¡Pongámonos las Pilas! Reflexiones y acciones concretas para asegurar la información en nuestras organizaciones sociales

Carolina Flores Hine
(con el apoyo y conocimiento de compañeros y compañeras de organizaciones sociales centroamericanas)

Flores Hine, Carolina ¡Pongámonos las Pilas! Reflexiones y acciones concretas para asegurar la información en nuestras organizaciones sociales.

2a. ed. Ciudad de México, México. 2009.

1. Seguridad de la Información

2. Nuevas Tecnologías

3. Política de Seguridad para Organizaciones Sociales

4. América Central

5. Derechos Humanos

6. Software Libre

Ilustraciones: Luis Enrique Gutiérrez

Diseño: Luis Enrique Gutiérrez

http://piensalibre.net caro@piensalibre.net

Los contenidos de esta publicación se desarrollaron con el apoyo de:

Fundación Acceso, Pablo Zavala y Arturo Chub de SEDEM, Markus Erb de SIMAS, Paul Menchú y Gamaliel Folgar de la Fundación Rigoberta Menchú Tum, Brenner Barrios del Centro de Acción Legal en Derechos Humanos, Giovanni Peruch de la Fundación de Antropología Forense de Guatemala, Byron Sandoval de la Fundación Myrna Mack, Jesús Laynes de Enlace Quiché y Jeffrey Esquivel de ABAX Asesores. En ella se integra además el valiosísimo aporte de las organizaciones sociales de Costa Rica, Nicaragua, Honduras, El Salvador y Guatemala que participaron en el taller: "Sensibilización y evaluación de riesgo para el manejo seguro de la información" (que por seguridad no mencionaremos pero a las cuales, enviamos nuestro agradecimiento). A la Fundación Friedrich Ebert en Guatemala, muchas gracias por brindarnos el espacio para el taller de capacitación técnica. Un agradecimiento especial a Robert Guerra de Privaterra, Dmitri Vitaliev de Tactical Technology y a Raquel Chacón de HIVOS por su colaboración para la seguridad de la información en Centroamérica .

Índice

Presentación

El programa "Medios, Información y Comunicación para el Desarrollo" de HIVOS promueve el libre flujo de información y la creación de espacios democráticos para el debate y la participación política. Dentro de estos espacios democráticos, la Internet y los teléfonos celulares se han constituido en vías privilegiadas para el flujo de información, la coordinación y para las convocatorias a la participación. A su vez, las nuevas herramientas han facilitado enormemente las labores de archivo y disposición ágil de los datos.

Esto sin embargo, ha generado nuevas necesidades en cuanto a la seguridad informática. ¿Qué tan libre es el flujo de información? ¿Qué tantos insumos de una organización son vulnerables a ser interceptados? ¿Hay una conciencia real en las organizaciones acerca de la importancia de manejar apropiadamente su información?

Estas y otras preocupaciones motivaron a HIVOS a convocar al "Taller Centroamericano Ampliando la Libertad de Expresión: Herramientas para la colaboración, información y comunicación seguras", realizado del 28 al 31 de agosto de 2006 en Antigua, Guatemala. Tiempo después, HIVOS financió el proyecto de seguimiento a ese taller para saber cuáles de las organizaciones participantes estaban haciendo uso de las herramientas que se conocieron y para dar un mejor impulso a la incorporación de medidas de seguridad de la información entre sus organizaciones contrapartes trabajando en derechos humanos. Fundación Acceso de Costa Rica fue la organización coordinadora de ese seguimiento, trabajando en alianza con SIMAS (Servicio de Información Mesoamericana sobre Agricultura Sostenible) de Nicaragua y consultando técnicamente con SEDEM (Asociación para el Estudio y la Promoción de la Seguridad en Democracia) de Guatemala.

Es así como en el año 2007 desde Fundación Acceso, se reinició el contacto con las organizaciones participantes en el proceso anterior y en el año 2008, se realizaron talleres regionales con las contrapartes que acudieron al llamado y con organizaciones invitadas. Posteriormente, se conformó un grupo de técnicos informáticos de toda la región centroamericana que participó en un taller y contribuyó enormemente con sus aportes para la presente publicación.

Como fase final de dicho proyecto, se publicó la primera edición de este folleto, el cual tiene como objetivo, abrir espacios de discusión sobre la seguridad dentro de nuestros ámbitos de trabajo y preparar mejor el terreno para la implementación de medidas que disminuyan los riesgos y nos permitan proteger a nuestros compañeros y compañeras, así como a las poblaciones que han puesto su información bajo nuestro cuidado.

Es importante destacar, que el folleto que usted tiene en sus manos no es un manual de instrucciones para usar herramientas informáticas específicas. Hemos concebido esta publicación como la puerta de entrada a la creación de una política interna de seguridad en las organizaciones sociales. Muchas de las herramientas informáticas necesarias para apoyar esta política pueden encontrarse en la compilación Llave en Mano para ONG (NGO in a Box) edición de seguridad, elaborada por los compañeros de Tactical Technology y Front Line Defenders[1]

En esta segunda edición se han incorporado pocos, pero importantes cambios. Los conocimientos sobre las mejores formas de protegernos y sobre los errores que nos ponen en riesgo, crecen constantemente y fue necesario clarificar algunos asuntos. Conforme vayan cambiando las herramientas, el contexto y los riesgos, esperamos ir incorporando más cambios a la presente edición.

1 http://security.ngoinabox.org/html/sp/content.html

Quienes trabajamos en organizaciones sociales centroamericanas hemos visto enormes cambios en las últimas décadas. La mayor parte de ellos se relacionan con los avances tecnológicos, las transformaciones en los sistemas políticos y la globalización del sistema capitalista.

En poco tiempo hemos pasado de almacenar los documentos en carpetas de cartón, guardarlas en enormes archivadores con etiquetas adhesivas y de enviar informes por correo postal o encomienda, a almacenar grandes cantidades de información en carpetas virtuales en nuestras computadoras y a enviar documentos en formatos electrónicos.

Este cambio ha abierto una nueva brecha entre las poblaciones con acceso y capacitación para el uso de la Internet y quienes no tienen acceso a este recurso de comunicación e interacción, pero también ha posibilitado que construyamos redes más amplias con personas que trabajan temas comunes, ha abierto canales de comunicación con otros países y ha agilizado las comunicaciones en los niveles interno y externo de nuestras organizaciones.

Sin embargo, si vemos con detenimiento esos pasos, hemos dado un salto desde los tiempos en que manteníamos nuestros archivadores asegurados bajo llave en nuestras oficinas(donde el

riesgo de robo, fuego o pérdida lo minimizábamos con puertas, candados, cajas de seguridad o duplicados en fotocopias) hasta el día de hoy, en el que las computadoras almacenan grandes cantidades de datos, transportamos carpetas enteras de trabajos en nuestras memorias portátiles [2], enviamos la información por correo electrónico o almacenamos en servidores ubicados en nuestras oficinas, el fruto del esfuerzo de varios años de labores. La pregunta que nos corresponde hacer ahora es ¿qué pasó con las llaves de los archivadores? ¿dónde están los candados? ¿cómo estamos asegurando nuestra información privada?

