

---

Asociación para el Progreso de las Comunicaciones

---

Proyecto:

**“Participar con seguridad”**

RESUMENES de INTRODUCCION  
A  
LA SEGURIDAD Y PRIVACIDAD  
DE LA  
INFORMACION

Traducción libre, adaptación y actualización del informe original elaborado para:  
**APC, Asociación para el Progreso de las Comunicaciones:**

*“Introducing Information Security”*  
escrito por Paul Mobbs, March 2002

**Carlos E. Alvarez, Red Wamani, Argentina, Marzo 2003**  
**Licencia GPL de Documentación Libre**

## INDICE GENERAL

Página:	3 - Introducción a la version en español
Página:	5 - Resumen 1: Introducción a la seguridad en la Información
Página:	24 - Resumen 2: Resguardando sus datos
Página:	45 - Resumen 3: Control de acceso y contraseñas
Página:	52 - Resumen 4: Uso de encriptación y firmas digitales
Página:	57 - Resumen 5: Virus de computadoras
Página:	64 - Resumen 6: Usando internet con seguridad
Página:	80 - Resumen 7: Viviendo bajo vigilancia

### Licencia de la Documentación libre:

*Registro la propiedad literaria © 2001, 2002, 2003 Asociación para el Progreso de las Comunicaciones, Paul Mobbs (versión original en inglés), Carlos Alvarez (traducción libre y adaptación versión en español).*

*Contribuciones, corrección y traducción original en la versión en inglés hechas por Karen Banks, Michael De Beer, Roman Chumuch, Jim Holland, Marek Hudema, Pavel Prokopenko y Pep Turro.*

*El proyecto para desarrollar esta serie de capítulos o resúmenes de información se manejó por la Asociación para el Progreso de las Comunicaciones, financiado por la OSI.*

**Se concede permiso para copiar, distribuir y/o modifica este documento según las condiciones de la Licencia GNU de Documentación Libre, Versión 1.1o cualquier versión posterior (vea <http://www.gnu.org/copyleft/fdl.html> para una copia de la licencia).**

*Por favor note que el título del resumen de información, y el de "Licencia de Documentación Libre" están protegidas como "secciones invariantes y no deben ser modificadas".*

*Para mas información sobre el Proyecto "Participando con Seguridad" o si usted tiene preguntas sobre los resúmenes o capítulos contacte a:*

`secdocs@apc.org` <<mailto:secdocs@apc.org>>

## INTRODUCCION a la VERSION en ESPAÑOL

---

En este nuevo trabajo realizado para **APC**, estamos introduciendo conceptos principales y comparaciones prácticas que permiten a cualquier usuario de sistemas de información, sean o no informáticos, disponer de los elementos básicos necesarios para tomar decisiones respecto a la seguridad y los resguardos necesarios para la gestión de su información.

Respecto al informe original en inglés, hemos tomado la facultad de reformular los conceptos a fin de hacerlos mas claros a la ideocincracia de nuestro idioma y región, así como incorporamos, donde se han dado novedades tecnológicas, nuevos elementos de comparación.

Día a día aparecen nuevas opciones tecnológicas y otras reducen los costos haciendo que los equipos o dispositivos que no se podian usar ayer, hoy sean una opción real.

Del mismo modo, vamos avanzando en el conocimiento de los sistemas de seguimiento y monitoreo de información y al mismo tiempo, de las posibilidades de prevención y resguardo que podemos definir, cuando es posible hacerlo.

Es importante que, sean individuos u organizaciones de cualquier tipo, conozcamos el contexto tecnológico, legal, político y social en que operamos con nuestra información.

Sean datos económicos, sociales, políticos y/o particulares, todos son pasibles de ser perdidos, modificados, revisados y copiados para un sin fin de objetivos, lícitos o no, y cada una de esas posibilidades deben ser tenidas en cuenta en nuestro trabajo de todos los días.

Agradecemos la colaboración en la traducción inicial de Antonio C. Alvarez.

**Carlos E. Alvarez**  
**Wamani Networks**  
Marzo 2003

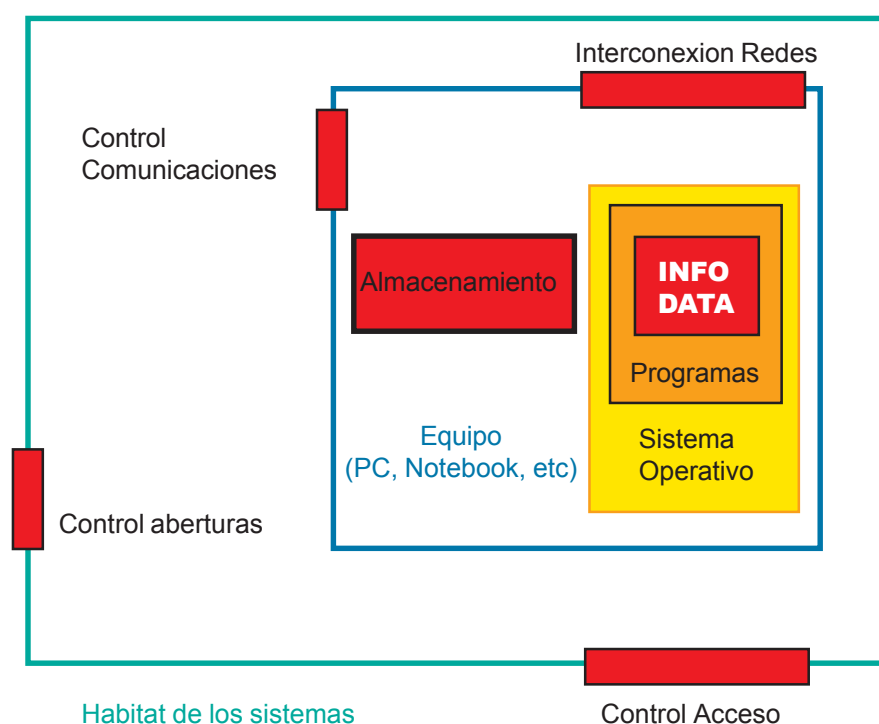
## ELEMENTOS INICIALES de ANALISIS

Como en todo análisis de sistemas, siempre es conveniente tratar de definir cuales son los elementos que interactúan en él.

Aunque podremos ver en las siguientes secciones los grandes temas que conforman la temática de seguridad y privacidad en la información, creemos conveniente clarificarlos inicialmente.

Elementos que conforman este tema:

- Programas que gestionan los datos
- Sistema operativo y control de acceso, usuarios y permisos.
- Equipo de computación y almacenamiento de datos
- Sistemas de copias y resguardo de datos
- Interconexión de los sistemas en red
- Interconexión a sistemas de comunicaciones
- Virus e intrusiones informáticas.
- Sistemas de seguridad y control de acceso físico a los equipos
- Sistemas y normas legales que afectan potencialmente su trabajo.



# 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

## Introducción

Usar computadoras es una actividad compleja. Para usarlas apropiadamente no sólo debe aprender las funciones del procesador de texto o base de datos que utiliza; también necesita aprender a organizar su computadora y la información que contiene para protegerla contra la pérdida accidental (o no) de su información.

También es importante preparar su computadora, su información y su lugar de trabajo (oficina, hogar, institución), para prever la posibilidad de daño externo deliberado que podrían causar tanto los virus de computación, cada vez más comunes, la interceptación de información, el monitoreo de sus comunicaciones, así como los procedimientos (lícitos o no) de las fuerzas estatales u otras que puedan oponerse a su trabajo.

Este resumen es el primero de una serie sobre la seguridad (y privacidad) de la información. Debería leerse junto con los otros resúmenes que se concentran en los aspectos prácticos de la seguridad. Ellos tratan los siguientes temas:

- Resguardando sus datos**
- Las contraseñas y el control de acceso**
- Usando encriptación y firmas digitales**
- Los virus de computación**
- Usando Internet con seguridad**
- Viviendo bajo vigilancia**

Este resumen define los puntos básicos principales que necesita considerar al encarar la seguridad de sus computadoras y sistemas. Los otros capítulos miran en más detalle los rasgos que se mencionan aquí.

Mucho de lo que se discute en este capítulo es teórico. No puede proscribirse en forma genérica, porque es dependiente de las necesidades y circunstancias del individuo (y/o de su organización). Aunque el volumen del resumen puede parecer demasiado e intimidante, leyéndolo logrará un contexto adecuado para luego integrar los conceptos que se desarrollan en los otros capítulos, dándole los elementos como para lograr definir un **sistema de seguridad** en lugar de un poco fiable sistema de protección.

## La necesidad de seguridad

La Seguridad de la información (también conocida como "Seguridad en informática" o Infosec) es la teoría y práctica de usar computadoras y sistemas de información considerando que:

*-Se prevea la pérdida accidental o daño a la información y a los sistemas de las computadoras por las personas que las usan;*

*-Se desarrollen y preparen los sistemas para asegurar tanto fiabilidad y como seguridad (eso significa: proteger sus equipos, prevenir los virus, las fallas de hardware, etc.),*

*-Se proteja del acceso no autorizado de otros (es decir: los hackers / crackers y otras personas que se interesen en influir en lo que usted o su organización esta haciendo) causando la pérdida accidental o deliberada o daño a sus datos y equipos.*

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

La lista anterior de amenazas potenciales a la seguridad, está en orden decreciente de probabilidad.

### Los objetivos de una buena seguridad

Los ingredientes de un buen plan de seguridad de información plantean controlar el nivel de sensibilidad de los datos, la seguridad, el acceso, y la performance de sus datos y sistemas:

**-La información debe controlarse según su sensibilidad** - esto le exige que decida qué seguridad requiere cierta información determinada, y clasificarla luego en función de su grado de sensibilidad (impacto o efectos de tenerla o no, de que la copien para terceros, de perderla o de que sea reemplazada por datos erróneos o equivocados) y su carácter de irremplazabilidad (es decir, que no pueda recomponerse o volver a conseguirse en todo o en parte);

**-Las barreras de Seguridad deben prevenir el acceso desautorizado o la alteración de datos** - usted debe combinar las barreras físicas (como las cerraduras) con las barreras lógicas o programables (como partes de programas de computación o del sistema operativo de la computadora);

**-Las personas deben poder acceder la información que necesitan usar de la manera más eficiente.** Esto exige que las personas entiendan cómo es el sistema de acceso a la computadora, el uso del sistema de información, y dispongan de las claves de acceso pertinentes de forma tal que pueda satisfacerse las necesidades de dichos usuarios.;

### Cómo acercarse a la seguridad de la información

La mejor manera de acercarse a el problema es desarrollar sistemas y ciclos:

Los **Sistemas** son los métodos por los cuales la información es asegurada - por ejemplo la organización de la información dentro de su computadora para que sea más fácil encontrarla o resguardarla;

Los **Ciclos** son períodos de tiempo en los que la seguridad de la información y su integridad se revisan y evalúan - por ejemplo: podría tener ciclos para cambiar las contraseñas y otros para realizar una copia de resguardo de sus datos en forma regular.

La seguridad es un proceso y no un producto. **NO puede comprar seguridad e instalarla.** Necesita definir un sistema que implica un conjunto de tareas y procedimientos (y seguramente algún equipamiento específico) de acuerdo a su forma de trabajar, sus necesidades, los tipos de riesgo y niveles de seguridad que requiera su tarea así como los posibles recursos (económicos, expertos informáticos, etc) que pueda utilizar.

### Evaluando los riesgos

Los riesgos cotidianos más comunes que probablemente puede enfrentar son, en orden decreciente de probabilidad:

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

- los errores del mismo usuario** (manipulando mal sus datos, anulando los medios de comunicación, borrando o reemplazando accidentalmente datos ya almacenados o por almacenar)
- los problemas con el software** (sobre todo Windows) por mal funcionamiento
- el daño deliberado** (los virus, el daño motivado)
- fallas en el equipo.**
- el robo o sustracción** de equipos
- problemas en la alimentación de energía** de sus equipos, **desastres naturales y accidentales** (inundaciones, terremotos y/o incendios, etc).

También habrá riesgos que sólo pueden ser aplicados a su persona, como resultado del tipo de trabajo que realiza, o debido a la situación particular de su equipo (ubicación geográfica, ambiente de trabajo, etc).

Cuando organiza su información, sus sistemas y equipos, necesita considerar qué riesgos encara y cómo puede planear acciones y resultados para cada contingencia. En el ámbito de grandes organizaciones (estatales, empresariales, organismos internacionales) esto se denomina "Plan de contingencia" y está orientado a garantizar, en la medida de lo posible, la continuidad del trabajo aunque puedan suceder determinados escenarios.

¿Considere varios escenarios "**Que pasaría si ...**":

Cómo sus datos podrían perderse, transferirse en forma no autorizada, comprometer su integridad (modificarse) o dañarse accidentalmente?

Para cada escenario que pueda prever, considere el posible riesgo de que esa serie de eventos pueda pasar; qué medios técnicos podría usar para recuperar o proteger los datos o la información, y cómo reducir el riesgo de que ocurran; las consecuencias de tomar esas acciones (podría preveer el riesgo propuesto ante un incendio, por ejemplo, guardando copias de información en otra ubicación, pero tendría que encontrar también una manera de proteger esas copias de otros riesgos, como el robo).

Para cada una de sus soluciones, evalúe la posibilidad (y la pérdida) que el riesgo conlleva contra el costo o dificultad de la solución técnica y decida si merece la pena el tiempo, el dinero y el esfuerzo. Por ejemplo, si ha puesto una copia de un archivo en Internet, o lo distribuyó a muchas personas, no necesita darle el mismo nivel de protección que a uno de sus propios archivos locales más confidenciales.

Trate de plantear sistemas simples, realizables - introduzca procedimientos, sistemas y ciclos para tratar con cada riesgo uno-por-uno. Si intenta contemplar todo de una vez, la tarea puede parecer agobiante. Puede encontrar que una forma de prevenir un riesgo resuelve a menudo los problemas creados por otro. Por ejemplo, puede desear resguardarse contra un robo, y puede determinar que los mismos procedimientos pueden servir contra una intervención del estado o de otros que se oponen a su trabajo.

### Cuidando su información

En general, el 75% de la pérdida de información o daños en los sistemas son causados por el error del personal, en lugar de por la acción de fuerzas externas (como hacker/crackers o virus). Analice sus propias capacidades para encarar la seguridad de la información, e identifique donde necesita entrenamiento adicional o recursos para realizar las tareas necesarias para responder a sus necesidades.

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

### Organización

Desde los gabinetes donde guarda sus archivos a los discos flexibles, pasando por cómo genera, resguarda y recupera la información, forma parte de cómo organiza sus datos.

Necesita asegurarse que sea:

**Accesible** - necesita encontrar las cosas cuando las necesita - eso no significa necesariamente que adopte estructuras estrictas, pero todos aquéllos que necesitan acceder a sus datos, deben saber donde están y cómo llegar a ellos.

**Cuantificable** - necesita tener una idea precisa lo que tiene, para poder evaluar si ha sido afectado por una pérdida, un robo o una intrusión - debería notar cualquier manipulación de sus computadoras o sistemas de archivos, así como si todo su software está propiamente registrado en caso de que alguien lo quiera verificar, o si es consciente del volumen de papel e información digital que almacena y si contiene información que podría ser considerada ilegal.

**Transparente** - considerando el caso de que usted o alguna otra persona importante en su red de trabajo sea detenida o eliminada o se vea afectada por una enfermedad o alguna acción mas deliberada, de forma de poder contemplar que otras personas puedan necesitar acceder a sus datos para continuar con su trabajo.

**Recuperable** - necesita poder reconstruir los datos fácilmente si se dañan - eso significa que trata de tener la información más "útil" en sus archivos principales y trate de tener una cantidad mínima de datos inútiles o superfluos que complican el proceso de organización y resguardo de su información.

Desarrollar y organizar un buen sistema de información es un **proceso de aprender, y experimentar** con ideas diferentes hasta que encuentre un sistema que pueda aplicara su trabajo, a quienes trabajan con usted y que contemple sus formas de trabajo y niveles de riesgo. Aprenda de sus errores.

### Las barreras de Seguridad

Como ha notado antes, necesita preparar barreras para que las personas no accedan a su información a menos que así lo decida.

La información guardada sobre soporte en papel es bastante fácil de proteger porque es voluminosa; debería detectar cualquier sustracción. La información digital o electrónica es más difícil de controlar porque se copia muy fácilmente; alguien podría irrumpir en su oficina con una computadora portátil, transferir "su" información hacia el otro equipo, y usted no tiene manera de saber que información han llegado a copiar.

*Una palabra de cautela - si su sistema también dispone de un buen índice, o una muy buena clasificación de archivos y cajas o directorios, entonces es más fácil para las personas localizar la información delicada dentro de ese sistema de archivo.*

*Por consiguiente, es una buena idea tener algunas excepciones e incluso algunas*

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

*reglas prácticas "ilógicas" respecto a su propia forma habitual de trabajo, de manera de asegurarse que sus archivos mas sensibles no se detecten facilmente a otros que tengan capacidad para analizar su "lógica" de trabajo. En concreto: considere aplicar "distintas" logicas de organización a su trabajo de organización de archivos.*

### Protegiendo su información

Hay varias maneras en que su información puede verse comprometida (en orden creciente de severidad):

**La infiltración** - las personas que desarrollan su trabajo en su oficina, o formando parte del grupo con quien trabaja, pueden lograr un acceso más fácil a su información;

**El robo** - las personas logran acceder a sus equipos, a su computadora o a la información (copiando, dañando y/o destruyendo);

Los **procedimientos estatales** - el uso del poder del estado para ganar acceso a sus sistemas y computadoras y llevarse su información (vea la discusión debajo);

**Incendio provocado** - la manera más rápida y eficaz de prevenir el trabajo de activistas o competidores, es incinerar su equipo e información, como para evitar que puedan seguir trabajando eficazmente en el futuro.

Resguardarse contra los primeros dos es bastante simple - las barreras de acceso básicas y las medidas de seguridad previenen sobre el acceso ilegal, y si el hecho ocurre, puede reponerse rápidamente.

Resguardarse contra procedimientos legales (o no tanto) y el incendio provocado es más difícil, y finalmente inútil. Prevenirse eficazmente contra un incendio provocado puede ser caro, y se resuelve más eficazmente guardando copias de la información importante y archivos en otra ubicación.

Ser eficaz para reponerse de las consecuencias inmediatas de un ataque o de una incursión, implica que debe asegurar también que siempre puede solicitar el acceso o pedir prestado una computadora compatible con el equipo que estaba usando.

### La Intervención Estatal

Resguardarse de una acción de los organismos estatales implica un conjunto diferente de problemas.

El propósito de tener barreras de acceso es aumentar la cantidad de tiempo necesario para ganar acceso a su información. Aquéllos que buscan acceso en forma circunstancial a sus datos y equipos pueden detenerse si tiene buenas barreras de acceso que les implique usar mucho tiempo en ser superadas.

Cuando las acciones son producidas por actos estatales oficiales, no tienen este condicionamiento. Pueden actuar abiertamente todo el tiempo necesario. Puede emplear personal y herramientas de especialistas para ayudarles a conseguir el acceso a sus

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

datos. También tienen los recursos jurídicos completos como para anular cualquier acción que usted haga para detener o frustrar sus esfuerzos por lograr el acceso. Y tarde o temprano, lo conseguirán.

No importa qué seguridad física tenga usted en el lugar de trabajo; los funcionarios del estado entrarán en sus ambientes y pertenencias violentamente y destruirán o quitarán el equipo de computación si ellos creen que tiene la información oculta allí. Incluso si ellos no están contentos, tomarán a las personas que ellos creen tienen la información que buscan y los retendrán o los interrogan hasta que ellos se la revelen. Los más grandes riesgos normalmente se presentan cuando tiene un buen sistema de seguridad, ya que las personas que poseen las contraseñas de los sistemas o los códigos de encriptación, o quién conoce la situación de como se resguardaron los datos, serán las que reciban la mayor presión para revelar lo que saben.

Aunque las barreras de acceso no proporcionan una protección eficaz a la acción del estado, pueden proporcionarle tiempo valioso para permitir que tome otra acción. Por ejemplo, llamar al apoyo legal u a otra organización que le pueda proporcionar la ayuda necesaria. Si usted tiene buena una buena seguridad física, también podría tener tiempo de encriptar las bases de datos sensibles, o resguardar su trabajo actual fuera de la computadora, en algún lugar oculto, para el caso de que se lleven la computadora.

La mejor defensa contra las incursiones del estado es tener muchas copias de la información que estima más valiosa repartida entre varias personas. En caso de una incursión ellos pueden hacer circular las copias y pueden publicar el trabajo de aquéllos que han estado sujetos a la acción del estado, según las instrucciones les haya dado. Del mismo modo, pueden iniciar acciones para proteger o resguardar su seguridad física personal.

### Las barreras de Seguridad

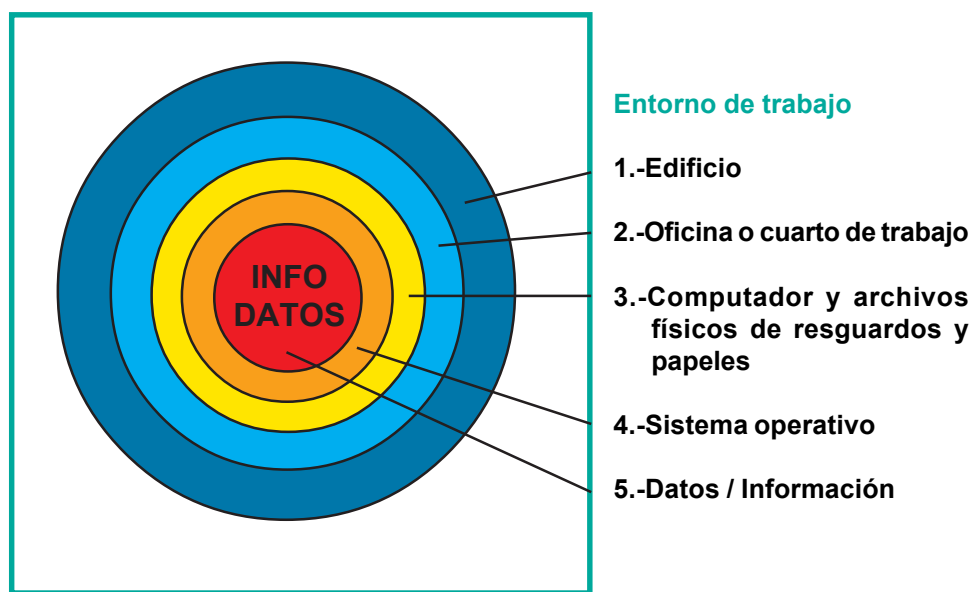
Un sistema de Seguridad está compuesta por capas de protección que proveen barreras de acceso. Debe construir diferentes capas de protección - como las capas de una cebolla - alrededor del equipo y la información importante. necesita proteger el acceso a:

- 1.-El edificio o local dónde se localizan su equipo y/o archivos;**
- 2.-El cuarto dónde se localizan su equipo y/o archivos;**
- 3.-El hardware de su computadora(s);**
- 4.-El sistema operativo instalado en su computadora(s), y donde se guarda cualquier caja o armarios dónde imprimen información;**
- 5.-Sus archivos y datos (incluso la información en papel).**

Otro problema importante son los servicios, como la energía eléctrica, redes, comunicaciones e Internet que penetran a través de dichas capas. Éstos también deben controlarse si quiere tener una seguridad eficaz. En particular, las redes o conexiones de Internet deben usar cortafuegos ("firewalls" en inglés) para prevenir el acceso remoto a la misma red. También debe considerar otras maneras por las que puede abrir una brecha de seguridad secretamente y puede intentar minimizar la posibilidad de que eso ocurra (vea el Resumen Nro.: 7: Vivir bajo vigilancia).

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

### Niveles de Seguridad para analizar:



### Nivel 1: Asegurar sus pertenencias

Afianzar su edificio es una acción de sentido común. ¿Si perdiera sus llaves, podría entrar en su oficina? Si puede encontrar una manera de entrar, es probable que alguien más pueda encontrar la misma manera de hacerlo.

Necesitará considerar primero los tres tipos de intrusión que puede esperar:

Los **ladrones oportunistas** sólo quieren su equipo, no los datos que contiene. Una buena puerta y cerraduras, también en las ventanas, normalmente son bastante como para evitar que logren acceso. Los ladrones oportunistas no tienen ninguna motivación fuerte para entrar en su propiedad específicamente - ellos escogerán cualquiera que esté vacía, o la propiedad que sea más fácil de ingresar. Una buena seguridad externa los podrá detener.

Los **robos planificados** (donde alguien está intentando entrar en sus propiedades debido a quién es usted y a lo que usted hace) es una cuestión diferente. Aunque tenga una buena seguridad externa, estos ladrones intentarán superarla y si tienen los recursos necesarios, lo harán. Su defensa debe ser proteger los artículos (equipos, información, documentos, dinero, etc) que probablemente estén buscando.

Las **incursiones hechas por el estado** y/o policía no puede prevenirse, pero puede llegar a hacerla más difícil. Si ellos no pueden entrar con su cooperación, ellos forzarán su entrada. Si intenta esconder las cosas en el edificio, ellos realmente destruirán alegremente el edificio hasta encontrarlas. No hay posibilidad legal de ocultación ante un mandato de registro (mandamiento de registro, orden de cateo u orden de allanamiento, según se diga en cada país), no hay ninguna acción que pueda intentarse sobre este punto. Ellos convertirán toda la oficina en un gran desastre y la destruirán hasta encontrar lo que buscan.

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

### **Planifique una incursión o ataque catastrófico**

*Una parte importante de la evaluación de los riesgos que debe considerar en "que pasa si..." son los dos problemas mas significativos (dependiendo de cual sea el caracter de su trabajo, por supuesto):*

**-una incursión o procedimiento de la fuerza del estado, o  
-un ataque de quienes buscan remover o destruir sus datos y equipos.**

*En el caso de una incursión usted debe tener establecidos los procedimientos a realizar:*

*-llamar o informar a otras personas y/o organizaciones que trabajen con usted, obtener apoyo legal, si es posible inmediatamente, en orden de minimizar los daños o el impacto de la incursión; disponer de una red de amigos y soportes que puedan activar inmediatamente su causa y le permitan difundir la situación del raid así como acotar y condicionar los posibles efectos, las acciones del poder estatal, y las condiciones de detención y eventual liberación de personas, si las hubiera.*

*-clasificar la información como: "General", "Irreemplazable", o "Sensible" le permite a proveer la protección adecuada a cada tipo con mínimo esfuerzo. Si la información es clasificada adecuadamente, resguardada según su importancia, y protegida según su sensibilidad, la pérdida de información no debe producir mayor obstáculo para su trabajo.*

*-si aplica técnicas de encriptación a la información más sensible y las contraseñas no están fácilmente accesibles, puede asumir que la información no estará disponible (pero debe prever que esto no pasará si alguien que conoce las claves es presionado para revelarlas)*

*Lo más importante es que debe asegurarse que pueda reconstruir sus elementos de trabajo y volver a comenzar. Por esta razón debe intentar realizar algún acuerdo con quien pueda darle acceso a un computador compatible con el suyo donde pueda volcar la información resguardada. También deberá asegurarse que si los programas originales, las copias y sus licencias son destruidos, pueda obtener nuevas copias de las licencias desde sus fabricantes, así como de los programas y aplicaciones, para poder reinstalarlos cuando consiga un nuevo computador de reemplazo.*

*Finalmente, luego de una incursión o ataque, **debe cambiar TODAS las contraseñas** o claves, tanto de computadores, sistemas operativos, acceso internet, correo electrónico, y programas de encriptado que utilice usted y su grupo. Debe generar nuevas claves y al mismo tiempo resguardar las viejas para poder descifrar los datos sensibles que se hayan copiado anteriormente y re-encifrarlos con las nuevas claves.*

Al evaluar las medidas de **seguridad físicas**, considere los puntos siguientes:

**Las puertas** - Usar una cerradura automática (que cierre sola) le impedirá a las personas abrir la puerta desde el interior sin una llave, haciéndole más difícil quitar el equipo. Puede fortalecer las puertas. Ellas solo necesitan ser lo bastante

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

fuertes como para evitar que alguien pueda abrirlas haciendo presión con una palanca o dándoles puntapiés con una bota. Si la puerta es demasiado fuerte, la brigada de incendios no podrá entrar si su edificio está bajo fuego en una situación de incendio (accidental o provocado).

**Ventanas** - Use cerraduras (o cierres) fuertes para asegurar los marcos de la ventanas (los ladrones profesionales llevan una gran variedad de llaves inglesas y alfileres que abren con facilidad los cierres normales de las ventanas). Los ladrones a menudo pueden romper los vidrios de una ventana pero como es arriesgado pasar por esos vidrios rotos, de forma que impedir una apertura fácil de los marcos es una medida práctica de disuasión.

Un vidrio blindado o de mayor espesor puede ayudar a prevenir también ese tipo de acceso, pero también puede atraparlos si hay fuego adentro. Lo mismo se aplica si usted instala rejas o barras sobre las ventanas. Le da mayor seguridad pero incrementa el riesgo en caso de incendio para sus ocupantes.

Si usted obstruye una ventana que puede ser un medio de escape en una emergencia, asegúrese que el marco en donde se sujetan las barras o rejas sea tipo bisagra y pueda abrirse rápidamente desde el interior con un mecanismo adecuado a una emergencia..

**Las paredes** - es más fácil quebrar una pared débil que una puerta fuerte. Muchos de los edificios más nuevos no tienen paredes interiores sólidas, sólo divisiones o particiones o paredes de materiales livianos. Si necesita una buena seguridad, necesitar considerar la probabilidad de que alguien quiera ingresar desde otra parte del edificio. (el caso de las bóvedas bancarias puede ser tomado como ejemplo extremo de este tipo de protección)

**Los espacios en el tejado o techo** - Si usted comparte los espacios del tejado con edificios u otros sectores inmediatos, debe instalar cerraduras para prevenir el acceso por estas áreas de la construcción.

El tejado y los espacios del techo son buenas ubicaciones para los dispositivos de escucha y vigilancia porque ellos otorgan espacio para los equipos, y además tienen cables y fuentes de alimentación que los atraviesan.

Como los sistemas de alarmas para cubrir todos los sectores de los edificios son muy costosos, deberá estar atento a las señales indicadoras de intrusiones desde un tejado que son agujeros pequeños en el techo, su superficie interior y/o daños o raspaduras de la pintura cuyo origen no sea explicado fácilmente por deterioro normal o trabajos específicamente realizados por usted o su personal. Debe restringir la posibilidad de acceso de las personas al espacio del tejado en general..

### Nivel 2: Asegurando la habitación o cuarto de trabajo

Puede afianzar una casa u oficina hasta cierto punto, pero no tanto como para que en una emergencia no pueda ingresar ayuda cuando usted realmente la necesita.

Una vez que ha hecho lo posible para asegurar su edificio debe considerar asegurar su cuarto, o cuartos donde usted guarda la información delicada.

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

Hay cosas básicas que puede hacer:

-**Instalar cierres y/o cerraduras** en cualquier apertura que tenga el cuarto, sean puertas, ventanas y/o cualquier ducto de ventilación / acondicionamiento de aire, ductos de ingreso de cables de energía eléctrica y/o comunicaciones.

-**Use armarios y cajones para guardar el material**, y cierrelos con llave o fíjelos a la pared o al piso para detenerlos estando alejado.

-También pueden **fijarse a estantes o bancos de trabajo** (o echarle el cerrojo) a los **equipos vitales**. Puede conseguir anaqueles o jaulas de metal para las computadoras, asegurando estos sistemas importantes al suelo o a los estantes. Rejas con cerraduras en esos gabinetes (o racks) permiten un nivel adecuado de protección.

-Aunque los **sistemas de la alarma** para un edificio entero pueden ser caros, puede mejorar la seguridad de un cuarto utilizando sistemas simples que descubren el movimiento dentro de un cierto espacio, sin necesidad de realizar mucha instalación de cables adicionales.

Tenga en cuenta que solo sistemas con sensores combinados permiten asegurarse contra intrusiones más profesionales. Detectores de movimiento por temperatura, por ultrasonido, por rayos infrarojos, peso, etc son varios de los disponibles en nuestros mercados.

### Nivel 3: Sus equipos (Hardware) de computación

El hardware de computación (los componentes físicos de su sistema) normalmente viene con varias características que hacen más difícil (aunque no imposible) que las personas desautorizadas puedan usar el sistema de computación.

Estas opciones son una mezcla de cerraduras físicas y "de firmware" (el hardware programable):

La mayoría de las computadoras tiene la posibilidad de configurar una contraseña para dar entrada al inicio o encendido del computador.

La contraseña se graba en una área de memoria dentro de los circuitos de las computadoras, pero sólo es segura si la persona no puede conseguir el acceso al interior de la computadora. Si accede a su interior y desconecta la batería (o realiza un puente o inserta un switch, según sea el caso), la contraseña se borrará de la memoria después de una hora (o antes) y cualquiera podrá iniciar la computadora. Pero... si el intruso no supo la contraseña original, sabrá que alguien violó su acceso.

Algunas (pero no todas) las computadoras tienen "puertas traseras" instaladas en el firmware de la computadora. Ellas permiten a la policía, consultores de seguridad, etc., lograr el acceso al sistema con una contraseña confidencial única a cada tipo de sistema de computación. Si duda, pregúntele al fabricante antes de comprar el sistema. Aunque cada día más, los mismos fabricantes advierten públicamente que están instalando estas puertas traseras (o "backdoors" en inglés) para, supuestamente, cumplir con los requisitos que están imponiendo muchos gobiernos.

Las cerraduras de teclados son pequeñas cerraduras de activación en el frente de la

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

computadora que desconecta el teclado del sistema de computación, haciéndolo inutilizable.

Las cerraduras de teclado se fuerzan fácilmente, o pueden puentearse (saltarse, desviarse) manualmente si alguien logra acceder al interior de la computadora - no son por consiguiente ninguna garantía para restringir el acceso.

Las cerraduras de la unidad de diskettes son almohadillas planas insertadas en la unidad de diskettes (como un disquete flexible normal). La mayoría requiere de una llave para insertarla o retirarla. Si alguien intenta quitarla sin la llave, dañará la unidad de disco, haciéndolo inutilizable.

El objetivo de una cerradura de la unidad de diskettes es prevenir el levantamiento de datos del sistema, pero pueden superarse fácilmente - por ejemplo, simplemente reemplazando la unidad de diskettes original por otra sin cerradura.

