar información los grupos de derechos humanos?

R: Todo el mundo debería encriptar, porque la comunicación digital no es segura. No obstante, las personas que trabajan en derechos humanos corren más peligro que la mayoría de la gente, y sus archivos y comunicaciones contienen de hecho información confidencial; así pues, para protegerse y para proteger a las personas a las que intentan ayudar, es imperativo que encripten sus informaciones.

La tecnología digital es un beneficio para los grupos de derechos humanos, pues les facilita la comunicación, les hace ser más eficaces y les abre más puertas. No obstante, los beneficios no nos libran de los riesgos. Usar un cinturón de seguridad no implica necesariamente que vayamos a tener un accidente; conducir en una situación más peligrosa, como por ejemplo en una carrera, hace que usar un cinturón sea más necesario pues estamos corriendo más riesgos.

Las personas que trabajan en derechos humanos son vigiladas. Como los correos no encriptados pueden ser leídos por casi cualquiera, es casi inevitable que alguien vaya a leer nuestros correos no encriptados en algún momento. De hecho, es posible que nuestros oponentes ya estén leyendo nuestros correos y que no vayamos a enterarnos nunca. Conviene recordar que los oponentes de las personas a las que estamos intentando ayudar son también los nuestros.

P: ¿Es ilegal encriptar información?

R: A veces. En la mayoría de los países es perfectamente legal encriptar información. Sin embargo, existen excepciones. En China, por ejemplo, las organizaciones tienen que pedir un permiso para poder hacerlo, y si tu ordenador portátil dispone de tecnología para encriptar información, tienes que declararlo al entrar en el país. Singapur y Malasia tienen leyes que obligan a quienes encriptan información a desvelar sus claves a las autoridades. En India se están preparando leyes en ese sentido. Existen más excepciones.

En el Electronic Privacy Information Center (EPIC; centro para la privacidad de la información electrónica) podemos encontrar un estudio sobre las políticas de encriptación, el International Survey of Encryption Policy, en <http://www2.epic.org/reports/crypto2000/>, donde se examinan las leyes de casi todos los países. Actualizaron esta lista en el año 2000. Para solucionar dudas sobre si se puede o no usar la tecnología de encriptación en determinado país, podemos recurrir a Privaterra.

P: ¿Qué necesitamos para la seguridad de nuestros sistemas de tecnología de la información?

R: Depende de nuestro sistema y de nuestras actividades. No obstante, en general, deberíamos disponer de:

- Un cortafuegos (firewall).
- La posibilidad de encriptar nuestros discos.
- Un programa (como PGP - ver nota abajo) para encriptar y firmar digitalmente el correo electrónico.
- Software para la detección de virus.
- Copias de seguridad: podemos enviar por correo electrónico todos los materiales a un sitio seguro, además de hacer copias de seguridad semanales en un CD-RW (CD reescribible) que guardaremos en un lugar distinto y seguro.
- Claves de las que podamos acordarnos pero que no puedan ser adivinadas.
- Un sistema de acceso a nuestra información: no todo el mundo en la organización necesita tener acceso a todo tipo de información en nuestros archivos.
- Coherencia: no podemos usar unos recursos y otros no; isi no los usamos todos todo el tiempo, ninguno funcionará!

No obstante, tener el software adecuado no basta. **Normalmente, son las personas y no la tecnología nuestro punto más débil.** Encriptar información no sirve de nada si las personas no usan el recurso como debieran, si le dan sus claves a cualquiera, o las dejan a la vista, por ejemplo, en un post-it pegado a la pantalla del ordenador. El software para hacer copias de seguridad no sirve de nada (p.e., ante la eventualidad de un fuego o un ataque o redada) si no guardamos esas copias en un lugar diferente y seguro. La información confidencial tenemos que darla con cuentagotas (saber lo estrictamente necesario) y no contársela a todo el mundo en la oficina... por eso hay que crear jerarquías y protocolos. En general, es importante tener en cuenta los temas de privacidad y seguridad en cada cosa que hagamos en el día a día. A esto es a lo que llamamos "una sana paranoia".

P: ¿Cómo elijo el software para encriptar?

R: Normalmente, preguntando a las amistades; y podéis confirmarlo con nosotros. Tenemos que hablarlo con ciertas personas y grupos, así, si están usando determinado sistema para encriptar, podríamos elegir el mismo para facilitar nuestra comunicación. No obstante, conviene comprobar las cosas con otra fuente (p.e., nosotros): algunos paquetes de software no sirven para lo que están hechos y otros son "zanahorias". Las zanahorias nos atraen para que usemos un software gratuito y aparentemente excelente que de hecho nos está proporcionando gente que desea espiarnos. ¿Qué puede ser mejor para acceder a nuestras comunicaciones más sensibles que ser quienes están a cargo de super-

visar nuestro software de encriptación? De todos modos, existen muchas marcas buenas tanto de software que se compra como de freeware; lo único es que debemos examinarlo bien antes de usarlo.³

P: ¿Encriptar puede incrementar el riesgo de que caigan sobre nosotros/as?