Aún en nuestros países, donde las cifras de acceso a la Internet son considerablemente bajas, el uso del correo electrónico ha comenzado a sustituir el correo postal hasta alcanzar niveles sorprendentes. Por ejemplo en Nicaragua, donde la penetración de Internet es de un 2.7% [3](el nivel más bajo de la región), *"los envíos de paquetes y correspondencia a través de Correos de Nicaragua han registrado una drástica reducción desde el año 2000. Informes de la empresa muestran que en ese año, los envíos ascendían a 1 millón 441 mil paquetes, destinados a diferentes partes del mundo. Sin embargo, desde el 2005 se ha empezado a percibir un descenso del 61 por ciento, que implican 877 mil envíos menos"* [4].

Es evidente, nos estamos comunicando y estamos enviando nuestra información por medio del correo electrónico. Esto nos brinda mayor agilidad, más rapidez de respuesta, nos puede ahorrar costos, nos permite crear redes amplias de cooperación y solidaridad e incluso, fortalecer la incidencia de nuestras denuncias; sin embargo ¿cuáles son las diferencias con el correo postal? ¿cuáles son las desventajas? y sobre todo ¿cómo podemos disminuir las desventajas y proteger mejor nuestra privacidad?

---

2 Llamadas más comúnmente llaves usb, llaves maya etcétera.

3 http://www.internetworldstats.com/stats10.htm#spanish

4 http://impreso.elnuevodiario.com.ni/2006/10/19/nacionales/31751

En tiempos de paz, guerra de información

En muchos de nuestros países, en contextos de guerra, quienes tenían información valiosa creaban códigos secretos o escondían porciones de papeles repartidos entre varias personas. De esta manera, disminuían la posibilidad de que se conociera cuáles eran sus movimientos, quiénes integraban los grupos organizados y muchos otros datos. Es comprensible que en el momento en que desaparecen los conflictos armados ese conocimiento sobre el cuidado de cierta información haya quedado en desuso pero es posible que ahora estemos en el otro extremo y que estemos compartiendo nuestra información privada y valiosa de formas riesgosas.

Actualmente, se esperaría que haya un estado de paz marcado por la democracia, las negociaciones políticas, el razonamiento y el uso de recursos no violentos. Sin embargo, como expone el psicólogo Rubén Benedicto, si observamos los manuales y la doctrina militar "*... veremos que los profesionales de la guerra han diluido las fronteras entre la paz y la guerra, lo civil y lo militar, y que operan en consecuencia*" [5] de manera que cuando "*existe una alta posibilidad de actitudes de oposición social interna contrarias a la implementación de las medidas necesarias para el control de la población tales como el control de comunicaciones, suspensión de garantías individuales, necesaria violación a derechos humanos para la conservación de un bien prioritario, la seguridad... Esas oposiciones internas serán también consideradas como enemigo a batir*" (Ídem).

5 Benedicto, R. "Guerra de Información en el Referéndum sobre el Tratado de Libre Comercio en Costa Rica: un Análisis Psicosocial Crítico desde la Observación Electoral". http://www.liber-accion.org (biblioteca virtual).

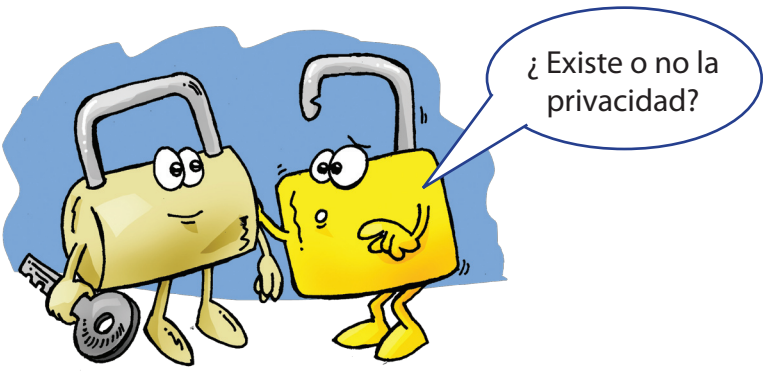
Los cambios en las legislaciones estadounidenses (como la "Patriot Act") que se han realizado a partir de los atentados del 11 de septiembre del 2001, han restringido muchas libertades y han abierto posibilidades de acceso a la información privada y de vigilancia a los ciudadanos y ciudadanas en todos los ámbitos. Estos cambios han tenido repercusiones en distintos procesos regulatorios en toda la región centroamericana.

Las organizaciones sociales de nuestra región, comprometidas con el respeto por los derechos humanos, los derechos civiles y la crítica a las contradicciones del sistema capitalista, manejamos información que es muy valiosa y estratégica para algunos grupos con mucho poder económico y político. Pensemos en esto: si usted fuera el o la gerente de una compañía minera y todos los días debe lidiar con movimientos sociales de resistencia (grupos ecologistas, población desplazada, sindicatos, etcétera) ¿es posible que quiera saber quiénes son los líderes de esos movimientos? ¿le serviría conocer dónde viven y con quiénes se reúnen? ¿le gustaría saber qué acciones están planificando? ¿necesita saber cómo obtienen el financiamiento para sus actividades?

Entonces, no se trata de exageraciones. La información acerca de la vida personal de quienes trabajan para la organización, con quiénes se reúnen, quién apoya el trabajo, cuál es su posición frente a la realidad nacional, cuáles son sus bases políticas o sus estrategias de acción, se puede obtener por medios electrónicos o por descuido en la seguridad de los correos, los teléfonos celulares o las bases de datos.

Incluso, asuntos que consideramos sin importancia, como los hábitos de consumo y las rutinas del personal abren espacios de riesgo.

Por otra parte, nuestro trabajo cotidiano no se realiza en abstracto. Además de la información de nuestro personal, las organizaciones manejamos datos e información delicada de otras organizaciones, de la gente con la que desarrollamos los proyectos, de todas esas personas que confían en nosotros y nosotras. ¿Qué tanto cuidado le estamos dando a esa información? Y lo que es más importante ¿estamos poniendo en riesgo a esa misma gente que apoyamos y por la cual, existimos como organización?



En Centroamérica, aunque los casos no se difunden apropiadamente, es evidente que la libertad de expresión y asociación se ha venido debilitando a partir del recrudecimiento de la represión y el espionaje en el ámbito internacional. Las comunicaciones electrónicas, si no se protegen, son el espacio idóneo para que esto suceda.

Como se denunció en el año 2005, en la región existen empresas privadas que venden los datos privados de las personas a compañías extranjeras. Estas compañías a su vez pueden vender esos datos a los gobiernos de los países, sin que se investigue de dónde obtienen la información.

Por otra parte, los allanamientos y robos en los que "casualmente" sólo se roban las computadoras, son cada día más comunes en nuestro contexto. Si la información dentro de esos equipos estuviera cifrada [6] , los "ladrones" no lograrían su objetivo.

Además, se han dado varios casos en donde la estrategia para dañar a una organización se centra en sus correos electrónicos. Las contraseñas compartidas o inseguras pueden ser obtenidas fácilmente para tener acceso a las cuentas de correo, pero también, es posible suplantar una dirección institucional y enviar comunicaciones que afecten las relaciones con otros actores importantes.