Un dispositivo para hacer removible el disco duro ("rack and caddy", en ingles) permite que el disco duro entero de la computadora pueda ser quitado fácilmente y guardado en un lugar seguro bajo llave, o trasladado fuera de la oficina. Ésta es la opción más segura para los sistemas de computación. Si el disco duro conteniendo todos los datos del sistema, está alejado, no hay ninguna manera posible de accederlo, obviamente en el lugar original.

Como contrapartida, estas unidades de disco duro pueden ser quitadas fácilmente por los visitantes no deseados mientras están insertadas en el dispositivo del computador, por lo que se utilizan pequeñas cerraduras para bloquear la remoción fácil del disco. Todas las observaciones hechas sobre las cerraduras de teclados y de equipos son aplicables en estos casos también, con la excepción que mientras esta instalado la llave no bloquea el acceso desde el sistema sino su simple remoción.

Algunos computadores incluyen gabinetes que se cierran con llave para prevenir el acceso al interior del equipo. Pero muy a menudo, las cerraduras son de baja calidad y pueden forzarse fácilmente. Sin embargo, usted puede comprar tensores con cerraduras o incluso gabinetes, o jaulas, con cerraduras más fuertes en su frente, de forma de poder fijar el computador a una mesa, un escritorio, el piso, otra superficie o a un rack.

Son buenos dispositivos antirrobo porque no solo previenen la remoción completa de la computadora, sino que también impiden el acceso a su interior y a los componentes removibles que pueda contener y al mismo tiempo permiten controlar incendios en los equipos.

Hasta donde quiere llegar en asegurar el acceso a su hardware, dependerá mucho del tipo de amenazas que está contemplando.

**-El robo del oportunista** - Fijar con llave su equipo a un escritorio o a una superficie de trabajo es la opción más segura. Algo menos de seguridad con alguna dificultad puede asegurar la base de su gabinete a la superficie de trabajo donde está su computador.

**-El robo planificado** - Si alguien está detrás de sus datos, ellos pueden superar cualquier seguridad que el hardware puede ofrecer, con la excepción de unidades de disco duro removibles. Para proteger sus datos, instale una unidad de disco

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

duro removible, y quite la unidad y lleve a otro lugar con acceso mas seguro y controlado al final del día y tendrá la mejor situación posible dentro de este tipo de análisis.

El hardware, en particular el monitor (la pantalla) emite ondas electromagnéticas muy fuertes. Éstas señales pueden recepcionarse usando equipos especiales a unos cientos de metros de donde está usando la computadora. Alguien con el equipo adecuado puede reproducir la imagen que usted está viendo en su computadora (el código militar para este tipo de sistema es "tempest")

Si bien esta posibilidad es real, del mismo modo que es posible captar a distancia las señales generadas al tipear en un teclado, no son equipos accesibles a cualquiera.

Si está preocupado porque la información que está desplegándose en su sistema es tan sensible que usted no puede arriesgarse a ningún descubrimiento, deberá adquirir un costoso escudo (o blindaje) para su monitor.

Este tiene una malla de metal que corre dentro de la carcasa del monitor, y la pantalla de vidrio se entrelaza con los alambres de la malla, para prevenir las emisiones de ondas electromagnéticas. La opción más fácil es usar una computadora portátil que posee un tipo de pantalla (monitor de plasma, cristal líquido o matriz activa, etc) que tienen muchísima menos emisión de radiación o agregar o cambiar nuestro monitor por una pantalla del mismo tipo (de las que ahora se llaman "planas").

Si quisieramos sitios realmente seguros, deberíamos contemplar cabinas con blindaje electromagnético para realizar su trabajo con máxima seguridad.

### Nivel 4: Su sistema operativo

Como hacer más seguro su sistema operativo depende fundamentalmente del tipo de amenazas que usted enfrente. Si quiere asegurarse contra daño eventual o robo, los sistemas operativos no proporcionan mucha protección adicional. Si quiere protegerse contra el robo o daño de los datos, el sistema operativo es muy importante.

Windows (el sistema operativo del escritorio más popular en el mundo, hasta el momento) no tiene casi ninguna seguridad a nivel del sistema operativo:

- Puede superarse fácilmente el control de acceso de las cuentas de cada usuario

- Una vez superado el acceso al sistema, todas las áreas del sistema están abiertas a la lectura y escritura de datos.

- Algunas versiones de Windows, como NT (o versiones mas nuevas, 2000, XP), tienen una buena seguridad y segregación de partes del sistema entre usuarios diferentes. Pero el sistema operativo Windows es notoriamente fluctuante cuando se analiza la seguridad, y la mayoría de sus características de seguridad pueden superarse.

- Facilmente pueden dañarse o adulterarse por equivocación los programas y archivos que hacen al funcionamiento del sistema, porque Windows no les impide a los usuarios tener acceso a los mismos.

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

-En particular el Outlook (programa de correo electrónico de Windows), es muy susceptible a los virus de computación.

Debe entenderse que hay dos conceptos contrapuestos y casi excluyentes:

**Seguridad siempre se antepone a comodidad.** Mientras Windows ha sido un sistema desarrollado para darle comodidad al usuario, padece de toda la inseguridad que ello ocasiona. El objetivo de automatizar funcionamientos ha permitido que sea al mismo tiempo fácilmente vulnerable al responder en forma autónoma sin tomar recaudos para evitar procesos no deseados o voluntariamente dañinos a los datos y sistemas.

Una casa sería más cómoda de ingresar sin tener que abrir cerraduras... pero sin lugar a dudas sería más insegura.

La mejor manera de tener seguridad aplicada en la capa del sistema operativo está en la encriptación del disco duro.

Si usted usa Windows que usted debe ser consciente que:

*La encriptación del disco que viene con las últimas versiones del sistema operativo no es muy fiable, y puede ser fácilmente "superado" por la policía o consultores de seguridad.*

*Es posible conseguir programas para encriptar porciones del disco duro en los sistemas de Windows, pero ellos no son totalmente fiables ya que siempre hay áreas del disco no encriptadas donde pueden grabarse, en forma temporal, y por tanto estar disponibles a cualquiera que tenga el conocimiento como para explorar y leer la superficie del disco.*

*La encriptación del disco duro usa mucho poder del procesador, y por consiguiente sólo debe usarse en las computadoras más poderosas; ya que disminuirá la performance en forma muy significativa en las computadoras más lentas.*

Una manera simple y eficaz de proteger su sistema cuando las computadoras están encendidas es usar un protector de pantalla con la protección de contraseña activada: Si deja su computadora, y se demora más tiempo del que usted supone, el protector de pantalla se pondrá en marcha después de unos minutos y previene que otros estén viendo su trabajo, quiten datos o adulteren los volúmenes de su computadora. Si está trabajando en algo sensible, y quiere dejar la computadora, puede activar el protector de pantalla para impedir un acceso ocasional a su sistema. Si sale para contestar el llamado a su puerta, y pasa a ser un ataque o procedimiento estatal, el protector de pantalla puede cerrar con llave la computadora para prevenir el acceso. Para que esto ocurra, debe fijarse un límite de activación no mayor a 3 o 4 minutos y de ninguna manera impide que vuelva a accederse al equipo si este se reinicia.

Los protectores de Pantalla no son totalmente seguros. Hay maneras de engañarlos, aunque necesitaría la ayuda profesional para hacerlo.

### Nivel 5: Protegiendo sus datos a nivel del programa

Muchos programas incluyen niveles de seguridad donde los usuarios usan contraseñas para acceder a los procesadores de textos, planillas o bases de datos.

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

Los sistemas de las protecciones por contraseña disponible con la mayoría de los programas de escritorio (u oficina) de uso corriente son completamente inseguros. Ellos trabajan negando simplemente acceso al archivo; como ellos no encriptan los datos de un archivo, permiten que puedan ser leído los datos guardados por quien sabe cómo hacerlo.

Otros sistemas trabajan "picando" ("hashing" en ingles) los datos. Éste es un formato muy débil, de bajo nivel de encriptación que es fácilmente quebrada. Puede encontrar disponibles en internet los programas que le permiten hacer esto.

La forma principal de trabajar al nivel de seguridad de los programas es usar programas de encriptación segura, como el PGP, que encripta los archivos. (vea el Resumen Nro.4 de Uso de encriptación y Firmas Digitales) .

No debe confiar en la encriptación como forma de tener seguridad total en sus datos. Cuando edita (modifica) los datos en su computadora, los programas usan áreas del disco duro para crear archivos temporales de trabajo. Estos archivos no se borran totalmente del disco duro cuando cierra el archivo que está revisando, y estos datos siguen estando, probablemente por varios días más disponibles para quien sepa leer el disco en bruto.

Recuerde que el caso mas común en los diversos sistemas operativos que utilizamos, cuando borra un archivo, en realidad solo se marca en el disco que el espacio que ocupaba está disponible... y los datos continúan allí, hasta que otro programa necesite ese espacio.

El único resguardo cierto contra esto es encriptar su disco duro a nivel del sistema operativo.

Una opción menos fiable es usar un programa que al ejecutarse borra las áreas sin usar de su disco duro con datos aleatorios y elimina completamente cualquier archivo temporal que no esté en uso . Si usa esta clase de programa, debe recordar ejecutarlo en una forma regular, ya que su olvido pondrá en riesgo su seguridad.

El otro aspecto esencial de seguridad a nivel de programas está relacionada con el mantenimiento del sistema y su protección contra virus de computación. Hay una gran variedad de programas específicos disponibles para ayudarle en esta tarea:

- Las herramientas de limpieza para usar en su disco duro, reparan y quitan los datos corruptos del sistema. Esto hará su sistema más rápido y más fiable, y también lo ayudará respecto a su seguridad.

- Cuando se borran los archivos, realmente no se anulan - ellos simplemente son eliminados del índice de archivos en el disco. Puede conseguir programas que hacen sobregabación del espacio ocupado anteriormente por dichos archivos borrándolos con datos aleatorios y sin sentido.

- Quite los archivos dañados (usando las utilidades como Scandisk para Windows), y reorganice los archivos en el disco en un orden más lógico (usando utilidades como Defrag para Windows). Esto hará que sea más difícil para los intrusos acceder a los archivos que se han anulado y/o a cualquier archivo temporal que se haya creado cuando revisó o editó sus datos.

- Use un programa anti-virus para sistemas operativos que son susceptibles a los virus. Principalmente para aquéllos que estén usando el sistema operativo de

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Windows, y utilicen tambien el software para Internet y Correo Electrónico basado en ese sistema.

Recuerde que debería actualizar su sistema operativo y/o programas mas expuestos cada vez que se anuncia un "parche" o corrección del programa original por problemas de mal funcionamiento y/o debilidades frente a posibles ataques o virus. Tambien debe consultar previamente si dicho parche no ocasionará problemas en su instalación (que a veces, sucede).

Ningún software Anti-virus puede garantizarle protección. Simplemente porque primero se produce el virus y luego de su difusión es detectado, estudiado e incorporado a los antivirus para su protección. En los tiempos que estamos viviendo, el período de tiempo entre que se detecta circulando y que se produce la vacuna (en el mejor de los casos) puede estar en el orden de 1 semana o más. Esto significa que aunque tenga un antivirus actualizado a la fecha de hoy, puede estar siendo afectado por un virus aun desconocido y que recién podrá inmunizarse (reiteramos, en el mejor de los casos) dentro de 1 semana.

Nuevos virus se recopilan y analizan todo el tiempo, así que si es usuario de software antivirus, prepárese a pagar por las actualizaciones en forma regular, o utilice sistemas o programas en versiones freeware o sistemas y programas menos expuestos a la acción de los virus

La mayoría de los virus de computación atacan a sistemas Windows, y se propagan a través del Outlook como correo electrónico, o a través del navegador (internet Explorer). Usted puede mejorar la seguridad usando una alternativa al Outlook para el correo electrónico, al Explorer para su navegación (Mozilla, Opera, etc) , o incluso usar un sistema operativo alternativo que mantenga un nivel superior de seguridad y esté menos expuesto, por su diseño, tal como Apple Macintosh o el sistema operativo GNU-Linux, FreeBSD, etc.

Los programas de la encriptación tienen a menudo otras funciones útiles dentro de ellos. Algunos tienen funciones que borran completamente los datos del disco (vea anteriormente). Otros tienen funciones de cifrado que borran áreas sin usar de un disco para quitar archivos borrados y cualquier archivo temporal creado por el sistema operativo (vea anteriormente).

La mayoría de los programas tiene una opción que le permite grabar automáticamente a intervalos regulares ("autosave") y esto le permite regresar a las copias anteriores de archivos con que está trabajando en caso de necesidad.

Ésta es una buena manera de asegurarse contra la pérdida de información si se bloquea o "cae" (en el sentido de dejar de funcionar) la computadora cuando está trabajando, o si anula una cantidad grande de datos accidentalmente y no puede deshacer esa operación y regresar a los datos originales. Creando la copia de seguridad también copia formas de acceder a versiones más viejas de sus archivos y en consecuencia acceder a los datos perdidos.

Esto puede ser útil si revisa y edita un archivo equivocado o elimina datos en forma equivocada o regraba sobre un archivo y no puede recuperarlo. Únicamente una copia de resguardo anterior podrá permitirle recuperar la situación previa a la falla o error.

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

### La persistencia

Los archivos en papel son fáciles de destruir. Se pueden tirar o hacer "pulpa", o las partes o secciones más sensibles pueden sobrescribirse con tintas indelebles (observe igualmente que ya hay técnicas complejas que permiten relevar los datos tachados con tintas). Pero los datos resguardados en soportes informáticos son mucho más difíciles de eliminar:

Las computadoras guardan grandes cantidades de información muy eficazmente. Nosotros ya discutimos anteriormente que incluso cuando se borran archivos, en realidad quedan "restos de datos" (en todo o en parte) dentro de su disco a menos que usted haga una sobrescritura del mismo con nuevos datos, coherentes o no.

Esta propiedad de "*persistencia*" de los datos puede terminar incriminando a aquellos cuyo trabajo puede disgustar a los poderes del estado o a otros grupos. Esta *persistencia* también presenta un riesgo al momento de retirarse el personal. Por consiguiente, la persistencia de la información puede, sin duda, poner en riesgo su seguridad.

Los problemas de esta persistencia se incrementan particularmente cuando usted resguarda datos en discos como los CD de sólo escritura (CD-Rs). Éstos no pueden borrarse. No pueden sobrescribirse. Ellos deben destruirse cuidadosamente (la manera mejor de destruir un CD-R es romperlo en y cortarlo en cuatro o mas pedazos con una guillotina). Otros medios de soporte de información, como son las cintas magnéticas de resguardo o discos de gran capacidad, deben ser procesados (destruidos, eventualmente) cuidadosamente al final de sus vidas activas.

A menudo nosotros tenemos fallas en los soportes de resguardos de información por su uso habitual. El desgaste produce que una cinta magnetica, por ejemplo, no pueda utilizarse más, luego de "x" cantidad de veces de ser usada. Y debemos tener en cuenta que, a pesar de haber quedado inútil para su uso habitual, técnicos expertos pueden llegar a reconstruir información de sectores o partes que no esten dañados. Debe contemplar entonces, desarmar y asegurar la destrucción total del soporte magnético de esa información.

Si un disco duro falla, no podra asegurar la desmagnetización de toda la información que contiene. La única via posible de destrucción es desarmar su carcaza, tomar los platos internos (los discos en si mismos) y partarlos, cortarlos y disponer sus restos en diferentes lugares por separado para asegurar que no puedan recomponerse, y para ello deberá usar seguramente, herramientas de corte de gran fuerza.

Los CD-R (discos de solo escritura) debe cortarse o procesarse en tiras delgadas (algunas destructoras de papel pesado pueden realizar este trabajo. Consulte su manual de operación o su proveedor)

En el caso de cassettes, deben quitarse las cintas, cortarse las bobinas que contiene por la mitad (o en cuatro) y los pedazos pequeños se deben dispersar al azar con diferentes deshechos.

Los disquetes flexibles también pueden ser un problema porque las personas tienen una tendencia a enviarnos "floppies" que contienen los archivos sin dar ninguna importancia al contenido que pudo albergar anteriormente. Si los datos no se borraron sobrescribiendo totalmente el disco o haciendo un re-formato completo, parte del mismo puede estar

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

accesible aún para usuarios con poco conocimiento técnico (un simple programa “unerase” o de desborrado, puede habilitar un archivo viejo, supuestamente borrado)

Debe prestar una cuidadosa atención a la disposición de sistemas de computación y componentes cuando ellos alcanzan el fin de sus vidas útiles. Los discos duros no sólo contendrán la información personal inicialmente muy sensible; ellos también pueden ser los soportes donde tiene los datos para proteger la seguridad de otra información con que usted trabaja, como contraseñas o llaves de encriptación. La simple función de “borrar” los archivos **no es en absoluto suficiente**.

Antes de disponer cualquier equipo de computación, borre completamente el disco duro usando un programa que sobrescriba los archivos. Igualmente, antes de reemplazar el disco duro por uno nuevo.

### El correo electrónico y la Internet

El uso de correo electrónico y la navegación por la Internet, para intercambiar datos presenta también problemas de persistencia. Dependiendo de los requisitos que impusieron por ley (según los diferentes países), algunos Proveedores de Servicios Internet (ISP) guardarán algunos o todos los datos que ha transferido por Internet. De acuerdo a esto, no solo estará visible, potencialmente, el texto que usted envía, sino también los archivos que adjunta. La única solución a este problema es enviar toda la información que considere delicada o sensible (sea por motivos personales, como institucionales, comerciales, políticos, etc) usando mensajes y archivos adjuntos encriptados.

Aún así, por el solo hecho de haber enviado sus datos a través de internet, genera, por sí mismo, datos adicionales relacionados al tráfico de esa comunicación: todo proceso de mensajes registra, en forma normal y desde el inicio de los sistemas de correo electrónico, quién envía, a quién lo envía, cuando lo hace - fecha y hora - así como desde qué lugar se conecta (lugar de red, no necesariamente físico, pero siempre es posible asociar ese lugar de red a un teléfono - que también puede registrarse - o la punta del enlace o la banda ancha utilizada) y el camino o ruta por donde circula el mensaje, el tamaño de lo que envía y eventualmente, su contenido. Si bien no es norma (salvo en algunos países) registrar o guardar copia de su contenido, esto es posible de hacer y pasa totalmente inadvertido para el usuario final.

Estos datos del tráfico de comunicación, aún sin tener copia del contenido, es una información muy valiosa para los sistemas de vigilancia de los estados y servicios de seguridad ya que permiten identificar nexos entre personas u organizaciones leyendo e interpretando los datos de tráfico de los mismos. Si bien para esto se requiere acceder a un caudal de datos realmente enorme, ya disponen de la tecnología para hacerlo (y lo están haciendo en numerosos países).

### Avanzando más allá de la seguridad pasiva: “la contravigilancia”

Afianzar el espacio donde trabaja es el primer objetivo. Si cualquiera puede caminar en él y usar sus computadoras u otro equipo, no tiene seguridad. Pero después de eso debe considerar utilizar o desarrollar sistemas que le permitan detectar y eventualmente evitar la vigilancia de sus actividades.

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El primer elemento a considerar es la seguridad de la propia computadora. Así como debe asegurar su sistema operativo, tal como lo hemos escrito anteriormente, debe tomar el camino de afianzar su hardware o equipo. Puede usar cerrojos y dispositivos de cerradura. Pero es saludable utilizar algún tipo de sello o marca que ayude a detectar que un tornillo ha sido girado o una puerta de gabinete ha sido desplazada.

Una opción para controlar no solo equipos de computación sino también cualquier dispositivo o mobiliario que este cerrado, es implementar marcas que necesariamente deben ser destruidas o dañadas visiblemente si se intenta abrir dichos equipos. Tome un cepillo muy fino, y una tarro (o pote) de pintura de esmalte con un color elegido al azar (o una mezcla especial de colores) y traze una pequeña línea encima del hueco diminuto entre la cabeza del tornillo y la base del gabinete (pero no pinte encima de la cabeza del tornillo!). Entonces, si los tornillos se desenroscan se deshace la pintura y la intrusión será obvia. La razón de escoger un color aleatorio es que cualquier esfuerzo por restablecer la marca de la pintura se descubrirá a menos que ellos puedan coincidir con su color. (poco probable si disponen de poco tiempo y no han "visitado" el sitio físico con anterioridad).

Debe asumir que todas las cerraduras mecánicas pueden ser abiertas en un operativo donde actuen profesionales. Por consiguiente no asuma que las cerraduras buenas aseguran su área de trabajo. Busque afianzar su lugar de trabajo más a fondo, previendo que aunque accedan al lugar físico, se pueda frustrar el acceso a la información allí guardada. Hay varias opciones para hacer esto:

*-Asegure que usted tiene cerraduras de buena calidad. En los cuartos interiores las cerraduras son normalmente de una calidad mas baja. Usted puede mejorar la seguridad usando mejor calidad de cerraduras con llave en las puertas interiores.*  
*-Defina un área cerrada con llave dentro del lugar donde guarda el material sensible, de forma de hacer más difícil el acceso al mismo. Si este espacio puede contener armarios o gabinetes de almacenamiento más específico con cerraduras de buena calidad y los puede fijar al piso y/o a la pared, mejora su seguridad en este aspecto.*  
*-Un sistema de la alarma en las puertas o ventanas puede proporcionar buena seguridad inicial. Pero alguna clase de detector de movimientos (ya hablamos de los diversos tipos existentes) permite una mejor detección a distancia por si alguien logra burlar los sensores en la aperturas. Si bien los sistemas de alarma son caros, los detectores de movimiento proporcionan un medio barato, ya que requieren realizar un mínimo cableado dentro del edificio y trabajan cubriendo un área grande del espacio a controlar. Tenga muy presente que hay muchos tipos de estos sensores y debe tratar de elegir aquellos que sean más difíciles de engañar: por ejemplo, que puedan detectar si alguien simplemente los ha tapado con material atermico.*

Aquéllos que desean acceder a su información, si realmente es así, pueden quebrar sus sistemas de seguridad y finalmente acceder a ella. Por eso, el objeto de implementar sistemas de seguridad en su entorno de trabajo tiene como objetivo hacer más difícil el acceso, así como prevenirse del robo en general.

El acceso planificado es un problema mayor, porque además tratará de evitar que advierta que alguien ha intentado (o logrado) acceder a su información. En estos casos, la seguridad en su ambiente de trabajo deberá tender a forzar las evidencias que resalten que ese acceso se ha producido. Si detecta un acceso ilegal, puede (y debe) incrementar sus niveles de seguridad habituales.

## 1 - INTRODUCCION A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

---

Si detecta que se ha intentado acceder a su ambiente de trabajo debe realizar una exploración y búsqueda completa, lo mas profundamente posible sobre toda el área involucrada.

Su primera meta debe ser verificar que todas sus computadoras están intactas. Luego debe verificar que las copias de seguridad de los datos y los discos que guardan la instalación de los programas están intactos e incorruptos. Si encuentra que se estuvo tratando de acceder a su computadora, debe asumir que la computadora puede haber sido contaminada con un virus u otro programa que permita intrusiones por via electrónica. Debe desconectar el equipo de cualquier red antes reencender el computador, extraer todos los archivos de datos que no pueden portar virus y limpiar el disco para re-instalar el sistema operativo y los programas usados en su equipo.

Después de solucionar los problemas inmediatos que genera cualquier esfuerzo por acceder a su espacio de trabajo (reemplazo de cerraduras forzadas, vidrios de ventanas, etc, también deberá verificar sistemáticamente todo su equipo de comunicaciones. Pueden controlarse los accesos a las instalaciones telefónicas y de otros equipos de comunicaciones utilizando la técnica simple de pintar esas líneas de pintura como se ha descrito anteriormente. Esto pondrá en evidencia cualquier esfuerzo por abrirlas. Pero también debe verificar cualquier daño a las paredes, techo o suelo del cuarto, o cualquier esfuerzo por enmascarar el daño de la pintura. Esto puede ayudar a descubrir si se ha instalado algún dispositivo de vigilancia. Deben verificarse también los enchufes así como toda tapa de instalaciones eléctricas y artefactos de iluminación que son lugares ideales para estos dispositivos por la posibilidad de conectarlos a fuentes de alimentación de energía externas y hacerlos de uso ilimitado.

Si cuenta con el equipo adecuado, deberá hacer una exploración radioeléctrica, barriendo toda el área sensible, como para chequear que no se haya instalado ningún dispositivo que esté transmitiendo (sonido y/o imagen) hacia el exterior de dicha área. Pero a menos que usted tenga o alquile un equipo de exploración profesional, lo más probable es que, eventualmente, solo pueda detectar equipos de escucha o vigilancia de tecnología muy básica o amateur.

La contra-vigilancia es una tarea difícil y se describió de manera general. Esto es porque en general, los requerimientos de seguridad en la computación son muy diferentes, siendo muy específico a la situación y diseño del area y del equipamiento que debe ser protegido. Hay una información mas extensa sobre este problema en el Resumen Nro.: 7 - Viviendo bajo vigilancia.

## 2 - RESGUARDANDO SUS DATOS

Este Resumen es el segundo de la serie de Seguridad y Privacidad de la Información. Los temas que trata son:

- Por qué, cuando y cómo usted debe resguardar los datos e información de su computadora.
- El almacenamiento, seguridad, costos y legalidad
- Organizando su información
- Los métodos de resguardo
- Los problemas a considerar:
  - la longevidad,
  - seguridad,
  - recuperación y
  - redundancia
- Los discos de instalación
- Resguardando con Linux

### ¿Por qué "resguardar"?

**Nota de traducción:** El término en inglés: "BackUp" es ampliamente utilizado sin modificación en muchos de los países hispanohablantes. De todas formas, aplicamos una de las posibilidades de traducción a los fines de mantener coherencia en el texto. "BackUp" se puede traducir como "Respaldo" o "Resguardo". Ambos son conceptos similares y equivalentes a los fines prácticos y esperamos no impidan captar la esencia de este tema.

La información sobre su computadora es muy vulnerable: los discos duros pueden fallar, los sistemas de computación pueden fallar, los virus pueden borrar un disco, los operadores descuidados pueden eliminar los archivos, y los operadores muy descuidados pueden anular áreas enteras de los discos duros por equivocación. También pueden dañarse las computadoras o pueden ser robadas. Por estas razones resguardar sus datos es esencial. Esto involucra la generación de copias de los archivos esenciales de su sistema y el mantenimiento de esas copias en otra computadora o en medios de almacenamiento adecuados.

Asegurarse de que usted puede recomponer rápidamente su información es importante a la hora de definir cómo organizar su información en su computadora. El objetivo es lograr que cada usuario tenga un área propia, fácilmente identificable y fácil de encontrar en el disco.

Esto se logra preparando una serie de directorios (O carpetas, según se llame en su sistema operativo este tipo de ordenamiento interno de los archivos) en el disco que contiene las diferentes áreas de trabajo de un usuario. Esto es lo que generalmente se denomina "**área de trabajo del usuario**" ("workspace" en inglés, y en algunos sistemas, se denomina también su "**home directory**") - un área del disco que contiene todo lo relacionado al trabajo individual de cada usuario y que sólo él, en principio, puede acceder.

Este tipo de organización de información permite que pueda identificar fácilmente las áreas que son propias de un usuario y no están compartidas con otros, como forma de evitar la duplicación de información en copias de resguardo. Usted sabe que esas áreas deben copiarse específicamente porque nadie más las comparte.

No es mala idea plantearse la organización de las áreas del disco en dos aspectos,

## 2 - RESGUARDANDO SUS DATOS

---

cuando definimos los accesos por grupos de usuarios:

**Áreas verticales:** donde incluimos el acceso y el intercambio de archivos de todo un sector, como por ejemplo: centro documental, administración, prensa, etc, a donde tendrán acceso todos los que pertenecen a ese sector, y,

**Áreas horizontales:** donde incluimos todos los usuarios que poseen el mismo nivel de acceso (y/o seguridad) y a donde se ponen los archivos que se pueden compartir entre quienes comparten este nivel. Los niveles superiores (que requieren acceder a material más sensible) pueden acceder a todos los niveles inferiores y así sucesivamente. Por ejemplo: los coordinadores tienen su área de intercambio así como los gerentes la suya, y los empleados y operarios la suya.

No está demás resaltar que esta organización respetará la forma organizativa que tiene cada grupo o institución o movimiento.

### Cuándo resguardar

Resguardar (respaldar) los datos puede ser una tarea difícil donde hay muchos archivos para copiar. La primera regla del resguardo eficiente es minimizar la cantidad de datos que tiene guardados y quitar, descartar o destruir los archivos inútiles o anticuados, actualizando regularmente su sistema.

También es importante incorporar el hábito de usar distintos tipos de resguardar los datos (diferentes soportes, diferentes lugares, etc) con el objetivo de aumentar la fiabilidad de su "resguardo" y asegurar la posibilidad de poder recuperar la información y sus sistemas.

Debe considerar realizar resguardos:

- Cuando ha hecho una cantidad grande de trabajo en un período corto de tiempo; debe resguardar todos los sectores de su área de trabajo.

- Cuando ha completado la parte principal de un proyecto / trabajo - debe limpiar el directorio que contiene los archivos temporales así como de los archivos de trabajo que ya no tienen utilidad y luego copiar todo el área involucrada en su desarrollo (no olvide imágenes, fotos o gráficos que pueden estar en otros directorios compartidos)

- Como criterio básico, debe copiar todos sus archivos personales (su propia área de trabajo) así como todos los archivos esenciales del sistema, que le permitan reponer la misma situación de trabajo anterior al evento que nos requiera recurrir a la copia de resguardo. No se olvide la importancia de resguardar copia (o los datos esenciales para obtener una nueva copia u original) de los programas que esté utilizando, así como tener el equipamiento compatible que garantice que puede volver a la misma situación anterior.

De nada sirve una buena y completa copia, si para acceder a los datos por ella guardada requerimos un equipo que se dejó de fabricar varios años atrás...

### Cómo resguardar

Cómo usted va a realizar los resguardos depende del tipo de equipo usted tiene, y del

## 2 - RESGUARDANDO SUS DATOS

---

volumen a resguardar, así como del soporte elegido para respaldar la copia.

Resguardar su trabajo actual es un trabajo simple; es improbable que haya generado un volumen muy grande de datos y se puede incluso realizar con una buena reorganización de los datos en su disco local, así como eventualmente alguna copia a discos extraíbles, sean o no flexibles.

Dentro de una organización es más probable que tenga una red de computadoras, y que pueda organizar parte de su resguardo usando recursos (normalmente otros discos) compartidos en la red. Se puede destinar, en forma absoluta o parcial, una de esas computadoras como para mantener las copias de resguardo de los sistemas y los datos.

En una rutina regular de resguardo, es importante la copia de los archivos de datos actualizados de su área de trabajo, pero también lo es la copia de los diccionarios propios que cada usuario que ha utilizado, tipografías especiales, los directorios usados en los programas de correo electrónico, sus agendas de direcciones, así como las historias de navegación y los índices de favoritos o marcas de navegación de cada uno, así como los archivos esenciales del sistema y todos los datos compartidos por los usuarios que no estén incluidos en sus propias áreas de trabajo.

Haga los arreglos necesarios para garantizar que copias de resguardo estén ubicadas fuera de la ubicación central de su trabajo, al menos en otro edificio cercano, pero no tanto como para que se pueda ver afectado, por ejemplo, por un incendio. Estos resguardos no serán probablemente actualizados en su proceso de resguardo diario, pero le garantizan poder reconstruir todo el contexto de trabajo con sus computadoras si ocurriera una catástrofe (natural, accidental, ocasional o intencionada). Aún en caso de grandes incendios, si dispone de una copia fuera del alcance eventual del fuego (una estimación práctica es contemplar guardar copias a una distancia mayor a 200 metros) usted sabe que cuenta con un punto de partida más actual a los fines de reprocesar la información de los últimos 15 días, un mes o una semana de trabajo.

### El almacenamiento

Otro problema respecto a los resguardos es cómo se guardan los datos. Según sean los diversos formatos de los datos originales, es posible pre-procesarlos, comprimiendo y/o buscando redundancias (coincidencias, reiteraciones) de forma de ocupar menor volumen final en el resguardo además de contemplar si debe pensar en cambiar los formatos originales. (este tema, relacionado con la longevidad y durabilidad de los datos lo trataremos más adelante).

Muchas personas usan programas que comprimen grandes cantidades de datos en un espacio menor, y que empaquetan varios archivos pequeños en otro archivo más grande.

Aunque ésta es una manera útil de resguardar datos en el corto plazo, en un plazo más largo implica tener consideraciones de seguridad y problemas de fiabilidad.

Los formatos en que se almacenen los datos en los archivos son también fuertes condicionantes a la hora de evaluar la posibilidad de leer nuevamente una información generada, por ejemplo, con un procesador de textos de hace 20 años atrás. Del mismo modo, un programa de compresión puede dejar de existir o simplemente no puede utilizarse a partir de alguna actualización del sistema operativo e invalida la posibilidad de descomprimir y reutilizar los datos del archivo original de resguardo.

## 2 - RESGUARDANDO SUS DATOS

---

### La Seguridad

Los resguardos de información tienen también otras implicancias de seguridad.

Cuando la información en el computador esta protegida dentro de diferentes tipos de barreras de seguridad, los datos de una copia de seguridad son mas vulnerables, ya que son una estructura abierta, fuera del control de acceso del sistema operativo e incluso de los mismos programas, estan soportadas por un dispositivo normalmente portátil (cinta, disco removible, CD-R, CD-RW, Memoria compacta, etc) que facilita su extracción, y debe entonces encarar seriamente la ubicación del resguardo y el control de acceso al mismo en los mismos niveles que tienen los sistemas y áreas principales.

En situaciones donde tenga que recuperar datos especialmente sensibles, es más seguro plantearse un sistema de respaldo de información mas común, con un control de almacenamiento normal y un juego de copias de los datos sensibles, resguardados con un control de almacenamiento mayor, en ubicaciones separadas.

### Los costos

Fundamentalmente, sus políticas de resguardo / respaldo de información son simplemente una cuestión de dinero (y/o de importancia política estratégica) . Si un computador almacena todo el trabajo que usted ha producido durante 2 años, y el costo de producir ese trabajo es \$5 a \$10 por hora, el valor de la información que contiene esa computadora podría ser \$15,000 o más si tuviera que rehacerse. Esto sin contemplar que habrá muchas cosas que seguramente no puede reconstruir más. Si el valor de una computadora es de solo \$1,000, y el costo de almacenamiento de un disco o CD está entre \$1 a \$10 cada uno, el resguardo de información es imprescindible a la hora de comparar el perjuicio económico que ocasionara la pérdida de su información. Debe evaluar el uso de los sistemas de respaldo de información como cuotas de un seguro que evitan (o minimizan) la pérdida masiva de datos de su negocio o de la actividad de su organización.

