GUIA DE PROTECCIÓN PARA DEFENSORES DE DERECHOS HUMANOS, PERIODISTAS, Y OPERADORES DE JUSTICIA

SEGURIDAD EN DEMOCRACIA
- S E D E M -

Presentación

Esta Guía de Protección fue preparada por SEDEM, (Seguridad en Democracia), una ONG que promueve la reforma de los servicios de inteligencia en Guatemala[1]. Una privera versión del texto fue presentada en el Foro: "Cómo Protegerse de Espionaje y Allanamiento Ilegal", celebrado en la Ciudad de Guatemala el 5 de marzo del 2001.

"La Guía", como se le conoce, nació como una medida proactiva del personal de SEDEM, frente a una serie de circunstancias inquietantes que podrían ser interpretadas como amenazas veladas a la seguridad física personal de la institución. Luego de recibir llamadas extrañas y observar indicios de vigilancia, hubo preocupación y perturbación, pero sobre todo confusión y poca preparación para saber qué hacer. ¿Cómo reacciónar? ¿Se corría algún riesgo? ¿Cómo había que protegerse? ¿Éra SEDEM la única institución a la cual le estaban pasando estas cosas? ¿Qué seddebía hacer?, fueron las preguntas en SEDEM se hicieron una y otra vez.

En medio de esta gama de preocupaciones y dudas, no había mucha orientación o información sólida que guiara el que hacer.

A pesar de trabajar en el área dedicada a promover reformas a los órganos de inteligencia, resulta que había en SEDEM muy poca preparación en el ámbito de la seguridad personal y de la seguridad de la informática como tal. SEDEM no tenía presupuestado ni el equipo de seguridad básico. Así las cosas, las únicas salidas a la angustia, resultaron ser comentarios a los amigos y a colegas en forma casual.

En ese intercambio, tanto por medio de la prensa como por contacto personal, se constató que otras entidades colegas también tenían problemas. Entonces, nació la idea de un enfoque más informado y sistemático:

a. comparar situaciones con otras organizaciones,
b. buscar información básica sobre las amenazas a la seguridad y,
c. reunir información sobre opciones en el área de medidas de seguridad.

De esa cuenta, SEDEM empezó a recolectar orientaciones básicas de seguridad para uso propio, y decidió compartiralas. Por eso, ahora las ofrece a las demás personas e instituciones del movimiento de derechos humanos, promoción de justicia y periodismo, con la esperanza de que también les sea de utilidad. En el área de la seguridad, la información y la planificación valen oro: así que, encontrarán acá por lo menos un avance en este proceso tedioso, pero siempre vital y necesario para proteger las libertades fundamentales de la persona y garantizar la continuidad del trabajo de las instituciones.

[1] Con dicha reforma, contenida en los Acuerdos de Paz suscritos en 1996, se pretende que ante la inevitabilidad de su existencia, tales servicios funcionen dentro de los ámbitos del control democrático.

Para quienes conocen poco de la labor de SEDEM, les informamos que el trabajo de incidencia en favor de la reforma de los servicios de inteligencia en Guatemala, se hace posible gracias al proyecto "El control democrático de los servicios de inteligencia en Guatemala," apoyado por Dan Church Aid, Proyecto Incidencia/USAID, la Fundación Soros de Guatemala y la Fundación Tinker de New York.

Una colaboración adicional para capacitar a los grupos afectados, en esta Iniciativa de Protección contra Espionaje y Allanamientos, fue aportada por el Programa de las Naciones Unidas para el Desarrollo, PNUD, y la Fundación Soros de Guatemala. Al mismo tiempo el Proyecto Inidencia/USAID prestó asistencia técnica en la seguridad informática.

El contenido del material acá presentado provino de sitios web de seguridad, incluidos http://www.seprin.com y http://www.j2.com.ar así como varios sitios de empresas que venden equipos de seguridad.

También se hizo consulta extensiva del material siguiente:

a) Estrategias prácticas para grupos pro Derechos humanos, publicado por el Center for Sustainable Human Rights Action 2000 (CESHRA).

b) US Department of State. Overseas Security Advisory Council. 1994 "Security Awareness Overseas: An Overview." and "1994 "Guidelines for Protecting U.S. Business Information Overseas.

c) Naciones Unidas. 1998. "Seguridad sobre El Terreno: Información para los funcionarios del sistema de las Naciones Unidas." Oficina del Coordinador de Medidas de Seguridad de las Naciones Unidas. Información para funcionarios del sistema de las Naciones Unidas. Naciones Unidas, Nueva York, 1998.

Las secciones de la denuncia y la acción internacional: acciones urgentes, protección internacional, medidas internacionales y medidas cautelares, son un aporte especial del Centro para la Acción Legal en Derechos Humanos (CALDH). Computer Professionals for Social Resonsibility, de Canadá, aportó orientación en las secciones referentes a encriptación. El ingeniero José Cruz trabajó en la elaboración de las secciones técnicas. Un valioso aporte a la primera edición fue realizado por Rachel Garst, primera directora ejecutiva de SEDEM. A cada una de las personas y entidades mencionadas se les agradece sus valiosos aportes. La responsabilidad de la presentación y el contenido finales, sin embargo, la asume SEDEM como entidad editora de esta guía.