En nuestros países, en algunos casos el propio gobierno está realizando espionaje a las organizaciones sociales, con el argumento de Seguridad Nacional. En el año 2007, la Asociación para el Estudio y la Promoción de la Seguridad en Democracia (SEDEM) envió una alerta a los medios guatemaltecos por algunas acciones de espionaje gubernamental a las organizaciones políticas, empresariales y sociales. Como se publicó en CERIGUA (Centro de Reportes Informativos sobre Guatemala, medio de comunicación que ha sido intervenido también) *"en menos de siete días el Ejecutivo señaló que las organizaciones defensoras del medio ambiente son una amenaza a la gobernabilidad y las vinculó con grupos del crimen organizado".* [7]

6 El proceso de cifrado (llamado también "encriptación") en este caso consiste en utilizar una herramienta informática con la que podemos proteger los documentos usando una contraseña segura. Si se tiene acceso a la información pero no a la contraseña de protección, los datos visibles son incomprensibles.

7 http://www.cerigua.org/portal/Article7608.html

En este contexto, la seguridad de la información se convierte en una necesidad urgente para las organizaciones sociales que luchan por el respeto a los derechos humanos, porque en este momento, apoyar a los campesinos y campesinas, a las personas portadoras del VIH; dedicarse a investigar los crímenes de guerra y a combatir la impunidad; coordinar movimientos de resistencia frente al capitalismo, la sociedad patriarcal y la inequidad socioeconómica; denunciar y trabajar con las comunidades en las que se está destruyendo el medio ambiente; luchar por reivindicar los derechos de las mujeres; en fin, defender nuestros derechos y hacer resistencia al sistema imperante constituye una ocupación riesgosa y vulnerable. La opción no es desistir, porque esas mismas razones que nos ponen en riesgo son las que nos mueven a seguir trabajando fuertemente. La opción es mejorar la forma en la que nos comunicamos y compartimos nuestros conocimientos, buscar formas de trabajo más seguras para nosotros y nosotras, y para la gente que confía en nuestras organizaciones. Conociendo e implementando algunas estrategias sencillas, podemos iniciar ese camino.

Algunas verdades incómodas

Un correo electrónico sin cifrar es una tarjeta postal

Vamos a ir mirando en este documento, cómo el correo electrónico no se parece en mucho a las cartas que enviábamos metidas dentro de un sobre de papel. Pensemos por ejemplo: ¿cuántas copias quedaban almacenadas en nuestros escritorios cuando enviábamos una carta escrita a mano?

Entonces, pasamos de escribir a mano o a máquina (copiando con papel carbón) a escribir nuestras cartas en computadoras que pueden guardar múltiples copias. Ahora enviamos una de esas cartas por correo electrónico y queda una copia en la computadora, una en los correos enviados, una en el buzón de la persona destinataria. Y en el camino ¿cuántas copias quedan?
Desde el punto de vista del derecho informático: *"si el correo tradicional tuviese la misma característica, desde el momento en que una persona deposita una carta en el buzón, copias de la misma estarían no solo en poder del servicio postal sino también de un infinito número de personas en todo el mundo".* [8]

8 Barrera y Montague. Recreando privacidad en el ciberespacio. http://www.alfa-redi.org/rdi¬articulo.shtml?x=345

¿Qué pasa cuando enviamos un correo electrónico? ¿cuál es la ruta que sigue?

Los buzones de las cuentas de correo están almacenados en servidores de correo. Para enviar un correo electrónico se requiere de un servidor SMTP (que significa Protocolo Simple de Transferencia de Correos) que permite que dos servidores se intercambien mensajes. Para recibir los mensajes se necesita un servidor POP (Protocolo de Oficina de Correos) o un IMAP (Protocolo de Acceso a Mensajes de Internet) que permiten que la persona usuaria tenga acceso a los correos recibidos.

De todo eso, es importante comprender que los correos se almacenan en servidores y que para tener acceso a ellos, necesitamos de un "cliente" que ejecutamos desde nuestra computadora (como el Mozilla Thunderbird, Evolution o el Microsoft Outlook) o de un "cliente" que ejecutamos usando la web (como el Gmail, Hotmail, Yahoo, SquirrelMail etcétera).

También es importante saber que los correos pasan de un servidor a otro en varias direcciones y que esos datos en la mayoría de los casos viajan abiertos, es decir, son mensajes que viajan sin ningún tipo de protección. Eso significa, que en caso de que alguien intercepte nuestras comunicaciones, todo lo que hemos enviado por esa vía puede ser leído sin problema.

¿Cómo se pueden proteger esos datos? La respuesta es: cifrando y usando firmas digitales que certifican nuestra identidad. En nuestro caso, usando alguna herramienta informática que cifra y descifra la información para que sólo pueda ser leída por la persona a la que va dirigida y que además firme digitalmente y verifique firmas para garantizar que el remitente es quien dice ser.

Para poder habilitar el cifrado y firmado digital es necesario que instalemos una aplicación y que la configuremos para nuestro uso. Después de eso, es cuestión de acostumbrarnos a proteger nuestra información. Esta aplicación además nos permitirá almacenar archivos protegidos.

Vamos a regresar al ejemplo del correo postal, para aclarar el asunto de la protección de los correos:

Un correo electrónico sin cifrar es como una tarjeta postal:
cuando pasa de mano en mano (de servidor a servidor) quien tenga acceso a la postal, puede leer lo que está escrito en ella, incluso una vez que el mensaje llega al servidor de entrega (lo que podría ser el cartero o quien nos atienda en el mostrador de la oficina postal).

Entonces, si usamos un correo gratuito, estamos usando la "oficina postal" de otras personas. Si por el contrario, nuestra organización tiene una cuenta institucional de correo electrónico, lo más probable es que estemos usando una "oficina postal" propia (por ejemplo, si estamos pagando por un espacio de hospedaje o *hosting* en algún servidor de un proveedor de servicios). ¿Es más seguro tener una "oficina postal" propia? Sí y no. Los datos que almacenamos en los servidores que alquilamos, deben ser cifrados para que realmente estén protegidos. De otra manera, sería como si alquiláramos un espacio en un edificio, colocáramos nuestra propia oficina postal y dejáramos las puertas sin llave.

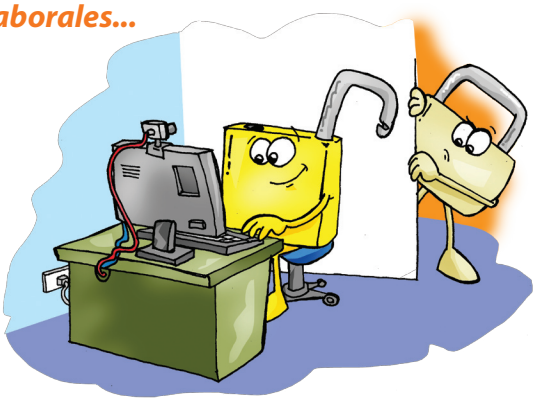
Se hace camino al andar (y se guardan "cookies" al navegar)

Entonces, ya vimos que si enviamos nuestros correos electrónicos sin protección, éstos pueden ser leídos. Vimos también que los buzones de correo electrónico están almacenados fuera de nuestras computadoras (en servidores de servicio gratuito, en servidores alquilados por nuestra organización, etcétera) y que si no usamos herramientas de seguridad, esos datos son legibles por cualquier persona que tenga acceso a ellos.

Lamentablemente, no tenemos mejores noticias acerca de la navegación en la Internet. Cada vez que ingresamos a un sitio web se guarda información en archivos llamados cookies (que significa galletas en idioma inglés), que son archivos que se guardan en nuestras computadoras y permiten registrar nuestras comunicaciones, de manera que cuando navegamos en la Internet y saltamos de un sitio a otro, nuestras huellas quedan almacenadas y es posible reconstruir por completo la ruta que hemos recorrido.