R: Nadie sabrá que estamos usando un programa de encriptación a no ser que ya nos estuvieran vigilando. Si fuera así, ya habrían leído nuestra información privada, por lo que ya sabrían cómo descifrarlo todo; ya estarían sobre nosotros. Si quienes nos vigilan no van a poder leer nuestros correos, quizá deberíamos considerar qué otras medidas podríamos adoptar, por lo que cuando empecemos a encriptar debemos conocer bien a nuestras y nuestros compañeros, que llevemos con la máxima cautela el tema de las copias de seguridad y que sigamos todas las medidas de seguridad acordadas en la oficina.

(Nota: No disponemos de información de casos en los que el uso de software para encriptar haya causado problemas a las y los defensores. No obstante, debemos considerar esta posibilidad antes de empezar a encriptar, especialmente si nos encontramos en un país con un conflicto armado (la inteligencia militar podría sospechar que estamos pasando información importante desde el punto de vista militar) o si pocas organizaciones de defensoras o defensores usan la encriptación (podría atraer una atención no buscada).

P: ¿Por qué habría que encriptar documentos y correos todo el tiempo?

R: Si sólo encriptamos materiales sensibles, quienes nos estén vigilando o nuestros clientes sabrán cuándo la actividad es confidencial, y será más probable que caigan sobre nosotros entonces. Aunque la información encriptada no pueden leerla, sí pueden saber qué archivos están encriptados y cuáles no. Si de pronto hay una tanda de documentos encriptados, esto podría provocar un ataque o redada, por eso es mejor empezar a encriptar antes del comienzo de proyectos especiales. De hecho, lo óptimo es que la comunicación sea regular: podemos enviar correos encriptados regularmente aunque no haya nada nuevo que comunicar; de este modo, cuando tengamos que enviar información sensible, no se notará tanto.

P: Si tenemos un cortafuegos (firewall), ¿por qué habría que encriptar los correos?

R: Los cortafuegos evitan que los hackers accedan a nuestro disco duro y a nuestra red; sin embargo, cuando enviamos un correo a Internet, éste queda expuesto al mundo entero. Por tanto, habría que protegerlos.

P: No ha entrado nadie en la oficina, ¿por qué habría de usar software de privacidad?

R: No sabemos si estarán entrando en nuestro sistema o sacando información de él. Sin comunicación encriptada, seguridad física o protocolos de privacidad,

³ Por ejemplo, el PGP (Pretty Good Privacy; privacidad bastante buena) es un programa bastante conocido y seguro. Su finalidad es proteger la información enviada por Internet usando la criptografía de clave pública, y también se usa para autenticar documentos con firmas digitales. Se puede bajar de <http://www.pgpi.org/>.

cualquiera podría estar accediendo a nuestros archivos, leyendo nuestros correos, y manipulando nuestros documentos sin que lo sepamos. Si nuestra comunicación es abierta podríamos estar poniendo a otras personas en peligro allí donde los ataques o redadas de motivación política ocurren con más probabilidad. Si usamos buenos cerrojos en las puertas, deberíamos encriptar nuestros archivos; es así de simple.

P: No tenemos acceso a Internet y tenemos que ir a un ciber café. ¿Cómo podemos proteger nuestras comunicaciones si utilizamos un ordenador de fuera?

R: A pesar de eso, podemos encriptar los correos y nuestros archivos. Antes de ir al ciber, encriptaremos todos los archivos que vayamos a enviar por correo electrónico y copiaremos la versión encriptada en el CD o disquete. En el ciber, nos registraremos en un servicio de encriptación de correo electrónico, como el de www.hushmail.com, o en un servicio de anónimos, como www.anonymizer.com, y enviaremos nuestros correos desde allí. Recordatorio: quienes reciben estos correos deben ser también usuarias o usuarios de este servicio.

P: Si es tan importante proteger nuestros archivos y nuestras comunicaciones, ¿por qué no lo hace todo el mundo?