La primera edición de "La Guía" fue un documento borrador del cual se distribuyeron cerca de 500 ejemplares en Guatemala, desde su aparicion en febrero del 2001, hasta septiembre del 2002. Algunos ejemplares adicionales se distribuyeron en el stand de Amnistía Internacional, en el XXIII Congreso de la Asociación Latinoamericana de Ciencias Sociales (LASA), realizado en Washington DC, en septiembre del 2001. Esta edición, corregida y aumentada, así como una serie de talleres sobre medidas de protección es factible gracias a un aporte específico, facilitado por la Organización Intereclesiástica para Cooperación al Desarrollo (ICCO), de Holanda.

Guatemala, diciembre del 2002

Introducción

Este documento es para la persona que teme amenazas a su seguridad o privacidad, surgidas de motivaciones políticas, de intimidación o de los servicios de inteligencia. Estas acciones podrían incluir desde la intervención de sus comunicaciones, pasando por allanamientos, amenazas u hostigamiento, hasta ataques físicos a su persona, sus colegas o miembros de su familia.

En Guatemala, país en el cual surge esta guía, existe una historia triste de represión oficial en donde agentes estatales han efectuado acciones de espionaje político y de represión violenta contra la misma población. Estas acciones se han concentrado, en particular, en activistas de derechos humanos, periodistas, miembros de partidos políticos, y operadores de justicia.

También actividades de espionaje y hostigamiento pueden ser llevadas a cabo por personas privadas, con motivaciones románticas, de robo de secretos comerciales, de extorsión y secuestro económico, o incluso de venganza personal. En el ámbito comunitario, pueden ser figuras locales que se amparan en las estructuras de impunidad y el apoyo implícito de su partido político, para cometer actos de corrupción y reprimir a sus opositores.

La Constitución Política de la República de Guatemala establece que es obligación del Estado proteger la vida y los derechos de privacidad de las personas, artículos 1º, 2º, 23, 24, 25 y 44[2]. Las instituciones estatales deben investigar, de oficio, todos los casos de violación de la seguridad e integridad de la persona, así como de violaciones a su privacidad, especialmente en cualquier caso que se sospecha la acción de agentes estatales. Las personas y organizaciones afectadas deben, por lo tanto, documentar y denunciar los hechos e insistir en la plena aplicación de la ley.

También es necesario comprender y enfrentar el hostigamiento al nivel individual, desde el ámbito de la persona afectada en su intimidad. La lógica de la represión es imponer una consecuencia desproporcionada a la gravedad de la actividad que se pretende reprimir. De tal manera que, por publicar un artículo en la prensa, uno puede pagar con su vida. Así se obliga a la persona a tomar decisiones siempre infelices, en las que se contraponen los principios y valores, con la seguridad personal. Muchas personas optan por desistir de sus actividades políticas, a costa de la democracia. Otros siguen en sus actividades

Entre algunas personas del movimiento de derechos humanos en Guatemala, existe la visión de que nadie debe dejarse amedrentar por las amenazas, hasta el extremo de no

[2]Además de los artículos citados, según el artículo 31 de la misma Constitución, toda persona tiene derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales. El mismo artículo prohíbe la existencia de registros o archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos.

ponerles ninguna atención ni denunciarlas. También hay quienes creen que se debe hacer todo públicamente porque al fin, la actividad que se realiza es completamente legal.[3]

Al respecto de lo anterior, este folleto propone una visión un tanto diferente. A cambio de no hacer caso a los hostigamientos, argumenta la importancia social y personal de denunciarlos y documentarlos. A cambio de actuar con total transparencia, sugiere la legitimidad de resguardar la privacidad de las comunicaciones y de los archivos frente a las nuevas amenazas de la era informática, incluso con medidas tecnológicas tales como encriptación.

Sobre todo, esta Guía pretende ser un apoyo directo y práctico a la persona o institución afectada por amenazas, hostigamientos e invasiones a su privacidad, quienes requieren de apoyo y orientación para que tomen sus decisiones sobre cómo proceder, estando bien informados. En la medida de lo posible, necesita ser protegida en su seguridad personal, y requiere de información que le ayude a interpretar y afrontar su propia situación de riesgo. Esta Guía de Protección pretende contribuir en esa línea, brindando información que facilite poner en práctica los consejos básicos siguientes:

A. **Entender las amenazas.** El ciclo de seguridad siempre empieza con tener información fidedigna sobre las amenazas enfrentadas. En este caso, a la persona hostigada podría ayudarle a la interpretación de sus circunstancias, tener información comparativa sobre lo que está pasando a otros. Asimismo, conocer las capacidades tecnológicas actuales de espionaje y su posible nivel de uso en Guatemala, que es otra forma de avanzar en la identificación de riesgos. De esta manera, se ayuda a las personas a distinguir entre amenazas políticas, amenazas delincuenciales y hechos puramente casuales.

B. **Considerar opciones de seguridad.** Es útil conocer todas las opciones físicas y tecnológicas de seguridad, así como su forma de adquisición y costos. Entre otros elementos, se refiere a cajas fuertes, puertas reforzadas, seguros de oficina, cámaras de vigilancia, programas de encriptación. Las instituciones podrían considerar los gastos de protección básica de la persona y de las oficinas e incluirlos en sus planes y presupuestos, o bien establecer un fondo de emergencia. El apoyo institucional en caso de problemas de seguridad es un beneficio laboral de considerable importancia, y una buena prueba de un acompañamiento de verdad, por lo que cada institución y donante podrían prever en sus políticas institucionales.