### La legalidad

Hay implicaciones legales al momento de decidir que resguardar. Cuando la ley de derechos de propiedad intelectual se vuelve más restrictiva, afecta los derechos legales que usted tiene para realizar copias de seguridad o resguardo de la información de su disco duro.

Cuando la información se ha creado por alguien más, sea un libro o un correo electrónico, técnicamente es propiedad de esa otra persona u organización. La copia de resguardo de información solamente para su propio uso, es una área gris en la ley en muchos países. Pero dónde más de una persona tiene acceso a los datos, por ejemplo como parte de un organizacion comunitaria o grupo, pueden plantear que hacer copias de información para otras personas sin su permiso es una infracción a sus derechos de propiedad intelectual. En algunos países éste será un delito penal, aunque en otros será una ofensa civil dónde el dueño del derechos de propiedad intelectual debe intervenir y promover la causa.

La manera más fácil de encarar los problemas de derechos de propiedad intelectual en los sistemas de resguardo es separar la información según el carácter legal de su origen y disposición, su grado de libertad para ser copiada y eventualmente distribuida. De esta forma, usted copiará solo la información que tiene posibilidad legal de ser copiada y eventualmente, realizara las copias permitidas (mucho software comercial admite una única copia de resguardo a fines de superar problemas de deterioro y/o destrucción del

## 2 - RESGUARDANDO SUS DATOS

original - lea la licencia que acompaña al software). Usted no debería copiar a discos u otros soportes la información que no puede ser distribuida a otras personas u organizaciones.

Recuerde que muchos de los problemas legales se pueden superar, utilizando software del tipo "fuente abierta" o "software libre", ya que no tienen límites en cuanto a la cantidad de copias y distribución sin modificación de los originales.

En general, situación normal, **debe intentar evitar** copiar/resguardar:

*-Cualquier software - sea el original de instalación o los programas instalados - donde hay posibilidad que una copia puede terminar en las manos de alguien más;*

*-Cualquier página web o correo electrónico donde el la página o el correo electrónico contiene un mensaje de derechos de propiedad intelectual específico; (hay incluso quien plantea que si la información no dice claramente que es de libre disponibilidad, usted esta sujeto a padecer acciones legales si la copia sin permiso específico)*

*-Cualquier información, y sobre todo los libros y los trabajos multimedia, a menos que ellos tengan una autorización específica, o que circulen específicamente bajo la licencia de "open content" es decir, contenido de libre disponibilidad, respetando siempre las cláusulas de especificación del autor/autores*

### Organizando la información:

Que tan eficaz es su sistema de resguardo depende de cuan bien organizada está su información.

Si su computadora tiene el muchos datos insignificante mezclados con sus archivos más importantes usted el corre el riesgo de borrar o eliminar datos importantes al editar los de menos valor. Usted también gastará tiempo y dinero para resguardar una gran cantidad de información mayor de la que realmente necesita guardar. La Organización de información teniendo en cuenta su importancia también significará que usted usa su sistema de computación más eficaz y eficientemente

Para asegurar la buena práctica en la organización de su información, usted debe:

*-Use directorios (o carpetas) para cada usuario dentro de su computadora y áreas diferentes para cada trabajo. De esta manera usted puede guardar todos los archivos, y directorios que contienen un proyecto entero, el área de trabajo entera de un usuario, o los datos de todos los usuarios que usan una computadora en particular.*

*-Asegúrese que los archivos compartidos entre muchos usuarios se guarden separados de los archivos individuales de cada usuario.*

En más detalle, esto significa:

*-Siempre tenga un directorio para cada usuario que usa la computadora, y quizás un 'área para el usuario invitado', un directorio para los usuarios ocasionales (si los hubiera);*

## 2 - RESGUARDANDO SUS DATOS

---

-Intente guardar el trabajo finalizado y el trabajo en proceso en lugares separados; el trabajo acabado debe resguardarse para un almacenamiento a largo plazo mientras que el trabajo en proceso debe resguardarse regularmente, dejando fuera los archivos de resguardo más permanente ahorrando espacio en los soportes del resguardo ;

-Al empezar un nuevo proyecto, siempre cree un directorio para él y guarde toda la información relacionada al proyecto en ese directorio - de esta manera puede guardar una copia de seguridad regular del proyecto copiando el directorio entero de una vez;

- Cuando el proyecto contiene un volumen grande de archivos, intente dividir en más subdirectorios esa información, de manera de admitir copias de resguardo en diferentes soportes. Esto es dependiente de que tipo de soporte esté utilizando (fundamentalmente capacidad y velocidad de transferencia-copia);

-Si está usando una red para acceder y hacer el resguardo, siempre intente guardar los archivos que todos compartimos separados de los de cada usuario. Entrene a los usuarios en el hábito de colocar y actualizar los archivos compartidos en determinadas ubicaciones - esto previene sobre la confusión que se genera cuando hay diferentes versiones del mismo archivo guardadas en diferentes áreas del sistema en la red.

Organice su resguardo de forma que reproduzca la organización de trabajo que tiene en su computador. Esto significa que en caso de que un archivo o un disco completo se dañan o adulteran, el trabajo puede restaurarse fácilmente; también significa que pueden restaurarse las copias de resguardo recreando el mismo entorno de trabajo que los usuarios ya encuentran familiar.

### Los métodos de resguardo

No hay ninguna manera correcta específica de resguardar. Dependerá de:

- qué tipo (forma) de datos tiene usted,*
- cuántos datos desea resguardar (volumen)*
- qué equipos (dispositivos) y programas usará para el resguardo*

Hay varias opciones para resguardar cantidades pequeñas y grandes de datos. Los factores críticos que necesita considerar son los costos y la capacidad involucrada en cada opción además del período en que pueden sostenerse los datos sin padecer degradación o corrupción. Otro elemento importante a considerar cuando maneja grandes volúmenes de información es la velocidad en que se procesan las copias de los datos.

### Los disquetes flexibles

Todos los PCs (por el momento) vienen con una unidad de diskettes. Hasta no hace mucho tiempo la capacidad del disquete flexible era suficiente para resguardar los datos de un usuario normal. Pero con el tiempo, los programas se han hecho más complejos, los archivos han crecido y el tamaño de los discos duros también ha crecido de algunos megabytes a varios gigabytes (recuerde, 1000 MB = 1 GB). usar diskettes flexibles para resguardar estos discos duros de gran volumen ya no son una opción viable.

## 2 - RESGUARDANDO SUS DATOS

A pesar de su pequeña capacidad, los disquetes flexibles son todavía una buena manera de resguardar cantidades pequeñas de datos - respaldando el trabajo de un día por ejemplo. Pero los disquetes flexibles se están utilizando menos hoy día por el uso creciente del correo electrónico y el desarrollo de internet. Anteriormente las personas enviaban los datos de un lugar a otro mediante la copia en diskettes mientras ahora la misma información viaja largas distancias como archivos adjuntos a los correos electrónicos

Tabla de comparación de capacidad y costo		
<b>Baja capacidad</b>	<b>Bajo costo</b> disquete flexible - 1.44MB correo electrónico - 1 a 2MB	<b>Alto costo</b> servidor seguro - 1 a 25MB
<b>Capacidad media</b>	Disco ZIP - 95MB- 240 MB Disco CD (CD-R) - 550 - 700 MB	Disco Jazz - 900 a 2000 MB Disco CD re-grabable CD-RW - 550MB Memorias Portátiles 8 - 512 MB
<b>Alta capacidad</b>	Cintas QIC 500 - 4,000MB	Cintas DAT o sistemas de 8mm 2,000 - 7000 MB o más Disco DVD (DVD-R) 4,700MB Disco DVD regrabable (DVD-RW) 4700 a 9000 MB Disco duro removible 20000 MB a 80,000 MB o más+
Todas los datos están en megabytes - MB (1 MB = 1 millón de bytes o caracteres)		

### Las redes locales

Resguardar datos sobre una red local, a otro computador en el mismo cuarto o en el mismo edificio, puede hacerse a gran velocidad y manejar grandes volúmenes de datos, permitiendo incluso compartir dispositivos más profesionales de resguardo, como unidades de cintas, discos removibles, grabadoras de CD o DVD. De todas formas, seguirá teniendo el problema de como resguardar los archivos que se localizan en cada una de las computadoras y que no han sido copiados a la red y el control de acceso a estos equipos.

Cuando hace una copia de resguardo a los discos de una red, está realizando un resguardo a otro disco duro. La posibilidad de que dos discos duros fallen en forma simultánea es muy remota, de forma que podrá recuperar la información en la eventualidad del fallo de uno de los discos recuperando lo guardado en el otro.

Muchos sistemas de red incluso trabajan con discos espejados, es decir, que automáticamente copian la información de uno en el otro, de forma tal que si uno falla continuará trabajando con el otro casi sin notarlo. Por supuesto que la implementación de este tipo de sistemas depende fundamentalmente de los costos, es decir, la pérdida económica, que puede ocasionar el corte que se produce cuando falla un disco y se paraliza la actividad de todas las personas involucradas en ese sistema.

## 2 - RESGUARDANDO SUS DATOS

*El único problema que usted tendría con una red local sería si se robaran todas las computadoras de su oficina al mismo tiempo. Para prever esta circunstancia, debe asegurar mucho más el equipo que utilice para hacer resguardos en dicha red, sea colocandolo en jaulas que lo fijen a la habitación, o en un armario ventilado y con muy buena cerradura, hasta ubicarlo en un lugar diferente, lejano y no lógico para instalar un equipo, de forma de tener mas margen frente a una incursión no prevista.*

### La Internet

Una opción más segura es realizar un backup a través de internet hacia un server seguro, o hacia otra persona con quien ya tenga un acuerdo para resguardar sus datos. Estos equipos pueden encontrarse en otra ciudad, en el mismo país, o mejor aún, en otro país donde las leyes sobre privacidad y protección de datos brinden mejor protección para su información.

Este tipo de resguardo proporciona mayor seguridad porque traslada su información a un ámbito físico distinto al habitual, dificultando enormemente las incursiones planificadas, y al mismo tiempo, asegurando disponer de copias de información fuera del alcance de desastres locales, naturales o provocados (inundaciones, incendios, terremotos) y agregando la posibilidad de disponer de la información bajo otras normas legales, que puedan ser mas beneficiosas para usted y el trabajo de su organización.

Hay dos opciones:

*-Con un servidor seguro usted puede acceder el sistema cuando quiera para guardar o recuperar los datos. Usted debe poder guardar los datos en un formato encriptado para que sólo usted pueda accederlo, pero la conexión entre su sistema y el servidor debería contar también con algún sistema de encriptado para que la transferencia tambien sea segura y nose modifiquen los datos durante la misma.*

*Para esos estados dónde guardar los datos en formatos encriptados es un problema, o donde la posesión de cierto tipo de información es un problema, los servidores seguros son una solución simple para la seguridad del datos.*

*-Si usted tiene un acuerdo informal con otros activistas o grupos en otro país, usted puede intercambiar la información vía Internet y ellos pueden cuidar una copia de sus datos.*

El único problema con esto es que, en general, los traslados no son automaticos, debe confiar en que guarden los datos en forma cuidadosa y que se lo devuelvan o pueda acceder a ellos cuando lo necesite. En muchos casos, usted puede hacer este trabajo en forma rutinaria, compartiendo su información con otros grupos y activistas para que ellos tambien la usen. De esta forma, sus datos están más seguros porque otros también los tendrán y podrán seguir usándolos aunque su trabajo sea censurado, restringido o incluso prohibido o eliminado.

El problema que debe evaluar seriamente cuando plantea hacer una copia de resguardo via internet es el volumen de información que debe transferir. Las conexiones por acceso telefónico si bien son suficientes para la mayoría de los intercambios de correo y navegación web, son claramente insuficientes para transferir grandes volúmenes de información.

## 2 - RESGUARDANDO SUS DATOS

---

Tenga en cuenta que conexiones telefónicas de 56 kbps (el máximo normal de los modems actuales) solo permite transferir alrededor de 300 kbytes por minuto, unos 18 MB en una hora (en la práctica, unos 15 MB o menos).

Si en cambio utiliza conexiones tipo “banda ancha” con velocidades de 128, 256 o 512 kbps, usted podrá transferir entre 45 MB a 180 MB. Pero debe tener en cuenta que siempre depende no solo de la velocidad de su conexión, sino también de los enlaces que esté usando (y usted no controla esto) hasta el server seguro a donde se está comunicando.

### Unidades ZIP/JAZZ

Las unidades ZIP y JAZZ son dispositivos que manejan discos removibles de alta capacidad.

Las unidades ZIP pueden tener discos de 100 MB y de 250 MB según el modelo que adquiera. Algunos modelos pueden conectarse al puerto Paralelo (se intercalan entre su impresora y la computadora) o en puertos tipo USB o SCSI, con unidades externas en ambos casos o pueden instalarse como unidades internas, en las variantes IDE, SCSI, como si fuera una unidad de diskette adicional de alta capacidad y velocidad.

Las unidades JAZZ se diferencian porque poseen mayor capacidad, con modelos entre 1 y 2.5 GB (1000 y 2500 MB).

El único problema que debe encarar es cuánta cantidad de datos necesita resguardar y donde va a guardar los discos una vez grabados. Los discos JAZZ son indicados para resguardar archivos grandes como los que se generan al trabajar con video digital, mientras que los tipo ZIP son indicados para resguardo de trabajos en proceso, tanto diario como mensual. No son lo mas indicado para resguardar mucha información en forma permanente porque necesitaría muchos discos y su valor es significativo.

Debe tener en cuenta que no es una tecnología muy difundida, pero es altamente segura en cuanto al funcionamiento de los dispositivos y la baja tasa de fallas en los discos, además de admitir muchísimos ciclos de grabación, regrabación, borrado y lectura de los datos.

Como contrapartida, perderá mucha información si pierde o deteriora un disco JAZZ, mucho más que si pierde un disco ZIP.

Las copias en discos ZIP brindan un muy buen medio de resguardar la información a corto y mediano plazo.

### Unidades de cinta magnética QIC / DAT / 8 mm

Las unidades de cinta magnética pueden estar ubicadas tanto dentro de su computador (muchos servers de media performance las poseen) o como unidades externas, conectadas por alguna de las interfases del computador (normalmente, puertos SCSI, e incluso Paralelo o USB en dispositivos de menor costo)

## 2 - RESGUARDANDO SUS DATOS

---

Hay de varios tipos:

*-QIC ("cartucho de un cuarto de pulgada") Son unidades de cinta que trabajan en forma semejante a los reproductoras/grabadoras de los cassettes de audio. Las cintas QIC tiene capacidades de entre 40 MB a 4 GB.*

*-DAT ("cinta de audio digital") o de 8 mm, son unidades que trabajan en forma similar a los grabadores de video; en general son dispositivos de mayor costo, menor tasa de fallas y mejor velocidad. Hay dispositivos que manejan de 2 a 20 o 30 GB. e incluso existen unidades robotizadas para poder usar numerosas cintas de resguardo y procedimientos de rotación de uso, sin intervención humana.*

Estas unidades permiten realizar copias parciales o totales de los discos duros. Su uso esta limitado por el costo de adquisición. Aunque el valor unitario de las cintas es el de menor costo relativo al volumen de información que puede almacenar. Puede conseguir cintas a un costo de unos \$ 35.- y almacenar un disco que cuesta 4 veces más, aunque la cinta usa un menor volumen físico y peso.

Debe evaluar muy seriamente la velocidad de transferencia (de copia) de cada unidad al momento de definir su compra, porque esto condiciona seriamente la realización de los procesos de resguardo. Si la unidad es muy lenta para el volumen de información a transferir para su resguardo, terminará NO haciendo los resguardos (o no haciéndolo en la frecuencia que debería hacerlo).

Con este tipo de unidades se pueden establecer procedimientos de resguardo que se realicen mediante la rotación de 7 o más cintas (una por día hábil, 1 cada 15 días y una cada mes, etc) y que garanticen que puede tener diversos puntos de retorno si tiene problemas con su información. Son los esquemas más fiables de trabajo respecto a copias de seguridad. Si a esto le agrega que cada 15 días, o cada mes, usted envía una cinta con la copia completa de su información a otra ubicación física, queda muy protegido frente a cualquier tipo de situación.

Las unidades de cinta de mejores características no son equipos de bajo valor, y las unidades de soporte (cintas) no tienen buena fama respecto a su tasa de fallas. Se desgastan mucho con su uso, al igual que el cabezal de grabación/lectura del dispositivo. Sin embargo, una buena política de rotación de cintas, de limpieza y mantenimiento de la unidad grabadora y de prueba de que los resguardos pueden retomarse sin problemas genera un sistema de resguardo fiable para la gran mayoría de las actividades.

Debe contemplar la situación de robo, pérdida y/o deterioro de la unidad de cinta, para que pueda volver a adquirir (comprar o pedir prestado) un modelo compatible con los datos que tiene guardado en sus cintas de respaldo. Esto puede ser un problema serio en algunas ciudades alejadas de grandes centros urbanos e incluso en países enteros, donde el acceso a dispositivos tecnológicos más profesionales es difícil, e incluso económicamente inviables.

### **EI CD ROM Grabable / Regrabable (CD-R / CD-RW)**

EI CD-ROM grabable y re-grabable puede almacenar de 550 a 650 MB (algunos modelos nuevos, más aún) por disco (normalmente especifican 600, 700 MB o de más capacidad, pero utilizan unos 50 a 100 MB para armar los directorios y la estructura interna de archivos).

## 2 - RESGUARDANDO SUS DATOS

---

Los discos solo grabables una vez (CD-R = 'CD de lectura') es bueno para hacer las copias de seguridad de archivos permanentes, pero puede tener mucho desperdicio ya que en principio solo se graban una vez y no puede adicionar luego mas información. Esto no es estrictamente cierto, porque tiene alternativas para grabaciones que se denominan de "multisesión" y permiten adicionar datos varias veces hasta completar la capacidad del disco, aunque siempre es de única vez., ya que no puede re-escribir lo ya grabado.

Si usa estos discos para generar su resguardo, en la medida que la información crezca y deba reemplazar un CD por uno mas nuevo, tendrá un problema de seguridad al tener que disponer en forma segura de los discos que descartará.

Con la actual caída de los precios de unidades grabadoras y de los discos CD-R en si mismos, es una alternativa muy válida para disponer información en resguardos permanentes, almacenar todos los datos relacionados con un proyecto o trabajo ya terminado, e incluso distribuir información en grandes volúmenes.

Los CD Re-escribibles (CD-RW = 'CD-read/write') es una alternativa mejor para los procesos normales de backup. Los discos pueden agregar, borrar y reemplazar información sin problemas, siendo ideales para el traslado de información de alto volumen con posibilidad de reutilizar el mismo medio de soporte una y otra vez. Aun nose conoce en forma fehaciente la duración de los datos en estos medios pero se estima en 500 las veces que pueden grabarse y regrabarse los datos en estos discos antes de tener deterioros en el material del medio. Cada proceso de grabación en estos discos genera una degradación del material con que están contruidos (polímeros de grabación)

Los CD Re-escribibles, es una alternativa competitiva frente a las unidades de cinta magnética debido a su buena fiabilidad , velocidad de copia, versatilidad y costo bajo (cualquier unidad regrabable puede costar actualmente lo mismo que costaba una unidad de lectura de CD hace pocos meses atrás). Pero las unidades de cinta magnética todavía ganan en la mayor capacidad por unidad.

### Unidades DVD

Los discos DVD-R (sólo lectura) pueden manejar una capacidad de más de 4 Gigabytes y hay versiones de 9 Gigabytes. (1 Gigabyte = 1000 Megabyte)

Si bien los discos no son caros para el volumen de información que manejan, las unidades de grabación pueden costar de 5 a 10 veces lo que cuesta una unidad CD-RW (grabadora-regrabadora de CD). Si bien su costo viene bajando sustantivamente en estos ultimos tiempos, podemos esperar que proxicamente (un año a la fecha de este informe) su costo sea realmente accesible.

Quizás ahora estén fuera de alcance para la mayoría de las organizaciones, pero ya se planifica su adopción para todos aquellos sistemas que guarden grandes volúmenes de información, por ejemplo, bibliotecas digitalizadas, colecciones de imágenes, películas, etc..

Las excepciones actuales son aquellas organizaciones que ya trabajan con medios de comunicación digitales, ya que no solo son necesarios para los procesos de resguardo de archivos grandes, sino que son tambien los soportes para distribuir las producciones multimedia.

## 2 - RESGUARDANDO SUS DATOS

---

Las unidades DVD re-grabables son opciones de costo mayor respecto al volumen de datos a manejar aunque es esperable que esto se modifique en el próximo año.

### Las unidades de Memoria Portátil

De reciente aparición para uso masivo (no están incluidas en el trabajo de APC en inglés) estos dispositivos permiten manejar volúmenes medios y altos de información (4, 8, 16, 24, 32, 64, 96, 128, 256, 512 MB) en unidades muy pequeñas, de escaso volumen y peso, fáciles de almacenar, resguardar y trasladar.

Este tipo de dispositivo contiene una memoria no volátil, es decir, que no necesita alimentación de energía para mantener lo grabado en ella. Tienen un uso casi masivo en todo lo que significa fotografía digital (memorias tipo CF - Compact Flash, MMC - multimedia memory card, SM Smart Media, etc) y está presentándose como alternativa real al uso de los viejos diskettes.

Al no tener partes móviles, es ideal para traslados.

Al tener un volumen físico pequeño, son ideales para resguardar en lugares remotos o bien escondidas.

Los dispositivos que se plantean como alternativa a los diskettes traen incorporados puertos de conexión del tipo USB, lo que les da una buena velocidad de transferencia e independencia de dispositivos lectores adicionales.

Si queremos utilizar las unidades de nuestras cámaras digitales (foto y video) con nuestra computadora, probablemente tengamos que adquirir algún pequeño equipo que lea y grabe este tipo de memorias, y que normalmente vienen con posibilidad de conexión al puerto USB.

Esto nos remite a uno de los problemas de estos dispositivos en la actualidad: dependemos 100% de tener puertos USB en nuestros equipos de computación.

Esto es normal en equipos de 2 a 3 años de antigüedad, pero en equipos más antiguos, estos puertos no existen y la única alternativa, frente a la necesidad de cambiar el equipo completo, es agregar alguna placa adicional que instale esos puertos en nuestro viejo equipo. También debe contemplar que su sistema operativo tenga la posibilidad de manejar estos puertos.

El costo actual de los dispositivos es relativamente alto para el volumen de datos de maneja (0.50 a 1 U\$S por Megabyte almacenado) pero se justifican plenamente en dispositivos donde la capacidad de grabación y regrabación en muy pequeño volumen físico es muy valiosa, como en las cámaras fotográficas y de video.

Se estima que pueden guardar información por el lapso de 10 años sin degradación.

### Las unidades de disco duro removibles

Las unidades de disco duro removibles pueden sostener la misma capacidad de datos que cualquier otro disco actual. Y puede brindarle posibilidades de procedimientos de

## 2 - RESGUARDANDO SUS DATOS

---

seguridad muy eficaces. Sin embargo, puede necesitar mayor ayuda técnica adicional que las otras opciones para manejar inicialmente sus opciones.

Puede establecer una rutina de trabajo para que al terminar el día quite el disco duro de su equipo y los guarda bajo llave, (gabinete ignífugo, caja de seguridad, etc), lejos del mismo.

Una gran ventaja si tiene una red local, ya que también podría disponer de una unidad adicional removible, resguardar el disco principal y volcar en él las copias de resguardo de todos los usuarios de la red y llevar el disco removible a otra ubicación, para incrementar su esquema de seguridad.

Este método es muy eficaz respecto al espacio y volumen de datos resguardados, porque un disco guarda en si mismo muchísima información.

También es una ventaja la velocidad en que se pueden transferir los datos comparando con cualquier otra alternativa accesible en la actualidad. La lectura de un disco y la grabación en otro esta limitada por la velocidad de los mismos y de la conexión entre ambos, y es sustancialmente mayor que las otras alternativas.

El disco duro tiene una buena protección física (debe cuidarlo de los grandes golpes) y el tamaño pequeño lo hace accesible para su traslado y su guarda.

Hay alternativas de discos removibles que viene ya preparados en los equipos que usted compra y también hay Kits para adaptar los que ya tiene, compuestos en general por una bandeja a donde se fija el disco duro y un dispositivo para conectar / desconectar el disco al equipo, mediante su introducción o remoción.

Debe tener en cuenta que el punto débil de estos dispositivos son justamente el funcionamiento de las conexiones, ya que sufren desgaste al introducir y retirar el disco y deben ser preservadas con un buen trato y mantenimiento. Un uso diario de estos dispositivos (por ejemplo si usted retira y guarda su disco en una caja de seguridad al final del día) requiere que la bandeja y el adaptador sean de buena calidad.

Muchos de estos dispositivos tiene fijaciones con cerraduras simples para bloquear la extracción física del disco de la computadora e incluso incluyen opciones de ventilación forzada del disco, que aumentan el tiempo de vida útil del mismo.

En dispositivos mas profesionales se puede encontrar incluso que puede conectar y desconectar sus discos removibles estando el sistema encendido y funcionando (se denominan "hot swap" en inglés) evitando tener que realizar cortes en el uso de los equipos donde se instalan los discos removibles.

Tenga en cuenta que muchas veces el disco duro tiene instalado el sistema operativo, de forma tal que una buena copia podría permitirle instalar el disco en otro equipo y poder retomar rápidamente su actividad en caso de alguna emergencia o problema con el original. En caso de desastre, esta forma de resguardo sólo requiere un computador semejante al original para poder reinstalar el disco duro podrá contar con todas las aplicaciones, programas y datos nuevamente, tal cual estaban al momento de su copia.

Tenga en cuenta que este tipo de disco puede requerir algún tipo de dispositivo controlador no standard (controladora de dispositivos SCSI, por ejemplo)

## 2 - RESGUARDANDO SUS DATOS

---

Podría contemplar también encriptar toda la copia en el disco removible.

Es importante en el momento de definir alternativas, contemplar que programas (software) y/o drivers necesita para realizar los resguardos completos de los datos.

Por último, debe tener presente aquí muy especialmente las consideraciones de organización de la información, sus usuarios y los archivos asociados.

Tenga en cuenta que no es muy factible usar copias de disco duro como alternativa de resguardo para equipos con sistema operativo Windows. Este sistema es altamente dependiente para su funcionamiento del hardware que tiene configurado en su equipo y no se traslada y funciona fácilmente en otro. En algunos casos, puede ser casi imposible.

Tiene que contemplar probablemente nuevos drivers y reinstalar todo o parte del sistema con el consiguiente riesgo de perder información o que haya aplicaciones que no vuelvan a funcionar.

*Una primer consejo básico es definir al menos dos particiones en su disco duro de windows al instalarlo, así puede asignar la segunda partición y sucesivas al guardado de los datos por usted generados. Así, ante un problema serio con el funcionamiento de windows, usted puede llegar hasta a dar formato nuevamente a la partición original de arranque de windows y aun así mantener sus datos en el disco.*

El nuevo Windows XP no trabajaría en absoluto si usted tiene que instalar una copia en otro equipo diferente al original. Con Windows su opción mejor está en conectar su equipo con otro, via puerto USB o via una red local, y realizar una copia de los datos hacia otro equipo, con los mismos programas, de forma de asegurar que las aplicaciones pueden funcionar sin depender de su copia de resguardo de datos.

El sistema operativo GNU- Linux, por otro lado, se presta muy bien a ser usado con unidades de disco duro removible. Es muy portátil, e incluso en computadoras con el hardware muy diferente se puede reconfigurar y continuar trabajando como antes.

### La longevidad (y persistencia), seguridad, recuperación y redundancia

Al resguardar los datos usted está confiando en que el sistema que está usando devolverá esos datos cuando usted los requiera. Hay cuatro problemas importantes que debe considerar para asegurarse que sus datos permanecerán disponibles para cuando los necesite:

**Longevidad** - cuánto tiempo los datos permanecen confiables;

**Seguridad** - proteger los datos de daños o robos;

**Recuperación** - que pueda leer sus copias de seguridad; y

**Redundancia** - asegurarse que tiene bastantes copias, por si tiene algún accidente o daño o pérdida en alguna de ellas.

### Longevidad

La longevidad es un problema importante si busca guardar los datos durante varios años. El tiempo de vida útil y la degradación de los materiales que usa para las copias de seguridad es crítico; tendrá muchos datos guardados en un espacio muy pequeño, y la degradación de esos materiales puede destruir sus copias de seguridad en forma total.

## 2 - RESGUARDANDO SUS DATOS

---

Todos los medios de soporte magnético - disquetes flexibles, discos ZIP / JAZZ, cintas y discos duros - son vulnerables y se pueden dañar por campos magnéticos.

Esto incluye:

- fuentes fuertes de campos electromagnéticos, como el monitor de su computadora, teléfonos y altavoces;
- imanes de cualquier tipo y el campo magnético de la Tierra.

Un disquete flexible guardado sin blindajes apropiados tendrá sus datos adulterados después de unos años porque se dañan por las variaciones en el campo magnético natural de la Tierra, y por la proximidad a los campos magnéticos de los equipos eléctricos que puede tener cerca.

Para asegurar una larga vida a los datos guardada en los soportes magnéticos regularmente debe "refrescar" o renovar la información sobre los discos. Toda la Información guardada en discos ZIP / JAZZ, disquetes flexibles o cintas, deberían copiarse nuevamente a un computador y luego volver a grabarse en los discos cada año o año y medio. Debe aprovechar a reformatar el disco, y reescribir los datos en los discos nuevamente.

Guarde todos sus soportes magnéticos dentro de armarios de almacenamiento de metal, tan lejos de fuentes de campos eléctricos y magnéticos como sea posible. Si piensa guardar el disco por períodos largos de tiempo y no tiene un gabinete de metal adecuado, ponga una capa de metal (film de metal de cocina, por ejemplo) alrededor de los discos para reducir la influencia de campos electro-magnéticos significativamente.

Con las cintas (QIC/DAT/8mm) no tiene el problema de renovar sus datos porque no están siendo usadas para almacenamientos prolongados de información, sino para resguardar la información (total/parcial) de uno o varios discos duros. Debe protegerlas siempre de quedar expuestas a la influencia de fuertes campos magnéticos locales, porque estos siempre pueden degradar la información que contienen. Recuerde que un efectivo blindaje magnético solo se obtiene con la utilización de materiales especiales (mu-metal, etc) de muy alto costo.

Las cintas que deban guardarse por varios años deberían probarse todos los años, haciendo una lectura de test y rebobinando la cinta para evitar que se peguen sus superficies entre sí.

Los **CD ROM** de sólo lectura (CD-R), así como los reescribibles, CD-RW y los DVD-R, no son susceptibles a los campos magnéticos.

Los CD en cambio, son sensibles a la luz, particularmente al componente ultravioleta en la luz del sol, porque degrada los polímeros plásticos del disco.

El soporte del CD grabable también es sensible al calor. El calor puede degradar la película de material donde el CD guarda los datos. Los CD deben protegerse en recipientes fuertes a prueba de luz, y de los cambios extremos de temperatura, así como de los cambios regulares de temperatura.

Todos los medios de soporte de copias de seguridad deben guardarse en condiciones ambientales libres de humedad, y a una temperatura constante. Las variaciones extremas

## 2 - RESGUARDANDO SUS DATOS

de temperatura pueden dañar los plásticos o polímeros que hay en ellos. Las variaciones de temperatura ambiente, también pueden causar daño a través de la condensación, ya que el aire húmedo y caluroso se condensa en las superficies frías de los medios de soporte.

El área del almacenamiento debería estar libre de grandes vibraciones porque esto causará tensión mecánica en los polímeros. También es importante proteger los discos duros, si los usa para resguardar, de la electricidad estática para que no afecte sus circuitos electrónicos; esto se hace fácilmente guardándolos en bolsas antiestáticas.

### La Seguridad

Al realizar copias de resguardo de su información está generando la necesidad de asegurarse que en caso de un robo o incursión, dichas copias no sean fácilmente accesibles. Obtener una copia de resguardo es en sí mismo una muy buena manera de obtener la información que buscan otros sobre su actividad, cualquiera sea, ya que es fácilmente portable y ocupa muy poco volumen físico.

La única manera de proteger estas copias de resguardo es estableciendo barreras físicas para acceder a ellas. Puede encriptar los datos que esta guardando, pero esto tiene implicancias al momento de necesitar recuperar sus datos (vea "Recuperación" mas adelante).

Para prevenir que cualquiera no se lleve sus copias de seguridad:

*-Guárdelas en recipientes seguros que estén fijos al edificio, de forma de evitar que sean removidos y transportados con facilidad;*

*-Separe sus copias de seguridad según la clasificación de sensibilidad e importancia de los datos. De esta manera usted puede guardar sus datos más sensibles bajo la mayor seguridad ;*

*-Considere la posibilidad de armar escenas o "señuelos" en las áreas de almacenamiento poniendo sus datos menos importantes o las copias de seguridad más viejas claramente a la vista, y definiendo lugares mas secretos y seguros para los datos más importantes. Tenga siempre en cuenta las condiciones ambientales de estos lugares (temperatura, humedad, etc).*

*-Si es posible, utilice gabinetes a prueba de fuego (ignífugos) y de agua (estancos)*

La opción más segura, para los soportes de datos y para los archivos en papel importantes, es guardar las copias en otra ubicación física. Aunque las copias de seguridad fuera de su lugar habitual de trabajo quizás no estén tan actualizadas como aquellas que sí están en su oficina, ellas sobrevivirán cualquier esfuerzo por privarlo de sus computadoras y datos, sobre todo por organismos estatales u otros que intenten detener su trabajo. Y confiscar sus equipos y datos es una manera muy eficaz de hacerlo

Otra manera muy eficaz para cualquier otro que desee detener el trabajo de los grupos o individuos es incendiar sus oficinas (una táctica visto en países como EE.UU.). Si prevee tener copias de seguridad fuera de su sitio habitual y puede acceder a otras computadoras, nuevas o prestadas, equivalentes a las que tenía, podrá continuar con su trabajo poco tiempo después de cualquier pérdida catastrófica de datos o equipos.

## 2 - RESGUARDANDO SUS DATOS

---

La verificación de la integridad de los datos guardados en medios o soportes que pueden ser editados (discos magnéticos, CD-RW, etc) debe ser otra prioridad para su seguridad. No necesita verificar los discos de solo lectura como los CD-R, pero debe autenticar la copia de alguna manera como para evitar que la sustituyan por otra. Técnicas de pintura no corrosiva exterior en el caso de los CD-R ya le permiten disponer de cierto indicador físico para intuir una sustitución. El registro (separado y resguardado) de los números de serie del disco CD-R (único para cada disco) también ayuda a su control.