R: Esta tecnología es bastante nueva. Aun así, su uso se está popularizando. Los bancos, las multinacionales, las agencias de noticias y los gobiernos lo encriptan todo: lo ven como una inversión sensata y uno de los precios de poder hacer negocios. Las ONGs corren riesgos más graves que las compañías pues a estas últimas las reciben con los brazos abiertos casi todos los gobiernos. Una ONG, con toda probabilidad, será objeto de vigilancia, por lo que las ONGs tienen que ser capaces de poner la tecnología a su servicio. Además, quienes defienden los derechos humanos se preocupan por proteger a personas y grupos que están siendo perseguidos. Para hacerlo, guardan bien los archivos que pueden identificar y localizar a esas personas. Si resulta que se puede tener acceso a esos archivos, estas personas pueden ser asesinadas, torturadas, secuestradas o se las podría "convencer" de que no vuelvan por la ONG en cuestión. La información de estos archivos puede ser también utilizada como prueba contra la ONG y sus clientes en persecuciones políticas.

P: Uno de nuestros principios es la transparencia. Nuestro trabajo incluye presionar al gobierno para que sea también más transparente en sus actuaciones. ¿Por qué tenemos que usar una tecnología de la privacidad?

R: El respeto a la privacidad es coherente con el ser abiertas/os. Si el gobierno desea pedirnos abiertamente nuestros archivos, puede hacerlo, siguiendo procedimientos adecuados y conocidos. Lo que la tecnología de la privacidad evita es que puedan acceder a nuestra información de manera clandestina.

P: Seguimos todos los protocolos de seguridad y privacidad y aun así se filtra información, ¿qué está pasando?

R: Podríamos tener una o un infiltrado en la organización o sencillamente a alguien incapaz de entender que una información sea confidencial. Trabajaremos la jerarquía creada para el tratamiento de la información para conseguir que

menos personas tengan acceso a la información más sensible y vigilaremos estrechamente a esas pocas personas. Las grandes compañías y organizaciones distribuyen cada cierto tiempo, como parte de su trabajo habitual, fragmentos de información falsa a personas concretas que van variando. Si esta información falsa se filtra, la fuente puede ser localizada de inmediato pues sabemos a quién le dimos tal o cual información.

Lo que podemos y no podemos hacer al usar la encriptación

- **SÍ** encriptarlo todo, todo el tiempo. Si sólo encriptamos material confidencial, quien nos esté vigilando el correo sabrá cuándo algo importante va a ocurrir. El que de pronto haya muchos documentos encriptados cuando no suele haberlos puede provocar un ataque o redada.
- **NO** poner información clave en los títulos de los correos. Aunque el mensaje vaya encriptado, la línea del asunto del mensaje no suele ir encriptada.
- **SÍ** utilizar una clave hecha con letras, números, espacios y puntuación que sólo tú puedes recordar. Algunas técnicas para crear claves seguras son trazar dibujos en el teclado o elegir palabras al azar intercalando símbolos. Por lo general, cuanto más larga sea, más segura será.
- **NO** usar una sola palabra o nombre, una frase conocida o una dirección de nuestro listín de direcciones como clave. Las descifran en cuestión de minutos.
- **SÍ** hacer una copia de seguridad de la clave privada (el archivo que contiene nuestra clave privada para encriptar) y guardar, encriptada, en un solo sitio seguro y diferente, como un disquete o en una memoria USB, pequeña y extraíble.
- **NO** enviar material sensible a alguien sólo porque esa persona nos ha enviado un correo encriptado usando un nombre que podemos reconocer. Cualquiera puede imitar un nombre (spoofing) haciendo que su dirección de correo se parezca a la de alguien que conocemos. Siempre hay que verificar la identidad de la fuente antes de confiar en ella: la comprobaremos comunicándonos en persona, haciendo una llamada telefónica o enviando otro correo.
- **SÍ** enseñar a otras personas a encriptar. Cuanta más gente lo use, más seguras y seguros estaremos todos.
- **NO** olvidar firmar el mensaje además de encriptarlo. Queremos que la destinataria o el destinatario sepa si nuestro mensaje ha sido modificado en su tránsito.
- **SÍ** encriptar archivos que se envíen como adjuntos por separado. Por regla general, no se encriptan automáticamente cuando enviamos un correo encriptado.

Gestión más segura de la oficina

El tema de la seguridad en la oficina tiene relación con nuestras costumbres, que pueden ser útiles para nuestra seguridad o peligrosas. Para desarrollar costumbres útiles, tenemos que entender las razones que hay detrás. Hemos elaborado una lista de hábitos que pueden ayudarnos a gestionar la información de una manera más segura. Pero esto sólo ocurrirá si desarrollamos esas rutinas y conocemos su importancia.

¿Qué es lo más importante para la privacidad y la seguridad en la gestión de la oficina?