C. **Fomentar la preparación y la disciplina.** Se debe hacer un análisis de riesgos y tomar las medidas de precaución que se consideren necesarias y que se puedan implementar. Es importante hacer un estudio calmado de las necesidades reales de la institución y de cada oficina, frente a las amenazas específicas sufridas. También debe recordarse que la seguridad no depende solamente de inversiones en equipo, transporte, y otros gastos, sino también exige cambios en conducta y una disciplina

[3]La actividad de las organizaciones de la sociedad civil está constitucionalmente garantizada, entre otros, por los artículos, 26, 28, 33, 34, 35 y 45.

constante. Es importante que las personas afectadas modifiquen su comportamiento ante los riesgos evidentes, para evitar situaciones inseguras.

D. **Documentar toda actividad sospechosa.** Se deben documentar los hechos sospechosos en forma sistemática y recoger evidencias de tales actividades (fotos, placas, vehículos sospechosos, etc.), a fin de tener más elementos de apoyo para la interpretación de los hechos y más pistas y elementos de prueba en caso de una investigación. También es aconsejable informar a los demás miembros del grupo de referencia (tanto de la familia, como personas de la misma institución y otros colegas) qué está pasando exactamente y cuáles son los hechos concretos ocurridos.

E. **Denunciar los hechos ilegales.** Se debe denunciar cualquier actividad ilegal o intimidatoria, ante el Ministerio Público, la Procuraduría de los Derechos Humanos, Minugua (Misión de Naciones Unidas para Guatemala)[4] y otras entidades competentes, además de exigir que respondan a la denuncia. Un trabajo constante en el ámbito judicial hacia quienes atenten contra la legítima labor de las personas que trabajan por los derechos humanos, les enviará un claro mensaje para que cesen en su empeño.

[4] Mientras dure su mandato en Guatemala y por lo tanto tenga presencia en el país.

I. LAS AMENAZAS

I.1 Los Derechos Políticos y de Privacidad

Ninguna ley, y ninguna acción estatal, debe violar los derechos fundamentales definidos en la Constitución de su Estado, y por ende estos constituyen el marco de referencia que limita cualquier trabajo policial o de inteligencia. Según la Constitución actual de la República de Guatemala, el Estado garantiza a las personas los derechos siguientes:

Articulo 3. Derecho a la vida. El Estado garantiza y protege la vida humana desde su concepción, así como la integridad y la seguridad de la persona.

A**rtículo 5. Libertad de acción.** Toda persona tiene derecho a hacer lo que la ley no prohíbe; no está obligada a acatar órdenes que no estén basadas en la ley y emitidas conforme a ella. Tampoco podrá ser perseguida ni molestada por sus opiniones o por actos que no impliquen infracción a la misma.

Artículo 6. Detención legal. Ninguna persona puede ser detenida o presa, sino por causa de delito o falta y en virtud de orden librada con apego a la ley por autoridad judicial competente. Se exceptúan los casos de flagrante delito o falta. Los detenidos deberán ser puestos a disposición de la autoridad judicial competente en un plazo que no exceda de seis horas, y no podrán quedar sujetos a ninguna otra autoridad.

Artículo 14. Presunción de inocencia y publicidad del proceso. Toda persona es inocente, mientras no se le haya declarado responsable judicialmente, en sentencia debidamente ejecutoria.

El detenido, el ofendido, el Ministerio Público y los abogados que hayan sido designados por los interesados, en forma verbal o escrita, tienen derecho de conocer, personalmente, todas las actuaciones, documentos y diligencias penales, sin reserva alguna y en forma inmediata.

Artículo 23. Inviolabilidad de la vivienda. La vivienda es inviolable. Nadie podrá penetrar en morada ajena sin permiso de quien la habita, salvo por orden escrita de juez competente en la que se especifique el motivo de la diligencia y nunca antes de las seis ni después de las dieciocho horas. Tal diligencia se realizará siempre en presencia del interesado, o de su mandatario.

Artículo 24. Inviolabilidad de correspondencia, documentos y libros. La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.

Los libros, documentos y archivos que se relacionan con el pago de impuestos, tasas, arbitrios, y contribuciones, podrán ser revisados por la autoridad competente de conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley.

Los documentos o informaciones obtenidas en violación de este artículo no producen fe ni hacen prueba en juicio.

Artículo 25. Registro de personas y vehículos. El registro de las personas y de los vehículos, solo podrá efectuarse por elementos de las fuerzas de seguridad cuando se establezca causa justificada para ello. Para ese efecto, los elementos de las fuerzas de seguridad deberán presentarse debidamente uniformados y pertenecer al mismo sexo de los requisados, debiendo guardarse el respeto a la dignidad, intimidad y decoro de las personas.

Artículo 30. Publicidad de los actos administrativos: Todos los actos de la administración son públicos. Los interesados tienen derecho a obtener, en cualquier tiempo, informes, copias, reproducciones y certificaciones que soliciten y la exhibición de los expedientes que deseen consultar, salvo que trate de asuntos militares o diplomáticos de seguridad nacional, o de datos suministrados por particulares bajo garantía de confidencia.

Artículo 31. Acceso a archivos y registros estatales. Toda persona tiene derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos.

Artículo 33. Derecho de reunión o de manifestación: Se reconoce el derecho de reunión pacífica y sin armas. Los derechos de reunión y de manifestación pública no pueden ser restringidos, disminuidos o coartados; y la ley los regulará con el único objeto de garantizar el orden público.

Artículo 34. Derecho de asociación: Se reconoce el derecho de libre asociación. Nadie está obligado a asociarse ni a formar parte de grupos o asociaciones de autodefensa o similares. Se exceptúa el caso de la colegiación profesional.