Una mayor seguridad puede tener si considera instalar algún tipo de autenticación usando chequeos de integridad o firmas digitales en sus archivos, en todos o en parte. Esta firma digital o, sistema de comprobación de contenidos no modificados, (Hash, MD5, etc) le permitirá definitivamente asegurar que su copia no ha sido modificada por terceros.

Si las copias de seguridad no se encriptan, no tiene una buena seguridad física, o se guardan en una computadora fuera de su control directo, este tipo de comprobación le ayuda a asegurar que su copia de seguridad no sea manipulada por nadie. Esto no previene que la copia de seguridad pueda leerse. Apenas asegura que nadie puede cambiar su contenido e introducir datos erróneos o eliminar información que usted guardaba, e incluso verifica si algún virus pudo haber afectado la misma información.

La comprobación puede ser tan simple como tener un listado del directorio(o carpeta), (que incluye nombres de archivo, tipo, fecha y hora de última actualización, así como el tamaño de cada archivo) que usted guarda en un disco diferente al soporte a controlar para verificar la información guardada sobre él - en particular el tamaño del archivo.

(No aplicable al caso de algunos virus, que enmascaran su tamaño usando técnicas de compresión de datos que le permiten mantener el tamaño original del archivo que están infectando, sin embargo esto no es viable en archivos que contienen solo datos y no programas).

La manera más segura de controlar la integridad de los datos es aplicando algún tipo de total de control (el mismo concepto que se aplica a los dígitos de paridad en datos numéricos largos o importantes, como cuentas bancarias, documentos, etc) o firmas digitales:

-Un total de control es un análisis numérico simple del contenido de un archivo o grupo de archivos. Hay programas que generan los totales de control, pero ellos no se suministran normalmente con el sistema Windows. Algunos controladores (o programas anti-virus) de virus podrán también generar los totales de control guardados en un archivo separado.

-Una firma digital es un análisis del contenido de un archivo o grupo de archivos que está protegido con una clave y cifrado.

*Pueden forzarse los totales de control. No pueden forzarse las firmas digitales a menos que las personas que modifican los datos tengan la clave para el cifrado. Las firmas digitales pueden ser producidas por la mayoría de los programas PGP de encriptación; el archivo puede firmarse y la firma se agrega al archivo, o la firma puede generarse y guardarse separadamente.*

*La firma o el total de control deben mantenerse alejados separadamente de los datos para que pueda modificarse (aunque una firma no puede falsificarse, puede adulterarse al controlar la autenticidad de una copia de seguridad). Ejecutando la*

## 2 - RESGUARDANDO SUS DATOS

---

*firma o total de control contra la copia de seguridad usted no sólo puede verificar cualquier corrupción de los datos, sino también, si el riesgo existe, que otro haya manipulado los datos de sus copias de seguridad.*

### Recuperación

Debe poder recuperar sus datos. También debe planear siempre que puede necesitar recuperar sus datos en una computadora distinta a la que uso para generar su copia de seguridad. Esto tiene implicaciones sobre la manera en que hace sus copias de seguridad.

*Siempre debe verificar inmediatamente su copia de seguridad después de crearla.*

*Por ejemplo, algunos CD pueden contener errores creados en la parte del proceso de "quemado" o grabado del CD). Ellos no pueden descubrirse en el dispositivo de CD-RW pero puede prever realizar una lectura de la información que acaba de guardar en una unidad normal de CD-R.*

*Si puede leer la copia de seguridad recientemente creada en una unidad común de CD-ROM se asegura que el CD ha sido creado correctamente.*

*Los problemas también pueden ocurrir con los disquetes flexibles porque las cabezas de la unidad de disco están desalineadas. Aunque el disquete flexible trabajará bien en la máquina que se creó, otras unidades de diskettes pueden ser incapaces de leer el disco, en todo o en parte arruinando su posibilidad de recuperar los datos..*

*El formato en que guarda los datos es también un tema muy importante - hay formatos de archivos que se han vuelto anticuados e ilegibles, y algunos formatos de almacenamiento de datos son más fácilmente vulnerables a la corrupción de los datos que otros.*

Si está usando formatos de archivos propietarios (por ejemplo si archiva datos generados por su procesador de palabras) debe asegurarse que está usando un formato extensamente compatible. El formato más reciente de una aplicación en particular puede hacer que los datos que genera tengan poca compatibilidad (o muy difícil de lograr) con los sistemas de otras personas. Igualmente, si está usando formatos de datos menos usados (un problema específico por ejemplo, de usuarios del sistema Linux, si no utiliza opciones más difundidas) puede tener un problema de compatibilidad. Si trabaja en una comunidad más amplia de funcionarios o usuarios de computadora, necesita llegar a un acuerdo en qué formato/s de archivos usarán para asegurar que los datos estén disponibles para el mayor número de usuarios, ahora y en mediano plazo.

La compresión de los datos, usando programas como Pkzip, GNUZIP, etc., es una manera muy útil para colocar muchos datos en un espacio menor.

Hay también riesgos altos involucrados al usar la compresión de datos:

*Si tiene un error pequeño en la información guardada, tiende a perder todo o porciones grandes de los datos comprimidos. Esto se produce porque los datos se procesan como un conjunto largo de datos continuos, un sólo error de lectura en el proceso de descompresión causa la falla, y;*

## 2 - RESGUARDANDO SUS DATOS

*Con la compresión está procesando normalmente más de un archivo, y si bien un error en los soportes de almacenamiento podría causar sólo la pérdida de un archivo, si el error lo tiene en un archivo comprimido, puede perder todos los archivos que tenía guardado dentro de él.*

*Diferente es el caso de que el mismo hardware que maneja la copia de resguardo realiza algún tipo de compresión en su grabación. Algunas unidades de cinta disponen de esas opciones, incrementando la capacidad de almacenamiento de cada unidad de cinta.*

Encriptar los resguardo de los datos puede ser muy arriesgado. Aunque la encriptación de datos representa una manera muy segura de sostener los datos, es arriesgado porque siempre necesita lo siguiente para descifrar sus datos y volver a acceder a ellos::

*-Un archivo pequeño con la clave de la encriptación (llave "privada") y/o*

*-una frase contraseña o clave.*

*-A los fines de mayor seguridad, siempre guarde sus datos encriptados, la llave privada y las claves o frases contraseñas en lugares separados. Si no, disminuye la seguridad que da la encriptación. Recuerde que si pierde la contraseña o llave privada nunca podrá recuperar los datos.*

Como la compresión de datos, la encriptación trabaja con un conjunto continuo de datos. Algunos sistemas de la encriptación también comprimirán inicialmente los datos para reducir el tamaño del archivo creado. Los errores en el almacenamiento o de lectura de los soportes de almacenamiento le impedirán acceder al contenido del archivo encriptado.

Por consiguiente, nunca confíe en un archivo encriptado como su copia de seguridad principal. Las copias de seguridad encriptadas son una manera de protegerse contra una seguridad física pobre, pero siempre debe intentar guardar una copia de seguridad normal en una ubicación más segura.

### Redundancia

Las leyes de probabilidad dicen que, en algún momento, sus medios y/o equipos de resguardo de datos fallará. Usted puede minimizar la probabilidad de este acontecimiento, adoptando las recomendaciones de "buena práctica" que se perfilaron anteriormente. Pero usted siempre debe asumir esto en algún momento: su sistema de resguardo funcionará mal. Para cubrirse de esto, haga copias de resguardo redundantes, para ser usadas en caso de un problema con su última copia de seguridad.

Hay dos maneras de guardar copias de seguridad redundantes:

Las **copias de seguridad históricas** - esto involucra la guarda de una copia de seguridad regular de información, pero sin anular las copias de seguridad más viejas. Esto es muy fácil de hacer con discos CD-R. - ya que guarda una copia en un soporte barato, como estos discos de solo lectura, almacenando los discos mas viejos por si se dañan las copias mas nuevas.

**Copias de seguridad duplicadas** - esto implica que cuando hace la copia de seguridad, la hace en más de un soporte, guardando los dos por si falla la copia primaria. Si le agrega que la copia secundaria se guarda en otra ubicación física, mejora mucho su

## 2 - RESGUARDANDO SUS DATOS

esquema de seguridad.. Esto implica que tiene que poder copiar sus medios de soporte, o realiza la copia de seguridad dos (o más) veces.

Las copias de seguridad dobles tienen la ventaja de que siempre son más actuales que las copias de seguridad históricas, donde seguramente no tiene resguardada la última información con que está trabajando.

Si usa copias de resguardo en CD-Rs, hará las copias de seguridad históricas más eficazmente porque siempre tendrá los discos más actuales encima de las copias de seguridad anteriores. Recuerde que luego de un tiempo, necesitará disponer cuidadosamente de ellos; o podría usarlos como copias de seguridad fuera de la ubicación normal de trabajo.

Hacer un duplicado de las copias de seguridad también generan más trabajo. Si hace una copia directa de la copia primaria, puede estar heredando también los errores generados al hacer la primera copia. Aún con copias de seguridad dobles, cualquier error que salga de su sistema (un error en el archivo o un virus en el archivo) siempre existirá al recuperar sus datos. Con copias de seguridad históricas tiene siempre la posibilidad de remontarse en el tiempo hasta encontrar una versión sana o sin errores de un archivo.

Teniendo este esquema de seguridad, cuando usted actualice las copias de seguridad que tiene fuera de su sitio habitual de trabajo, deberá copiarlas o generarlas dos veces. En la práctica no importa qué opción use - puede escoger cualquiera, o usar las dos en forma conjunta o alternada.

Debe desarrollar sus propios procedimientos de resguardo y seguridad, de acuerdo a las capacidades tecnológicas de su sistema, a los riesgos que asuma y a sus propias necesidades por la forma de trabajo de usted y su grupo.

No importa cómo lo hace, con tal de que lo haga regularmente, la información se guarde en forma segura, y pueda ser accesible y reutilizada si necesita recuperarla

### Los discos de la instalación

Normalmente se tratan los temas de cómo resguardar los datos relacionados con su trabajo con la computadora. Un problema que raramente es considerado es el resguardo de los discos u otros medios de soporte que permiten la instalación de los diferentes sistemas operativos, programas y aplicaciones que también utiliza en su computadora.

Cuando usted instala su sistema o configura su computadora, utiliza el software que proviene de disquetes flexibles o CD ROMs. Éstos son importantes por tres razones:

*-Si los usa o los trata incorrectamente, no funcionarán, y no podrá instalar su software;*

*-Si los pierde, tendrá posiblemente que reemplazarlos, o actualizar sus programas, lo que podría involucrar un gran gasto adicional; y*

*-Si los usa incorrectamente podría infectar sus discos de instalación con un virus - y no podría liberarse de él porque afectaría todo lo que funciona asociado con él cada vez que instala o reinstala esas aplicaciones, y aún si son los originales del sistema operativo.*

El CD ROM (a menos que sean copias de software en CD RW re-escritibles) es inmune

## 2 - RESGUARDANDO SUS DATOS

al ataque de virus porque ellos no pueden modificarse. Sin embargo, los medios de soporte magnéticos - por ejemplo el diskette de inicio que viene con los sistemas operativos, puede infectarse con los virus. Los programas que se descargan desde Internet, como todo archivo ejecutable también puede infectarse (o venir infectado) con los virus.

En la práctica sus discos de instalación no son muy vulnerables al robo ocasional, ya que la registración única del software los hace identificables. Pero si alguien quisiera desactivar el trabajo de un activista o grupo de campaña, no sólo buscaría desactivar su equipo - también tomarían los discos del software. Tomando o dañando los de discos de software buscarán que le lleve más trabajo (y eventualmente, más recursos económicos) volver a empezar porque tiene que comprar u obtener nuevamente el software que utilizaba. Para activistas que están usando muy a menudo sistemas más viejos, con software más viejo esto puede significar también que puede necesitar pagar por uno nuevo, más caro porque las copias de los sistemas más viejos que estaban usando son difíciles de conseguir o ya no las soporta su fabricante (si es que no desapareció).

Cada vez más, las personas están descargando los programas via internet u otras redes, en forma completa, o actualizaciones / parches para los sistemas existentes. Todos estos archivos deben guardarse en cuanto los haya recibido. Y en este caso prestar atención ya que no dispone de discos de instalación originales, aunque muchas veces puede generar su resguardo sobre discos tipo CD-R.

El mayor problema con las copias de seguridad de los programas en CD-ROM son los recientes sistemas de protección anticopia de algunas aplicaciones y sistemas operativos.

Los programas y aplicaciones más viejos, y el software desarrollado para entornos mas abiertos como Linux, no restringen la creación de copias de seguridad. Pero los sistemas propietarios, como Windows, no permiten copiar. Hay dos opciones:

*-Puede intentar y puede engañar a los sistemas de la protección anticopia para hacer su copia de seguridad, haciendo por ejemplo una "imagen" del CD-ROM y escribiendo la imagen en otro CD, si tiene el software para hacer esto. No sólo no pueda hacer este trabajo con algún software, sino que también se puede encontrar cada vez más que este tipo de acción se está volviendo ilegal bajo las nuevas leyes de derechos de propiedad intelectual.*

*-Podría comprar otra copia de la aplicación, en una feria de computación u otro lugar, sin un certificado de la licencia; esto no tiene valor legal técnicamente, pero tendría una sola copia original con una licencia. Guarde esta copia para que, si alguna vez necesita una copia de seguridad, pueda usar este disco con la licencia que obtuvo con su copia original.*

Las leyes que tratan la generación de copias de seguridad son vagas. La práctica durante muchos años era ignorar la restricción de realización de copias de seguridad del original, con tal de que la copia sólo fuera usada cuando la copia primaria estaba corrupta, y el uso subsecuente de la copia de seguridad estaba de acuerdo con la licencia para el software.

Pero las recientes enmiendas en la legislación sobre los registros de propiedad intelectual de muchos países, definen como ilegal la copia de discos, así como prohíben engañar a los sistemas de protección anti-copia que están instalados en los discos. Esto plantea la pregunta acerca de cómo se supone que el público protege su (y a menudo muy caro) software de daño o corrupción. Actualmente el equilibrio se ha roto hacia el lado del beneficio exclusivo de los productores de software

## 3 - CONTROL de ACCESO y CONTRASEÑAS

Este Resumen es el tercero de la serie sobre Seguridad Informática. Trata los siguientes temas:

- Control de accesos y clasificación de los datos.
- Las contraseñas y autenticación
- La utilización de contraseñas
- La utilización de contraseñas para mejorar la seguridad

### Un resumen sobre el control de accesos.

#### **Control de accesos:**

“Control de accesos” es todo aquello que concierne a asegurar que una información es accesible a todos aquellos que la necesiten pero no a aquellos que no deban hacerlo. Esto no siempre se lleva adelante tal como se ve, porque siendo muy estricto en los accesos se puede perder el acceso de quien necesita realmente la información.

Para controlar efectiva y eficientemente los accesos tiene que pensar en términos de capas o niveles:

-No debe confiar que uno o dos niveles de acceso puede ordenar y eventualmente obstruir el acceso a todo eficazmente.

-En general no se controla el acceso a la información o a los recursos a menos que exista una buena razón para ello. Crear barreras innecesarias justamente pueden representar un gran trabajo adicional y un desperdicio de recursos.

Así por ejemplo, si su computadora puede navegar sobre Internet, es una buena idea controlar quien la está usando, toda vez que alguien podría usar su computadora para hacer cosas sobre Internet en su nombre. Pero es preferible, a cerrar totalmente el acceso a la computadora, que sea necesario establecer la conexión en forma manual, haciendo que , por ejemplo, pida la clave de conexión telefónica, evitando las conexiones automáticas. De esta manera otras personas podrían usar la computadora pero puede controlar quien consigue el acceso a Internet a través de ella.

#### **Clasificación de Datos**

Puede buscar clasificar sus datos de acuerdo a su sensibilidad o importancia; puede luego administrar los accesos sobre la base de la sensibilidad de los recursos y a la información relacionada, y no solamente sobre la base de quien eventualmente tiene, explícitamente, uso de la computadora y consigue acceso a Internet a través de ella.

Cuando esté considerando como proteger la información que usted mantiene, debe recordar que tal acceso deberá estar controlado por varios medios, pero siempre asumirá que alguno de los datos guardados en la computadora es vulnerable y pueden ser revelados. Recuerde que:

\* Cerraduras físicas, y claves de acceso sobre el hardware y en el Sistema Operativo pueden ser eludidas.

\* Los bloqueos de archivos pueden ser eludidos facilmente si tiene los programas adecuados para hacerlo.

### 3 - CONTROL de ACCESO y CONTRASEÑAS

\* Algunas máquinas o redes que están conectadas a Internet, especialmente aquellas máquinas que siempre están conectadas, son vulnerables por tener el sistema operativo "hackeados" (invadidos) por otras personas que quieren ganar acceso remotamente.

\* Alguna máquina conectada a una red, es vulnerable al ataque de otras máquinas sobre la misma red y especialmente por cualquier máquina que supervise el tráfico enviado a través de la red.

\* Los datos encriptados que se encuentran en la computadora no son completamente seguros si las llaves que controlan el proceso de encriptamiento están guardadas en la misma máquina; y

\*Una vez que una persona ha tenido acceso al disco duro en el interior de su computadora, puede copiarlo íntegramente, y usar otros sistemas para recuperar los datos existentes en él.

*Puede minimizar la probabilidad de que la información sensible sea descubierta, pero no puede evitarlo, en caso que una fuerza esté determinada a obtener acceso a la información que tiene con acceso protegido.*

*Por ejemplo una incursión de fuerzas del estado puede actuar sobre su computadora y pueden acceder a sus datos encriptados; en muchos estados la imposibilidad de romper las claves de encriptado y de acceso puede implicar su encarcelamiento; y en esas circunstancias tendrá que elegir entre su libertad abriendo su información más secreta, o permanecer encarcelado, posiblemente bajo presión.*

En términos de control de accesos, esto nos lleva a tres reglas simples:

\* Si la información no es de alguna manera sensible, únicamente necesita controlar mínimamente sus accesos y esto ahorra el trabajo de proteger información que no requiere mucho control.

\* Si la información es sensible, pero necesita usarla regularmente, deberá guardarla sobre computadoras que deberán tener barreras adicionales que impidan su libre acceso –por ejemplo utilizando palabras de paso sobre archivos individuales, y

\* Si la información es extremadamente sensible, no deberá guardarla completamente en la computadora – hay varias opciones: desde guardar los datos encriptados en un disco flexible, o sobre un servidor seguro, a la utilización de un disco duro removible en la computadora e intercambiarlo con un disco duro que contiene su información más sensible y que usted guardara seguramente en forma menos visible. (Esta última forma requiere de más técnica para configurarla, pero es fácilmente usada por la mucha gente).

#### **Contraseñas de paso y Autenticación**

Muchas personas no se molestan en utilizar contraseñas (palabras clave o de paso), por que la variación de éstas puede traer confusiones y si comete errores, pierden o les es negado el acceso a sus datos o sistemas.

**Las contraseñas** – ampliamente utilizadas, desde el número PIN de la tarjeta de crédito

### 3 - CONTROL de ACCESO y CONTRASEÑAS

---

a las más complejas controladas por programas encriptadores. Pero la idea es que usted tenga una única clave que lo identifique, basada en una cadena de caracteres y / o de números que le garanticen el acceso a un sistema;

**Llaves o señales** – son llaves físicas, tarjetas codificadas o tarjetas inteligentes, las cuales únicamente validan la identidad por simple posesión de la misma, y permiten el acceso a las áreas permitidas por tales llaves;

**Biométricas** – mediante la lectura de sus características físicas, tales como sus impresiones digitales, las características del iris de sus ojos o del rostro, que se supone lo caracterizan de forma única, y a partir de esto, establece la condición de su acceso. (En el estado tecnológico actual, tienen muy baja confiabilidad si se aplica en grupos grandes de personas y se engañan fácilmente - Tienen tasas de errores de cerca del 50%)

Las computadoras pueden usar la totalidad de estos métodos. La mayoría de las computadoras no corporativas utilizan solamente contraseñas o palabras de paso, aunque puedan adquirirse tecnologías con otras formas de autenticación

*En la practica, la autenticación es utilizada únicamente cuando los sistemas están preparados para implementar efectivos controles sobre los accesos. Bajo el Sistema Operativo de Windows (95/98/ME, etc.) el desarrollo standard es tal que una sola contraseña es utilizada para acceder al sistema, pero eventualmente esta contraseña puede ser eludida y obtiene un acceso completo al sistema.*

*En este ambiente de trabajo (nos referimos al sistema operativo) la complejidad de sus contraseñas y o la regularidad con la cual efectúe sus cambios, hace muy poca diferencia. Puede construir su seguridad por otros medios, pero eventualmente estos métodos adicionales pueden ser eludidos por usuarios habilidosos o por expertos en seguridad.*

Existen otras opciones para implementar medidas de seguridad sobre los sistemas basados sobre Windows, por ejemplo utilizando contraseñas de acceso para guardar los archivos del procesador de palabra y de los archivos creados por muchas otras aplicaciones de oficina o comerciales.

*Pero porque Windows no prohíbe la ejecución de software nuevo por algún usuario, mucha gente puede correr programas que les permitan usar los recursos de su propia computadora para romper la seguridad de las contraseñas de acceso a Windows, como también las contraseñas de acceso utilizadas para proteger el más popular de los procesadores de palabra y de otros archivos.*

Usted puede adquirir recursos adicionales para mejorar la seguridad de Windows, utilizando una variedad de sistemas de autenticación, pero como no son standards y están diseñados para usar en ambientes comerciales o corporativos, son costosos

Existen también otros productos propietarios que puede adquirir y que proveen una cierta protección extra para los sistemas instalados, o para prevenir el acceso a ciertas áreas del sistema que no tienen contraseñas. Pero estos productos han sido desarrollados para el mundo de los negocios por compañías de seguridad y por lo tanto son también costosos.

La opción más segura y fácil, disponible para ser usada con los sistemas de Windows es el encriptado de archivos o su ubicación en áreas encriptadas del disco duro. Programas

### 3 - CONTROL de ACCESO y CONTRASEÑAS

tales como el PGP Free lo hacen posible. ( Ver el Resumen Nro.4 sobre uso del PGP Free), y un programa como éste está disponible desde un gran número de fuentes. La utilización de encriptación requiere la utilización de claves para acceder o decodificar los archivos, y también provee niveles adicionales de seguridad.

Utilizar la misma contraseña por un largo periodo no es arriesgado con tal que sea apropiada para su uso y nivel de peligro. En muchos sistemas debe tener una sola contraseña para encender su equipo, otra para abrir el sistema, y otras tres o cuatro o más, para conectarse en línea para conseguir su correo electrónico. Si a esto se suma que las contraseñas no puedan repetirse, y que les obligue a cambiarlas frecuentemente, y estará creando problemas para mucha gente.

Necesita cambiar las contraseñas únicamente cuando exista la probabilidad que otras personas puedan descubrirlas. Por ejemplo, si tiene una computadora muy segura, no utilizada por otros, en una oficina de su uso exclusivo, no necesitará cambiarla con mucha frecuencia. Pero ciertas contraseñas, como las que utiliza para acceder a redes (inclusive las utilizadas sobre la red, como las que controlan el acceso a su correo electrónico o a servidores de archivos compartidos) deberá cambiarlas con más regularidad porque ellas pueden ser extraídas de la red por aquellos que tienen habilidad para obtenerlas.

#### Utilizando contraseñas:

Como hemos visto, también las contraseñas son inseguras para la protección de los sistemas. Para ser útiles ellas deben ser memorizadas, pero esto es una gran mentira porque en los hechos suelen ser tan simples que pueden ser adivinadas o reveladas por accidente por el mismo usuario.

La fuerza o el valor de una contraseña es muy dependiente de su largo, y la variante o número de caracteres disponibles para cada posición. Muchas contraseñas permiten el uso de mayúsculas y minúsculas, los números de 0 a 9 y el carácter de subrayado. Algunas contraseñas limitan la longitud de la clave, mientras que otras, entretanto imponen una longitud mínima. Deberá probar exactamente que cantidad de caracteres le permite usar su sistema para definir sus claves y así asegurar su fortaleza.

La protección proporcionada por las contraseñas, particularmente sobre Internet o sobre redes de computadoras, esta relacionada con su habilidad para resistir intentos de intrusión ("cracking") y con la cantidad de combinaciones posibles que puedan ser usadas.

Las contraseñas no deberán ser nombres, palabras de diccionario, u otra información que describa o se relacione con la información conocida sobre usted ( fechas de nacimiento, números de domicilio, nombres de amigos, parientes, mascotas, socios, siglas, iniciales, etc.).

Por ejemplo, utilizando únicamente mayúsculas, existen 26 posibles opciones, de manera que una contraseña de seis dígitos puede llegar a tener casi 309 millones de combinaciones posibles (puede calcular el número de combinaciones elevando a la potencia del número de caracteres que utiliza su contraseña) Si nosotros usamos todos los símbolos posibles que pueden ser fácilmente tipeados en el teclado de una PC compatible, combinando sobre la base de 96 símbolos y 6 caracteres de longitud, las posibilidades llegarán a 782 millones de combinaciones. Pero en la práctica las palabras comunes son utilizadas como parte de las contraseñas, reduciendo las posibles combinaciones a unas pocas decenas de miles, aunque esto puede ser notoriamente

### 3 - CONTROL de ACCESO y CONTRASEÑAS

---

incrementado agregando números, caracteres no alfabéticos, o eventualmente mediante la utilización de palabras de otros lenguajes mezcladas, además del idioma nativo.

Hay muchas reglas estrictas y rápidas sobre como definir contraseñas o palabras de paso, pero para la mayoría de la gente el trabajo que involucra el cumplir todas estas rígidas reglas, es demasiado oneroso. Muchas personas desarrollan sus propias reglas de acuerdo con la sensibilidad o la importancia que ellos asumen, y de la forma en que su computadora o sus sistemas están configurados en general.

- \* Las palabras de paso idealmente deben ser una secuencia aleatoria de caracteres alfanuméricos que no tengan una cantidad menor de seis caracteres. – Si no – asegúrese de insertar por lo menos un número u otros caracteres no alfabéticos con alguna palabra que usted utilice como contraseña

- \* Nunca utilice contraseñas hechas con palabras secuenciales (nombres de santos, meses, títulos de libros o películas, etc.)

- \* No vuelva a reutilizar contraseñas, o deje pasar un año o dos después de su última utilización.

- \* Las contraseñas de inicio o encendido de la computadora (‘front line passwords’ o ‘boot passwords’) que son utilizadas para iniciar la computadora o encender el sistema operativo deberán ser reemplazadas cada pocos meses, donde exista el riesgo que las mismas puedan ser descubiertas por otras personas. O sino reemplácelas simplemente cuando sienta la necesidad de hacerlo.

- \* Las contraseñas que protegen la utilización de otras contraseñas son más seguras, y no requieren ser cambiadas frecuentemente. (Pero bajo el sistema operativo de Windows, todos los archivos quedan abiertos para todos los usuarios, de manera que no constituye una protección para ellos).

- \* Si tiene razón para creer que alguna otra persona ha tenido acceso a su sistema sin su permiso o supervisión, cambie sus contraseñas inmediatamente.

- \* Si tiene razón para creer que se ha bajado información de su sistema, no solo deberá cambiar sus contraseñas sino también, deberá cambiar las claves de encriptación guardadas sobre su sistema.

- \* Nunca confíe en que son seguros los archivos encriptados usando procesadores de texto u otros programas. Si necesita proteger información sensitiva o importante, utilice un sistema propio de encriptación tal como el PGP para esta tarea.

- \* Nunca discuta la utilización de las contraseñas en publico, teléfonos o las escriba en mensajes puestos por email o por correo común.

- \* No utilice nunca alguna información personal en poder de terceros: nombres, bancos, números de cuentas bancarias, teléfonos, documentos. etc.

- \* Nunca utilice la misma contraseña más de una vez sobre el mismo sistema.

- \* Nunca utilice en sistemas semipúblicos (webmails gratuitos, servicios de mensajería gratuitos, etc) contraseñas que use en otros sistemas privados.

### 3 - CONTROL de ACCESO y CONTRASEÑAS

#### La utilización de contraseñas para mejorar la seguridad

La mayoría de los sistemas informáticos recomiendan lo siguiente para mejorar la seguridad de sus sistemas.

- \* **Establezca una clave en el BIOS** (programa de arranque de su computador). Cuando usted encienda la computadora tiene la opción de utilizar una contraseña para proteger el sistema de arranque. Las mas nuevas computadoras tiene dos claves en el BIOS, una que permite el arranque, y otra para que el 'supervisor' pueda cambiar la configuración del BIOS si es necesario. Esta es una de las maneras simples de proteger una computadora porque a menos que el sistema arranque, no podrá accederse nada del sistema. Esto no es totalmente seguro, porque los usuarios expertos pueden conocer una puerta trasera (backdoor password) para el BIOS, y en algún caso ellos podrían acceder a sus datos removiendo el disco duro e insertándolo luego en otra computadora. Pero la palabra de paso que controla el BIOS es una buena manera de prevenir el acceso a los datos por personas no expertas.
- \* **Establezca cuentas de usuarios.** Sobre el sistema de Windows las cuentas de usuarios no proveen seguridad, pero son una manera para diferenciar los trabajos de cada usuario individual, archivos, directorios, etc.
- \* **Para archivos sensitivos o importantes, utilice contraseñas.** Muchos programas de oficina tienen la habilidad de mezclar el contenido de los archivos, utilizando una débil forma de encriptado. Esto lo puede realizar utilizando una función específica, o especificando una contraseña cuando se guarda un archivo, la cual debe permitir luego que tal archivo pueda ser abierto nuevamente. Esto provee un moderado nivel de seguridad cuando se combina con otras medidas de seguridad. Pero hay un varios programas disponibles que están en condiciones de romper la débil encriptación sobre estos archivos, para aquellos que puedan localizarlos y disponer de ellos.
- \* **Para la información más sensitiva, utilice programas de encriptado.** Los sistemas de encriptado proveen un alto nivel de protección, codificando el archivo, o el mismo disco duro, utilizando complejas funciones matemáticas tales que otros no podrían nunca acceder sin el archivo llave y su contraseña. Para mayor información vea el resumen 4 Using Encription and Digital Signatures

#### Contraseñas sobre Linux

Linux provee un nivel más alto de seguridad que los proporcionados por el sistema basado en Windows. El nombre del usuario y la contraseña requerida para ganar acceso al sistema, y el acceso concedido es únicamente para las áreas del sistema permitidas para este usuario. El sistema protege las cuentas de usuario denegando el acceso a la información propiedad de otros usuarios, a menos que el usuario propietario lo permita.

La instalación de nuevo software tampoco es permitida en Linux a menos que usted tenga las contraseñas del administrador de la computadora o es un usuario "root". Linux no es totalmente seguro, y usuarios expertos, tienen los medios para rodear o eludir la protección dada a los usuarios y pasar sobre los controles del sistema operativo. Pero comparado con los medios de las más populares versiones de Windows, es más seguro.

### 3 - CONTROL de ACCESO y CONTRASEÑAS

---

El nivel de seguridad significa que las contraseñas en archivos no son tan importantes comparadas con Windows, pero muchos programas , tales como Star Office, permite que usted las instale.

Por todo esto para quienes pueden tener problemas con una excesiva seguridad, tales como los chicos jóvenes, Linux permite la utilización de cuentas sin claves de acceso, utilizando las opciones de configuración abiertas para los usuarios administradores. Esto significa que sobre la misma computadora usted puede dar diferentes tipos de acceso al sistema, tanto a usuarios regulares como irregulares con una buena seguridad para sus datos.(También sepa, que también es posible que usuarios expertos de Linux puedan abusar del sistema desde una cuenta sin contraseña de acceso)

## 4 - USANDO ENCRIPCIÓN y FIRMAS DIGITALES

### ¿Qué es la encriptación?

Encriptar es una forma de codificar información de manera tal que no podrá ser decodificada y leída, sin la utilización previa de una llave o clave. Las computadoras han revolucionado la encriptación porque ellas pueden codificar y decodificar a muy alta velocidad y estos procedimientos ahora vienen como módulos adicionales del software común. Estos también pueden usar sistemas muy complejos de encriptación que hacen lejana y difícil la posibilidad de romper estas barreras y acceder al contenido original.

Los sistemas viejos de encriptado requerían para la transmisión de un mensaje encriptado, trasladar también una clave para hacer posible la decodificación. Esto es sin duda un problema porque requiere que tenga los recursos para asegurar el envío de la llave (o clave) al receptor del mensaje antes de que pueda recibir el mensaje cifrado. Es decir, requiere de un "canal de comunicación seguro" para trasladar información (la clave), para poder enviar la otra información (el mensaje) por un canal inseguro. Un contrasentido en sí mismo.

Este problema fue solucionado en los 80s.

Con un nuevo sistema llamado de "doble clave de encriptación". Esta clave utiliza dos llaves, una, la pública es utilizada para encriptar los datos, y la otra (la privada) es utilizada para descifrarlos. La llave pública de encriptado es un sistema basado en funciones matemáticas complejas, pero tan complejas que no pueden ser solucionadas sin una única combinación de las dos llaves. Tomaría una impracticable cantidad de tiempo de una super computadora para encontrar la solución al problema matemático que permita la decodificación. Esto significa que usted puede hacer pública la mitad de sus llaves a cualquiera para encriptar un mensaje con ella, pero la encriptación completa del sistema implica que la llave privada no puede ser definida solo con el contenido de la llave pública.

*Nota: En la actualidad, con la potencia de cálculo de las supercomputadoras, puede estimarse que se logra quebrar este tipo de barrera en lapsos menores a 2 meses, e incluso menores a 2 semanas. Lo cierto es que requieren de una capacidad de proceso excepcionalmente poderoso y esto solo es posible para unos pocos.*

*Pero, no debemos confiar en que no puedan ser abiertos... solo podemos esperar que tarden mas tiempo que el que les lleva abrir otro tipo de barrera y, en la medida que el material a descifrar sea mucho y masivo, realmente, les lleva mucho proceso y tiempo. Y una información desactualizada no tiene el mismo valor.*

*Si cada uno de nosotros tomara como costumbre "encriptar" nuestras comunicaciones habituales, seria hoy practicamente imposible para cualquier agencia de vigilancia acceder al contenido de todos los mensajes en tiempos razonablemente útiles.*

Existen varios sistemas de llaves públicas para el encriptado de datos. Lo que determina la fuerza de dichos sistemas es el largo de la llave; cuanto más larga es la llave, es más segura, porque requiere de computadoras más potentes para romperla y decodificar el mensaje.