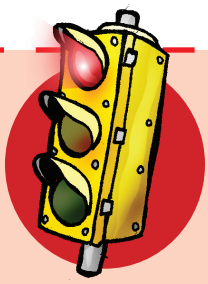
Probablemente, cuando pensamos en los sitios web que hemos visitado en los últimos dos días, pensemos que no hay nada ahí que pueda preocuparnos...

Más allá de que alguien sepa que visitamos el Hi-5 en horas laborales...



... pero ya que hablamos del Hi-5 pensemos en cuánta de nuestra información personal podemos encontrar en la Internet. Con sólo poner nuestro nombre en un buscador o con tener un perfil en sitios como Hi-5 o Facebook es posible encontrar muchos de los datos que consideramos personales. Sin embargo, eso es sólo lo visible: los bancos, las aseguradoras, las empresas encuestadoras, los médicos, abogados, psicólogos, sacerdotes, todos ellos manejan información que consideramos privada.

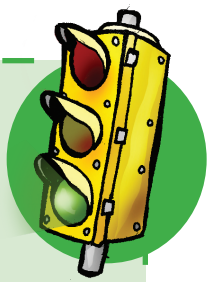
Los compañeros y las compañeras de organizaciones sociales participantes en los talleres "Sensibilización y evaluación de riesgo para el manejo seguro de la información" (de Honduras, Nicaragua, Costa Rica, El Salvador y Guatemala) coincidieron en categorizar así sus datos personales:



Información confidencial

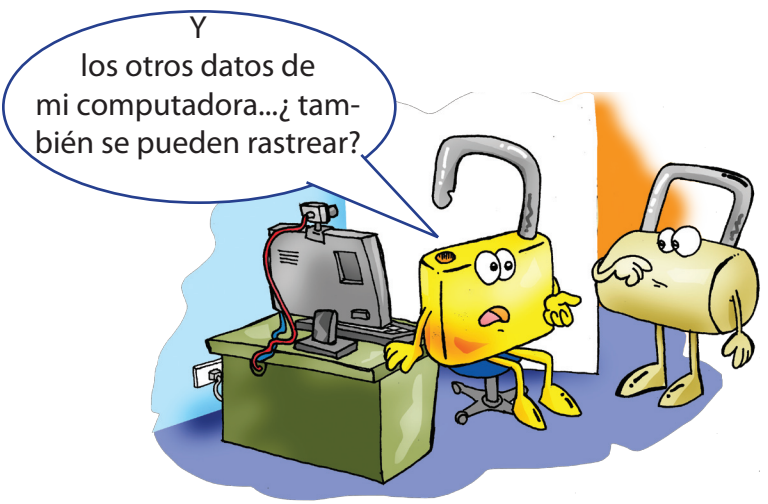
- Monto del salario que se recibe
- Transacciones bancarias
- Deudas o créditos
- Capacidad de consumo
- Hábitos de consumo (restaurantes frecuentados, tiendas
- visitadas etcétera)
- Lugar de estudio de los hijos
- Contraseñas

Información pública



- Nombre propio y el de nuestros familiares
- Cargo que se ocupa en el ámbito laboral
- Números telefónicos
- Dirección del domicilio
- Número de Indentificación
- Consumo en servicios de electricidad, teléfono y otros
- Números de cuentas bancarias
- Patrimonio
- Firma

Algunos de esos datos se sometieron a discusión porque se consideraban como algo delicado, sin embargo, concluimos que nos guste o no, mucha de nuestra información "privada" está difundida en el ámbito público.



Virus, espías, crackers... ventanas abiertas, puertas de par en par

Una computadora conectada en una red interna (sin acceso a la Internet) se encuentra en un ámbito cerrado. Es posible ingresar a ella sólo desde una computadora que se encuentre conectada a la misma red (por ejemplo, dentro de la misma oficina). Por lo tanto sus datos están en cierta manera, más protegidos porque para sacar información es necesario que alguna persona ingrese desde otra computadora o inserte un dispositivo de almacenamiento externo (como una memoria usb) para llevarse la información. Este es el caso de los allanamientos, robos de equipo o asaltos en los que la organización pierde una computadora portátil. En este punto, es necesario aclarar que es cierto que una computadora que no esté conectada a la Internet es menos vulnerable al robo de datos, pero será mucho más vulnerable a los virus (si trabaja con el sistema *Windows*) porque no se actualiza constantemente.

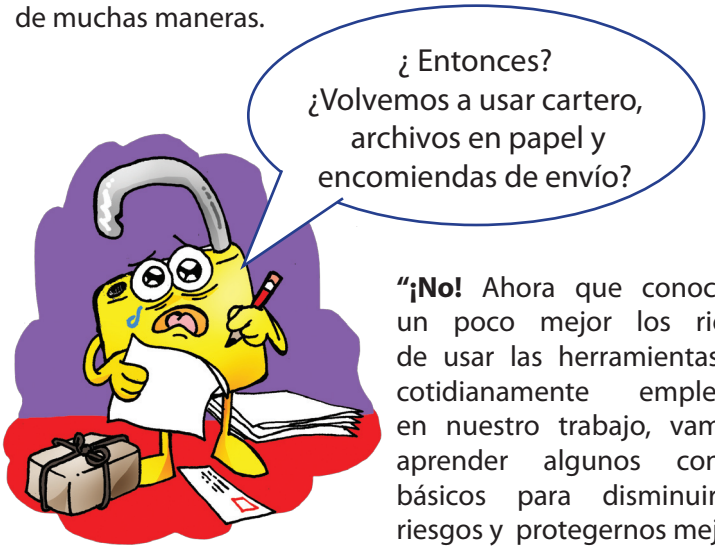
Cuando la computadora está conectada a la Internet por medio de un cable, la información automáticamente se pone en un mayor nivel de riesgo. Desde la Internet es posible acceder a la computadora de manera remota (es decir, sin que alguien esté exactamente dentro de la oficina tocando el equipo). Las carpetas compartidas del programa de conversación en línea (conocido como chat o *messenger*) son un buen ejemplo de una puerta abierta de par en par.

Por otra parte, en sistemas operativos vulnerables a ataques de seguridad -como el *Windows*-, los virus y programas espía (*spyware*, en inglés) o algunos tipos de *gusanos* informáticos se instalan y pueden enviar toda la información de nuestra computadora. Usualmente llamamos virus informático a cualquier aplicación que contamina y afecta el funcionamiento de nuestra computadora, sin embargo, hay algunas diferencias que podemos reconocer.Los *virus* son archivos ejecutables que se copian automáticamente ellos mismos y se propagan dentro de los sistemas.

Los gusanos son programas que aprovechan un error en el código de un programa para infiltrarse en un sistema. Estos son los que entran por esas "puertas" que mencionamos anteriormente. Dentro de estos gusanos, existen unos específicos llamados *troyanos*, que permiten que una persona ajena entre a nuestros sistemas de cómputo.

Estos programas espía usualmente se instalan sin que nos demos cuenta y vienen "de regalo" con programas gratuitos que se descargan de la Internet. Incluso, la misma compañía proveedora de los programas que usamos puede estar obteniendo información privada de nuestra computadora por medio de las actualizaciones automáticas y reportes de error que el usuario envía.