Artículo 35. Libertad de emisión del pensamiento: Es libre la emisión del pensamiento por cualesquiera medios de difusión, sin censura ni licencia previa. Este derecho constitucional no podrá ser restringido por la ley o disposición gubernamental alguna. Quien en el uso de ésta libertad faltare el respeto a la vida privada o a la moral, será responsable conforme la ley.

No constituyen delito o falta las publicaciones que contengan denuncias, críticas o imputaciones contra funcionarios o empleados públicos por actos efectuados en el ejercicio de sus cargos.

I.2 Las Amenazas Enfrentadas

Si bien en la actualidd, los niveles de violaciones de derechos humanos en Guatemala están por debajo de los registrados en años anteriores, aún hay irrespeto a los mismos.

De hecho, persisten problemas importantes de inseguridad en ese campo. El décimo informe de la Minugua sobre la situación de los derechos humanos en Guatemala reportó: "Desde el inicio de la Misión, las denuncias admitidas por amenazas e intimidaciones han tenido una tendencia decreciente. Sin embargo, a partir del período cubierto por los dos informes previos, se ha registrado un aumento progresivo de las denuncias, afectando principalmente a personas y entidades que trabajan en la protección de los derechos humanos. En este período la tendencia se mantiene, lo que podría vincularse con la presentación del Informe de la CEH y con algunos procesos judiciales con gran impacto en la opinión pública."[5]

Estas tendencias han continuado y se han acrecentado desde el año 2000, fecha en la cual el Frente Republicano Guatemalteco, FRG, asumió la dirección del gobierno (particularmente desde el ejecutivo y legislativo). Entre los numerosos hechos registrados durante este gobierno, destacan los siguientes:

a) La desaparición de la psicóloga Mayra Gutiérrez, ocurrida el 7 de abril del año 2000.

b) El allanamiento de las oficinas de la organización Familiares de Desaparecidos de Guatemala, FAMDEGUA, con su personal presente, el 4 de septiembre de 2001.

c) Al allanamiento y los ataques violentos hacia integrantes de la Asociación Mujer Vamos Adelante.

d) Numerosas amenazas contra periodistas, incluyendo el Equipo de Investigación del matutino El Periódico, el periodista del matutino Prensa Libre José Eduardo Zarco, personal de la agencia de prensa CERIGUA, entre otros.

e) Numerosas amenazas contra miembros de la Organización de Derechos Humanos del Arzobispado ODHA y el juez Eduardo Cojulún, con relación aparente al caso por el asesinato del obispo Juan Gerardi.

f) Numerosas amenazas contra Rigoberta Menchú y el asesinato de Guillermo Ovidio Ovalle, contador general de la Fundación Rigoberta Menchú, ocurrido en mayo del 2002, con relación a su intento de impulsar un juicio sobre el genocidio guatemalteco, en España.

[5] MINUGUA. Décimo informe sobre la situación de derechos humanos en Guatemala. MINUGUA, Guatemala enero 2000. Página 5.

g) El asesinato de seis abogados, empezando en octubre del 2000 con la muerte de la Licda. Maura Ofelia Paniagua González.

h) La circulación de un listado de amenazados de muerte, por una organización paramilitar clandestina destacando la figura de Hellen Mack y de varios periodistas, ocurrida en mayo del 2002.

i) Asesinato del periodista Mynor Alegría el 5 de septiembre del 2001

j) Allanamiento a por lo menos 15 organizaciones de derechos humanos y movimiento social, con robo de equipo de computación.

k) Asalto, allanamiento de oficinas y violación a dos integrantes de la organización"Mujer vamos adelante".

l) Amenazas de muerte a los equipos de antropólogos forenses que trabajan en exhumación de cementerios clandestinos.

m) Amenazas e intimidación a líderes comunitarios de las poblaciones donde se realizan las exhumaciones.

n) Colocación de escuchas telefónicas en la oficina del fiscal general de la república.

o) Colocación de escuchas telefónicas y micrófonos de largo alcance en el despacho del Procurador de Derechos Humanos.

p) Amenazas por la vía telefónica a defensores de derechos humanos y operadores de justicia en casos paradigmáticos.

De manera que, el clima de intimidación es fuerte y por ello se hace necesrio adoptar medidas de protección. Sin embargo, antes de cualquier indagación sobre el tipo de vigilancia, o medio que puede amenazar a nuestra institución y a nuestro trabajo, es muy conveniente hacer un **análisis de vulnerabilidad** respondiendo a las siguientes preguntas:

- ¿A quién afecta nuestro trabajo y por qué?
- ¿Quién o quiénes estarían interesados en vigilarnos o amedrentarnos?
- ¿Qué información específica les interesaría más y dónde se encuentra?
- ¿En dónde podrían atacarnos y cómo?
- ¿En dónde y en qué medida somos más vulnerables?
- ¿Qué tan seguros estamos en lo que consideramos nuestras áreas vulnerables?
- ¿Cuáles serían los resultados de una pérdida de confidencialidad de nuestra información clave?

La mayoría de los actores de la sociedad civil cuenta con un conocimiento muy impreciso sobre los métodos y recursos técnicos que pueden ser volcados en su contra por los aparatos de control. Utilizan confiadamente el teléfono, el fax y el correo electrónico para sus comunicaciones. Las computadoras en las que elaboran y guardan sus documentos y bases de datos no están sujetas a procedimientos sistemáticos de seguridad. Operan desde oficinas abiertas al público en las cuales sostienen reuniones y guardan sus documentos y activos con precauciones limitadas y a menudo, no efectivas.