En uno de los primeros sistemas, denominado D.E.S. (Data encryption Standard), utilizaba una llave de 56 bits. El número de permutaciones con 56 bits en binario es 2 elevado a una potencia de 56, lo que da un total de 72 millones billones de combinaciones. El

## 4 - USANDO ENCRIPCIÓN y FIRMAS DIGITALES

standard más común actual esta basado alrededor del programa "Pretty Good Privacy" (PGP). El PGP Utiliza un conjunto de algoritmos matemáticos que usan una llave de 128 bits a 2048 bits o aun más. Esto da un número muy alto de combinaciones; un número demasiado grande para escribirlo en esta página como número real.

La flexibilidad de las computadoras significa que los sistemas de encriptado, tales como el PGP, pueden ser utilizado para un número de diferentes propósitos para ayudar a la seguridad de los datos almacenados, o transmitidos por un sistema de computadoras.

*\* Los Mensajes que serán enviados sobre la internet pueden ser encriptados para protegerlos contra cualquiera que intente leer su contenido.*

*\* Los Mensajes pueden ser rutinariamente "firmados", utilizando la firma digital basada entorno a la encriptacion, para que pueda demostrarse que la fuente del mensaje es auténtica;*

*\* La información contenida en el disco de la computadora puede ser encriptada para protegerla contra aquellas personas que pueden tener acceso al disco, por ejemplo si la computadora o el disco es robado; no podrán hacerlo sin conocer la llave privada; y*

*\* Los sistemas de encriptacion pueden ser inter-construidos en los aparatos y sistemas de comunicaciones, tales como teléfonos o en los navegadores web, para proveer encriptacion en tiempo real y protegerlo contra la intervención o la interferencia de sus comunicaciones.*

Eventualmente si no desea hacer secreta sus comunicaciones, algunas funciones del encriptado pueden desactivarse, y usar solo la firma digital, ya que tiene una manera muy útil de autenticación del origen del mensaje por la facilidad con que la firma digital puede ser copiada, manipulada o borrada. Aunque no pueda utilizar la encriptacion para enviar mensajes, deberá encriptar su información personal, o la información que tiene obligación de proteger bajo la ley de protección de datos como los de un cliente importante o los de un cliente de un profesional (fichas médicas, por ejemplo).

### Utilizando la encriptacion

El encriptado utilizado anteriormente era una operación técnica. Hoy, la encriptacion de los sistemas es una parte inseparable en el uso del correo electrónico o de los navegadores web.

El más común de los programas de encriptacion, el PGP, viene en varias versiones. Muchas de ellas, tales como el PGP Free, están disponibles en Internet libre de cargo. Algunos sistemas operativos, tales como el Linux, incluyen usualmente PGP o programas similares como standard en sus distribuciones.

Muchos programas PGP recientes, se integran asimismo en el sistema de su computadora. Él le pregunta que sistema de correo electrónico utiliza, y le instala los módulos adecuados ("plug ins") para brindarle las funciones de encriptacion directamente dentro de sus programas de correo y en el escritorio de su sistema operativo. Algunas versiones de estos programas también proveen la opción de encriptar partes de su disco duro, o la encriptacion de archivos individuales como parte de otros programas. Muchos le permiten la utilización de la firma digital para firmar sus archivos y sus mensajes de correo.

## 4 - USANDO ENCRIPCIÓN y FIRMAS DIGITALES

---

Cuando usted instala un programa como PGP, le pedirá que realice la creación de su par de llaves (key par), la pública y la privada para ser utilizada en los procesos de encriptación. Puede utilizar actualmente más de un par de llaves, pero esto puede llegar a ser un problema si tiene dificultades tratando de recordar las complejas palabras de paso asignadas a cada par de llaves. También algunos programas, como los de correo electrónico, tienen problemas para aceptar más de una llave secreta para la encriptación.

Se genera un par de llaves utilizando una cantidad extremadamente larga de números primos. Estos forman la base de las llaves. Pero para adicionar una llave de acceso personal sobre el par de llaves también requiere disponer de una contraseña que pueda recordar, o la llave le resultara inservible. Las contraseñas deberán tener al menos 8 a 10 caracteres de largo. Pero si usted utiliza palabras más largas, el sistema será más seguro. (Las palabras de una canción, el párrafo completo de un libro, o un poema pueden ayudarle a recordar una extensa contraseña más fácilmente).

Cuando ha generado su par de llaves puede enviar la llave pública a sus amigos, o eventualmente ponerla sobre un sitio en Internet si posee uno. Pero no deberá descubrir nunca su llave privada, o la contraseña que utiliza con su llave cuando está descifrando mensajes. Deberá también resguardar su llave privada para prevenir pérdidas en caso que su computadora tenga fallas, especialmente, si utiliza su llave para encriptar archivos importantes. Necesita efectuar el resguardo de tal manera que ella no pueda ser fácilmente encontrada (por ejemplo, puede querer imprimir su llave privada y esconderla en la cubierta de un libro, pero será mucho mejor que usted mismo idea la manera de hacer invisible o guardar físicamente sus llaves).

Existen varias maneras con las que la encriptación puede ayudar al uso de las computadoras.

Nota: Tenga presente que algunos gobiernos ya limitan el tamaño de las claves que puede utilizar para generar mensaje encriptados. El Reino Unido, por ejemplo, impone un límite de 1024 caracteres en la longitud de estas claves. Nos da una idea de cuál es el poder de cálculo que tienen los gobiernos disponible para romper estas encriptaciones en forma masiva. Si su mensaje esta encriptado, los sistemas de vigilancia suponen que tiene algo para guardar (lo cual es realmente lícito respecto a su privacidad) y lo separan para analizar con más detalle aplicando técnicas de desencriptación o de rompimiento de códigos de acceso.

### Firma Digital

Eventualmente, si no desea encriptar sus datos, utilizando la firma digital es una muy fácil manera de proteger su identidad contra intrusos por Internet. El propósito de la firma digital es proveer un resumen encriptado que en base al contenido del mensaje se adiciona a la copia del mismo. Enviar el mensaje firmado implica usualmente un proceso igual al de un envío encriptado, con la diferencia que solo le pide al programa que genere la firma del mensaje o archivo. La firma es luego agregada al final del archivo o del email.

Cuando usted recibe un mensaje firmado le pedirá al programa de encriptado que verifique si tal mensaje no ha sido cambiado. El programa efectúa esto decodificando la firma del mensaje y comparando los resultados con el cuerpo del mensaje. Si el resultado es el mismo como el que obtiene del mensaje, la computadora le da su conformidad.

## 4 - USANDO ENCRIPCIÓN y FIRMAS DIGITALES

---

### Seguridad en los servidores WEB

Los servidores de Webs también deben dar soporte al encriptamiento de las comunicaciones según los protocolos denominados 'secure sockets' (conexiones tipo SSL). Estos protocolos permiten enviar información importante a través de la red, (tal como su número de tarjeta de crédito), sin la posibilidad de que otras personas (comunes) puedan leer sus datos en su viaje hasta su destino. La conexión (sesión) en la que operan los 'secure sockets' es habilitada por el servidor WEB al que usted se está conectando.

Siempre puede guardar control sobre si la sesión que usted está utilizando es encriptada porque la dirección a la cual usted está conectado puede tener un prefijo tipo 'https://' en lugar de 'http://' y el pequeño candado que está en la esquina de la pantalla del navegador puede estar cerrado en lugar de abierto. Las conexiones de este tipo dependen del servidor web, no de su opción de conexión. Es el programa que maneja el sitio web el que define si tiene esa posibilidad o no.

Los 'secure sockets' no utilizan una clave larga (48, 128 bits) y por consiguiente no es tan seguro como el uso de PGP y otros sistemas que le permiten el uso de llaves más largas para la encriptación. Sin embargo es la manera más satisfactoria por la cual su información personal puede ser procesada a través de los sistemas de redes de computadoras a las que está enviando sus datos.

Por eso, cuando tenga que dar información personal a otro sistema a través de la red, siempre deberá chequear primero que los operadores de dicho sistema tengan buena reputación respecto a su seguridad (buscando en Internet por el nombre de la compañía además de las palabras 'hack', 'crack' o 'security' lo cual constituye una manera simple pero no completa ni definitiva de hacer esto).

Debe tener presente que, si bien este tipo de conexiones permiten tener un buen grado de seguridad para la mayoría de quienes quieren visualizar su información, de ninguna manera igualan la fortaleza de los sistemas basados en PGP y pueden ser fácilmente abiertos por agencias del gobierno con los medios adecuados. Fue significativa la restricción a exportar estas tecnologías fuera de USA, hasta que los medios técnicos superaron el problema de poder visualizar el contenido de este tipo de conexiones por parte del gobierno.

### Encriptando Discos

Algunos sistemas de encriptación le permiten encriptar áreas de su disco duro, para guardar archivos encriptados de una manera más fácil. Esto permite guardar información de una manera muy segura, particularmente la información que debe utilizar en forma regular y debe mantener en secreto, tales como las listas de correo u otra información de tipo personal o relativas a otras personas. Encontrará una información más detallada sobre la encriptación de discos en el Sumario Nro. 2 relacionado con el Resguardo de la información.

### Encriptación y seguridad

La encriptación puede mejorar la seguridad – pero solamente si tiene cuidado de mantener su llave privada en secreto, lo mismo que su contraseña. Cualquiera que no tome los pasos necesarios para asegurar otras áreas de la computadora, tales como instalar una contraseña al encender o iniciar su sistema (boot), no podrá garantizar una encriptación segura.

## 4 - USANDO ENCRIPCIÓN y FIRMAS DIGITALES

Establecer la encriptación del disco duro, para guardar todos los datos sobre una computadora segura, puede hacer difícil el acceso de nuevos usuarios. Pero el esfuerzo empleado en hacer esto debe ser evaluado contra los riesgos de perder o que sean vulnerados, los datos personales. El uso diario de la firma digital y de la encriptación de la información más significativa llega a ser suficiente para la mayoría de la gente.

Pero para aquellos temerosos que consideran que sus datos en la computadora son vulnerables y puedan llegar a ser revelados, deben instalar o aconsejar la instalación de sus datos en un disco encriptado.

### Encriptando con Linux

Linux provee varias opciones para el uso del encriptado. Así como PGP para Windows, en los sistemas basados en Linux dispone de herramientas para manejar contraseñas y el encriptado y desencriptado de archivos. Esto está usualmente basado sobre un programa de consola llamado `gpg` – GNU Privacy Guard – aun cuando existen interfaces gráficas que trabajan con los escritorios de Gnome y KDE.

GPG no solo usa las llaves públicas de cifrado utilizadas en PGP Free y otros programas de Windows, ya que también puede utilizar variantes de otros encriptadores tales como el Triple-DES y Blowfish, y algoritmos de "hash" (utilizados para verificar la integridad de los archivos) tales como el MD5.

La utilización de las interfaces gráficas para el `gpg`, es similar a la utilización del PGP Free, mostrado en el apéndice de este sumario. Pero utilizar la versión de consola de `gpg` suele proveer mayor flexibilidad relacionado a como puede encriptar sus datos. Para más detalles sobre la utilización de `gpg` abra la ventana de la consola terminal e ingrese: `> man gpg`

Por ejemplo:

<code>Gpg -r fred -encrypt a_file_name</code>	Encripta un archivo con la llave pública de FRED's
<code>Gpg -decrypt encrypted_file</code>	Desencripta un archivo
<code>Gpg -help</code>	muestra la información sobre <code>gpg</code>
<code>information</code>	

Muchos otros programas pueden acceder a las funciones de `gpg` para habilitar el uso del encriptado como parte de sus funciones. Esto significa muchos diferentes programas, como los de correo electrónico, pueden acceder a los pares de llaves públicas y privadas mantenidas por cada usuario y utilizar la encriptación.

Cuando instala un sistema Linux también es posible instalar a nivel del núcleo ("kernel-level") la posibilidad de encriptación del disco duro de su computadora. Esta es una de las maneras más seguras de mantener la seguridad de la información sobre la computadora. No solamente le provee de una barrera extra dentro del Sistema Operativo. Si el disco duro es removido de la computadora y leído en otra máquina, o si padece un atentado o intentan leer una partición de Linux desde otra partición de Windows en un sistema con los dos sistemas, no sería posible acceder a la información.

## 5 - VIRUS de COMPUTADORAS

Este Resumen es el quinto de la serie sobre la seguridad de la información, y trata los siguientes temas:

- Qué es un virus
- Cómo trabajan
- Cómo los virus afectan a su computadora
- Recomendaciones básicas sobre la protección contra virus
- Virus y Linux

### Qué es un virus?

Un virus es un programa ejecutable, un conjunto de instrucciones que manipulan las funciones del sistema operativo de sus computadoras. Al principio, un virus simple consistía justamente de dos instrucciones – primeramente pregunta por una condición particular (puede ser la fecha o algún otro criterio) y luego llama al programa que da formato al disco duro.

Muchos de los primeros virus fueron transmitidos de archivo a archivo de las computadoras cuando la gente intercambiaba archivos en discos flexibles. Hoy la manera más común para adquirir un virus es por vía del uso de redes e Internet. Pero en lugar de algo tan simple como dar formato a su disco duro, los virus nacidos en internet son más complejos. Muchos pueden leer las direcciones de su correo electrónico y retransmitirlas, cuando usted procede a chequear su correo electrónico, a todos sus amigos (o a quienes no lo son...), difundir documentos privados que tiene en su equipo, etc. etc.

“Virus” es actualmente una denominación genérica para un software que es dañino para su sistema (o su privacidad). Ellos se propagan vía discos, vía conexiones de red, o vía servicios tales como el correo electrónico, Independientemente de cómo viajan los virus, su propósito es usar o dañar los recursos de su computadora o vulnerar su privacidad. Los virus más modernos se propagan por los servicios de internet, en particular por el correo electrónico y la navegación web.

El problema con los virus es que la amenaza es frecuentemente peor que la realidad. Por esta razón una parte de la gente ha acumulado dinero generando virus para luego vender los antídotos. Por ejemplo, muchos de los “X” miles de virus de los cuales las compañías hablan, nunca han llegado a entrar en el mundo real. Estos son el resultado de tests de laboratorio sobre problemas de seguridad de sistemas de computadoras para ver si un virus podría trabajar en tal o cual forma. Habiendo establecido que podría ser un problema, emiten un aviso de como serían las características del virus una vez adquirido y cuales son los chequeos que deben hacerse para ver si uno está infectado.

El mayor efecto de los virus tiende no a la destrucción de los datos, sino a utilizar tiempo de la gente. Por ejemplo: los virus engañosos propagados por correo electrónico tienden a surgir ahora y nuevamente más adelante, usualmente bajo el título “PENPAL GREETINGS” o algo parecido. Esto es un virus en si mismo, porque propaga el pánico cada vez que lo envía a sus amigos o conocidos, aunque no existe el virus como tal, el mensaje provoca una gran pérdida de tiempo y recursos de comunicación (ancho de banda, espacio ocupado en discos de mensajes, etc etc.).

Esas son las cosas que les pasan a las personas que usan las computadoras, un conjunto de personas que no saben como trabajan los virus, de tal forma que son fácilmente engañados e involuntariamente propagan avisos falsos que solo producen un mayor desperdicio de recursos técnicos y humanos.

## 5 - VIRUS de COMPUTADORAS

Los virus no se generan sólo como fruto de gente marginal o excéntrica. Algunos han hablado de los virus como un medio de controlar o verificar los defectos existentes en una red y automáticamente establecer los defectos en los programas. Más recientemente, el FBI (US - Federal Bureau of Investigation) ha sido objeto de un rumor sobre el desarrollo de un virus denominado ‘Linterna Mágica’ que puede penetrar en los sistemas computarizados y, bajo ciertas condiciones, enviar copia de las llaves de encriptaciones e información de seguridad de regreso al FBI. Por consiguiente los virus no son justamente una amenaza a un sistema – ellos son también una amenaza a la seguridad y privacidad en general.

### Como trabajan los virus

Es imposible recibir algún tipo de virus en el texto de un mensaje contenido en un correo electrónico, o en los archivos generados por los procesadores de texto, archivos de datos comprimidos (como PKZip/Gzip), bases de datos o hojas de cálculo – estos no son programas ejecutables. La única excepción a esto es cuando el archivo contiene programas de Visual Basic u otro código como parte de una macroinstrucción, algoritmo o programa, o como un “código objeto” embebido, y que pueda ser ejecutado por un software de aplicación en forma voluntaria (al abrir un archivo adjunto a un mensaje) o automáticamente como lo puede hacer el Microsoft Outlook con ciertos códigos que pueden venir en un mensaje de correo electrónico o al mirar una página web con el navegador web Microsoft Explorer.

Para hacer que el virus quede residente en su sistema usted tiene realmente que ejecutar el programa. Esto significa que:

*-Tiene que correr un programa bajado de Internet que esté infectado con un virus – la solución es controlarlo previamente con un explorador de virus.*

*-Tiene que correr un programa desde un disco flexible infectado con un virus, también la solución es escanear previamente el disquete con un explorador de virus. Hay algunos virus ya antiguos que se transmiten con solo leer el directorio del disco flexible.*

*-Tiene que abrir o correr un archivo con otro lenguaje de programación (Basic, C, etc.) que contengan un virus; la solución aquí es no correr ningún programa que usted no entienda o domine.*

*-Tiene que abrir o utilizar, (en los más avanzados procesadores de palabra o de hojas de calculo), archivos que contengan códigos objeto - instrucciones denominadas macros – y la solución más simple aquí es ir a la aplicación y desactivar la opción que habilita la utilización de macros en forma automática.*

Algunos años atrás, el mayor problema eran los virus que se transferían de un archivo de programa a otro, (fundamentalmente por diskettes) mientras que ahora estos están en declinación. Los grandes problemas hoy son:

*-los llamados “Macro virus”, que son pequeñas porciones de código interpretado, y que son transportados como parte de un correo electrónico (o incluso al ver una página web según sea el navegador que estamos usando)*

## 5 - VIRUS de COMPUTADORAS

-los programas **gusanos o basura**, los cuales son transportados como archivos adjuntos o agregados a los mensajes de correo electrónico.

Programas como Microsoft Outlook son muy inseguros porque tienden a integrar su correo electrónico con el resto de su sistema operativo. Si bien esto es una manera muy útil de simplificar la operación de la computadora para los principiantes, es un riesgo para su seguridad. Los autores de virus explotan la característica de autoejecutarse y autoinstalarse sobre su sistema. Esta característica no puede desactivarse en los sistemas basados en Windows, aunque luego de padecer el estrago causado por el virus denominado "I love you" algunas compañías han desarrollado un software para bloquear los virus que están explotando los defectos existentes en el Outlook de Microsoft y es posible limitar algunas de las funciones de autoejecución que tienen algunos programas.

Cuando la gente trata de leer su correo electrónico y este contiene códigos de Visual Basic, el programa de correo electrónico Microsoft Outlook fuerza al sistema a interpretar el código y su proceso produce la activación del macro virus.

Los archivos adjuntos o agregados a los mensajes constituyen otro problema. Cuando la gente recibe un salvador de pantalla o un programa promocional, suelen utilizarlos muy frecuentemente, porque no conocen el riesgo de correr dichos programas.

Los defectos que se acumulan en el sistema windows de Microsoft provocan que la vasta mayoría de los virus son específicos de este sistema y se evalúa que los usuarios de los sistemas basados en Macintosh o en Linux son relativamente inmunes a los problemas generados por los virus (en esto influye su menor difusión y las características intrínsecamente más seguras del diseño de estos sistemas).

Los mensajes que envía escribiendo con alguno de los programas más comunes de correo electrónico, se generan en formato texto y/o son codificados como archivo texto plano. Esto impide que pueda trasladar en forma oculta algún código malicioso ejecutable. La mayoría de los sistemas operativos deniega la posibilidad de tratar este tipo de texto plano como si fueran códigos de programas. De forma tal que no puede adquirir ni transmitir ningún virus mediante la simple lectura de un archivo texto o de un mensaje de texto plano (texto plano = texto sin formato). Así como tampoco puede trasladar virus si reenvía o copia texto de una aplicación a otra.

Un último peligro a considerar es cuando descarga o activa inconscientemente un programa que forma parte de un adjunto o agregado a un mensaje de correo electrónico.

Si usted guarda el archivo adjunto a su correo en un directorio separado de los archivos de sistema, el programa no podrá ser accidentalmente activado a salvo que usted así lo requiera.

### Como los virus infectan su computadora

La gran probabilidad de contraer un virus es desde Internet. El uso de programas antivirus en la industria de las computadoras ha detenido el crecimiento de muchos de los virus que se expandían vía discos flexibles. Pero los virus explotan la manera en que las computadoras ejecutan otro tipo de programas o textos como parte de los programas de correo o de programas y archivos compartidos (freeware y shareware incluidos).

## 5 - VIRUS de COMPUTADORAS

Cuatro son los orígenes más comunes de los virus vía internet

\* **Programas de computación** – puede tener un 99% de seguridad utilizando un detector de virus (o programa antivirus) actualizado para controlar estos archivos de programas antes de correrlos. Esto naturalmente no lo protege de programas basura o de la totalidad de nuevos virus que puedan existir.

\* **Java y otros scripts usados en internet y www.**- Ello es posible porque las computadoras pueden cargar códigos como parte de software propietario para Internet (por ejemplo: programas de conexión cliente servidor que utilizan bancos o grandes empresas en sus conexiones de servicios extranets). Esto ha llegado a crecer comúnmente en los sitios Web al cargar scripts de Java – programas cortos – en su navegador para ejecutar sonidos o gráficos animados (pero las instrucciones disponibles en estos casos son limitadas, de manera que ello no constituye mucho problema por el momento). Puede limitar los posibles daños desactivando Java y otras opciones de su navegador Web. Cuando el servidor web requiera cargar este tipo de scripts, su navegador preguntara primero antes de hacerlo. Básicamente, nunca debe contestar “sí” salvo cuando este dentro de un sitio sin riesgo.

\* **Códigos empotrados.**- Se trata de un código objeto, visual Basic, C, Pascal, programas o scripts que están empotrados (insertos) en muchas de las más modernas aplicaciones generadas desde procesadores de palabra, hojas de calculo, bases de datos, etc. Como las aplicaciones vienen a ser cada vez más complejas esto no posibilita que los programadores puedan escribir códigos que cubran todas las eventualidades. Para buscar dentro de estas pequeñas porciones de código incluidas en los archivos debe ejecutar determinadas funciones. Las funciones definidas por usuarios, particularmente en procesadores de texto, hojas de calculo o bases de datos, son guardadas como textos cortos denominados scripts. Es posible incluir instrucciones en scripts y ciertamente en código objeto que puede actuar como un virus. Programas troyanos o basura pueden estar dañando su sistema a una fecha determinada. Muchas aplicaciones le permiten abrir un archivo sin necesidad de activar sus macros si usted primeramente desactiva la opción respectiva en el programa que opera el menú de opciones. Naturalmente la manera de eludir tales problemas es aceptando únicamente archivos en viejos formatos que no contienen tales características, o solamente recibir archivos de orígenes seguros y confiables y mantener desactivadas las opciones de autoejecución.

\* **Código Fuente** – Son programas constituidos por un conjunto de instrucciones, que van a ser trasladadas a la computadora mediante un interprete o escrito como un programa por un compilador. Esto es una cosa comúnmente hecha en los sistemas basados en Linux donde muchos programas son distribuidos como código fuente, los cuales luego son compilados para trabajar con la configuración de su propio sistema. Hay también otros programas disponibles en internet en Basic, Visual Basic, C, Pascal, etc. En programas largos, particularmente donde los usuarios no conocen mucho sobre el lenguaje, o donde el programa es tá pobremente estructurado, es muy fácil no ver un comando basura, troyano o virus. No debe compilar / ejecutar ningún archivo a menos que usted sepa que es seguro. El código fuente – usualmente un archivo texto – es completamente inofensivo, eventualmente cuando está incluido como agregado a un mensaje de correo

## 5 - VIRUS de COMPUTADORAS

*electrónico. Solamente cuando carga el código fuente en el compilador o en él interprete es que se vuelve peligroso.*

El significado práctico de lo expuesto mas arriba, es que puede capturar un virus desde un archivo texto, o de un HTML o también de una conexión FTP/Gopher/Telnet. El máximo peligro proviene de los navegadores, si los 'helpers' (sistemas de ayuda) son activados para ejecutar programas.EXE" o ".BAT" cuando ellos están siendo cargados; usted deberá desactivarlos para prevenir la carga de virus.

Cómo debe resguardarse de los virus depende también de cuál es su rol. Este sumario evalúa un tratamiento adecuado a un usuario individual. Para usuarios que forman parte de redes locales (LAN) existen diferentes tópicos relacionados a los sistemas de trabajo en red. Por ejemplo, es muy importante prevenir el acceso de un virus a una parte de la red, por lo tanto el uso del disco flexible debe quedar restringido sobre una red de computadoras. También quien tiene a su cargo el servidor del correo electrónico tiene una responsabilidad que cumplir. Los servidores pueden tener programas anti-virus corriendo con el correo electrónico, previniendo la transmisión de adjuntos que se conocen como contenedores de virus. Los usuarios de Internet pueden preguntar si su proveedor de servicio posibilita el bloqueo de los virus sobre el servidor, y pedir instalarlo si todavía no se hizo.

### Recomendaciones básicas sobre protección contra virus.

Existen tres recomendaciones simples para reducir significativamente los riesgos de tener problemas con virus.

*\* Sea cauto cuando esta utilizando los servicios de internet*  
*-No clickear sobre agregados*  
*-Desactivar las macros en el procesador de textos*  
*-Desactive los scripts de Java*  
*-Configure el navegador para que no pueda correr programas*  
*-Si le es posible no utilice Microsoft Outlook*  
*(es el programa menos seguro de los comúnmente utilizados para el correo electrónico).*

*\* Si está utilizando Microsoft Outlook consiga la ultima versión, y los parches de las versiones existentes, y configurelo para que no pueda ejecutar o abrir agregados o programas automaticamente;*

*\* Utilice alguna suerte de programa antivirus para explorar entre los archivos que puedan venir adjuntos o agregados a su correo electrónico o directamente en un disco flexible.*

Si usted tiene un poco mas de conocimientos sobre la utilización de computadoras, lo siguiente puede serlo muy útil:

*\* Configure su sistema operativo de tal manera que pueda ver la extensión del nombre de sus archivos – esto le permitirá que pueda ver que tipo de archivo es e identificar si se trata de un archivo ejecutable o no. Deberá tener cuidado de los archivos que tiene una doble extensión, como por ejemplo: 'picture.jpeg.vb'.*

## 5 - VIRUS de COMPUTADORAS

*\* No ejecute ningún programa que reciba en disco flexible, o desde Internet, sin haberlo explorado previamente en busca de virus o chequeando que instrucciones incluye en su código. Esto incluye archivos ejecutables (éxe/'com'), salvadores de pantalla ('scr'), PKZIP y otros archivos batch.bat), Visual Basic o texto tales como el VBScript.vbs.bas') y cualquier programa interprete o compilado por programas fuente.*

*\* Asegúrese que los 'helpers' (sistemas de ayuda) o las opciones que puedan habilitar la actividad de extensiones de archivos que puedan eventualmente incluir potenciales códigos ejecutables infectados, sean puestos como "Ask User"(o el equivalente en su navegador) es decir, que antes de ejecutarse el sistema le pregunte si desea hacerlo (y no conteste "sí" a menos que esté seguro de que función cumplen). Nunca deje que su navegador ejecute automáticamente ningún programa. Coloque todas las opciones de Java tanto en "off" (desactivado) como en "ask" (que consulte o pida permiso para ejecutarse). Esto puede hacer que el navegador consuma mas tiempo pero será mas seguro.*

*\* Asegúrese que la orden de arranque ('boot order') en su sistema operativo este habilitada a operar sobre su disco C: únicamente (o también en C: y en A: si C: solo, no es permitido) – de manera que si usted arranca desde un disco flexible en la unidad de lectura, no podrá ejecutar el sector de arranque sobre el disco flexible e infectado potencialmente su sistema.*

*\* El procedimiento más efectivo y simple contra virus es una búsqueda regular del sistema (semanal, por ejemplo) o a continuación de cualquier descarga de programas (donde el software que controla virus explore cualquier archivo ejecutable o códigos objeto existentes en su sistema.) Utilizar códigos de control ("checksums") (que controlan el número y tamaño de los archivos guardados, verificando a través de los resultados si alguna parte de los archivos ha sido cambiado), es una manera muy efectiva, pero esto no constituye una prueba completa, y es realmente molesto cuando usted vuelve a controlar porque le va a indicar cambios en muchos archivos que han sido cambiados en forma normal y no por una infección.*

*\* No corra programas de orígenes no verificados - aun si ellos fueron chequeados con un buscador de virus. Esto es muy fácil de insertar una instrucción dañina en el programa que hará basura su sistema y esta no podrá ser encontrada por un buscador de virus.*

*\* Siempre haga un resguardo de su sistema de arranque con el verificador de virus instalado en el mismo, de esta manera si su sistema llega a ser infectado, usted podrá arrancar desde un disco flexible sin activar el virus existente en el disco duro y proceder luego a limpiar el sistema.*

*\* Proceda a depurar su sistema regularmente utilizando el scandisk (para el caso de Windows) – esto limpia todo dato extraño desde sus discos, archivos truncados, etc. También, guarde una mirada sobre los archivos temporarios.tmp' que no han sido borrados en su sistema. Una buena protección contra virus está relacionada a un buen administrador de sistemas, pero se hace más fácil limpiar un sistema infectado de virus si no existen archivos basura guardados en el mismo.*

## 5 - VIRUS de COMPUTADORAS

---

### Linux y virus

Los sistemas basados en Linux son menos susceptibles a los virus por el particionamiento del sistema y los controles utilizados sobre la instalación del software. Pero muchos usuarios de Linux intercambian y distribuyen programas sobre la red, y esto hace posible que algunos pueden distribuir programas basura. Mientras tanto, la probabilidad que tal programa pueda hacer un daño significativo al sistema es baja , aunque puede afectar al usuario que lo corra. Esto significa que el sistema no puede llegar a sufrir un daño fatal a menos que el programa explote algun defecto de seguridad del sistema operativo.

## 6 - USANDO INTERNET en forma SEGURA

Este es un Resumen de la Serie sobre Seguridad de la Información; y trata los siguientes temas:

- \* **Cómo Internet puede monitorear su actividad en línea.**
- \* **Minimizando los riesgos que sus actividades en línea sean monitoreadas.**
- \* **Minimizando los riesgos para su sistema.**
- \* **Privacidad y mantenimiento del sistema.**
- \* **Maneras comunes en que exponemos nuestra identidad sobre la red.**
- \* **Administrando la difusión de identidades: Personas alternas.**

### Cómo Internet puede monitorear su actividad en línea.

Internet es una red abierta, donde cualquier punto de la red puede ser accedido desde cualquier otro. Esto es lo que hace de Internet un medio masivo de acceso público. Provoca también que su utilización tenga implícito un riesgo concreto a través de la información que intercambia, y a través de las oportunidades que le brinda a otras personas de influir sobre su trabajo.

Internet presenta tres grandes riesgos, que exponemos en decreciente orden de importancia:

#### \* **Exposición de información privada.**

Cuando envía un correo electrónico o navega la red, usted no es un anónimo. Usted deja logs (archivos de registro de operación) de lo que ha estado haciendo sobre numerosos servidores. Otras personas pueden haber puesto interceptores ("taps", concepto semejante a "pinchadura") sobre sus conexiones de correo y grabar tanto sus entradas como sus salidas, además de su tráfico en la red.

#### \* **Daños a su computadora.**

*Cuando está en línea, en red, o utilizando los servicios de Internet, expone su computadora a virus informáticos y al posible trabajo de piratas.*

#### \* **Un perfil público indeseado: pérdida de su privacidad:**

Esta siendo cada vez más fácil compilar rápidamente perfiles sobre las personas y su comportamiento trayendo desde la red y relacionando información que revela el como son y cómo usan Internet.

Organizar bien su información y su sistema operativo y tener un buen resguardo de los datos es una buena manera para proteger su sistema (Ver especialmente el Resumen Nro.2 sobre Resguardo de Datos y el Nro. 5 sobre Virus Informáticos). Aprender cómo trabajar en línea y la manera de proteger su información, su identidad y si es posible su privacidad, es una parte importante de cómo trabajar internet con seguridad.

Enviar y recibir información privada usando Internet es un desafío. El proceso de enviar un correo es similar al proceso del envío físico de una carta. Imagine que está enviando realmente una carta con contenido secreto. Si deja un borrador de la carta en su casa, alguien lo puede encontrar. El cartero que reparte la correspondencia, podría enterarse a quien lo está enviando, y cuán pesado es su sobre. Si el cartero lo hace con cuidado, él

## 6 - USANDO INTERNET en forma SEGURA

---

podría abrir la carta y leerla. El cartero luego la despacharía en la oficina de correo local. De nuevo la oficina postal puede registrar quién envía la carta, a quién y en que fecha, y luego eventualmente abrir la carta. Su oficina postal local debería enviarla a la oficina postal cercana al destinatario, y finalmente entregarla a su destinatario. Si el destinatario deja una copia de la carta olvidada por ahí, hará posible que el contenido de la carta pueda ser descubierto.

Los riesgos son mucho mayores en el correo electrónico que en el correo real. En la metáfora anterior, su cartero es su conexión con su proveedor de servicios de Internet (ISP). Su oficina postal es donde tiene su cuenta de correo y por donde envía su correo saliente. Los destinatarios del correo son las casillas de correo electrónico de los proveedores, y los carteros son los ISP destinatarios.

Lo peor en Internet es que los proveedores siempre registran automáticamente quienes envía el correo y a quién (esto lo hacen desde siempre los programas que procesan los mensajes de correo electrónico). Y además, por defecto, nuestros correos lucen como escritos en una postal – el mensaje en sí mismo es fácilmente visible tanto para el cartero como para la oficina postal (si tiene los permisos adecuados o está espiando el tráfico en la red). Todo lo que usted haga sobre Internet pasará a través de su ISP. El defecto de la mayoría de los servidores de Internet es enviar todo en texto plano. Esto significa que, por ejemplo, el contenido entero de su correo es visible para cualquier persona con acceso a su red local o a la conexión en su ISP.

Es posible que tenga que proteger ciertos servicios configurando una encriptación automática de la conexión del servicio. Para la navegación por la WEB, puede utilizar los protocolos 'https' (SSL) en lugar del 'http'. El protocolo 'https' es el standard para todos los sitios que prestan servicios bancarios en línea y muchas páginas de control de acceso con contraseñas ('login'). Hay sistemas de correo que funcionan sobre páginas web y que también utilizan el protocolo 'https'. Si su proveedor de correo electrónico tiene la capacidad de usar SSL, puede configurar un 'tunnel' de seguridad hasta su ISP para recibir o enviar email. Esto es llamado POP/SSL y SMTP/SSL. Naturalmente, debe necesariamente confiar en cierto aspecto en su proveedor de correo y en como maneja su operación técnica y cuidado de los datos de tráfico.