Esos niveles de riesgo y vulnerabilidad se elevan aún más cuando las computadoras usan la Internet inalámbrica. Es prácticamente imposible asegurar las comunicaciones cuando se está usando una conexión inalámbrica, pues es posible interceptar la señal de muchas maneras.



"¡No! Ahora que conocemos un poco mejor los riesgos de usar las herramientas que cotidianamente empleamos en nuestro trabajo, vamos a aprender algunos consejos básicos para disminuir los riesgos y protegernos mejor".[9]

9 Para una lista de herramientas recomendadas vea el anexo al final de este folleto.

¿Cómo podemos prevenir para no lamentar?

Para que nuestros correos electrónicos no sean como las tarjetas postales:

Ya aprendimos un poquito acerca del cifrado de la información. Podemos cifrar y descifrar nuestros correos electrónicos, usando una herramienta instalada en nuestra computadora. Es posible también instalar ese sistema en la memoria usb, para que aún estando en computadoras ajenas, podamos proteger nuestros correos y descifrar los que nos llegan.

En caso de tener nuestra propia "oficina postal" (servidor de correo hospedado con un proveedor), es necesario que todos los datos almacenados ahí también se cifren. Esto mismo debería implementarse en los demás equipos de la organización, creando unidades cifradas dentro del disco duro de las computadoras y las memorias portátiles.

Cuando la información queda al arbitrio de cada usuario, una buena solución es la que brindan los servidores internos, porque es más fácil respaldar los correos y limpiar. Los correos ingresan al servidor, pasan por filtros antispam y por antivirus antes de ser distribuidos a cada estación de trabajo. Además quedan respaldados.

Para evitar que nuestros pasos queden grabados cuando navegamos en la Internet:

Si no queremos dejar demasiada información personal cuando navegamos en la Internet, también hay posibilidades de protección. Podemos usar herramientas de navegación anónima como TOR o instalar algunos complementos a nuestro navegador web (si usamos el Mozilla Firefox por ejemplo[10]).

10 Si se utiliza el buscador de Google con el navegador Firefox, puede usarse un agregado llamado CustomizeGoogle para elegir configura-

Por otro lado, es recomendable que si usamos herramientas de redes sociales virtuales (sitios donde colocamos nuestro perfil, las fotografías de la familia, nuestros lugares favoritos) lo hagamos con precaución.

Para evitar los daños por virus y gusanos:

En este punto, existen grandes diferencias según se usen sistemas operativos privativos [11] (como el Microsoft Windows) o libres (cualquier sistema de GNU/Linux como Debian, Ubuntu, Slackware y muchos más).

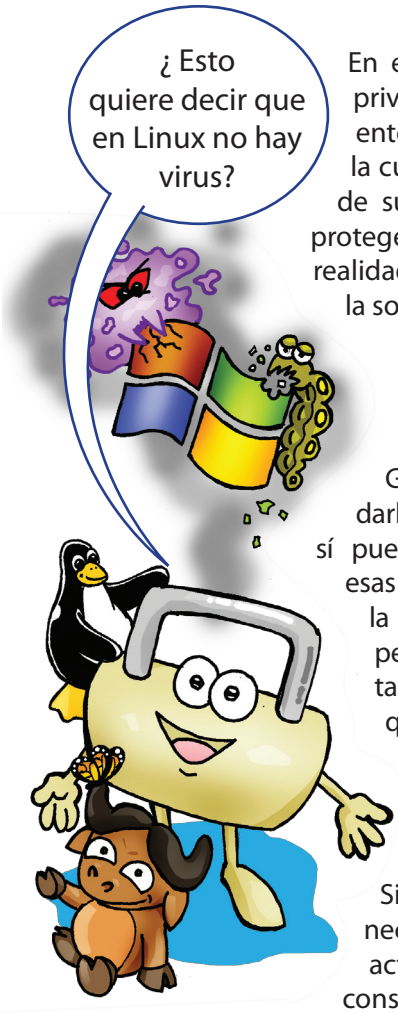
Todos los sistemas operativos tienen vulnerabilidades en seguridad. Los programas de computadora, siempre pueden contener errores que de alguna manera dejan puertas abiertas en nuestras computadoras. Sin embargo, los sistemas operativos libres, al dejar disponible el código que los conforma, permiten que cualquier programador capaz pueda resolver el problema y compartir esa solución.

Aún así, cuando usamos entornos de escritorio como Gnome o KDE (ambientes con botones y pantallas que nos facilitan el uso de los programas) debemos usar siempre los paquetes de instalación de la distribución que estemos usando. De esa manera, sólo instalaremos programas y actualizaciones que provienen de depósitos confiables. Y como en todo, la mejor protección es comprender qué estamos usando y cómo funciona. Si no sabemos qué hace un archivo que vamos a ejecutar, consultemos.

---

ciones seguras. Para evitar conexiones no deseadas que el Firefox hace sin consultarse pueden seguir estas recomendaciones: http://vostorga.org/?p=278. No se recomienda usar el navegador Google Chrome, porque aunque la compañía ha anunciado cambios en sus políticas de privacidad, hay serios cuestionamientos.

11 El software privativo (o no libre) limita el uso, las modificaciones y la distribución, afectando negativamente la libertad de las personas que lo usan. Hay más información en http://es.wikipedia.org/wiki/Software_libre.



En el caso de los usuarios de sistemas privativos como el Windows dependen enteramente de la compañía fabricante, la cual no menciona las vulnerabilidades de sus productos con el argumento de proteger los sistemas operativos. En la realidad, ésto solamente retarda y obstaculiza la solución al problema de seguridad.

Como los virus son "programas" que se instalan automáticamente, no pueden actuar en los sistemas de GNU/Linux (el usuario tendría que darles permiso para hacerlo). Los que sí pueden afectar son los gusanos pero esas amenazas son poco frecuentes y la respuesta de las comunidades de personas desarrollando soluciones es tan rápida, que prácticamente no hay que preocuparse por eso: "Por cada máquina atacada por un gusano existen miles (quizás millones) de equipos infectados por virus."[12]

Si estamos usando Microsoft Windows, necesitamos instalar un antivirus y actualizarlo automáticamente porque constantemente el sistema estará siendo atacado por virus y por gusanos. Es necesario ponerlo a revisar la computadora con cierta frecuencia (la periodicidad dependerá de si el equipo esta conectado a la Internet y si lo utiliza muchas personas). Debe ponerse atención especial en revisar las memorias usb porque es común que los virus se almacenen en ellas y se ejecuten automáticamente cuando se conectan al equipo.

12 http://www.wikilearning.com/tutorial/manual_faq_debian-porque_en_linux_no_hay_virus/6515-8

Si usamos un sistema libre de GNU/Linux no es necesario utilizar un antivirus, usualmente sólo revisamos el contenido del usb y correos y borramos los archivos ejecutables para Windows que son asociados a los virus y gusanos. Esto se hace como prevención para las personas que no usan sistemas libres y para no propagar los virus que no afectan nuestras computadoras.

Para cerrar el acceso a nuestra red:

Existen varias alternativas de Firewall o cortafuego para evitar que sea posible ingresar a nuestras redes desde la Internet. Una de ellas requiere que se compre equipo específico; otra se puede hacer con equipos antigüos instalando software como el IPCop (una distribución de Gnu/Linux que requiere dos tarjetas de red y computadora dedicada).

Hasta ahora, no hemos hablado mucho de las contraseñas aunque podríamos decir que la seguridad depende en gran parte de cómo son las claves que usamos y del manejo que hacemos de ellas.