Llevar a cabo el **análisis de vulnerabilidad** con la participación de las personas de mayor confianza dentro del equipo, permite alcanzar una noción más clara de cuáles serían las prioridades de nuestros adversarios y una hipótesis de hacia dónde orientarían sus mecanismos de control.

Este es un ejercicio que debe realizarse periódicamente, a fin de asegurar la adopción de correctivos oportunos. El análisis de vulnerabilidad debe convertirse en un paso fundamental del proceso de planificación estratégica y de evaluación de cada entidad.

II. MEDIOS COMUNES DE ESPIONAJE Y CONTROL INTRUSIVO

II.1 Informantes

Un Informante es alguien que pasa o entrega información sensible en forma secreta a una tercera persona. Las motivaciones del Informante pueden ser: económica (lo hace con el fin de recibir un pago); por identificación ideológica (está convencido que al pasar información está haciendo lo correcto); o por estar sujeto a chantaje (si no pasa la información se expone a sufrir daños contra su persona, su prestigio o su familia). Se distingue del agente secreto (infiltrado), en que no trabaja para el organismo de seguridad y que viene desde afuera con la intención de incorporarse, sino que, por el contrario, se le recluta específicamente por su cercanía o pertenencia a la organización vigilada.

Se sabe que esta práctica es parte del legado de la historia reciente del país. Según la CEH[6]: "En las áreas urbanas el control (del Ejército) se realizó en forma minuciosa utilizando una acción de vigilancia constante y de información de las actividades civiles. Dentro de cada manzana existió un líder de zona y de manzana, quien periódicamente daba cuenta al comandante militar o a la autoridad civil de la que dependía, de todos los movimientos ocurridos en su área de control."[7] Un memorando interno del Ejército Estadounidense de 1992 describe la organización del "Archivo," una rama del Estado Mayor Presidencial conformada por aproximadamente 60 especialistas del Ejército, *"La sección de operaciones tiene la capacidad de hacer vigilancia… y, a través de una red de informantes, recaba información de inteligencia."*[8] Los temas analizados incluyeron*: "partidos políticos, economía, religión, trabajadores y estudiantes."*[9] Según este documento, el Archivo *"mantiene una base de datos completa sobre guatemaltecos y extranjeros residentes en Guatemala."* –aseveración respaldada con el descubrimiento en marzo del 2000, de los trazos de una base de datos de 650,000 nombres en las computadoras de la Secretaría de Análisis Estratégico de la presidencia (SAE.)

Aunque al o a la informante se le puede utilizar en cualquier tipo de terreno, suelen ser un instrumento de vigilancia muy usado en áreas rurales, debido a la dificultad de emplear

[6] Comisión para el Esclarecimiento Histórico, fue establecida mediante el Acuerdo de Oslo, del 23 de junio de 1994, para esclarecer con toda objetividad, equidad e imparcialidad las violaciones a los derechos humanos y hechos de violencia que han causado sufrimientos a la población guatemalteca, vinculados al enfrentamiento armado. Produjo el informe Guatemala memoria del silencio.
[7] Cita
[8] cita
[9] cita

medios tecnificados o sofisticados por la inaccesisibilidad de energía y comunicación electrónica.

Cabe mencionar acá también, el problema no de informantes como tales, pero de trabajadores indiscretos. Las habladurías, jactancias, charlas descuidadas de personas, pueden ser una fuente rica de información aprovechada por algún agente. De igual manera, el personal puede ser reclutado posteriormente por la oposición, o entrevistado por ellos sin su conocimiento explícito.

II.1.2 Medidas de protección contra informantes

Es muy difícil detectar a los informantes, y la búsqueda de ellos dentro de una organización puede crear un ambiente de desconfianza que tiene un alto impacto negativo. Por estas razones, la mejor forma de protegerse contra esta amenaza es ser cauto con lo que se dice frente a otras personas, y tomar las siguientes medidas básicas para proteger su información:

a) Estudiar a los/as aspirantes a empleo. Pedir un currículum vitae detallado, con referencias personales y laborales, y luego chequear las referencias proporcionadas. Comunicarse con las personas listadas (preferiblemente en forma personal), y preguntarles qué tanto conocen a la persona solicitante. Detectar lagunas en el historial de empleo y pedir explicación. Podrían representar tiempos de encarcelamiento o de otra actividad que la persona no quiera revelar. Igualmente, insistir en conocer el historial militar y los antecedentes penales y policiales.

b) No hablar cosas sensibles frente a terceros y a personal de servicio. Nunca se sabe quién está enfrente. No dejar visitantes solos en las oficinas. Incluso con el mismo personal, compartir información sensible únicamente con los que necesitan saberlo.

c) Resguardar sus papeles. No dejar papeles importantes a la vista y mantener los escritorios y archivos con llave.

d) Resguardar la seguridad básica de su computadora, utilizando las palabras claves o pasaportes, guardando los disquettes bajo llave, etc.

e) Controlar el ingreso de personas en la institución, especialmente fuera del horario normal. No permitir que se saquen múltiples copias de las llaves, y fiscalizar estrechamente el control de las llaves que existen. Al contratar a una persona para limpiar la oficina, solicitar que trabaje de día. Cambiar periódicamente los registros de las cerraduras de la oficina.

f) Si su organización tiene un programa que mantiene información especialmente sensible, considerar la posibilidad de establecer un sistema de información clasificada combinada con “lugares restringidos”, a los cuales no deben entrar

visitantes, ni personas sin permiso de acceso. Para la seguridad de la información más sensible (por ejemplo: el testimonio de un testigo), es necesario resguardarlo de alguna forma. Esta práctica generalmente se llama clasificación y debe ser efectuada con toda la información sensible.