En el Resumen Nro.: 4 de esta Serie se explica el uso de la encriptación. Es posible enviar correos electrónicos encriptados usando programas de encriptación como el PGP. Las cabeceras (o "Headers") como 'From', 'To', y 'Subject' son claramente visibles para su proveedor ISP. Si usa técnicas de encriptación, esto solo se aplica al cuerpo del mensaje, no a dichas cabeceras.

Así como las cabeceras son los lugares donde los programas de correo de los servidores leen la información necesaria para despachar su mensaje y lo registran, del mismo modo, estos registros pueden y en muchos casos, son usados para controlar las actividades de grupos o individuos, permitiendo generar el perfil de qué es lo que está haciendo un individuo o un conjunto o grupo de individuos en línea, qué otros sistemas o direcciones de correo han contactado o por quienes han sido contactados, y las fechas y horas y eventualmente las ubicaciones desde donde los miembros de la red se han comunicado.

En general, la ubicación no es un dato directo. Los mismos ISP no registran eso en forma directa. Pero con la tecnología actual, es posible registrar el número de teléfono desde donde se llama al ISP, o, peor aún, si tiene un acceso continuo (también de banda ancha) en su oficina u hogar, se puede determinar sin dudas cuál es el usuario que está

## 6 - USANDO INTERNET en forma SEGURA

conectado en determinado momento y consecuentemente la dirección a donde llega esa conexión. He aquí un ejemplo de un mensaje encriptado. Puede observar que la información de la cabecera no está encriptada. (La cabecera está con tipografía en letra "negrita"). Podrá ver que hay una cantidad de información sobre el mensaje que no está encriptada y que serviría a fines de control y seguimiento.

**Delivered-To:** an-email-list@seven.gn.apc.org  
**Received:** from nfs1.gn.apc.org (nfs1.gn.apc.org [194.202.158.5])  
by seven.gn.apc.org (Postfix) with ESMTP id 3BBC23957  
for <an-email-list@seven.gn.apc.org>; Mon, 7 Jan 2002 09:58:52 +0000 (GMT)  
**Received:** from KBLAP.gn.apc.org ([194.202.158.101])  
by nfs1.gn.apc.org (8.9.3/8.8.8) with ESMTP id KAA17178  
for <an-email-list@gn.apc.org>; Mon, 7 Jan 2002 10:02:03 GMT  
**Message-Id:** <4.3.2.7.2.20020107095742.028fc888@pop.gn.apc.org>  
**X-Sender:** person@pop.gn.apc.org  
**X-Mailer:** QUALCOMM Windows Eudora Version 4.3.2  
**To:** an-email-list@gn.apc.org  
**From:** a.person <person@gn.apc.org>  
**Subject:** Re: [an-email-list] new member  
**Content-Type:** text/plain; charset="us-ascii"; format=flowed  
**Sender:** an-email-list-admin@gn.apc.org  
**Errors-To:** an-email-list-admin@gn.apc.org  
**X-BeenThere:** an-email-list@gn.apc.org  
**X-Mailman-Version:** 2.0.6  
**Reply-To:** an-email-list@gn.apc.org  
**List-Help:** <mailto:an-email-list-request@gn.apc.org?subject=help>  
**List-Post:** <mailto:an-email-list@gn.apc.org>  
**List-Subscribe:** <<http://mailman.greenet.org.uk/mailman/listinfo/an-email-list>>,  
<mailto:an-email-list-request@gn.apc.org?subject=subscribe>  
**List-Id:** <an-email-list.gn.apc.org>  
**List-Unsubscribe:** <<http://mailman.greenet.org.uk/mailman/listinfo/an-email-list>>,  
<mailto:an-email-list-request@gn.apc.org?subject=unsubscribe>  
**List-Archive:** <<http://mailman.greenet.org.uk/mailman/private/an-email-list/>>  
**Date:** Mon, 07 Jan 2002 09:59:37 +0000  
**X-UIDL:** 6cc!!S;n"!LjD"!~L-!!

—BEGIN PGP MESSAGE—

Version: PGPfreeware 7.0.3 for non-commercial use <<http://www.pgp.com>>

crzGA1pfOZIAgifhHeQtk4mseUO4BSIbRk1/K1HAbeJ9lSc+mVEL3V2tLxT3Eq6x  
ggNnhiyqYcnAkTw2FKvaYsHmrOH0cnxfypFjBvNiQE0q5rr4lJQ8lIlr2lzSE  
0XRXT+2GkiELlpuuY2U2BpYs7wAHPO8hp+nQTQQscSttE2utleC4n958DUE5w3zU  
Zd+S0Rqy7M6J6CJcAc4AVPK4X5A2abrsttVxEdeNXDvDldAbfFHpm0qHqoB2iUKl  
MbL+y9k+mPXVe6eRzb6j47/by/PuYLIE8i1cVVvYACMbjfJAtukFMRfqsDp7EWu  
pz9NPB4wCEL4qXQpMUHbM9FIVkmNJ3Y5UINslxsWlU241AZi+vPk1x/saLcIN5Kd  
JgoGkQaHLVvhKvAACdISgojemFfaCDe+buZ+qimBfhLj6GnadTMk84oIlX9j6evm  
f4zHj354ljQ2aGOrqdCo06sn7LVR2VaXP0U2/O5Vy/zPn1dPy4kY2JsqeN/30nX8  
WN8CAce0l2WWvJE=  
=LZSS

—END PGP MESSAGE—

---

an-email-list mailing list  
an-email-list@gn.apc.org  
<http://mailman.greenet.org.uk/mailman/listinfo/an-email-list>

## 6 - USANDO INTERNET en forma SEGURA

---

### Minimizando los riesgos de que sus actividades en línea sean monitoreadas.

Existe una cantidad de servicios en líneas y software que pueden ser usados para proteger su privacidad. En una próxima página tiene una tabla de las herramientas disponibles más comunes. Lo siguiente le permite evaluar cuando puede utilizar estas herramientas.

#### Correo electrónico seguro:

Si usted está enviando y recibiendo emails por su ISP, ellos pueden potencialmente leer todo su correo y no tiene manera de darse cuenta y pero aún de evitarlo. Esta situación puede ser o no aceptable para su interés, en función de su privacidad, su actividad profesional o voluntaria. Si la seguridad es de su interés, existen varias opciones que puede considerar:

Ejemplos de webmails privados con acceso libre

**S-Mail:** Configurando las direcciones de correo electrónico con el web-mail <http://www.s-mail.com>. Este sistema le permite controlar su correo electrónico en la red utilizando el protocolo seguro SSL (direcciones web con https). Si envía su correo con s-mail, su ISP puede no estar habilitado para ver que es lo que usted ha enviado. Al mismo tiempo, si el destinatario del correo es monitoreado, su correo puede no ser seguro. Si mantiene correspondencia regular con personas sobre asuntos sensibles (desde la perspectiva de seguridad o privacidad, suya o de terceros) debe aconsejarles conseguir una cuenta de correo, operada con el mismo sistema que usted está utilizando.

**Lock-mail:** Como otra alternativa, si intercambia mensajes con una persona que usa PGP, podrá interesarse en <http://www.lockmail.com>. Lockmail es similar al s-mail.com, y le permite conectarse usando SSL (https). Este sistema también le permite encriptar sus mensajes a personas que utilizan PGP. Utiliza un sistema "server-side PGP" (que el mismo servidor encripta sus mensajes de correo). Pero, seguramente no es un método tan seguro como utilizar directamente PGP sobre su propia computadora.

(VER CUADRO 6-1)

S-mail y Lokmail son libres, fáciles de utilizar y adecuadamente seguros. Sin embargo, ellos no son tan privados como usar PGP o Hushmail (los cuales son descritos en la próxima sección). La razón por la cual recomendamos S-mail en lugar de Hushmail es porque Hushmail cierra las cuentas libres de usuarios si ellos no las utilizan durante 3 semanas., Hushmail toma mucho más tiempo en reiniciar que S-mail. Si tiene necesidad de una seguridad fuerte, o no confía en s-mail o en Lokmail, puede considerar utilizar el servicio pago de Hushmail o utilizar el "pago por mayor privacidad" como una opción.

Si únicamente necesita enviar mensajes de correo electrónico seguros a cada momento, y necesita una fuerte encriptación, Hushmail es una buena opción. Hushmail utiliza un encriptado muy fuerte, y es fácil de instalar y de utilizar. Pero deberá pagar por el servicio de Hushmail si necesita un uso regular.

Si ambos, usted y la persona con la que se comunica utilizan Hushmail, ninguno puede monitorear lo que usted diga. Sin embargo, Hushmail puede ser lento para utilizarlo sobre un acceso por línea de teléfono común.

## 6 - USANDO INTERNET en forma SEGURA

Hushmail cierra las cuentas libres de correo si estas no son utilizadas continuamente durante 3 semanas. Si desea que otras personas estén habilitadas para enviarle mensajes, debe suscribirse al servicio pago de Hushmail y difundir su nueva dirección bajo Hushmail. Al mismo tiempo, puede configurar el sistema de Hushmail para que le envíe un mensaje de aviso si tiene un mensaje por leer hacia su cuenta normal de correo en cualquier otro sistema.

Existen redes asociadas a APC que también cuentan con servicios de webmail que usan accesos encriptados usando protocolos SSL.

Otra opción paga, es utilizar módulos adicionales en los programas (clientes) de correo como el Microsoft Outlook de Microsoft, Eudora, Pegasus Mail u otros, que pueden trabajar utilizando PGP. PGP es 'el standard' en seguridad para mensajes de correo electrónico. PGP utiliza un fuerte sistema de encriptado (Vea Sumario 4), y su ISP (en situación normal) no tendrá capacidad para descubrir el contenido de sus mensajes.

Sin embargo, hay algunos obstáculos para su uso efectivo:

*\* Al principio puede ser difícil entender como el sistema PGP trabaja las llaves públicas y privadas.*

*\* Algunas veces el uso de PGP dificulta las comunicaciones en donde se utiliza.*

*\* Aun si ambos utilizan PGP, su tráfico de datos de la cabecera de los mensajes (desde / a / sujeto) son todavía visibles para cualquiera que esté monitoreando su tráfico en Internet, como también es visible el hecho que ustedes están utilizando PGP. Mirando su datos de tráfico, cualquiera que lo esté vigilando, está habilitado para ver a quien le está enviando correo, cual es el asunto y que está utilizando PGP.*

El "a quien envía" así como de "quien recibe" correo es una información muy importante para aquellos que deseen monitorear sus actividades y las de las personas que se relacionan con usted.

Para eludir éste último problema, necesita utilizar POP/SSL, y SMTP/SSL con sus proveedores de correo y confiar además que sus proveedores no divulgaran sus datos de tráfico. Hay muchos servidores de web y proveedores de correo que ofrecen POP/SSL y SMTP/SSL como parte de un paquete de web-hosting. Si su proveedor de correo acepta las conexiones SSL, es bastante sencillo instalar las opciones correspondientes para que su programa de correo funcione con ellas.

La opción final son las cuentas privadas anónimas. Algunas veces hay personas que necesitan enviar un mensaje y quieren asegurarse que ninguno pueda enterarse quién lo ha enviado. Esto no es fácil de hacer hoy día.

Para alejarse del problema de rastreo del proceso de correo, se han creado los "anonymous remailers". Estos sistemas reciben mensajes con una dirección de reenvío (forwarding addresses) incluida y remiten el correo sobre el destinatario, omitiendo la información original del que lo generó. Luego el mensaje aparece como si hubiese sido

## 6 - USANDO INTERNET en forma SEGURA

enviado por el "remailer", en lugar de la persona que realmente lo envió. Algunos sistemas también anotan una dirección al azar que luego permite aceptar una respuesta. Pero, en los últimos años, muchos de estos "remailers" han sido cerrados, algunas veces por la presión de las disposiciones legales o de los servicios de seguridad, pero mayormente por las amenazas legales de aquellos que han sido atacados o difamados por mensajes anónimos.

Diferentes sistemas de "remailers" tienen diferentes políticas. Algunos son verdaderamente anónimos, y no requieren ningún dato que pueda identificar a sus usuarios. Otros requieren la apertura de una cuenta. Algunos son libres, y algunos pagos. Es difícil proveer una lista de "remailers" anónimos porque las políticas pueden cambiar regularmente, y mientras unos nuevos pueden aparecer otros cierran. Puede buscar en Internet una lista de los "remailers" anónimos. Utilizando por ejemplo un buscador como Google con las palabras "anonymous remailers" puede localizar varios de ellos.

Muchos servidores de correo electrónico resguardan los datos del tráfico que pasa a través de sus sistemas en función de que los mensajes puedan ser rastreados hasta su punto de origen si han de cumplir con requerimientos de las autoridades. El nivel de privacidad dado a esta información es primariamente dictado por leyes que rigen la privacidad y la protección de los datos en aquellos países en los cuales el "remailer" tiene su domicilio.

Alguno que necesite enviar un email que sea totalmente anónimo necesita ser un experto o requerir la asistencia de uno. Es fácil cometer un error y exponer su identidad en un email anónimo. La dirección web (URL) listado en la Tabla 6-1 es un buen lugar para empezar a mirar. [http://www.sendfakemail.com/~ts\[raph/remailer-list.html](http://www.sendfakemail.com/~ts[raph/remailer-list.html)

*De todas formas, recuerde que no puede evitar que el servidor que recibe el mensaje registre de que lugar de la red lo está recibiendo.*

### **Servidores Web Anonimos (proxy-servers)**

Generalmente, toda vez que esté utilizando la web, dos organizaciones conocen los sitios que usted visita

- \* Los sitios que usted visita registran que usted los ha visitado, además
- \* Su ISP puede también registrar que URLs ha visitado (es habitual pero no siempre es así).

Puede utilizar la web anónimamente a través de "servidores de web anónimos" o "proxy servers". Este sistema consiste en definir un sistema intermediario entre usted y el servidor a donde esta tratando de leer información, de la siguiente forma:

- \* Usted solicita una pagina web desde su navegador a un servidor anónimo.
- \* Se recupera la página y la información que se registra en el servidor de destino, es la del servidor anónimo, y no la de su propio proveedor de servicio de Internet.
- \* El servidor puede después modificar algunos enlaces en la página antes de reenviársela a usted. Esto significa que si clickea sobre alguno de los enlaces (links) en la página que esta viendo, probablemente también pueden hacer un requerimiento anónimo al servidor anónimo, y no en forma directa al servidor en

## 6 - USANDO INTERNET en forma SEGURA

donde se encuentra la página que está necesitando. Los servidores anónimos pueden también guardar registros de datos de conexión (logs) en uno y en otro sentido.

*Deberá chequear cuidadosamente las credenciales del operador de su servidor anónimo antes de utilizar sus servicios.*

Nota: Debe conocer que actualmente hay numerosos prestadores de servicio internet que utilizan sistemas de "cache" transparentes. A los fines prácticos, significa que están en condiciones técnicas de intermediar, le guste o no, en su navegación web. Potencialmente podrían registrar todo el tráfico que intercambia e incluso visualizar nombre de usuarios y contraseñas de los servicios que utilice y que no usen algún sistema de encriptación como para evitar ser fácilmente revelados. (vea en los párrafos anteriores el tema de uso de protocolos seguros, SSL, en la navegación web)

A la fecha de esta actualización, Mayo 2003, ya hay anuncios explícitos de parte de los principales fabricantes de los equipos que controlan el tráfico de internet que van a instalar accesos especiales (llamados "puertas traseras" o "back doors" en inglés) para que los gobiernos y agencias de seguridad puedan monitorear, a su entero capricho y voluntad todo el tráfico, incluso a nivel de contenido, de cualquier red que use dichos equipos.

### **Servidores anónimos de relevo.**

Debe saber que si bien puede usar un server anónimo para su navegación web, su proveedor de acceso puede permitir o cancelar su conexión a estos servidores anónimos, en forma general o especificando un servidor o grupo de servidores en especial.

Para eludir ser monitoreado por su ISP, puede intentar hacer un "túnel" en su conexión a un servidor seguro. Actualmente esto sólo está disponible a través de un servicio pago en: <http://www.anonymizer.com> . Ha existido otro servicio de "túnel" llamado "Freedom Network" desarrollado por Zero Knowledge, pero su servicio ha sido clausurado en el año 2001.

### **Minimizando los riesgos para su sistema.**

Conectarse a Internet, o a una red local, implica abrir una amenaza potencial a su sistema. Su sistema puede correr programas sin su conocimiento, desconocidos para usted, y ellos pueden dañar su sistema o exportar información a otras computadoras. Por lo tanto administrar los riesgos en su sistema incluye la utilización de programas que monitoreen la actividad de las conexiones a la red, y la actividad de los archivos y programas a los cuales ha accedido por Internet.

Existen dos importantes tipos de programas que usted debe instalar – un firewall (muchos traducen como "cortafuegos") y un explorador de virus.

## 6 - USANDO INTERNET en forma SEGURA

### Cortafuegos o "Firewalls"

Una conexión a Internet es un canal de doble vía. Dependiendo de cómo ha sido configurado, su sistema puede recibir y procesar los pedidos de otros servidores vía un "socket" (un "socket" es el nombre que recibe una conexión establecida en Internet o en una red local). Para limitar el potencial de cualquier "socket" deberá configurar una barrera que se denomina "firewall" o cortafuego.

Los "firewalls" en Internet controlan que programas están habilitados para conectarse a la red. La red puede ser Internet, o cualquier red local en la que deba conectarse.

Personalmente tiene que autorizar a cada programa en forma expresa, para que pueda usar su conexión de red antes que pueda utilizarla. Por tanto cualquier programa que esté tratando de conectarse a Internet desde el "background" (término que se refiere a procesos que no son visibles pero que están funcionando en su sistema, sea en forma legítima o no) de su computadora sin su intervención, será bloqueado, y usted recibirá un mensaje de advertencia.

El "Firewall" también previene que otras computadoras sobre la red, requieran servicios sobre su computadora vía sockets, a menos que ellos también estén autorizados para hacerlo. De esta forma, controlando lo que puede correrse a través de los sockets, controla qué datos tienen permiso para entrar y salir de su computadora.

Los "Firewalls" pueden también proteger su privacidad. Como anotamos más arriba, algunos programas tratan de conectarse a Internet para tramitar información, aun cuando no está usando dicho programa. Muchos programas pueden hacer eso cuando se instalan y ejecutan inicialmente pequeños programas al encender la computadora.

Cuando estos pequeños programas detectan que se establece una conexión a Internet despiertan el programa principal para ir "online". A menos que usted le haya dado permiso al programa para utilizar la red local o Internet, este intento de acceder al socket de la red será advertido por el "firewall". Luego puede denegar o permitir al programa que acceda a la red local o a Internet. Esto significa que cualquier software pirata, tal como sucede con un virus, o cualquier otro que se haya instalado en su sistema, no estará habilitado para exportar datos de su computadora sin su conocimiento.

El "firewall" también detiene el funcionamiento de los "spyware" cuyo uso se está incrementando de parte de los productores de programas propietarios en un esfuerzo para controlar la utilización de software sin licencia.

Nota: también se ha incrementado el uso de "spyware" como forma de obtener datos que afectan su privacidad: que sitios navega, que opciones usa y eventualmente direcciones, agendas, etc.

Existen varios "firewalls" que están disponibles para el sistema Windows. Incluso Microsoft Windows XP viene con un "firewall" incorporado, pero éste solamente trabaja sobre la conexión de datos entrantes. Por lo tanto los programas pueden acceder desde su computadora a la red, sin que se dispare ningún alerta para usted. Esto representa una falla importante de seguridad en el sistema. Muchos sistemas de "firewalls" monitorean tanto la entrada como la salida de datos de su computadora.

## 6 - USANDO INTERNET en forma SEGURA

---

Existen muchos programas firewall tanto de uso libre como comerciales. Puede buscar por "personal firewall" en un buscador en Internet, o ir directamente al sitio [www.firewallguide.com](http://www.firewallguide.com) para ver algunos de los más populares.

Algunos equipos actuales incluyen dentro de los programas que entregan con su hardware (principalmente con su placa principal o placa madre "motherboard") algún "firewall" con licencia de uso original.

Sobre los sistemas basados sobre Linux usted tiene muchas opciones para configurar un firewall, y las distribuciones más nuevas ya lo instalan cuando usted enciende la computadora. Recuerde igualmente que son programas que requieren manejar una configuración adecuada a su trabajo en red y que tipo de servicios utiliza y que riesgos quiere correr.

### Buscadores de Virus.

Los virus son un problema particular en los sistemas basados en Windows, porque ellos explotan los defectos de los programas en Microsoft para infectar una computadora y extender la infección a otras computadoras, en sus archivos o en el correo. Los scanners (buscadores de virus) son los medios más adecuados para prevenir su acción, advirtiéndole de potenciales daños a su sistema.

Los exploradores de virus trabajan tratando de detectar las firmas de los virus en el archivo o en el adjunto del mensaje de correo. Sistemas más avanzados verifican también su sistema, controlando agujeros (fallas) en su seguridad, y tentativamente tratando de arreglar las fallas del mismo.

Entendemos por firma de un virus a secuencias de ordenes específicas de cada uno y de sus variantes. Esto es lo que estudian las empresas y organizaciones que tratan el tema de los virus y generan los programas antivirus basándose en detectar la mayor cantidad de firmas y variantes que hay en los virus para poder evitarlos.

Si el scanner detecta la firma de un virus pone en cuarentena el archivo o el mensaje de correo para prevenir que el mismo sea abierto, y proporcionan una advertencia al usuario.

A medida que nuevas fallas de seguridad son descubiertas, y nuevos virus son escritos, los viejos exploradores no reconocen los nuevos virus. Por tanto, es importante actualizar regularmente el software relacionado con la búsqueda y la protección contra virus.

De todas formas, debe tener presente siempre que, tal como sucede en la realidad biológica, **primero existen los virus y luego aparecen, despues, las vacunas.**

En el estado de la informática actual, podemos comprobar que un virus nuevo puede empezar a propagarse e infectar miles de equipos (cientos de miles también) antes de ser detectado, investigado y generado una vacuna adecuada. Y en los tiempos actuales, esto puede significar que a veces hay 1 o incluso 2 semanas antes de una actualización adecuada de los programas antivirus. Mientras eso no ocurre, por mas actualizada que tenga la copia del programa antivirus y sus datos, no estará a salvo del "virus recién llegado".

La forma más importante de prevenirse de los problemas de los virus está en no utilizar programas, lenguajes y sistemas que son susceptibles a los virus. Esto significa eludir en

## 6 - USANDO INTERNET en forma SEGURA

---

lo posible la utilización del programa de correo Microsoft Outlook y restringir la utilización de lenguajes de programación como Visual Basic y Java sobre su sistema.

Cada vez que Microsoft introduce un nuevo sistema operativo es necesario ser más cuidadosos. Mientras las fallas en el sistema son descubiertas y explotadas por los virus hasta que aparecen los parches de seguridad para remediar dichas fallas, (aunque muchas veces generan problemas adicionales) hay que evitar su uso.

Una buena alternativa es utilizar un sistema operativo que no sea Microsoft, tales como Macintosh, BSD, Unix, FreeBSD o Linux, los cuales por su diseño son menos susceptibles a ser atacados por virus.

El resumen Nro.5 sobre los Virus Informáticos contiene una detallada información sobre los mismos y como eludirlos.

### **Privacidad y mantenimiento del sistema**

Como anotamos en el Resumen Nro.1 sobre Seguridad y privacidad de la Información (vea: Persistencia), es muy fácil acumular datos sobre el sistema (sobre todo ahora que los discos duros son cada vez mas grandes), pero a veces resulta muy dificultoso removerlos o incluso simplemente definir si son útiles para alguien o no.

Si usted utiliza Internet, su computadora estará acumulando datos sobre fechas, sitios y contactos los cuales pueden ser muy sensitivos o importantes para usted.

Administrar la información generada en su computadora como parte de su actividad relacionada con internet es una parte importante de su privacidad en línea. La gran amenaza se produce si su computadora es accedida, robada o confiscada, y esa información relacionada sobre el uso de internet, pueda ser utilizada contra usted o contra terceros. Este riesgo no puede ser evitado pero puede ser reducido por una cuidadosa administración del sistema.

### **Correo Electrónico:**

Muchos programas de correo guardan sus datos sobre discos. La excepción es el Web Mail, donde los datos son almacenados en uno o varios servidores (a menos que usted guarde una copia sobre su propio disco rígido). Muchos programas de correos también almacenan datos separadamente, mayormente en los archivos agregados al correo. A veces los directorios asociados con un programa de correo pueden llegar a un atasco, mayormente con información fuera de uso, a menos que tenga el cuidado de depurarla regularmente. Los mensajes de correo por si mismos pueden también aumentar su volumen y cantidad, de manera que tenga cuidado de limpiar regularmente la carpeta de entrada y las otras carpetas del sistema de correo.

### **Encriptado**

Si usted tiene instalado un programa de encriptación, los mensajes que haya encriptado son automáticamente desencriptados cuando usted procede a la apertura de su correo.

Tenga cuidado: Los archivos adjuntos a sus emails no son automáticamente encriptados conjuntamente con los mensajes del correo. Los archivos adjuntos deben ser encriptados

## 6 - USANDO INTERNET en forma SEGURA

---

y descryptados separadamente, utilizando programas como el PGP Tools (Ver Resumen Nro.4). Si tiene información sensible que no ha sido encriptada, deberá considerar guardar esos mensajes como archivos texto, para luego encriptarlos utilizando su propia clave, en prevención que otros puedan tener un fácil acceso a ellos.

### **Archivos temporales de internet o "Web caches"**

Los servidores de Internet, a los efectos de aumentar la velocidad de acceso, guardan los archivos bajados de Internet en un "cache" (cache = memoria intermedia). Este "cache" varía el tamaño dependiendo de la configuración de su sistema. Pero a menos que usted limpie el cache regularmente, particularmente después de haber efectuado un trabajo sensible sobre Internet, el cache puede proporcionar un detallado registro de la información que usted ha estado viendo durante algunos días o incluso semanas. También es posible que las páginas web contengan información invisible en imágenes o archivos que igualmente han sido bajados pero no mostrados en pantalla. Esto también estará guardado en su cache en su disco duro.

Limpiar el cache es por lo tanto una manera simple de limpiar algún dato escondido en las paginas web de su sistema.

### **Web - Archivos historicos**

Otro archivo significativo guardado por el navegador es la lista histórica ("history"). Esta lista contiene la dirección de todas las páginas que usted ha estado visitando recientemente. Cuando mira una página web, verá que hay enlaces que aparecen de un color y otros de diferente color. Esta diferencia le avisa cuando un enlace ya ha sido visitado, y el control de esta diferencia se realiza usando la lista histórica que tiene grabada el navegador.

El periodo después del cual expira la dirección en la lista está definido en la configuración del navegador y puede ser modificada por usted. Si esta puesto para 30 días, toda vez que la pagina vuelva a ser visitada volverá a ser registrada en la lista histórica. Si se establece que nunca expirada ("never expire") cada página que el navegador visite será considerada como si fuera la primera vez.

Usted tiene la opción de limpiar o depurar esta lista histórica. "Deberá hacerlo en forma regular. El navegador también gestiona el archivode favoritos o "bookmarks" que contiene las direcciones de los links de los sitios visitados y que usted ha querido marcar de alguna forma para regresar posteriormente. Este archivo debe ser regularmente editado, parcialmente para remover algún dato inútil. Cuando no necesite más de ellos, remueva cualquier referencia a sitios sensibles.

### **"Wiping" y borrado de archivos.**

Como hemos anotado en nuestro Resumen Nro.1, cuando elimina archivos de su sistema, en realidad esta eliminando únicamente la referencia en un archivo índice donde se marca que ha sido borrado y por lo tanto el espacio utilizado esta disponible.

Administrar sus correos y archivos adjuntos, limpiar el "cache" de los navegadores y editar la lista de historia o los archivos de direcciones favoritas("bookmarks") no es suficiente para remover esos archivos del sistema; solamente remueve la referencia de los índices de los archivos del sistema.

## 6 - USANDO INTERNET en forma SEGURA

Así que, después de hacer una depuración de los archivos de su sistema, también deberá limpiar el espacio "supuestamente libre" de su disco duro.

Esto puede hacerse simplemente ejecutando utilitarios como el "Scandisk" y el "Defrag" para aquellos sistemas basados en Windows. Pero para estar absolutamente seguro que no quedan datos de sus archivos borrados, necesitará sobre-escribir el espacio libre del disco con nuevos datos. Existen varios programas para hacer esta tarea, pero las más efectivos son aquellas que vienen con los sistemas de encriptados.

Estos sistemas sobre escriben el espacio con información generada al azar con el propósito de enmascarar cualquier dato que pudiera estar grabado previamente y después borrado. Para información adicional vea el apéndice del Resumen Nro. 4

Nota: También puede sobrescribir ese mismo espacio guardando un archivo con datos intrascendentes con el mismo nombre que tiene el archivo a eliminar. Tenga cuidado en que este último archivo sea igual o mayor al archivo original para asegurarse que todos los datos anteriores han sido sobrescritos y eliminados.

Para asegurar la eliminación de un archivo en Windows NT, Windows 2000, o en Windows XP, usted necesita asegurarse tanto el borrado del archivo como limpiar el espacio libre. Estos sistemas operativos utilizan un sistema de archivos denominado NTFS, el cual guarda en forma alternada los sectores de datos de los archivos eliminados.

### Perfil público no deseado.

Puede exponer datos sobre su identidad por diversos factores a considerar:

*\* Usted debe tener una dirección de correo electrónico. Esto lo identifica como único usuario de una computadora en particular en la red. Pueden identificar la red que atiende su servicio de correo y esto puede actuar como puntero a donde acudir para obtener cualquier información adicional sobre usted (datos de tráfico, contenido de mensajes, etc).*

*\* Puede tener un sitio web. El nombre del dominio del sitio web, dependiendo sobre quien lo haya registrado, puede suministrar la información sobre quien esta corriendo el sitio. Observando las direcciones numéricas, se puede encontrar quien opera el sitio web y donde está ubicado.*

*\* Puede ser miembro de una lista de correo, o integrante de una lista de noticias en la red. Muchos de esos correos pueden ser archivados, aún mucho tiempo después de haber sido hechos, y pueden ser accesibles a través de motores de búsqueda. Esto hace que la información que a le interesa sobre ciertas materias, como también la asociación con otras personas o grupos con que esta trabajando, quede abiertamente en evidencia.*

*\* Cuando navega sobre internet, está depositando información sobre otras computadoras las cuales identifican univocamente la computadora que está utilizando en esos momentos. En los sistemas de navegación web, esto se realiza con pequeños archivos que son agregados a los datos que maneja su navegador y se denominan "cookies". Estos archivos mantienen pequeñas cantidades de*

## 6 - USANDO INTERNET en forma SEGURA

información sobre el uso de su sistema y quizá también de sus preferencias personales. En otros sistemas, le piden ingresar su dirección electrónica, la cual luego puede ser utilizada como dato clave en una base de datos, que siga su uso dentro del sistema.

\* Probablemente proporcionará información sobre su persona en orden a tener acceso a otros servicios. Mucha de esta información es vendida a compañías de marketing, y estará disponible para todos aquellos que estén en condiciones financieras de adquirirlas. Aun cuando es una actividad rara por los costos que involucra, es posible obtener un perfil de sus actividades online adquiriendo sus datos de compañías que han recopilado información de Internet.

*El riesgo más grande para su seguridad es cuando toda esa información acumulada sobre usted es relacionada para producir un perfil. Piratas u operativos de vigilancia pueden reunir bastante información sobre su persona como para elaborar fácilmente un plan de vigilancia a distancia. Utilizando esta información ellos pueden mapear su trabajo en la red así como de sus corresponsales habituales, identificando información sobre usted, su casa y sus hábitos de trabajo, temas que le interesan, etc. A través de la investigación de la información que pone (o incluso lee) en Internet, se puede también reunir información sobre su acceso a recursos de información, su competencia técnica, y quizás identificar a quienes pueden tener interés en descubrir o dañar la información sobre su persona.*

### Administrando el perfil: Personas o nombres alternativos.

Su identidad online puede ser una responsabilidad. Debe tener una identidad en orden para acceder a servicios que le requieren registrarse previamente para acceder a darle información. Como señalamos mas arriba, esta información potencialmente puede ser usada en su contra, robada o abusada. Para solucionar este problema deberá considerar la creación de una o más "personas alternativas" para usar en Internet.

Otros nombres o alias, son utilizados a menudo por las personas que charlan (salones de chats) en reuniones virtuales en Internet. Si guarda notas sobre la información que usa para enmascarar su otra identidad, otros también podrían usarla. Para actuar como una persona diferente necesita establecer:

\* **Un nombre** – esto puede ser un alias, o un nombre completo obviamente inventado;

\* **Una cuenta de usuario** – para asegurarse que su navegador o su correo electrónico proporcione al exterior, que parte de esas transacciones con el otro servidor, deben instalarse como una cuenta de usuario bajo el nuevo nombre (pero cuidando, que la información empotrada en sus archivos puede suministrar su nombre real a terceros).

\* **Una dirección** – esto puede ser difícil de hacer, porque aunque no esté referida a un nombre o dirección real, deberá tener un nombre de calle y código postal válidos, ya que muchos sistemas validan la dirección ersus el código postal antes de su aceptación. Hay sistemas que incluso llegan a relacionar datos personales con direcciones y telefonos.

## 6 - USANDO INTERNET en forma SEGURA

\* **Una nueva dirección para su correo electrónico** – esto puede ser una dirección adicional a su cuenta ya existente, pero debe asegurarse que su proveedor de servicio no proporcionará información alguna relacionada con las cuentas asociadas a su dirección.

\* **Contraseñas** – necesitará guardar las contraseñas que serán utilizadas por sus alias de manera que ellas no puedan confundirse con otras;

\* **Una historia o “leyenda”** – necesitará guardar un registro de alguna información personal suya creada para esta persona, tal como sexo, edad, gustos, intereses, etc. , de manera que pueda suministrarlos si le son requeridos. (Algunos servicios validan su acceso habilitándolo con el ingreso de ciertos atributos personales.)