Lo primero que debemos hacer es valorar el nivel de seguridad de nuestras contraseñas. Éstas son inseguras cuando:

- Se pueden adivinar fácilmente: estas son las contraseñas que incluyen datos personales del usuario/a, como fechas de cumpleaños o aniversarios, nombres de parientes cercanos, mascotas o localidades conocidas.
- Se comparten entre varias personas (por ejemplo, por un mal uso del correo institucional o para transacciones bancarias).

- El lugar donde se respaldan las contraseñas es de fácil acceso (notas escritas, datos almacenados en los teléfonos celulares, etcétera).
- Se informan usando correos electrónicos sin cifrar o llamadas telefónicas.

Una vez que sabemos qué tan inseguras son nuestras contraseñas, podemos tomar en cuenta algunos trucos para tener un nivel medio de seguridad. Para eso, es necesario usar palabras mezcladas con números, hacer analogía de números con letras (por ejemplo 4n4lu1$4 "ana luisa") o usar palabras en un idioma extranjero no muy conocido. Sin embargo, esto en realidad no es lo más recomendable. Lo mejor es seguir las siguientes recomendaciones o usar una herramienta como *Keepass* [13].

Contraseñas seguras y muy seguras:

Las contraseñas seguras tienen las siguientes características:

- Están formadas por más de 8 caracteres.
- Contienen letras mayúsculas y minúsculas, números, signos y caracteres especiales como (_\}[¬1/2~·@|) .
- Se cambian regularmente.
- No están anotadas en ningún lugar accesible ni se comparten por ningún motivo o medio (cuando es absolutamente necesario compartir una contraseña, debe cambiarse al menor tiempo posible de haberla compartido).

13 http://keepass.info/

Algunos trucos posibles:

- Seguir un dibujo o forma escribiendo en el teclado (por ejemplo, imaginar un triángulo partiendo de una letra específica).

- Crear una frase sin sentido aparente.

- Incluir faltas de ortografía en la frase.

Para tener contraseñas muy seguras, existen herramientas informáticas muy útiles para almacenar contraseñas. Si se utiliza *Keepass,* únicamente debemos recordar una contraseña muy segura que abre el depósito donde estarán las demás. Dentro de ese depósito, podemos tener contraseñas generadas por nosotros o claves generadas por el sistema, las cuales serán extremadamente seguras.

Lo que hacemos cuando usamos una herramienta como ésta es abrir el depósito, buscar la contraseña que necesitamos, copiarla y pegarla en el formulario de acceso de lo que necesitamos abrir. Si el sistema generó la contraseña, probablemente nos será imposible recordarla y eso es mucho más seguro, siempre que no olvidemos la llave maestra que abre nuestro depósito.

Aunque el programa Keepass permite que usemos un archivo como llave, lo recomendable es usar una contraseña muy segura, ya que el programa abre la carpeta que contiene el archivo y encontrar la llave será sólo cuestión de probar los archivos uno por uno.

Aspectos principales para una política interna de seguridad de la información

Existen muchas opciones para asegurar mejor nuestra información. Algunas de las medidas necesarias involucran a las personas que trabajan en el soporte técnico, porque son las encargadas de instalar correctamente las herramientas. Sin embargo, dentro de una organización la seguridad depende de la existencia de políticas claras; así como tenemos reglas para uso de la oficina o de los vehículos, necesitamos reglas para la protección de los datos.

Una organización o institución está conformada por personas que trabajan guiándose por una visión, una misión y unos objetivos. Cuando alguien ingresa a trabajar en una organización se realiza un proceso de inducción, en el que se informa -entre otras cosas- cuáles son las políticas y reglamentos que la persona deberá conocer para realizar su trabajo en esa organización.

Usualmente, dentro de ese proceso de inducción, no se incluye el tema de la información y se pasa por alto que ésta es un bien institucional, generado dentro de la institución y por lo tanto, debe ser cuidado como cualquier otro bien. La formación y capacitación del personal no debe dejar por fuera algunos puntos, como cuál sistema operativo tienen las computadoras, cuáles herramientas de ofimática (procesadores de textos, hojas de cálculo, presentaciones, etcétera) se usan , qué se puede y no se puede hacer en la computadora.

El diseño y el monitoreo del cumplimiento de la política de seguridad no depende solamente del personal técnico.

Dentro de las organizaciones debe haber una o dos personas encargadas de velar por la seguridad de la información y no es conveniente asignar estas labores al técnico (al menos en su totalidad) porque:

- Cuando la información de contraseñas y sistemas está concentrada en una sola persona, se genera demasiada dependencia y hace que la institución y la persona de soporte técnico sean muy vulnerables.

- El personal de soporte técnico o informático no tiene el nivel jerárquico necesario para tomar las decisiones estratégicas ni dar seguimiento. Tampoco puede tomar medidas cuando alguien debe ser sancionado si está incumpliendo las políticas de seguridad.

- La mayor parte de las soluciones dependen de las actitudes de las personas, no de las herramientas técnicas que se utilicen.

A continuación, vamos a enumerar algunos ejes importantes que deben ser tomados en cuenta, si se piensa elaborar una política de seguridad dentro de la organización.

Niveles de confidencialidad de la información

Para determinar cómo debe manejarse la confidencialidad dentro de la organización es necesario:

- **Identificar el tipo de información que se maneja**

Por ejemplo: datos del personal, información contable, datos de activistas o colaboradores externos, información interna de otras organizaciones aliadas, comunicaciones para la prensa, investigaciones y fuentes confidenciales

- **Observar cuáles instancias o personas manejan esa información**

Por ejemplo: recepción, transportes, dirección, oficina de prensa, soporte técnico, investigadores externos, consultores, donantes y agencias de financiamiento .

- **Determinar si los flujos actuales son apropiados para el tipo de información que se maneja:**

En este punto, lo más importante es que se evidencie que la información que se comparte de manera más fluida basándose en niveles altos de confianza, es la que debe resguardarse mejor por las consecuencias de la pérdida de esos datos.

- **Identificar grupos externos interesados en la información :**

Debe clarificarse bien quiénes son aliados y quiénes no. De igual manera, crearse criterios para el manejo de la información de investigaciones que se comparten con la prensa o con otras instituciones.

- **Determinar si se deben efectuar cambios en el manejo de la información:**

Por ejemplo: si en los espacios de atención al público se entrevista a víctimas , si la red de cómputo no tiene niveles de acceso diferenciados según el cargo, etcétera.

Comunicaciones institucionales:

Las comunicaciones institucionales merecen un espacio aparte, porque muchas veces, las organizaciones envían comunicados en archivos adjuntos editables. Esta costumbre debe respaldarse con un comunicado publicado en la web de la organización (puede ser en un blog [14] , si la organización no cuenta con un sitio fácilmente editable) para que el público pueda corroborar si la copia recibida es igual a la copia oficial difundida por la organización, ya que a un archivo adjunto es muy fácil quitar o agregar párrafos, firmas, etcétera y después reenviarlo como si fuera de la organización. No debemos adjuntar imágenes de nuestra firma personal, ya que es posible cortar y adjuntar esa imagen a otros documentos.

Aunque ha sucedido la suplantación de direcciones (es decir, se recibe un comunicado de una dirección aparentemente igual a la de una organización específica) y el robo de contraseñas (lo cual permite que se ingrese al buzón y/o se envíe un correo desde la dirección violentada), ni siquiera es necesario llegar a tanto para enviar un correo simulando otra dirección de correo. Los correos electrónicos reenviados, únicamente se identifican por el "FWD" en el espacio del asunto y por un texto que es posible simular.