Consiste en:

1) Tener un responsable de revisar toda la información y codificar su grado de sensibilidad sobre la base de parámetros definidos.

2) Tener un inventario y un control físico de la información clasificada, evitar su divulgación excepto a personas que por su función necesitan conocerla, llevar una fiscalización estricta de cualquier reproducción o diseminación de la misma

g) Si se trabaja con personas cuya identidad debe ser confidencial, se deben codificar sus nombres en toda información escrita o grabada.

h) Debe considerarse limitar o centralizar el uso de la fotocopiadora en la oficina, para dificultar que otras personas puedan sacar copias de documentos confidenciales o sensibles. Por ejemplo, asignar códigos de uso al personal, o encargar todos los pedidos de copias, a una sola persona.

i) No echar documentos sensibles a la basura. Destruirlos antes rompiéndolos o quemándolos. Se puede comprar una máquina trituradora para este fin.

j) Evaluar periódicamente al personal para establecer si pudieran convertirse en informantes voluntarios o involuntarios. Cabe analizar cambios abruptos e inexplicables en el patrón de consumo (gasta más que antes); sufre depresión o pánico inexplicable (podría estar siendo víctima de chantaje); Sus relaciones personales con otros miembros del equipo se han tornando conflictivas (encontrando argumentos para debilitar su lealtad a la institución).

k) Instruir al personal acerca de los métodos de reclutamiento y persuadirlos a informar de cualquier situación anómala que les ocurra.

l) Manejar los disquetes con tanto cuidado como los documentos impresos. Recuerde que es posible que quede una copia de los documentos ya borrados en el disco duro de su computadora (como archivo temporal, de respaldo, o invisible). Hay programas especiales que pueden prevenir esta eventualidad (WipeDisk y WipeFile de Norton, PGP cuenta con una herramienta similar).

m) Si se teme el robo o la alteración de sus papeles personales y legales, es aconsejable guardar los originales en un lugar seguro y trabajar diariamente con fotocopias sencillas o legalizadas de los mismos. Por lo mismo, siempre resguarde copias de sus archivos y comunicaciones electrónicas, en un sitio seguro.

n) Las redes computarizadas son un sistema particularmente vulnerable desde el punto de vista de la privacidad. Por ende, es necesario establecer una serie de reglas de uso en favor de la seguridad de la información, por ejemplo:

   a) Tener un responsable con conocimiento técnico encargado de velar por la seguridad de los sistemas computarizados

   b) Tener diskettes que entran en el sistema de documentos clasificados o que se mantengan encriptados permanentemente por sus creadores

   c) Comprobar que todos los equipos mantengan “clave de acceso”,”clave de red,” y “clave de protector de pantalla”

   d) Asegurar que se tenga copias de resguardo en un lugar seguro

   e) Usar un programa especial para limpiar información borrada.

   f) Manejar archivos fundamentales con sistema de Scram disk (ver sección especial en esta guía).

   g) Definir y llevar a la práctica una política institucional de seguridad informática.

II.2 Cámaras de Vigilancia

Un objetivo básico de los Aparatos de Control es identificar de manera fehaciente a las personas que van a ser vigiladas y al conjunto de su red de relaciones políticas, sociales, laborales y familiares. También podría interesar un registro de las personas que visitan o están vinculadas al lugar de trabajo. Para este propósito, se pueden usar personas de vigilancia (véase sección pertinente) o bien emplear cámaras ocultas de diversa índole, por ejemplo:

a) Cámaras fotográficas operativas: Se caracterizan porque el lente de la cámara está colocado en la parte de atrás, de manera que la persona objetivo no se da cuenta que le están tomando fotos de manera disimulada. Únicamente ve a una persona sacando fotografías a otros.

b) Cámaras fotográficas normales con objetivos intercambiables desde 28mm (gran angular) hasta 1000mm (zoom de alta potencia): Estas son cámaras iguales a las que usamos todos los días a las cuales se les adaptan lentes zoom (de aproximación) que permiten tomar retratos cercanos desde distancias desde las cuales la persona fotografiada no puede ver al fotógrafo.

c) Cámaras de vídeo miniatura para vigilancia. Esta se puede “sembrar” (colocar) en el interior de un local. Transmite una señal con las imágenes captadas y las envía a un receptor remoto. Por ejemplo, existen las Cámaras fotográficas PIN HOLE para

tomar fotos a través de una cerradura. Estas cámaras altamente miniaturizadas toman fotografías digitales (que pueden ser vistas en una computadora).

d) Cámara de vigilancia color o B/N (según el grado de luminosidad) con detector de movimiento incorporado. Su característica es que se activa al detectar movimiento. En condiciones de poca luz graba en Blanco y Negro. También existen cámaras de vídeo digitales, con visión nocturna, con alcance de hasta 500 mts. Permiten hacer tomas de vídeo a larga distancia y en condiciones nocturnas si es necesario. Son el equipo complementario al micrófono direccional. Pueden ser colocadas en una casa, poste o vehículo vecino.

e) Cámara oculta portátil. Utiliza un celular motorola startack como transmisor que envía una señal de video y audio a un receptor no tan remoto, instalado en un portafolio común y corriente.

f) Para controlar o grabar las imágenes de vídeo, existen tres opciones: 1) Grabadoras de vídeo. Permiten colocar un puesto fijo de filmación para vigilancia permanente. 2) Emisor/receptor de señal de vídeo, permiten una vigilancia "en línea" desde un centro de control desde el cual se monitorea la actividad dentro de un local en directo. 3) Equipo de grabación de vídeo y transmisión de imágenes vía radio. Es una combinación de los dos anteriores.