El propósito de una identidad alternativa es proporcionar anonimato. Provee un medio para enmascarar su verdadera identidad cuando está usando servicios en línea, que podrían descubrir y revelar su información personal a otros. Esto evita que otros accedan a datos que podrían ser usados por alguien interesado en marketing directo, y también evita que accedan a datos que pueden ser utilizados para organizar una vigilancia sobre usted y sus actividades.

### Personas que pretenden sustituirlo vía email

El mayor problema relacionado con la protección de su identidad es la seguridad en el manejo de su dirección de su correo electrónico. Muchas personas también utilizan web-mail manejado a través de un web-server. El web-mail produce un conjunto de problemas ligeramente diferentes, pero los principios generales son los mismos.

Existen tres maneras de que su identidad pueda ser robada:

*-La información puede ser puesta a su nombre, supuestamente por usted, pero actualizada o enviada desde diferentes direcciones reales. Muchas personas no siempre leen la información que viene en la cabecera de un mensaje, y puede creer que tal información proviene de usted. Una de las maneras más fáciles de hacer esto es confeccionar un mensaje y enviarlo como si fuera un mensaje reenviado – eliminando la información de la cabecera del mensaje que identifica al emisor de forma unívoca.*

*-La dirección del correo puede ser cambiada o “engañada”. Los servidores de correo no siempre brindan seguridad para la salida de los emails.(por ejemplo: controlar el nombre del remitente para asegurar que es una cuenta válida dentro del sistema) Esto significa que tales direcciones de correo electrónico pueden ser alteradas, cambiando las características de las direcciones del correo electrónico saliente. Numerosas listas de correo únicamente discriminan por la dirección electrónica, y por lo tanto, si el nombre en el email parece que viene de usted el mensaje puede ser reenviado a la lista. Otro problema es, que mientras otras personas pueden estar mirando su correo personal, ellos no se tomaran siempre la molestia de controlar la información de cabecera para asegurarse que la información realmente proviene de su servidor de correo. El engaño es un problema en muchos países porque no está considerado fuera de la ley, mientras la intención de enviar ese correo falsificado no sea para defraudar al destinatario a nivel de bienes o dinero.*

## 6 - USANDO INTERNET en forma SEGURA

---

*-Su cuenta de correo puede ser invadida y ocupada. Esto es en general bastante difícil de hacer, porque alguien debería obtener la contraseña de su cuenta. Pero si usted no asegura su computadora (especialmente si es una laptop) o si utiliza sistemas de web-mail que no tienen un acceso seguro (es decir que utilicen protocolo SSL) esto es posible. Puede también ser hecho engañando a su proveedor de servicios internet para que le proporcione detalles por teléfono, utilizando quizás información que haya sido obtenida investigando su perfil además de otra información relacionada obtenida online. Los proveedores de servicio pueden ser engañados fácilmente, ya que ellos a menudo no conocen a sus clientes personalmente, sino solamente por la información contenida en sus bases de datos. También podrían tratar de ingresar de forma ilegal en el servidor donde opera su correo electrónico, aunque es más difícil de realizar. Ambas opciones son consideradas ilegales en muchos países por que constituyen un acceso no autorizado a un sistema computarizado. Recuerde que debe evaluar que el estado puede obligar, según las leyes vigentes en cada país, a interceptar y copiar el correo electrónico directamente en el servidor de su prestador de servicios internet. Siempre es adecuado tener cierto grado de confianza como para estar advertido de una situación así, si es posible.*

Todos estos problemas, con la excepción de tener una seguridad débil sobre su computadora, pueden ser fácilmente tratados mediante el uso de la firma digital en su correo electrónico, al menos en los mensajes más sensibles.

### **Identificación incorporada (o empotrada)**

Los programas de uso habitual en las computadoras pueden insertar su identificación personal en los archivos que ellos generan. Por ejemplo, Microsoft Word guarda el registro de quién es la persona que ha escrito o modificado los archivos

La información empotrada fue usada originalmente como un medio de proteger los derechos del autor de los programas. La información que tenga un valor comercial puede igualmente contener una información empotrada, o una marca de agua digital que es producida para identificar quien utiliza o produce los datos, y por lo tanto, si los derechos de propiedad han sido burlados. La información empotrada también provee un medio de identificación individual, guardando información acerca de sus preferencias, e incluso monitoreando la utilización de un servicio.

Las marcas de agua digitales y la información empotrada es un tema importante en relación a la libertad de conciencia y de expresión. Ellos pueden amenazar nuestro derecho humano básico a entablar un diálogo, informar hechos o realizar denuncias en forma anónima. Tanto las computadoras como los programas se están volviendo cada vez más complejos, y sobra la perspectiva de mayor interacción y control de su uso, se erosionan todas las posibilidades de anonimato que deberíamos tener.

Otro proceso refinado de información empotrada es la registración "online" de los programas, cuando el proceso de registro lo realizan y controlan los programas que genera el mismo fabricante del producto a registrar. Estos programas pueden pasar información sobre su computadora y los programas y los datos contenidos en ella.

Por ejemplo, la registración en línea del sistema operativo basado en Windows 95 deriva en el envío de información a los sistemas de Microsoft. El último sistema de Microsoft, el Windows XP, avanza un paso más en este tipo de procesos: requiere que se registre en

## 6 - USANDO INTERNET en forma SEGURA

línea, y lo obliga a divulgar información sobre su sistema, de forma que genera luego un código de activación para que pueda usar el programa en su computadora. Si efectúa cualquier cambio significativo en sus sistemas, inmediatamente el sistema operará con fallas, ya que está asociado a los datos que reveló originalmente y que incluyen características únicas de su hardware.

Deberá registrarse nuevamente, enviando un nuevo resumen sobre la nueva información de su sistema a Microsoft. Dado que asigna a cada computadora una identidad única, Windows XP puede también crear una huella digital que puede ser incluida en los archivos que genere o modifique y que puede ser usada para determinar la localización de la computadora donde fue creada, ya que puede relacionarse inicialmente con el dueño de la licencia obtenida en línea..

Registrado o no, los programas pueden ser usados por los fabricantes del sistema, para introducirse, en forma total o parcial, en su computadora cuando efectúa una conexión internet. Algunos programas hacen esto como un medio de controlar las actualizaciones o nuevas ofertas. Pero esto significa que del mismo modo, el programa podría pasar cualquier otra información sobre el uso de su computadora y del programa (e incluso de otros programas).

Provocar que una computadora genere procesos sin la autorización de su dueño o su usuario, es un crimen en muchos países. Pero debe recordar que, en la mayoría de los programas, usted debe activar su instalación aceptando los términos de una licencia y en muchos casos, está aceptando que esos mismos programas envíen (vía internet o de cualquier otra forma) determinada información a sus fabricantes o productores.

El mayor riesgo que genera una identificación empotrada se produce cuando un informe o documento está siendo generado excluyendo deliberadamente cualquier identificación, y el programa, por su propia iniciativa, incluye la información de autor, según su licencia, dentro de él. Muchos procesadores de texto insertan información sobre la fecha y la hora del momento en que el documento fue producido, y permite al usuario poner el nombre del autor. Pero aunque eventualmente limpie esta información, es posible que los datos de registración del programa, incluido su nombre pueda quedar codificado dentro del archivo.

La forma más simple para eludir cualquier riesgo de que una información sensible quede empotrada en un archivo, es utilizar archivos texto. Y si requiere algún tipo de formateo, debería usar los viejos formatos de archivos que llevan menos información, tales como el Word 6, o utilizar el formato de grabación: RTF (rich text format).

## 7 -Viviendo bajo vigilancia

Este Resumen es el séptimo de la serie “Participando con Seguridad” y trata los temas de:

- \* **Vigilancia y contra vigilancia**
- \* **Manipulando oficial o ilegalmente las comunicaciones telefónicas**
- \* **Controlando los teléfonos móviles y el correo**
- \* **“Sensores”, micrófonos, y vigilancia basada en computadoras.**
- \* **Fotografía y pistas documentales.**
- \* **Recomendaciones para una contra-vigilancia básica**

### Vigilancia y contra-vigilancia.

Vigilancia es el arte de controlar las actividades de personas o grupos sin que ellos tengan conocimiento que están siendo vigilados. La vigilancia ha sido una parte intrínseca de la historia humana. Sun Tzu, en “The Art of the war”, escrito hace 2500 años atrás, discute como los espías deben ser utilizados contra personas enemigas. Pero la moderna electrónica y la tecnología de las computadoras han dado a la vigilancia un medio de operación realmente nuevo. No solamente puede ser utilizado por agentes, sino que también puede ser automatizado mediante el uso de computadoras. Ya no tienen que hacer mucho trabajo para que las personas sean monitoreadas, ya que sus propias actividades normales crean registros que describen sus actividades.

Contra-vigilancia es la práctica de eludir o hacer que la vigilancia sea más difícil. Con anterioridad a las redes de computadoras, la contra vigilancia involucraba agentes elusivos y comunicaciones secretas. Con el reciente desarrollo de internet y las bases de datos computarizadas la contra vigilancia ha crecido. En la actualidad la contra vigilancia incluye todo lo que va desde el conocer como realmente se borra un archivo en una computadora hasta evitar convertirse en blanco de las acciones directas de las agencias.

El gran impacto que tiene la vigilancia es el número de organizaciones involucradas en su operación:

*El Estado y los servicios de seguridad todavía tienen los sistemas de vigilancia más poderosos, porque ellos están habilitados por ley y manejan recursos suficientes. Hoy día los niveles de la vigilancia del estado han crecido y utilizando computadoras ahora están habilitados para reunir muchas fuentes de información para producir perfiles de personas o grupos en la sociedad.*

*Muchas corporaciones importantes utilizan en la actualidad varias formas de vigilancia pasiva. Esto es, primariamente, un medio de controlar las actividades de los directivos y controlar las relaciones públicas. Pero algunas corporaciones importantes realizan varias formas de vigilancia activa para controlar las actividades de activistas y grupos de campañas que pueden impactar en sus operaciones.*

*Muchas compañías comercian información dentro de la ley, comprándola o adquiriéndola de otras compañías o de agencias locales del gobierno que la recolectan. Estos datos son usualmente adquiridos por compañías que desean utilizarlos para propósitos publicitarios o de marketing. Y también se da el caso inverso: que agencias del gobierno adquieren, en forma lícita o no, grandes bancos de datos, oficiales y privados, a los fines de aumentar la vigilancia de la sociedad en su conjunto mediante el cruzamiento de datos y la elaboración de*

## 7 -Viviendo bajo vigilancia

*perfiles de personas y grupos.*

*Información relativa a personas es obtenida por muchos pequeños grupos o individuos. Algunos de ellos la buscan con el propósito de hacer daño, pero la información personal más sensible esta siendo obtenida para propósitos criminales, tales como los relacionados con el uso ilegal de las tarjetas de crédito o para otro tipo de fraudes.*

Por todo ello, para aquellos que están trabajando pacíficamente para cambiar la sociedad, el tema de la vigilancia representa un problema. Particularmente con posterioridad a los hechos acaecidos en Nueva York el 11 de setiembre del 2001, muchos estados consideran la política de disenso como un problema, y han introducido nuevas leyes para fortalecer sus poderes de vigilancia. Muchos estados también han redefinido su definición legal de terrorismo no solo para incluir los actos violentos, sino también a las acciones directas de protesta. Aun cuando hay grupos que no tiene vínculos con la violencia, estados y corporaciones pueden tratar de usar la información obtenida sobre grupos o personas para desacreditar su labor.

Así como el alcance de la vigilancia crece, es importante que los grupos e individuos manejen su exposición a los diferentes tipos de vigilancia para limitar el daño que esta pueda causarles tanto a ellos como a su labor.

Los métodos modernos de vigilancia no pueden ser totalmente eludidos. Si el estado utiliza todos sus recursos para investigar sus actividades, él está habilitado para hacerlo, tiene los recursos económicos y técnicos para lograrlo. Mientras tanto, organizaciones no-estatales (o para-estatales) pueden emplear técnicas de vigilancia contra su organización, y algunas precauciones pueden reducir sus posibilidades de éxito.

Este resumen explora los medios por los cuales el impacto de la vigilancia puede ser disminuido. Este resumen está desarrollado con la finalidad de establecer una base de discusión, y no es un manual completo de contra-vigilancia.

Nota: en todas las formas de vigilancia mencionadas mas arriba, la búsqueda de definición de “patrones de comportamiento”o “patrones de conducta” es uno de los núcleos del trabajo de vigilancia. Buscan “predecir” acciones, comportamientos. Si analizamos una pieza de comunicación (un mensaje, una grabación, una actividad) en forma aislada no nos genera mucha información adicional fuera de lo directamente expresado por ella e incluso pueden parecer un conjunto inútil de datos. Pero, si podemos reunir un conjunto de piezas, un lote amplio de información de diverso formato y origen, podremos componer un cierto patrón de temas y comportamientos, relaciones y modelos de trabajo, contacto y hábitos personales / grupales, que es lo que buscan realmente los sistemas de vigilancia. La magnitud de los datos que hay que procesar para lograr este objetivo es muy grande, y actualmente se logra fácilmente con el uso de computadoras trabajando con grandes bancos de datos de muy diverso origen y forma.

### Teléfonos

#### ***La intervención oficial de las líneas telefónicas.***

Los contratos o licencias por los cuales el estado controla las compañías de teléfonos incluyen cláusulas que especifican que deben proveer acceso al control de las líneas

## 7 -Viviendo bajo vigilancia

---

para los servicios de seguridad, de investigación judicial o de la policía.

Cuando las conexiones telefónicas eran mecánicas las escuchas debían ser instaladas por técnicos, ligando circuitos para seguir la señal de audio de llamada. Ahora dado que muchas conexiones están siendo convertidos a nuevas tecnologías digitales la instalación de escuchas es muy simple, y puede ser hecha instalando pequeños conectores, o eventualmente por computadora. Los servicios telefónicos provistos por compañías de TV cable son intervenidos de manera similar.

A menos que la intervención este muy mal realizada, no es posible que detecte si su línea esta siendo o no intervenida. Los ruidos que hacen creer a algunas personas que su teléfono ha sido intervenidos son realmente ruidos creados por la inducción de señales de otras líneas telefónicas. Porque la intervención es hecha al momento de la conexión, es muy difícil decir si una línea esta intervenida porque no se notara una diferencia apreciable de volumen. Pero independientemente de la intervención del contenido, la comunicación de los datos puede ser siempre recolectada automáticamente, y guardados para un uso posterior por departamento de facturación de su compañía telefónica o por los servicios de seguridad.

Para los servicios telefónicos que procesan sus conexiones en forma digital, la información generada puede consistir de una lista de los números telefónicos a los que usted ha llamado, la duración de tales llamados, y también un registro del tipo de medios de comunicación que han sido utilizados (algunos servicios envían datos y voz comunicándolos por diferentes rutas para conservar ancho de banda).

### La intervención no oficial de las líneas telefónicas

También es posible que las conversaciones pueda ser intervenidas no oficialmente. Hay una variedad de maneras técnicas posibles para controlar conversaciones telefónicas:

**\*Grabando las conversaciones** – tanto la persona que hace o la que recibe el llamado graba la conversación utilizando un adaptador asociado al micrófono o al auricular telefónico, o conectando directamente la línea intervenida a un grabador de audio. Ambos elementos pueden ser fácilmente adquiridos en proveedores de artículos electrónicos o de telefonía. La mayoría de las personas que registran conversaciones telefónicas, como los periodistas, los utilizan para su propio trabajo privado. Debe tener cuidado en cualquier cosa que diga en forma telefónica a otros, porque nunca sabrá si lo están grabando y si luego pueden utilizar esas grabaciones para otros propósitos diferentes a los originales.

**\* Interviniendo por una línea directa.** Esto es lo que el estado realiza vía las conexiones telefónicas normalmente en las mismas Centrales telefónicas que manejan las compañías de comunicaciones. Pero se puede efectuar una intervención no oficial, cuando la línea es intervenida físicamente cerca de su domicilio. La intervención puede realizarse tanto por medio de una conexión eléctrica directa sobre la línea, o por medio de una bobina magnética colocada alrededor de la línea para captar la señal por inducción. Esto puede disminuir el nivel de la señal porque hay una pérdida de energía en la línea, y también puede generar ruido en la misma línea. Las intervenciones directas sobre la línea requieren un mantenimiento regular, o por recambio de las cintas grabadas o reemplazando las baterías, lo cual puede ayudar a señalar su actividad.

## 7 -Viviendo bajo vigilancia

\* **Intervención por radio** – esto es como un “bug” (qué es un bug?), el cual es apto para trabajar sobre líneas telefónicas. El estado no lo utiliza normalmente porque tiene un acceso directo vía las conexiones en las centrales. Puede estar propiamente en un micrófono dentro de la casa, o afuera, sobre la línea telefónica. Esto puede producir ruido (puede eventualmente detectar la señal de retorno desde un equipo hecho por un aficionado) para alertarlo, pero es probable que no detecte nada anormal. Si la unidad es alimentada desde la línea una vez que está instalada está libre de mantenimiento, y solamente transmite cuando existen llamadas en progreso. Mientras tanto sus equipos tienden a perder potencia por que el consumo sobre la línea llega a ser bastante grande. Además el receptor debe estar instalado a unos pocos cientos de metros del transmisor. Las intervenciones vía radio, pueden ser detectadas de la misma manera que las intervenciones comunes, chequeando regularmente su línea.

*Para cuidarse contra intervenciones no oficiales de su línea, deberá saber por donde corren sus líneas telefónicas, y quizás inspeccionarlas regularmente para verificar que no haya nuevas uniones o empalmes, dispositivos o pequeños cables conectados a la línea.*

*Nota: “Bug” término que en traducción literal significaría “bicho” en este caso se aplica a pequeños dispositivos, de tipo electrónico, que permiten realizar diferentes tareas: monitorear audio, video, y cualquier otro tipo de señal pasible de ser captada. Normalmente estos dispositivos emiten en frecuencias de radio la información que registran.*

### Datos de localización y teléfonos móviles

El uso de teléfonos móviles genera, en términos de vigilancia, un mayor compromiso. Este compromiso se incrementó cuando fue introducida la tercera generación de teléfonos móviles, ya que las celdas (las estaciones con antenas de comunicación) están más cerca una de otra.

en el caso de los teléfonos móviles, la mayor amenaza es la captación de los datos comunicados. Los datos no incluyen solamente información sobre la hora y la duración de los llamados, sino también la localización geográfica de las celdas desde la cual la llamada fue hecha, además de por quién y para quién. Junto con los datos habituales de cualquier llamado telefónico, también es guardado el dato de la localización de la (o las) celda(s) que se han usado para dicho llamado.

Se puede obtener una mayor precisión en la localización del móvil, combinando información de varias celdas alrededor de la posición de la persona, pero esta precisión adicional no es una operación ordinaria y debe ser habilitada especialmente por la compañía telefónica. No hay posibilidad de realizar contra-medidas para evitar que esto lo realice el estado y las compañías telefónicas. Toda transmisión electromagnética puede localizarse por medio de dos o más estaciones de escucha.

La vieja primera generación de teléfonos móviles podían ser fácilmente monitoreada por cualquiera que barriera (explorara) con un receptor toda la banda de los móviles, porque utilizaba un sistema de transmisión analógico – como un ordinario transmisor de radio. La segunda generación de teléfonos digitales era (es) más difícil de controlar porque utiliza

## 7 -Viviendo bajo vigilancia

un sistema de transmisión con compresión digital. Recuerde que el estado siempre puede controlar los teléfonos móviles con la cooperación de las compañías telefónicas. También es posible que algunas organizaciones, con los equipos técnicos adecuados, (al alcance de grupos poderosos y grandes corporaciones), puedan controlar las comunicaciones de los teléfonos móviles y descifrar sus mensajes.

Existen varias propuestas para utilizar un sistema de encriptado fuerte para los teléfonos móviles europeos, pero existe oposición de varios de los estados europeos.

Muchos teléfonos móviles pueden ser utilizados anónimamente, pero es muy costoso hacerlo. Los Teléfonos móviles con sistemas pre-pagos pueden ser adquiridos sin necesidad de dar detalles de su nombre y dirección, y como simplemente carga datos de tarjetas para usarlos, no tienen una información facturable que brinden datos para su localización. (Sigue vigente el concepto del párrafo anterior respecto a la localización de la celda desde donde llama o recibe llamados)

Sin embargo, una vez que ha sido identificado como utilizando un cierto equipo telefónico, puede ser rastreado como cualquier otro. De manera que si requiere permanecer en el anonimato durante cierto tiempo, tendrá la necesidad de cambiar el teléfono en cortos periodos de tiempo.

### Servicios Postales

Como muchas personas utilizan faxes y correo electrónico, la importancia del sistema postal esta decreciendo (esto no es aplicable a todos los países, si bien es cierto respecto a las comunicaciones internacionales, no es tan así en las locales, y menos aún respecto al despacho de encomiendas). Aun así, la interceptación del correo es muy importante para los servicios de seguridad.

No hay una manera fácil de saber si su correo esta siendo leído. Las maquinas utilizadas para procesar, clasificar y sellar las cartas a menudo lesionan su aspecto exterior de alguna manera, de forma que los daños ocasionados que puede ver en su exterior, no son un indicador cierto de que su correo esté siendo leído.

Una contra-medida simple para evitar que su correo sea abierto es poner una cinta adhesiva a lo largo de cada borde y las costuras del sobre, y luego firmar la cinta con un marcador indeleble. Esto previene la mayoría de las manipulaciones que pueden realizar los expertos.

Hay personas que envían discos flexibles vía postal. Hoy estos archivos pueden enviarse fácilmente vía correo electrónico. Sin embargo, es muy común el envío de discos tipo CD por correo postal, dado que permiten transferir un volumen muy grande de información (comparado con un disco flexible o un correo electrónico). Para asegurar que tales datos no sean abiertos y leídos por cualquiera, aunque fueran entregados erróneamente, debería encriptar los datos y recién luego grabarlos en un CD-R.

Recuerde que siempre puede identificar el número de serie del disco como otra forma de comprobación de que no haya sido reemplazado el disco original o mejor aún, utilizar una firma digital en su contenido, si no desea usar la encriptación total de los datos.

## 7 -Viviendo bajo vigilancia

### Dispositivos de vigilancia – “bugs”

Los dispositivos de vigilancia o “bugs” no son realmente medios de comunicación, pero son unidades que hacen uso de canales de comunicación. El concepto de un “bug” usualmente involucra un radio transmisor, pero hay muchas otras opciones para emitir una señal; puede enviar radio frecuencia a través de un cable de energía maestro de un edificio y tomar los datos afuera; puede interceptar la transmisión de un teléfono sin cables, y puede obtener los datos desde una red inalámbrica (“wireless networks”) de computadoras pobremente configurada, o sintonizar las emisiones de radio de un monitor de computadora.

Estos dispositivos (los “bugs” ) vienen en todos los tamaños y medidas. El propósito real inicial de los bugs era relevar sonido. Hoy la miniaturización de la electrónica ha progresado tanto que las imágenes de la televisión puedan ser captadas vía “bugs” que permiten la incorporación de vídeo cámaras en miniatura. (algunas de ellas se han hecho populares durante la cobertura de eventos deportivos, o en programas de investigación periodística, etc.)

Otros dispositivos utilizan bandas de radio VHF. Los más modernos, gracias a los desarrollos en electrónica utilizados para la telefonía móvil, trabajan en UHF o en bandas de microondas. La utilización de tecnología digital en lugar de la analógica, significa que los más recientes dispositivos de escucha pueden encriptar la señal, y cambiar la frecuencia de operación utilizando un falso modelo al azar para hacer más difícil su sintonización.

Nota: Este tipo de transmisiones, desarrolladas inicialmente para aplicaciones militares, utiliza el concepto de que los equipos usan frecuencias de transmisión y recepción variables segundo a segundo (a modo de ejemplo), de forma que si uno “escucha” una sola frecuencia, no detectaría mas que un pulso de datos cada “x” tiempo, imposible de usar para localizar el equipo y menos aún para conocer el contenido de lo transmitido. La secuencia de cambio de frecuencia se ajusta entre los equipos que se comunican entre sí y se supone que siguen un patrón único, no detectable por terceros. Estas técnicas permiten también compartir una banda estrecha entre varias estaciones ya que difícilmente se superponen dos señales en la misma frecuencia al mismo tiempo. Por eso mismo son muy difíciles de detectar sin tener equipos de rastreo o de contramedidas electrónicas, fuera del alcance de la mayoría, aunque disponibles para los estados (y los grandes grupos y corporaciones). Recuerde además que actualmente todas las empresas de equipamiento de este tipo están siendo obligadas (al menos en USA) a ofrecer formas de acceder al control de los equipos y los datos que transfieren..

El rango de estos dispositivos varía desde unos pocos cientos de metros a unos pocos kilómetros. Algunos de los estados utilizan dispositivos conectados a sistemas satelitales. Hay además un crecimiento del mercado comercial de dispositivos de vigilancia para conectar audio y circuitos cerrados de TV (CCTV) mayormente para la observación y control de la gente en sus lugares de trabajo. Oficialmente una muy pequeña parte de estos equipos es utilizada para espiar las actividades de grupos de presión (derechos humanos, medio ambiente, entre otros, o simples opositores políticos), pero el riesgo está presente.

Los dispositivos confeccionados por aficionados tienen usualmente el tamaño de un paquete de cigarrillos. Los dispositivos profesionales pueden caber dentro de lapiceras, calculadoras y otras cosas de uso común. Algunos son solamente del tamaño de pequeños botones – pero el poder y la vida útil de estos diminutos dispositivos, es muy corta. El

## 7 -Viviendo bajo vigilancia

problema principal es la fuente de energía para alimentar su funcionamiento. En la medida que se consiguen baterías de mayor capacidad y más pequeñas, el alcance y la autonomía de funcionamiento, aumenta. Si logran conectarlo a una fuente externa de energía, su funcionamiento es casi ilimitado.

Los dispositivos que puede adquirir sin tener un financiamiento adecuado a la compra de equipos profesionales (muy costosos) son muy básicos. Estas unidades pueden ser compradas en kits o por medio de revistas electrónicas, y los diseños para construirlos están disponibles en Internet. Tienden a operar alrededor de la banda de frecuencias VHF. Son dispositivos de gran volumen porque usan componentes electrónicos standards y baterías convencionales como fuente de energía.

Sin embargo, un dispositivo aficionado bien construido, puede ser tan efectivo como uno profesional para realizar una actividad de vigilancia.

Otro gran problema con la nueva tecnología es el desarrollo de equipos para aplicaciones inalámbricas. Para ser inalámbrico un equipo debe transmitir información, ya sea por ondas de radio o por luz infrarroja y esto potencialmente hace que la información transmitida por estas vías pueda ser accesible (e interceptada) por otros que no son los destinatarios originales. Las ondas de radio son la peor opción, pero también las señales infrarrojas pueden ser captadas a través de una ventana. Algunos equipos inalámbricos, como las redes de computadoras inalámbricas ("wireless networking"), encriptan sus transmisiones, pero la forma normal de encriptación es muy débil.

*Los dispositivos inalámbricos, pueden ser desde teclados, mouse, impresoras, tarjetas o placas de red, teléfonos inalámbricos, etc. y no deberían ser utilizados en cualquier entorno o con equipamiento donde se maneje información sensible o importante.*

Dispositivos que emitan ondas de radio. La contra-medida standard para estos dispositivos es realizar un barrido con receptores adecuados, buscando las emisiones de radio frecuencia. Estos equipos de barrido pueden ser muy costosos, según sea la frecuencia que desea explorar. Existen equipos de barrido con especificaciones técnicas más simples, que se pueden obtener por medio de revistas dedicadas a los aficionados a la electrónica o las comunicaciones, y también los puede encontrar en diseños publicados en internet.

Aún la búsqueda de señales de radio no nos dan plena seguridad. Los dispositivos avanzados pueden ser operados remotamente, admitiendo que se enciendan o apaguen a distancia, así como modificar sus patrones de cambios de frecuencia de trabajo con la finalidad de dificultar aún más su localización. Puede tratar de interceptar sus emisiones, pero puede no detectarlo porque cuando está efectuando un barrido de exploración y búsqueda, el dispositivo puede haber sido apagado.

Un problema más serio son aquellos dispositivos que no emiten señales de radio, y son muy difíciles de detectar. Los "bugs" son una solución técnica a un problema – escuchar (eventualmente, filmar) en forma remota las conversaciones de la gente.

Una opción más simple es usar una grabadora de cinta (o memoria digital) para grabar la conversación. Existen varias opciones para esto:

## 7 -Viviendo bajo vigilancia

\* **Grabadoras de bolsillo**, ambos como “gusano” o llevado en un equipaje, ligado a un pequeño micrófono de los que usualmente se montan en la superficie de un equipo de audio. Las grabadoras digitales, tales como los minidiscos o como las últimas palm camcorders, también proporcionan una gran calidad de grabación en unidades muy pequeñas.

\* **Grandes equipos de grabación** escondidos en un cuarto, por ejemplo suspendidos arriba de los techos. Esto es muy común en los lugares de trabajo para la supervisión de los jefes.

\* **Micrófono ultra direccional** Estos son como los micrófonos que ve sobre las cámaras de video portátil (camcorders), o los utilizados por los técnicos de sonido. Están contruidos para recibir señales desde una sola dirección. Los micrófonos direccionales de mejor calidad pueden captar conversaciones a distancias mayores a cien metros .

\* **Micrófonos laser**. Estos son equipos sumamente costosos y requiere una mayor técnica para operarlos. Hace rebotar un rayo laser en una ventana, o sobre algún objeto cercano a la conversación que desea escuchar para que resuene (por ejemplo, sobre una pintura o una pared). Cualquier objeto que pueda resonar o vibrar responderá a la presión de las ondas creadas por los ruidos o sonidos presentes en el cuarto. La electrónica asociada al laser detecta la minúscula diferencia en las distancias recorridas por la luz para capturar estas resonancias, y reproducir los sonidos que generan tales resonancias. Su alcance es significativamente mayor que el anterior.

Si un micrófono esta escondido en un cuarto es también casi imposible de detectar. Esto es porque no emite señales de radio. Equipos muy sensibles podrían ser utilizados para buscar campos magnéticos (de los microfonos, si fueran magnéticos) o ruidos procedentes del equipo de grabación. Es posible hacerlo porque la tecnología digital aplicada en los grabadores de cinta emite un ruido eléctrico muy característico. Pero si el lugar que va a ser monitoreado tiene un conjunto de computadoras, fotocopiadoras y otros equipos instalados, haría que la búsqueda sea muy difícil. Viejos equipos analógicos son difíciles de detectar.

### Vigilancia basada en computadoras

Cualquiera puede venir solo y acceder o remover su computadora y llevarse su información. Pero si alguien es capaz de instalar un software en su sistema, podría convertir a su computadora en un equipo de vigilancia al servicio de sus intereses.

La introducción de software en una computadora puede hacerse de tres maneras:

\* Puede obtener acceso a la computadora directamente – esto requiere que usted cargue un CD o un disco flexible en la computadora y transfiera el programa o los programas. Es posible si alguna persona utiliza su computadora para propósitos inocuos, o el o ellos ganan acceso mientras se encuentra ausente.

\* Puede recibir un virus informático, en forma de mensaje de correo electrónico o de un archivo infectado, los cuales pueden instalar un programa en su computadora. Esto permitiría a los “hackers” conseguir acceso a su computadora, o enviar información, tal como sus llaves de encriptación, a los servicios de seguridad (un

## 7 -Viviendo bajo vigilancia

proyecto del FBI está actualmente en curso y pretende realizar la distribución premeditada de una “especie de virus” que una vez introducido en su computadora, remita datos hacia sus sistemas de información).

\* Su computadora puede ser intervenida cuando está en línea, y más que dañarla, el hacker puede instalar un software sobre el sistema que lo habilita a ejercer su control, guardando información sobre él mismo, o leyendo sus archivos privados. Esto es un mayor problema para los servidores en internet, pero las computadoras que están permanentemente conectadas (o incluso conectadas eventualmente) con sistemas como los de “banda ancha” son susceptibles de este tipo de intrusión

La forma más simple de acceder puede ser a través de un nuevo y al mismo tiempo novedoso virus informático. Esto es posible porque inicialmente no puede ser reconocido por el software de detección de virus. Este también podría utilizar las aplicaciones que tiene instaladas en su sistema para compilar un resumen de la información y el uso de su computadora, y enviarla de nuevo a su base. Es posible también el acceso a su sistema durante su conexión en línea aunque puede ser dificultoso de iniciar porque a menos que tenga una conexión en línea continua todo el tiempo, él o ellos no podrían precisar cuando estará conectado a Internet.

*Para proteger contra el acceso de otras personas a su computadora desde internet, y proteger también contra robo de programas sobre su computadora, usted debería utilizar un “firewall” una barrera de protección respecto de su red local o de internet(Ver resumen 6 sobre Firewalls). Esta levantara una señal de advertencia toda vez que una tentativa de acceso no autorizado tenga lugar. Pero cuidado con el Firewall de Microsoft – este solamente trabaja sobre conexiones ingresando en su computadora, de manera que los programas robados pueden ser todavía llevados afuera.*

El acceso a su computadora es quizás el próximo paso más probable. Esto es una posibilidad real, y deberá asumir que existen personas ocupadas en este tipo de vigilancia, porque la técnica de superar las barreras requiere profesionales. Probablemente ellos también tendrán la capacidad para conseguir acceder a su casa o lugar de trabajo. Deberá en consecuencia tomar todas las medidas necesarias y posibles para limitar el acceso a sus sistemas.

El resumen sobre “Introducción a la seguridad de la Información” describe como proteger su información. Quizá una de las maneras más efectivas de prevenir el acceso de oportunistas, independientemente de la utilización de una palabra clave para la iniciación de la computadora, es la utilización de un salvador de pantalla y la utilización de una password de protección. Esta es una forma simple de prevenir un acceso eventual mientras está lejos de su computadora (aunque con estas medidas no detiene a ningún profesional).

Las redes de computadoras son otro problema de vigilancia. Las redes operan enviando paquetes de datos entre varias computadoras conectadas entre sí, pero solamente la computadora compara la dirección del paquete a procesar con la del paquete de datos. Utilizando programas denominados “**packet sniffers**” (literalmente: husmeadores de paquetes) es posible leer todos los paquetes que cruzan un sector de la red. Utilizando estos programas es posible para una computadora del sistema interceptar todos los datos o transacciones que se están transfiriendo por el sistema, o para uno solo de los equipos conectados. Nuevamente, esto puede ser realizado mediante la utilización de un software

## 7 -Viviendo bajo vigilancia

instalado en el sistema sin el conocimiento del operador de la red o la computadora. El problema puede llegar a ser la extracción de un gran volumen de información, que este análisis de paquetes puede llegar a generar. Pero en pequeños períodos de tiempo, los “paquetes registrados” pueden revelar mucha clase de información.