Uso de correos personales:

En algunas organizaciones, se utiliza la dirección personal para enviar y recibir comunicaciones institucionales o de trabajo. Esto genera problemas en términos de seguimiento y respaldo, porque si la persona sale de la organización, no deja respaldada las comunicaciones ni los contactos y a su vez podría seguir manteniendo comunicaciones como si siguiera trabajando en la institución.

14 Un blog es una bitácora hospedada en la Internet. Existen varias opciones gratuitas de fácil manejo, por lo que se pueden editar frecuentemente. Una opción libre y gratuita es: www.wordpress.com

Factores de riesgo por sucesos físicos:

1. Problemas con el flujo de corriente:

Para prevenir daños al equipo y/o pérdida de información causados por interrupciones abruptas del fluido eléctrico, rayos cercanos, etcétera , es necesario implementar:

- Un inversor o múltiples dispositivos de Sistemas de Energía Ininterrumpida (conocidos como UPS).
- Cableados de red especiales con puntas de metal.
- Protección de líneas telefónicas/red (los UPS tienen entradas para las líneas telefónicas).

2. Prevención de daños causados por temblores:

Es difícil pensar que en nuestras organizaciones, vamos a construir una habitación especialmente segura para tener el servidor donde resguardamos los datos. Por eso lo que se recomienda es que haya respaldos periódicos de la información en una caja de seguridad en un banco .

Deben existir al menos dos copias del mismo disco. Así, cuando necesitamos sacar una de la caja de seguridad, siempre quedará otra resguardada.

3. Prevención de daños por inundaciones:

Para los lugares con riesgo, se aconseja hacer un cableado (de red y eléctrico) a cierta altura del piso .

4. Prevención de daños causados por el polvo:

Tradicionalmente, se ha pensado que el polvo puede afectar mucho a los equipos, sin embargo, aunque es importante realizar limpiezas cada cierto tiempo (especialmente del

servidor) no es tan riesgoso (a menos que los equipos se usen para trabajar en áreas donde circula mucho polvo). No obstante, es importante conocer que los filamentos (como el cabello) pueden ser conductores eléctricos que se pueden cargar estáticamente. De igual manera, el polvo en exceso puede generar sobrecalentamiento en las computadoras y afectar el flujo de aire que disminuye la temperatura. Los procesadores nuevos tienen protecciones para esto, de manera que se apagan antes de dañarse por altas temperaturas, pero es importante hacer limpiezas eventualmente.

La energía estática puede ser peligrosa. En los lugares donde la humedad es alta no hay tanto problema pero en otros países se pide que se toque la fuente de poder antes de tocar los componentes electrónicos para evitar posibles daños.

5. Protección del cableado:

Las sillas, el paso de las personas, los zapatos de tacón dañan los cables que no están bien instalados. En ocasiones la limpieza del piso hace que los cables de red o electricidad se desconecten. Lo óptimo es hacer un cableado estructurado.

Factores de riesgo relacionados con el manejo de la información por parte del personal:

Las medidas relacionadas con las personas no dependen del personal técnico. No existen "soluciones informáticas", existen "herramientas informáticas" que permiten generar "soluciones más globales".

La seguridad de la información depende de procesos que debemos cumplir. Por eso, es fundamental que las organizaciones tengan normas claras, las cuales deben ser institucionales y contemplar sanciones en caso de incumplimiento.

Algunos puntos a contemplar para la elaboración de un reglamento:

- Las normas deben contemplar los temas de permisos, accesos y responsabilidades de forma diferenciada.

- Cada persona debe saber qué tipo de permiso tiene, cuánto acceso a información tiene y cuál es su responsabilidad por el acceso a datos.

- Es necesario clasificar los niveles y el flujo de la información: si no sabemos cuál es la información delicada o que implica un alto riesgo, no sabemos cuándo debemos cuidar unos datos de forma especial y quiénes deben tener acceso a cierta información y quiénes no. Es necesario determinar también hasta dónde puede entrar el público que nos visita y en cuáles espacios no puede entrar cualquier persona aunque trabaje con la organización.

- La organización debe tener claro cuáles contraseñas tiene una persona. En caso de tener que compartir una contraseña, debe haber una persona responsable de cambiarla cuanto antes.

- La organización debe definir cuáles programas usa y cuáles no, para que el personal no instale herramientas sin autorización. Los usuarios están acostumbrados a instalar programas y esto genera problemas de spyware, virus y software ilegal.

- Todas las normas deben relacionarse con procesos de capacitación.

- Monitoreo sobre las políticas: la aplicación de las políticas deben exigirlas quienes asumen roles de dirección y/o coordinación, pues el equipo de informática puede sugerir herramientas pero no es el encargado de velar por el cumplimiento de las medidas. Por ejemplo, el personal

de soporte técnico no tiene la autoridad para pedirle a un coordinador o coordinadora de área que le muestre su memoria portátil para revisar si está utilizando el cifrado de datos.

- Personal técnico: lo deseable es que haya dos personas en soporte técnico, para evitar la dependencia de una sola persona. Son muchos los casos en los que los avances tecnológicos se pierden cuando se va la persona encargada.

Factores de riesgo por criminalidad común y crimen político:

A continuación se presentan algunos puntos que es importante tomar en cuenta para disminuir el impacto de un suceso de criminalidad que afecte a las organizaciones:

- No se recomienda usar computadoras portátiles como estaciones de trabajo: lo más seguro sería usar computadoras de escritorio y usar laptops sólo cuando se necesita ir a algún lugar a hacer una presentación o a trabajar fuera de la oficina. De otra manera, estaríamos llevando en las portátiles demasiada información sensible.

La información debe ir cifrada siempre:[15] si la información que va en una computadora portátil está cifrada, la pérdida del equipo no implicará el acceso de la información por terceras personas. Esto mismo aplica para las memorias usb y los discos de respaldo.

15 Los programas que crean particiones ocultas dejan su rastro en la computadora. En caso de amenaza, es posible que nos pidan la contraseña. Existen estrategias para salir de esta situación. Sin embargo, lo mejor es almacenar los datos muy delicados en lugares seguros fuera de la organización.

- Es necesario tener un adecuado respaldo de contraseñas: en todas las organizaciones hay personas claves que tienen acceso a las contraseñas, sin embargo, no es seguro que una sola maneje todos los datos y no los respalde con otro de los miembros. Si una sola persona maneja mucha información o tiene todas las contraseñas, se convierte en blanco clave para la criminalidad.

- Cambio de contraseñas: cuando una persona deja de trabajar en la organización deben cambiarse inmediatamente las contraseñas que maneja. Esto supone que existirá además un respaldo de las contraseñas que esta persona usaba y de la nueva contraseña que se genere, para evitar que la persona cierre el acceso a la información e impedir problemas en el futuro. Los respaldos periódicos también previenen la pérdida de información por la salida de miembros del personal.

- Uso de claves en teléfonos celulares: se recomienda implementar el uso de claves para dificultar (al menos levemente) el robo de los números telefónicos del personal de la organización o de los actores clave de las comunidades y grupos con los que trabajamos.

- Políticas de contratación del personal: es importante que en nuestras organizaciones conozcamos quiénes son las personas que vamos a contratar. No debemos centrarnos solamente en capacidades profesionales, también debemos conocer su trayectoria y otros detalles que nos permitan establecer la confianza.