Por la movilidad y capacidad de empleo portátil y su uso sin energía eléctrica, también pueden ser usadas en zonas rurales por lo que las organizaciones que trabajan fuera del ámbito urbano no deben sentirse libres de esta amenaza.

II.2.1 Medidas de protección contra cámaras ocultas

En condiciones de actividad normal, que no requieren protección, no tiene caso pretender ocultar nuestra identidad. Nuestra actividad legal y pública no debe ser expuesta asumiendo actitudes pretendidamente conspiradoras. Sin embargo, en casos en los cuales se establece contacto con testigos clave y relaciones que necesitamos proteger, hay que planificar las reuniones para garantizar su confidencialidad. En estos casos excepcionales, vale la pena preocuparse por la posibilidad de las cámaras ocultas. Cuando exista la preocupación, se recomiendan las siguientes medidas:

a) Llevar a cabo la reunión en un lugar cerrado y seguro, pero no el habitual; mantener el control de la información sobre el lugar y acudir al punto de reunión luego de romper posibles seguimientos.

b) El establecimiento de un área de mayor seguridad al interior de nuestras oficinas, así como las mismas medidas contra la escucha electrónica, expuestas en siguientes apartados. En este caso, el control del ambiente físico podría ser combinado con la búsqueda y detección ocular de estos aparatos escondidos.

c) No orientar las pantallas de las computadoras hacia los vidrios de las ventanas para evitar la posibilidad de filmación de su contenido.

II.3 Micrófonos Ocultos

La capacidad de producir dispositivos miniaturizados es muy efectiva. Simplemente consideremos que un microprocesador Intel Pentium de última generación capaz de gobernar las complejas funciones de una PC, tiene un tamaño similar al de una moneda grande. Igual tendencia ha pasado con los micrófonos ocultos, o las escuchas ambientales, que son una forma siempre más barata y más utilizada, para invadir la privacidad de las personas.

Esta invasión de la privacidad puede representar riesgos importantes para las personas defensoras de derechos humanos, operadores de justicia o periodistas, quienes tienen la obligación profesional de resguardar información confidencial proporcionada por testigos, o información proporcionada por fuentes confidenciales. Igualmente, las instituciones querrán resguardar sus estrategias judiciales o deliberaciones internas. Finalmente, las personas que temen ataques físicos tal vez necesitan proteger y resguardar hasta información logística sobre sus planes diarios y horarios, entre otros.

Por estos motivos, es válido preocuparse de la posibilidad de un ataque a la privacidad, por medio de micrófonos ocultos o escuchas ambientales. El equipo utilizado para este fin, podría incluir dispositivos tales como los siguientes:

a) Micrófonos ocultos para vigilancia acústica. Fijos: se 2siembran" (colocan) dentro del local que se desea vigilar, ocultos en cualquier aparato eléctrico, tomacorriente, pared o mueble. Móviles: ocultos en plumas, calculadoras, ceniceros y otros objetos. (¡cuidado cuando le regalan algo!). Captan en un radio de 15 mts. y transmiten hasta 400 o 500 metros de distancia. El uso de estos dispositivos requiere la presencia de un centro de recepción dentro del radio de alcance de los transmisores (400-500 mts.). Este puede ser desde una Van o vehículo equipado para recibir y grabar las conversaciones, un cuarto en una casa contigua, o incluso hasta un maletín de negocios que luego es recogido por un "agente operativo"[10]. Igualmente se podría hacer un cableado hasta otra habitación desde el cual se escucha perfectamente todo.

b) Uso del teléfono como micrófono ambiental. Existen dispositivos que utilizan el micrófono del teléfono alámbrico para escucha ambiental cuando el teléfono no se está utilizando. El cableado telefónico opera como medio de transmisión, el cual es "pinchado" (intervenido), con dos "lagartos" (pinzas) conectados a un transmisor miniatura. Este dispositivo se activa mediante una llamada que puede realizarse desde cualquier lugar del mundo y se puede manejar desde una central telefónica, desde el cableado de la calle con un microtransmisor, o desde una caja de

[10] Agente operativo, persona encargada de completar una misión para servicios de seguridad o inteligencia.

contactos telefónicos ubicada en la banqueta de la esquina donde hay suficiente espacio para colocar una grabadora portátil.

c) Transmisores de audio para control de entrevistas personales, con su receptor. Estos se pueden disimular en una pluma, en una calculadora y son portados por una persona con la que está teniendo la conversación, o se dejan en el lugar para ser recogidos posteriormente o simplemente se abandonan. Algunos dispositivos son tan pequeños como la punta de un palillo de dientes. Al no requerir energía y por su facilidad de uso pueden emplearse tanto en zonas urbanas como rurales.

d) Micrófono direccional. Este potente micrófono para escucha a distancia en espacios abiertos, tiene un alcance de hasta 500 mts. Hace inseguras las "reuniones al aire libre" pues dentro de esa distancia es fácil ocultar el dispositivo y su operador. Es un dispositivo ideal de uso en zonas rurales.

e) Escucha externa vía láser a través de ventanas. El micrófono láser para este trabajo cuesta alrededor de $1,000.00. Los vidrios de las ventanas funcionan como micrófonos al reproducir las vibraciones de la voz que son captadas y transmitidas por un haz de láser al aparato que analiza la señal, la filtra y la graba o transmite a un centro de escucha. Al igual que el anterior se puede utilizar en zonas rurales.