Una de las formas de vigilancia menos conocida tiene el nombre de “Tempest”. Los monitores de las computadoras y algunos otros equipos digitales, emiten ondas de radio por el uso de poderosas bobinas y los transistores de potencia utilizados para crear y manejar las imágenes de vídeo. Este tipo de emisión puede ser utilizado por las compañías de TV por Cable para detectar si alguno de sus programas está siendo visto en un televisor ordinario sin que la respectiva licencia haya sido pagada. Usando una mejor tecnología, la imagen sobre el monitor de la computadora puede ser capturada y exhibida a distancia al momento que ocurre.

*Una solución para los problemas del sistema usado por “Tempest” es la utilización de pantallas de baja emisión, tales como las de una computadora tipo notebook o pantallas planas de matriz activa, etc. Pero es posible que tales pantallas (“o display”) puedan también emitir señales que puedan detectarse y reproducir las imágenes de la pantalla en otro lugar. La única manera correcta de encarar la solución frente al espionaje usando “Tempest” es blindar el monitor, lo cual no es fácil de hacer, o mejor dicho, adquirir un costoso monitor blindado o blindarlo con metales especiales.*

Finalmente, las computadoras pueden ser intervenidas físicamente. Por ejemplo, es posible colocar un dispositivo en su teclado de manera tal que transmita los códigos de las teclas presionadas – y de esta forma es fácil descubrir las contraseñas utilizadas para iniciar su computadora, como también las palabras de paso para acceder a internet, correo electrónico y las llaves de encriptado. De esta forma, cualquier dato que pase por su teclado puede ser captado por otro sistema fuera de su control.

### Fotografía

La fotografía esta siendo cada vez más valorizada como un medio de vigilancia. En años recientes ha tenido una significativa expansión en el desarrollo de la fotografía digital, y video fotografía, y así se ha visto en numerosas presentaciones públicas en muchos países. Al mismo tiempo ha habido avances en la tecnología referida a los circuitos cerrados de televisión (CCTV) y al procesamiento de imágenes computarizadas que permite comparar imágenes tomadas desde cámaras con imágenes almacenadas previamente en bases de datos.

Las fotografías han sido largamente coleccionadas como forma de evidencia. Tal como las protestas y la desobediencia civil están ocurriendo actualmente, hay una gran probabilidad de que los gobiernos y las corporaciones utilicen las imágenes recogidas no solo como evidencias para generar persecución, sino también como fuente de información. Las recopilación de fotografías y videos tienen también otra importante función: asustar a la gente.

Los circuitos cerrados de televisión (CCTV) donde las imágenes son vistas o grabadas, pero no transmitidas – fueron inicialmente desarrolladas como un medio de seguridad para los bancos. Hoy tiene un desarrollo tal que es una forma simple y bastante económica

## 7 -Viviendo bajo vigilancia

para utilizarla en los sistemas de seguridad de los hogares, para la vigilancia de todos los días.

Los cables tendidos de redes de CCTV utilizados por la policía y gobiernos han sido desarrollados los últimos 10 años. En el Reino Unido, pueblos y ciudades a través de todos los países han instalado una gran cantidad de cámaras conectadas con las autoridades policiales. La justificación del crecimiento de redes de CCTV en las ciudades es la de detener el crimen, aunque por ahora existe una clara evidencia que la red de CCTV reduzca la criminalidad. El reciente crecimiento de la red de CCTV en áreas pobladas también provoca serias discusiones sobre la cuestión de cómo la CCTV está siendo utilizada como medio de control social y no como un simple disuasivo del crimen.

Las primeras cámaras CCTV utilizadas en espacios públicos fueron en blanco y negro y de muy mala definición. Las modernas cámaras CCTV tienen una alta definición a color las cuales no solamente están focalizadas para resolver un minúsculo detalle, sino que también se conectan a una computadora desde donde se puede tener el control de la cámara (o de varias en simultáneo), y que permite perseguir los objetos semi automáticamente. Por ejemplo, pueden perseguir el movimiento a través de una escena aún cuando no se mueva, o también pueden enfocar un objeto simple en un ambiente muy ocupado, y seguirlo por donde vaya. Estando computarizado, el proceso del seguimiento puede ser realizado a través del control del trabajo de varias cámaras.

Corrientemente, en algunas áreas del Reino Unido, como Londres, redes de CCTV están siendo combinadas con sistemas de imágenes computarizadas para el seguimiento de los números de placas de los automóviles. Esto está siendo desarrollado en parte como una medida de seguridad, y/o como un medio de identificar los automóviles que han sido robados. Pero esta no es la razón principal, porque una red de cámaras de esas características puede ser utilizada para el seguimiento del movimiento de los individuos. El propósito del "road tolling system" para Londres está también relacionado con la lectura de los números de las placas de los automóviles para generar información facturable, además de producir una potencial fuente de información que permita la localización de personas y grupos.

Quizás la más perturbadora extensión de esta tecnología es el reconocimiento de caras a través de imágenes de alta definición obtenidas por cámaras CCTV. Con estas tecnologías, será posible determinar la identidad de una persona sin la necesidad de detenerla y hacerle preguntas en la calle, o aun alertarle que su identidad está siendo controlada y registrada. Los sistemas pueden controlar muchos miles de caras en una base de datos en menos de un segundo.

Los últimos desarrollos en CCTV y en las técnicas de procesamiento de imágenes, que se han desarrollado en Inglaterra y en EEUU, son sistemas de monitoreo computarizado que funcionan de tal manera que el operador de CCTV no tiene que mirar continuamente todas las pantallas. Esto significa igualmente que un operador puede estar controlando muchas más cámaras que antes. Estos sistemas no observan a las personas directamente; en lugar de ello siguen su comportamiento observando diferentes tipos de movimiento, o tipos de vestidos particulares o los equipajes que transportan. En lugares públicos las personas se comportan en un conjunto con patrones de formas predecibles. Las personas que no forman parte de un gentío, por ejemplo en el robo de autos, no se comportan de la misma forma. La computadora puede identificar estos movimientos, y alertar al operador que ellos están actuando fuera de los patrones ordinarios esperados. Potencialmente, si está esperando en una calle muy frecuentada para reunirse con alguien, puede disparar este sistema de alerta.

## 7 -Viviendo bajo vigilancia

El mismo tipo de sistema puede, si se requiere, ir un paso más adelante y seguir a un individuo identificando cómo se mueve a través del área cubierta por la red de CCTV. Este tipo de sistemas está siendo desarrollado en EEUU como parte de un proyecto desarrollado cofinanciado por la US Defense Advanced Research Projects Agency (ARPA). Con diversas herramientas de software, el sistema puede desarrollar modelos en tres dimensiones de un área y puede monitorear el seguimiento de objetos dentro de ella. El desarrollo de la CCTV en áreas públicas, conectada a bases de datos computarizadas de imágenes de personas y su identidad, presenta un serio riesgo para las libertades civiles. Potencialmente no podrá reunirse anónimamente en un lugar público. Tampoco estará habilitado para conducir o caminar anónimamente por la ciudad. Demostraciones y asambleas en lugares públicos pueden verse seriamente afectadas si el estado queda habilitado para recopilar listas de quienes las lideran, toman parte o de quienes conversen con los participantes de la protesta en la calle.

### Documentación de pistas

La sociedad moderna ha creado una gigantesca cantidad de datos. Toda vez que utiliza una terminal bancaria, paga con su tarjeta de crédito, utiliza la tarjeta telefónica o hace un llamado desde su casa, usted marca la hora en un registro electrónico de la transacción. En el pasado esto solía ser conocido como rastro escrito o de papel. Pero hoy muchos de esos registros son electrónicos. Esta información, si es obtenida por el estado, u obtenida por canales no oficiales (clasificando su basura o sobornando a aquellos que están a cargo de la custodia de tal información) puede describir también cómo vive y cómo trabaja.

El alcance de la información que puede ser obtenida desde pistas de papel está creciendo todo el tiempo a medida que nuestras vidas están siendo más monitoreadas. Una vez que muchas fuentes de información son relacionadas y comparadas como parte de un análisis inteligente, se puede producir un profundo estudio sobre sus hábitos, su trabajo y sus hobbies.

La abolición del efectivo, y la introducción de la moneda electrónica puede llegar a ser uno de los grandes golpes a la libertad de expresión y de asociación en tiempos modernos. Así como (algunos de) nosotros nos movemos a través de una sociedad sin efectivo (cash-less-society), todas las transacciones electrónicas pueden ser monitoreadas en mayor medida y en forma más intensiva para prevenir falsificaciones electrónicas. Ellos podrán disponer de detallados registros de todas las transacciones, y de las dos partes involucradas en la transacción. (Por ejemplo: Usted y un comercio) en orden a que cada débito o crédito puede ser controlado para asegurar que no ha ingresado un dinero extra en el sistema. Naturalmente, esto significaría que, a menos que haga trueque afuera del sistema, todas las transacciones pueden ser rastreadas por el estado, y posiblemente por las grandes corporaciones.

Una de las más grandes libertades que tenemos es comprar un libro, un periódico, o donar dinero a una causa y hacerlo en completo anonimato. En una situación donde todas las transacciones son electrónicas, y la información sobre todas ellas deben ser auditadas para prevenir fraudes, el anonimato está perdido.

Sin embargo, el problema primario relacionado con el uso de documentos y datos que se registran, no es el Estado. Comparando como las empresas de marketing y las compañías de relaciones públicas (PR Companies), acumulan datos sobre individuos, los servicios de seguridad pueden considerarse unos principiantes. Hoy una red de información muy completa es recolectada por compañías de marketing con el objetivo de venderle cosas,

## 7 -Viviendo bajo vigilancia

---

o determinar cómo otras compañías están ejecutando sus estrategias de mercado. Muchas personas no participan de esto intencionalmente. Hoy no tiene que llenar un informe para ser asediado con avisos comerciales por correo. Los detalles de un rango completo de transacciones, desde el monto de los créditos acordados, cómo los registros electorales, todos, pueden ser adquiridos por las compañías que se dedican a realizar investigaciones de mercado para proveerse de información sobre los hábitos del público como clientes potenciales.

### Recopilando datos del perfil

Mucha de la información descripta más arriba es general – identifica las tendencias desde una gran cantidad de datos y el rol del individuo es mucho menor. Desde otra perspectiva los sistemas de “datos del perfil” (“Data Profiling”), que realizan procesos donde hay búsquedas para conseguir tanta información sobre usted como sea posible – información personalizada – en orden de ensamblar una semblanza especificada de su vida y sus hábitos.

La búsqueda de datos sobre su persona es muy importante en las operaciones de inteligencia y tiene muchas aplicaciones – desde decidir cuando una persona es vulnerable a ser sobornada, hasta definir, a través del estudio del perfil de sus conducta cuando tiene sospecha, cuando debe ser aprehendido. El Estado tiene poderes para realizar todo esto mediante órdenes para que los bancos, compañías de crédito o su mismo empleador, le suministren todos los datos que acumulan en forma independiente. Pero también las corporaciones y los investigadores privados podrán acumular y relacionar ésta información si logran estar bien conectados. El problema principal es sí el conjunto de su información personal no está muy bien protegido. En general, pequeñas cantidades de información, en forma aislada, no son consideradas sensitivas. Pero una vez que ésta información es reunida y relacionada, ella puede describir acciones en detalle, hábitos y preferencias individuales.

### Identidades

La identidad es un tema importante en relación con las libertades civiles. Hay instancias donde nosotros deseamos ocultar nuestra identidad – para el envío de anónimos – por un extenso rango de motivos. La eliminación de esta posibilidad puede erosionar seriamente nuestras libertades. Y esto es posible a medida que nos movemos hacia el desarrollo de una “identidad electrónica”. Hay dos aspectos a considerar en esto:

:

**\* El desarrollo de un sistema de credenciales – cuando usted lleva una tarjeta o un documento y**

**\* El desarrollo de la biometría – donde usted es reconocido por sus características biológicas únicas.**

El desarrollo de sistemas de identificación está siendo empujado sobre dos frentes:

**\* La industria bancaria** – que desea encontrar una sistema completo de prueba para la verificación de las transacciones financieras tanto como la posesión de tarjetas de plástico o la utilización de la firma.

**\* La imposición de la ley**, que desea una manera de identificar fácilmente a los individuos, aún cuando ellos no estén deseosos de cooperar.

## 7 -Viviendo bajo vigilancia

---

Una de las formas más simples de identificación es la portación de credenciales. Algunos países tienen un sistema de tarjeta (cedula, documento de identidad, etc) para ayudar a su identificación. Otros documentos, como las licencias para conducir, tarjetas de librería, bancos o de crédito son también utilizadas para verificar identidades. El problema con la identificación basada en credenciales es que los individuos deben llevarla encima, para su identificación, de lo contrario serán penados legalmente. El problema es mayor si el sistema implementado en la tarjeta de identificación permite que haya datos que sean leíbles por un dispositivo (tarjetas magnéticas, de código de barras o con chips inteligentes) ya que en este caso origina un documento viajero que puede ser usado para la verificación de transacciones.

Como un medio para combatir el problema de personas que llevan o falsifican credenciales, los investigadores están incrementando sus miradas a la biometría, - midiendo las características físicas y biológicas de cada individuo – como una manera de determinar unívocamente su identidad.

Una de las más viejas formas biométricas son las **huellas digitales**. Cada uno (con excepción de hermanos idénticos) tiene un único modelo de impresiones digitales, y esto está siendo usada por muchos años para identificar sospechosos en los interrogatorios policiales. La impresión del dedo pulgar puede ser reducida a una breve descripción numérica, y tales sistemas están siendo utilizados en las áreas de seguridad de los bancos para verificar la identidad.

Un desarrollo más reciente incluye el proceso de ADN de las impresiones digitales, el cual observa alguna de las marcas principales en el DNA para producir una comparación con los datos almacenados. Por el momento, la comparación que produce es menos segura que las tradicionales huellas digitales porque aquellas identifican personas dentro de una familia y no individuos en sí mismos.

La **firma manual** – primariamente su firma – ha sido utilizada durante muchos años para determinar identidades. Mientras otras características de los individuos también pueden ser utilizadas para controlar la identidad. El análisis de la voz está siendo utilizado como medio para probar la identidad, pero no es conveniente para un uso portátil por los problemas de guardar un rango de voces impresas, además de contar con ambientes sin ruidos ni interferencias a la hora de registrar y comparar los patrones de sonidos.

Quizás los dos sistemas portátiles más viables, porque la identidad puede ser reducido a una serie de datos numéricos más que a una detallada imagen o registro de sonidos, son:

- \* **Reconocimiento del iris.** Algunos bancos están utilizando ahora este método de seguridad. El iris de las personas tiene un único modelo que puede ser descrito con una simple serie de números. Las lectoras del iris comparan el modelo del iris con uno guardado y verifica su igualdad.

- \* **Reconocimiento facial.** La configuración de los rasgos faciales puede ser utilizada para asegurar la identidad de una persona frente a otra. De nuevo, la configuración puede ser reducida a una corta descripción numérica.

Por la combinación de alguna forma de identificación de los rasgos personales, y un sistema de verificación es posible hacer cualquier cosa: desde comprar comida hasta viajar por el extranjero. La importancia de este tema es, cómo esta información es manejada

## 7 -Viviendo bajo vigilancia

en orden de reducir la probabilidad de un seguimiento. Si usted llega a combinar un sistema biométrico particular, con una nueva y elegante tarjeta tecnológica que guarde la descripción, este sistema podría ser inmune al seguimiento (a menos que la transacción produzca un documento electrónico de viaje). Pero si la identificación de las características es guardada en forma centralizada, y un gran conjunto de sistemas tienen acceso a tales descripciones en forma on-line, es posible que puedan hacer otros usos de sus datos, por ejemplo, utilizando las imágenes de alta resolución de las CCTV con bases de datos de identidades faciales en función de identificar personas al azar.

Piense en las implicancias de esto último en su derecho a manifestar disenso en regímenes democráticos y en aquellos que no lo son.

### **Operaciones de Infiltración e Ingeniería Social**

La forma más invasiva de vigilancia es la utilización de operativos de infiltración. Esto toma dos formas:

**\* El uso de las operaciones para infiltrar una organización**

**\* El uso de técnicas de ingeniería social para obtener información.**

En aquellos grupos que tratan asuntos que son directamente contrarios a las políticas de los gobiernos, el tema de la infiltración surge a menudo. También, cuando existen grupos opuestos a grandes corporaciones, y se teme la infiltración de agentes de las esas mismas corporaciones. En estas operaciones, la policía o los servicios de seguridad pueden aplicar presión sobre ciertos miembros de una organización para obtener la información que ellos guardan sobre otros miembros.

El desarrollo de estos operativos es muy costoso (en muy diversos aspectos), y el estado puede obtener la misma información con maneras menos conflictivas de vigilancia. Si estas operaciones son descubiertas, pueden también ser un desastre para las relaciones públicas del gobierno o de la corporación involucrada. Por estos motivos, el uso de operaciones para infiltrar organizaciones no tiene la gran extensión que muchos creen. Pero la infiltración puede ser muy útil para organizaciones que están motivadas para descubrir o monitorear el trabajo de campañas de otros grupos. Esto bien puede ser por motivaciones políticas o económicas. Existen también muchas otras conexiones entre las grandes corporaciones y la policía o los servicios de seguridad, y la comercialización de la información sobre grupos y activistas es parte de esta relación.

No es posible cuidarse contra la infiltración de una organización sin dañar la viabilidad y la eficacia de una organización. Un excesivo cuidado sobre la infiltración dentro de una organización puede producir falta de confianza y una mala relación de trabajo dentro de la organización. Más que otras formas de vigilancia, los operativos profesionales de infiltración dentro de una organización, son difíciles de evitar.

Otro escenario más probable, especialmente cuando está tratando con medios o corporaciones de relaciones públicas, es la ingeniería social. Esto se produce, por ejemplo, cuando alguien lo llama por teléfono, o casualmente le conversa en la calle y trata de hacerle creer que es uno más del conjunto, y que tiene un interés inocuo en usted. Pero su interés real es obtener información específica que él cree que usted pueda poseer.

Deberá desarrollar procedimientos claros para manejar preguntas sobre su trabajo. Por ejemplo, un día atiende un llamado telefónico diciéndole que le gustaría ir a su demostración

## 7 -Viviendo bajo vigilancia

contra la compañía X, para que le diga cuando y donde se hará, o que lo esta llamando de parte de Juan que ha perdido su contraseña para acceder a la computadora, a ver si se la puede facilitar. Deberá estar en guardia para no descubrir información de esta manera.

A menos que usted tenga una extrema buena razón para ello, no debería dar nunca ninguna información relacionada con la seguridad a través de comunicaciones telefónicas, y si es por vía Internet, la debería encriptar.

Los trabajos de ingeniería social son fácilmente identificables ya que efectúan una serie de preguntas para ver si la persona esta en conocimiento de hechos o futuros planes de los cuales no cualquiera debería tener conocimiento.

Los periodistas son un problema particular. Los periodistas que trabajan para un medio de comunicación conocido pueden ser verificados telefoneando al editor de tal organización, pero los freelance o los periodistas independientes deberían ser tratados con cuidado, porque podrían estar trabajando para cualquiera.

### Contra vigilancia personal

La contra-vigilancia esta basada en la planificación de un buen sistema de seguridad.

El resumen sobre "Introducción a la seguridad de la Información (Nro.1) "describe como proteger su información – incluyendo la contra-vigilancia en los lugares de trabajo. La protección de la información es la primera etapa de la contra-vigilancia. Pero la contra vigilancia debe ser también vista como un planteo de balance de objetivos opuestos.

Si es muy bueno restringiendo toda la información, el estado o las corporaciones tendrán problemas para monitorear sus actividades. Pero al mismo tiempo, probablemente también llegará a estar más aislado y reservado en los procedimientos, lo cual producirá un aislamiento respecto del público al que está tratando de conquistar. Asi como los procesos de seguridad de la información, los de contra- vigilancia requieren un esfuerzo para proteger las actividades o la información que es sensitiva, y mientras tanto estará dando menos énfasis a todas aquellas actividades que puedan estar abiertas a todos.

La seguridad de la información esta primariamente basada en la protección de los equipos con procedimientos de seguridad y barreras de protección. La contra vigilancia personal está basada en muchos de los mismos procesos, y deberá proveer seguridad y barreras entorno a hábitat personal. Como humanos, somos criaturas de hábitos. Si nosotros exhibimos hábitos muy predecibles, esto hará que el monitoreo de nuestras actividades resulte más fácil. En ciertas ocasiones nosotros podemos romperlos, aunque esto también puede delatar que estamos haciendo alguna cosa que no forma parte de nuestro trabajo o movimiento diario. Si este hecho es importante, puede relacionarse con un patrón de conducta personal.

La mejor manera de empezar a pensar sobre como eludir la vigilancia es pensar como romper los patrones de comportamiento regular en su vida Sin puede enmascarar su trabajo regular, estará dificultando una vigilancia rutinaria. Y deberá enmascarar también sus actividades especiales, .

Romper los hábitos regulares no significa estar yendo a la cama en diferentes horarios, o trabajar diferentes horas todos los días. Plantea que algunas actividades que desea que no sean objeto de vigilancia queden integradas con los otros eventos de su vida, pero no

## 7 -Viviendo bajo vigilancia

con la profundidad como para que llegue a ser predecible. Si cambia la ruta que usted toma para ir a su trabajo o al comercio sobre bases aleatorias, hará más difícil que sus movimientos puedan ser controlados. Si construye acciones irregulares agregadas a sus actividades que potencialmente involucran vigilancia, les crea “ruido” o distorsión en el modelo de patrón de sus actividades, que enmascaran algún cambio en sus hábitos.

Asegurar la información sobre su computadora deberá ayudar sobre todo a su seguridad. Si tiene una computadora portátil tendrá presente un nuevo y gran problema porque al trasladarla, está moviendo sus sistemas fuera del alcance de sus sistemas de seguridad y barreras físicas de acceso. Por lo tanto, debería tomar cuidados especiales cuando usa computadoras portátiles. (los mismo es aplicable a agendas electrónicas)

- \* El sistema debe ser asegurado con una contraseña desde el BIOS para prevenir el arranque.
- \* Encriptar el disco duro, cuando es posible, para prevenir el acceso a contenidos de dicho disco o su remoción de la maquina.
- \* Deberá asegurarse que su computadora portátil tenga contraseñas diferentes de las que están en uso en su equipo estático.

Asegurar su información es relativamente fácil. Pero el mayor problema es cuando debe considerar la vigilancia personal cuando la transportar a reuniones con gente con la que deba discutir asuntos sensitivos.

No debe buscar eludir la vigilancia por asuntos que no tienen importancia. Asuma naturalmente que el trabajo sensible es sólo una parte mínima de su trabajo. Cuando gran parte de su trabajo diario lo constituyen tareas sensitivas, la mayor dificultad es encontrar la manera de ocultar dichas actividades dentro de los patrones normales de su vida diaria.

Primariamente, cuando esta tratando información sensitiva, debe eludir la generación de alguna clase de documentación o de oportunidades para la vigilancia trabajando sistemáticamente para eludirla.

Cómo la sociedad esta llegando a ser altamente vigilada, cada vez es más difícil hacerlo. Cómo los gobiernos comienzan a utilizar comunicaciones y datos de transacciones en forma crecientemente y una parte significativa de sus esfuerzos son para monitorear las actividades de sus ciudadanos, debe trabajar de una manera que no genere sistemáticamente rastros documentales. Para hacer esto, deberá pensar como implementar las siguientes pautas, integrandolas en todo o en parte a su forma de trabajo:

### Viajes

- \* Si está viajando a una reunión importante tome una ruta diferente para la ida y para la vuelta, y si le es posible no utilice el mismo ómnibus o estación cuando llegue o abandone el destino a donde esté viajando. Esto disminuye la probabilidad de que su destino pueda ser identificado.
- \* Si esta viajando por temas importantes, trate de utilizar el transporte público. Utilizando su auto privado está facilitando el rastreo de su identidad y su seguimiento.

## 7 -Viviendo bajo vigilancia

---

- \* Para eludir los sistemas CCTV en lugares públicos muévase con las corrientes, no corra, no cruce fuera de las esquinas y no esté tratando de localizar las cámaras CCTV.
- \* Si puede coordinar la participación en otros eventos o actividades adicionales a su trabajo principal, puede producir distracción sobre los motivos principales para trasladarse a determinada área de un pueblo o ciudad.
- \* El reconocimiento facial trabaja primariamente sobre la configuración de los rasgos faciales. Para utilizarlo necesitan tener una buena vista de la cara. Caminar mirando con un ligero ángulo hacia la tierra, y utilizando un sombrero con borde, ayuda a burlar el sistema.
- \* Si viaja utilizando el sistema público de transporte, los boletos indefinidos o vagos son preferibles a los de viaje específico, ya que dan más flexibilidad para viajar y son más difíciles de asociar la ruta de viaje con un boleto en particular.
- \* Si está moviéndose en una ciudad, trate de evitar trasladarse a través de las áreas principales de los shopping, o de las áreas generalmente más controladas, como zonas bancarias y lugares de compras y turismo. Todos estos sectores seimpre tienen una mayor cobertura de cámaras CCTV.
- \* Siempre asuma que el transporte público tiene cámaras CCTV instaladas (sea en las unidades que se desplazan como en sus accesos y areas de espera, venta de boletos, etc), así que viajando durante las horas pico podrá enmascarar mejor su presencia.
- \* Para hacer más dificultoso un seguimiento de su persona o su detección en las redes de CCTV, no utilice ropas llamativas, objetos exóticos o mezclas de ambos .
- \* La oscuridad ayuda el anonimato, pero no es una solución completa dado que las ultimas cámaras CCTV pueden ver en la oscuridad.

### Los teléfonos móviles

- \* En caso de duda, apáguelo.
- \* Si esta viajando a una localidad importante, dentro de una área urbana no utilice su teléfono dentro de los dos a cuatro kilómetros de su domicilio. Esto evita la creación de un indicio que puede ser asociarlo a cuál es su ubicación durante ese día.
- \* Si el lugar de destino no es cercano a la ruta que utiliza en sus viajes regulares, apague su teléfono antes de iniciar su jornada.
- \* Si necesita desesperadamente enmascarar su localización, haga que alguna otra persona lleve su teléfono durante todo el día, pero esto será efectivo si toma todas las otras precauciones como para evitar que se generen otros rastros documentales mientras se está moviendo.

## 7 -Viviendo bajo vigilancia

---

\* Recuerde que un teléfono celular puede convertirse, naturalmente, en un excelente micrófono operado a distancia. Si está en reuniones importantes, o tratando temas sensibles, quítele la batería. Pueden encenderlo a distancia.

### Pagos

\* Si está viajando a un lugar sensible, no efectúe pagos con la tarjeta de crédito ni retire dinero de los cajeros automáticos.

\* Si necesita gastar dinero en efectivo cuando está viajando o trabajando en un lugar sensible, no gaste los billetes tomados de los cajeros automáticos (su secuencia numérica puede estar registrada). Guarde los billetes recibidos en cambio en cualquier lugar y haga uso de ellos.

\* Si necesita comprar alguna cosa cuando está viajando o trabajando en una localización sensible, no realice ninguna transacción con dinero electrónico, ni transferencias bancarias a sucursales de dicho lugar ya que ellas podrían ser rastreadas.

### Comunicaciones

\* Si necesita efectuar un llamado telefónico sensible que no quiera que esté directamente asociado con usted, hágalo desde un teléfono público. Igualmente deberá tener en cuenta, que si está relacionado con la persona que está al otro lado de la línea, y el contenido de sus llamados (sobre todo los datos de tráfico) está siendo monitoreado, su localización en esa fecha determinada, puede ser descubierta.

\* Si está usando cabinas telefónicas, trate de usarlas en forma aleatoria a través de un área extensa y prefiera aquellas que no le son cercanas. También trate de evitar las cabinas telefónicas que estén ubicadas directamente en las rutas que llevan a su casa o a su lugar de trabajo, así como el uso de telecentros, locutorios, y negocios de cabinas agrupadas, donde guardan registros y mayormente tienen sistemas de vigilancia con CCTV.

\* Si desea enviar alguna cosa sensible a través del correo, use ropa y guantes para evitar la impresión de huellas digitales cuando arma o empaqueta los artículos, no salive las envolturas, cierres o las estampillas para evitar la creación de muestras de ADN, y colóquela en oficinas postales distintas de las que normalmente despacha su correspondencia utilizando estampillas compradas durante diferentes días.

\* Si necesita enviar un fax sensible, utilice una oficina de comunicaciones que le brinde la posibilidad de usar el equipo como autoservicio.

\* Si necesita desesperadamente mantener una comunicación móvil, adquiera o alquile, si es posible bajo otra identidad (o a través de otra persona) un teléfono móvil y úselo por un día o dos, mientras está ocupado en un trabajo sensible.

### On line

\* Mantenga activas varias identidades (vea el Resumen Nro.: 6 Utilizando Internet con seguridad) sobre Internet, de forma de tener acceso a Web Mails y otros

## 7 -Viviendo bajo vigilancia

---

servicios que podría estar necesitando usar en cualquier momento.

\* Si necesita usar un acceso Internet, utilice un cibercafé, evite acceder a su sistema principal (siempre pueden monitorear la actividad suya en cada computadora) y utilice las identidades alternativas.

\* Si necesita ver un material y no desea que sea asociado como parte de su actividad en los registros de su proveedor de internet, utilice un cibercafé.

\* Si utiliza cibercafé como parte de sus comunicaciones, trate de no utilizar siempre los mismos lugares, menos aún las mismas computadoras.

\* Si tiene una computadora portátil, y desea enmascarar su localización, deje que alguna otra persona la utilice en línea, mientras está realizando en otro lugar un trabajo sensible.

### Reuniones

\* Cuando está organizando reuniones privadas, y no puede enviar detalles a todos los involucrados de forma que no puedan ser interceptadas, trate de establecer una reunión cercana al lugar de la reunión principal. Podrá dar el lugar definitivo directamente a la gente a medida que va llegando. Manteniendo en reserva la localización de la reunión privada dentro de un círculo limitado de personas, y revelandolá recién momentos antes de hacerla, disminuye la probabilidad de que el lugar sea vigilado o hagan alguna preinstalación de dispositivos de escucha. Por el mismo motivo, trate de no repetir los lugares donde hace este tipo de reunión.

\* Si la reunión es en la casa o edificio de otra persona u organización no efectúe llamadas telefónicas desde esos teléfonos a números que se identifiquen con usted, o desde teléfonos públicos en cabinas cercanas a tales edificios.

\* Si las personas están dirigiéndose a una reunión privada probablemente tienen teléfonos móviles, deberá solicitarles que los apaguen (y eventualmente, quiten las baterías) antes de viajar al lugar de la reunión. ( Si todos los teléfonos móviles de un grupo de personas están en la misma celda de conexión telefónica, el mismo día y hora, pueden asumir que han tenido o formado parte de una reunión).

\* Si necesita un lugar privado para realizar una reunión, trate de no usar siempre el mismo. Alternarlos en lo posible. También, si la reunión es en un lugar público, trate de elegir lugares con un alto nivel de ruidos de fondo, y con muchos obstáculos muros, o divisiones alrededor del punto de reunión, para evitar que las conversaciones puedan ser escuchadas o grabadas a distancia.

\* Si debe pagar por alguna cosa mientras está en la reunión, utilice efectivo. O, si no puede, consiga una persona que pague. De esta manera no estará generando rastros documentales que lo puedan conectar con la reunión.

\* Reuniones en espacios públicos, calles, en parques, o sobre transportes públicos no son buena idea – muchas de estas áreas están vigiladas con cámaras CCTV. Pero algunos bares, cafés y restaurantes tienden a no tener sistemas conectados a un control central, y restringen el uso de sistemas CCTV alrededor del mostrador o de las cajas.

## 7 -Viviendo bajo vigilancia

---

### En conclusión

No existe una fórmula completa para definir la contra-vigilancia. Si el estado dirige todos sus recursos para monitorear todos sus movimientos, realmente, podrá hacerlo.

Como miembros de una sociedad, trabajando para cambiarla por medios pacíficos, no es aceptable que seamos objeto de un alto nivel de vigilancia por parte del estado.

Nosotros no estamos proponiendo la abolición de las técnicas sofisticadas y costosas de los distintos sistemas de vigilancia. Estamos observando el alto grado de exposición que tenemos ante los sistemas de vigilancia pasiva utilizados por los estados sobre nuestras actividades diarias, y el riesgo que presenta dicho conjunto de información si es adquirida y utilizada por grupos o corporaciones interesadas en nuestras actividades.

Una regla importante para el tema de la contra-vigilancia es tener proporcionalidad. Buscando evitar toda vigilancia estaremos marcando patrones de comportamiento distintos a los habituales del conjunto de la sociedad y sin lugar a dudas, atraeremos la atención de quienes vigilan. Es importante aplicar un nivel de contra vigilancia en proporción a la sensibilidad de la información o de la acción involucrada. En esta forma nosotros protegemos nuestras acciones sin que mostremos patrones de comportamiento diferentes a los normales de cada sociedad. Así nuestro trabajo se realizará igual pero mostrando pautas normales.

El tema final con la contra-vigilancia es su justificación. Nosotros debemos ser capaces, si somos desafiados, de justificar nuestra utilización de técnicas de contra vigilancia. De otra manera la utilización de estas tácticas puede ser utilizada por el estado o los servicios de seguridad como una evidencia de culpa en la conducta de nuestras actividades.

Nosotros estamos actuando bajo las garantías de las Convenciones de Derechos Humanos: tenemos derecho a la libre expresión, asociación y conciencia. Estos derechos realmente pueden ser ejercidos cuando tenemos la posibilidad de interactuar con otros de una manera que pueda estar libre de rutinas de vigilancia y o presión ante los disensos.

Hoy, gracias a las nuevas tecnologías digitales, de proceso de información, etc, los sistemas de vigilancia están llegando a ser muy penetrantes sobre el ambiente en que nos movemos y están generando un contexto donde la posibilidad de ejercer los derechos humanos sin presión del estado o de intervenciones privadas, se hace más difícil.

Los derechos humanos son subjetivos.

Esto significa que los derechos humanos de alguno que está trabajando por un cambio de la sociedad pueden ser interpretados en forma diferente a los derechos de los que se ocupan de la organización de actividades deportivas de su localidad. Para todas estas personas ocupadas en estas formas legítimas y en actividades por un cambio de la sociedad o de protesta, y por quienes creen que su trabajo no está bien visto por las corporaciones o por el estado, la contra vigilancia es una parte legítima de su trabajo en orden al ejercicio de sus derechos humanos y sociales.