- Cuando se trabaja en el campo, las personas que salen deben dar todos los detalles del viaje, transporte, hospedaje etcétera para poder monitorear apropiadamente su seguridad.

- Respaldos: hay que implementar una política de periodicidad fija, que quede claro cuándo se debe respaldar, cómo se resguardarán esos datos y dónde.

Conclusiones

Las organizaciones sociales centroamericanas hemos transformado mucho nuestras modalidades de trabajo, a partir de los cambios tecnológicos de los últimos años. Esto nos ha traído enormes ventajas, pero a la vez nos plantea retos en cuanto al acceso, uso y apropiación de las herramientas que proveen las nuevas tecnologías de información y comunicación. No basta con saber usar una computadora, necesitamos aprender a asegurar nuestra información, cuidar más nuestra privacidad y utilizar herramientas más seguras en nuestra cotidianidad. Es urgente que implementemos medidas, no sólo por nuestra propia seguridad, sino la de todas esas personas que confían en nuestro trabajo y conforman redes de apoyo a nuestra organización.

En esta publicación, hemos repasado algunos de los temas más importantes que debemos tomar en cuenta. Sin embargo, no basta con leer y conocer, es urgente que actuemos. Poco a poco podemos ir discutiendo el tema, sensibilizando a las personas que trabajan en las organizaciones para llegar a plantear una política de seguridad que permita enmarcar el cambio.

La política de seguridad debe ser firme y su cumplimiento debe monitorearse constantemente, pero la implementación de las medidas es mucho más ágil si todos y todas comprendemos la importancia de los procedimientos. Por eso, la capacitación y los acuerdos son fundamentales.

Por otra parte, es muy importante que el uso de herramientas informáticas para seguridad implique un proceso continuado en el tiempo. Por ejemplo, puede suceder que años después de realizar un respaldo cifrado, la persona que conocía la contraseña del disco salga de la organización o que alguien haya olvidado guardar la contraseña en el depósito destinado para eso. Eso implicaría que no se puede tener acceso a la información respaldada, lo cual es un buen ejemplo de lo que puede suceder si los procedimientos no son claros y no existe constancia.

Otro detalle fundamental consiste en la reciprocidad de las demás organizaciones. Nuestra organización puede implementar muchas medidas de seguridad, pero ese esfuerzo no basta si nos comunicamos con otras instituciones que no aseguran su información apropiadamente. Como sector, necesitamos posicionar en nuestras redes la preocupación por la seguridad, no porque desconfiemos de de las instituciones con las que trabajamos, sino porque el tema de la seguridad de la información debe trabajarse de forma coordinada, logrando que las organizaciones cuidemos unas de las otras.

Por último, como se habrá observado, esta publicación menciona y recomienda constantemente programas informáticos y sistemas operativos de Software Libre. Esta preferencia no se basa solamente en los principios filosóficos que sostienen este movimiento mundial por la libertad y un futuro tecnológico más sostenibles y que son coherentes con los planteamientos que guían el trabajo de las organizaciones que trabajan por los derechos humanos; se fundamenta en la seguridad que los programas de código abierto brindan a las personas usuarias. El tener el código fuente hace que se puedan modificar los problemas o defectos de un software, porque las comunidades desarrolladoras comparten el conocimiento y la solución está al alcance de todas las personas. Además, sólo en el Software de Código Abierto es posible revisar si el programa hace lo que se supone que hace y NADA MÁS que eso.

Por otra parte, los altos costos de las licencias de Software privativo obligan a las organizaciones a gastar los recursos necesarios para el trabajo. Por esa razón, muchas veces se recurre al uso de software ilegal, lo cual se convierte en una enorme vulnerabilidad para las organizaciones sociales, por las consecuencias tan graves de las sanciones económicas y por el peligro de pérdida de información en allanamientos o procesos atropellados de migración o cambio a sistemas de Software Libre. Si ya existen herramientas libres, gratuitas y más seguras, lo recomendable es que las organizaciones sociales comiencen a plantearse la necesidad de asegurar su futuro cambiándose a sistemas operativos de Software Libre.

Herramientas recomendadas

Software Libre (corre con SO Windows y GNU/Linux)	Cliente para manejar correo electrónico	**Mozilla Thunderbird** http://www.mozilla-europe.org/es/products/thunderbird/
	Software para cifrar y firmar correos electrónicos (complemento para aplicaciones de Mozilla)	**Enigmail** http://enigmail.mozdev.org/home/index.php
	Navegar en Internet	**Mozilla Firefox** http://www.mozilla-europe.org/es/
	Navegación anónima en la Internet	**TOR** http://www.torproject.org/index.html.es
	Configurar privacidad de Google con Firefox	**CustomizeGoogle** http://www.customizegoogle.com/
	Antivirus	**ClamWin** http://es.clamwin.com/ **ClamAV (para GNU/Linux)** http://www.clamav.net/
	Protección de archivos mediante unidades y documentos cifrados	**Truecrypt** [16] **:** http://www.truecrypt.org
	Sistema para manejo seguro de contraseñas	**Keepass:** http://www.keepass.info
	Programa para Firewall o Cortafuegos	**IPCop** http://www.ipcop.org/
Software Privativo	Antivirus gratuito (no es código abierto)	**Avast** http://www.avast.com/esp/

16 Truecrypt es un software de código abierto con una licencia propia. Sus términos legales han sido discutidos aquí http://www.mail-archive.com/debian-legal@lists.debian.org/msg38222.html

❄ Para una compilación completa de herramientas:

Tactical Technology Collective y Front Line Defenders. NGO in a Box: Llave en Mano para ONG, edición de seguridad, octubre 2005.
Disponible en línea en: http://security.ngoinabox.org/html/sp/content.html

Fuentes consultadas:

Barrera, María Elene y Montague, Jason. Recreando privacidad en el ciberespacio. Obtenido en la Internet el día 19 de agosto de 2008 de la dirección:
http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D. Informatico.16.htm

Castells, Manuel. Internet, libertad y sociedad: una perspectiva analítica. En: Polis Revista On-line de la Universidad Bolivariana de Chile,Volumen 1, Número 4, 2003. Obtenido en la Internet el día 4 de septiembre de 2008 de la dirección:
http://www.revistapolis.cl/4/cast.htm

Colectivo Mononeurona. Manual/FAQ Debian - ¿Porqué en Linux no hay virus?
Obtenido en la Internet el día 19 de agosto de 2008 de la dirección:
http://www.wikilearning.com/tutorial/manual_faq_debian-porque_en_linux_no_hay_virus/6515-8

Benedicto, Rubén. "Guerra de Información en el Referéndum sobre el Tratado de Libre Comercio en Costa Rica: un Análisis Psicosocial Crítico desde la Observación Electoral". Obtenido en la Internet el día 14 de julio de 2008 de la dirección:
http://www.liber-accion.org/Joomla/index.php?option=com_docman&task=doc_download&gid=48

Foobar. How to write a Linux virus in 5 easy steps. Obtenido en la Internet el día 31 de marzo de 2009 de la dirección: http://www.geekzone.co.nz/foobar/6229

Temas consultados en Wikipedia:

http://es.wikipedia.org/wiki/Criptografía
http://es.wikipedia.org/wiki/Firma_digital
http://es.wikipedia.org/wiki/Criptología