- Ser conscientes de qué información tenemos y de quién tiene acceso a ella
- Desarrollar rutinas de seguridad y utilizarlas siempre
- Usar las herramientas adecuadamente

Administración

Muchas organizaciones tienen una persona a cargo de la administración de sistemas, o alguien con la responsabilidad y función administrativa de acceder al correo, a los ordenadores en red, y de supervisar la instalación del nuevo software. Si alguien abandona la organización o no está disponible, esta persona puede entonces acceder a la información y asuntos pendientes de quien se ha ido, dando así continuidad y evitando que el trabajo quede a medias o interrumpido. Además, es alguien que se encarga de que todo el software esté limpio y proceda de una fuente acreditada.

El problema radica en que algunas organizaciones piensan que este papel es meramente de apoyo técnico y permiten que una tercera parte se encargue de este trabajo. Este administrador o administradora controlaría de hecho toda la información de la organización, por lo que tendría que ser alguien que disfrute de total confianza en la organización. En algunas organizaciones las labores de administración las comparten la persona que representa a la organización y otra persona de confianza.

Algunas organizaciones recogen en un documento todas las claves privadas PGP, las encriptan y las guardan en un lugar seguro y distinto (una organización de su confianza). Esto evita problemas si a alguien se le olvida su contraseña o pierden su clave privada. No obstante, el lugar donde se guarden esos archivos tiene que ser un sitio totalmente seguro y confiable, y se deben crear protocolos concretos y exhaustivos respecto al acceso a esos archivos.

Las reglas:

- 1 ♦ NUNCA poner la administración de nuestros sistemas en manos de terceras partes. No solo no merecen la confianza que podamos darle a gente de nuestra organización; sino que puede ser difícil ponerse en contacto con ellas si se produce una emergencia.

- 2 ♦ Sólo las personas más fiables deberían tener acceso a la administración de nuestros sistemas.
- 3 ♦ Hay que determinar a cuánta información puede acceder quien(es) asuma(n) la administración: acceso a todos los ordenadores, a sus claves, a las claves de acceso, a las carpetas protegidas y a las claves del uso de PGP, etc.
- 4 ♦ Si decidimos guardar una copia de las claves y de las claves privadas de PGP en otra organización, tendríamos que desarrollar protocolos de acceso a las mismas.
- 5 ♦ Cuando alguien se marche de la organización, será preciso cambiar de inmediato sus claves y códigos de acceso.
- 6 ♦ Cuando alguien de la administración deje la organización, será preciso cambiar de inmediato TODAS las claves y códigos de acceso.

Administración del software

Usar programas piratas puede hacer que la organización quede vulnerable a lo que llamamos "la policía del software". Las autoridades pueden caer sobre una organización que use software ilegal, imponiéndola el pago de multas ingentes e incluso cerrándola. La organización en cuestión no recibirá apoyo de los medios de comunicación occidentales porque esto no se verá como un ataque a una ONG de derechos humanos, sino como una actuación contra la piratería. Debemos tener muchísimo cuidado con el tema de las licencias del software, y no permitir que nadie haga copias de cualquier cosa en la oficina. El software pirata es inseguro también porque contiene virus. Hay que usar siempre un antivirus cuando estemos instalando software.

Quien esté a cargo de la administración tendrá que supervisar la instalación de cualquier programa nuevo, para que podamos comprobar que todo está bien antes de hacerlo. No debemos autorizar la instalación de programas potencialmente inseguros, y sólo debemos instalar los programas que necesitemos utilizar.

Es preciso instalar los últimos parches de seguridad que tengan todos los programas que utilicemos, en especial del Microsoft Office, del Microsoft Internet Explorer y el Netscape. La más grave amenaza a nuestra seguridad procede del software y del hardware que ya tienen puntos débiles conocidos. Mejor aún, podríamos considerar pasarnos al software libre que no se rige por el modelo "seguridad a través de la oscuridad", sino que anima tanto a las y los expertos en seguridad como a las y los hackers a que sometan todos sus códigos a un riguroso examen. Usar el software libre y cualquier software que no sea el de Microsoft tiene el beneficio añadido de hacernos menos vulnerables a los virus más comunes y a los hackers que no tienen un objetivo específico. Se crean menos virus para los sistemas operativos de Linux o Macintosh porque casi todo el mundo usa Windows. Outlook es el programa de correo más utilizado, y por lo tanto, el objetivo más común para los hackers.

Hábitos con el correo electrónico

Deberíamos desarrollar la costumbre de encriptar los correos. Es más fácil acordarnos de encriptarlo todo que tener una política sobre qué se encripta y qué no. No debemos olvidar que si encriptamos siempre nuestros correos, quien lo esté vigilando nunca sabrá cuando nuestras comunicaciones son más importantes o sensibles.

Unos cuantos puntos importantes más:

- ❑ Si guardamos una copia de un correo encriptado, la copia debe estar encriptada también. Siempre la podemos desencriptar después; sin embargo, si alguien accede a nuestro ordenador y no lo hemos hecho, la información sería tan vulnerable como si nunca la hubiéramos encriptado.
- ❑ Debemos perseverar en nuestro esfuerzo por asegurarnos de que nadie con quien nos comuniquemos usando correos encriptados se dedique a reenviarlos después de desencriptarlos, o a respondernos sin molestarse en encriptar su propio correo. La pereza individual es la más grave amenaza a nuestras comunicaciones.
- ❑ Podría ser útil crear varias cuentas seguras para gente que esté en misiones de campo, cuentas que al no tan utilizadas, no serían tan fácilmente identificadas por los servidores de spam. Estas direcciones deberían ser verificadas regularmente, pero no utilizadas, salvo por quienes estén en la misión de campo. De esta manera podríamos destruir las direcciones de correo que están recibiendo mucho spam sin poner en peligro nuestra base de contactos.

Consejos generales para ciber cafés y similares

Los correos que enviamos por Internet en texto sin formato y sin encriptar pueden ser leídos por muchas partes diferentes, si se lo proponen. Una de estas partes puede ser nuestro servidor (Internet Service Provider, ISP) pero también podría hacerlo cualquier servidor por el que pasen nuestros correos. Un correo pasa por muchos servidores en su viaje de remitente a destinatario/a, ignorando las fronteras geopolíticas. Puede pasar por servidores de otro país cuando estamos enviando un correo dentro del país.

Unos consejos generales sobre temas que normalmente no entienden bien las y los usuarios de Internet:

- ❑ Proteger un archivo con una contraseña hace tan poco para proteger ese archivo que no merece la pena hacerlo con documentos que contienen información confidencial. Sólo da una falsa sensación de seguridad.
- ❑ Comprimir un archivo no lo protege.
- ❑ Si queremos enviar un archivo o un correo protegiéndolo, tenemos que encriptarlo (ver www.privatterra.com).

- Si queremos enviar un correo o un documento de forma segura, tenemos que encriptarlo todo en todas las fases del proceso hasta la recepción final. No sirve de nada enviar un correo encriptado, por ejemplo, desde un proyecto de campo a la oficina de Nueva York o Londres o donde sea, y después que se reenvíe ese correo desde ésta isin encriptar!
- Internet es global por naturaleza: no existe ninguna diferencia entre enviar un correo entre de una oficina a otra en Manhattan y enviar un correo desde un ciber café de Sudáfrica al ordenador de una oficina de Londres.
- Debemos encriptar tanto como nos sea posible, incluso si el correo o los datos **no** son confidenciales.
- Debemos comprobar que el ordenador que estamos usando dispone de un programa de protección de los virus. Muchos virus se diseñan para extraer información de nuestro ordenador, ya sea de nuestro disco duro o de los archivos de nuestro correo electrónico, lo que incluye además nuestro listín de direcciones.
- Debemos comprobar que nuestro software tiene todas las permisos que debe tener. Si estamos usando software sin licencias de ningún tipo, de manera inmediata, a ojos de los gobiernos y los medios de comunicación, pasamos a ser piratas y dejamos de ser activistas de derechos humanos. La mejor opción es la de usar software libre (ies gratis!).
- No hay una solución segura al 100% si estamos usando Internet. Hay que ser conscientes de que una persona puede entrar ilegalmente en un sistema haciendo que es alguien que no es, por teléfono o por correo electrónico. Debemos usar nuestro criterio y sentido común en todo momento.
- Debemos recordar que los interesados en nuestro trabajo no han necesitado esperar a las nuevas tecnologías para tratar de obtener información sobre nosotros.

Resumen

Recordar que las partes interesadas en nuestro trabajo no han esperado a las tecnologías para intentar conseguir información sobre nosotras o nosotros.

Muchas personas dedicadas a la defensa de los derechos humanos son reticentes a usar tecnologías de la información seguras; sin embargo, los procedimientos básicos para poder hacerlo son sencillos.

Esos procedimientos mínimos y sencillos son: discreción por teléfono y en la comunicación en persona, usar PGP en la comunicación por correo electrónico y con los archivos confidenciales, y las contraseñas para acceder a nuestros ordenadores.

No obstante, tener el software adecuado no lo es todo: **nuestro punto débil son normalmente las personas, no la tecnología.**