II.3.1 Medidas de protección contra micrófonos ocultos

La detección de micrófonos y transmisores ambientales es laboriosa y cara. Existen empresas que se dedican a "barrer" (buscar y limpiar) de **bugs** (micrófonos) un local donde se realizarán reuniones importantes. Tienden a ser caros y existe siempre la cuestión de su confiabilidad, pues muchos de sus propietarios y operadores provienen de los cuerpos de inteligencia que actuaron durante el conflicto armado interno. La contratación de este tipo de servicios, incluyendo la asesoría para la compra de equipo básico de Contramedidas para Vigilancia Técnica –TSCM por sus siglas en inglés– debe realizarse con suma cautela y buscando referencias de las empresas en cuestión.

Otra opción sería la de comprar uno mismo equipo antibug. Pero acá el asunto crítico no es contar con el equipo de "barrido" sino saberlo utilizar correctamente. De modo que la mera compra de aparatos no resuelve el problema, pues, además seimpre existe la distancia entre el avance tecnológico en equipo de escuchas y su detección. Esto requiere de una inversión constante y cara, para resultados de corta duración y escasa confiabilidad.

Finalmente, el problema de barrer contra las escuchas es que son fáciles de volver a colocar, por lo que también hay que intentar ambientes seguros. En todo caso, cuando haya necesidad de asegurar la privacidad de las reuniones o conversaciones telefónicas, recomienda lo siguiente:

A. Establecer un **sitio seguro** para llevar a cabo las reuniones importantes. El **sitio seguro** ideal tendría que reunir entre otras, las siguientes características:

   1) No tiene ventanas;

   2) No colinda con propiedades vecinas;

   3) No tiene conexiones eléctricas ni telefónicas en su interior;

   4) Está pintado de blanco para facilitar la detección visual de bugs;

   5) El mobiliario debe ser el mínimo necesario, incluyendo un pizarrón para escribir (no decirlos) nombres o palabras confidenciales;

   6) El acceso al lugar está físicamente restringido.

B. Antes de una reunión importante debe ser "barrido" de bugs. Lo mínimo podría ser aunque sea una inspección ocular en las paredes, dentro de los teléfonos, y otros aparatos. La inspección por medios tecnológicos se hace de varias formas.

   Una de las más comunes barre constantemente el espacio radioeléctrico. Se puede hacer lo mismo de forma rudimentaria usando un radio para detectar puntos en el cuarto en donde hay mayor interferencia en la señal. El receptor FM portátil ubica las radiofrecuencias RF de uso común para interceptación, provoca *feedback* (retroacción), y de este modo se detectan algunos micrófonos y transmisores. Generalmente se usa equipo mucho más sofisticado que efectúa barridos por una amplia gama de frecuencias y modalidades de emisión, emitiendo señales codificadas y reconociendo sus propias señales a fin de identificar una emisión proveniente de un dispositivo de escucha. No obstante, incluso el equipo más caro y sofisticado produce algún resultado en manos inexpertas. También es de considerar que existen "escuchas en fila" en donde al "caer" una, las demás se apagan, y hay otras que se apagan y se encienden a distancia o a ciertas horas. Entonces, la barrida anti-escucha tiende a ser cara y no siempre efectiva. Además, existe el problema de que luego de efectuarse una limpieza hay que restringir físicamente todo acceso al local.

C. Una alternativa eficaz y accesible consiste en grabar una sesión de charla intrascendente con la voz de los participantes en la reunión. También se puede usar música o un aparato especial que genera un ruido "blanco". Esta grabación repetida constantemente debe usarse como música de fondo de la reunión, y de esta forma ayuda a obstaculizar el filtrado de las voces.

D. Los participantes deben ingresar a la reunión con los medios indispensables: no llevar celulares, grabadoras, o equipo electrónico de algún tipo, ya que cualquiera de ellos podría tener colocada una escucha. Esta es una de las razones por las que muchas Embajadas requieren a las personas y sus pertenencias, pasar por máquinas de Rayos X.

E. Las notas sobre la reunión deben centralizarse y ser almacenadas de manera encriptada. Igualmente, cuando el riesgo de los micrófonos ambientales es muy alto, se podría considerar la posibilidad de usar el correo electrónico encriptado, en lugar de tener conversaciones telefónicas o reuniones personales, en donde la voz puede ser captada en su transmisión por el aire.

F. Si se considera el micrófono láser un peligro, no es suficiente con cerrar las ventanas. Debe ponerse bocinas a cada lado de las ventas, o hacer reuniones sensibles en ambientes sin ventanas.

II.4 Intervención telefónica y de fax

En Guatemala, el espionaje telefónico es ilegal[11]. No obstante, se trata de un fenómeno incontrolable, que según los expertos consultados es practicado por múltiples actores estatales así como por el sector privado. Además, también se usa por las agencias internacionales de inteligencia quienes luego comparten las informaciones entre ellas y con otros gobiernos. Algunos de los aparatos necesarios se venden en el mercado por sólo Q700.00, aparte de que es, prácticamente, imposible saber cuándo le están interviniendo su teléfono, ya que puede intervenirse en cualquier punto del recorrido desde el aparato mismo hasta la central. Por eso se considera una práctica aunque igela en Guatemala, lamentablemente endémica.

Una llamada puede ser intervenida en cualquier de los puntos siguientes:

a) Con la instalación de un emisor dentro del mismo aparato telefónico (aprovechando el micrófono del mismo).

b) Pinchando el cableado de su línea telefónica con los “lagartitos” desde el teléfono, pasando por el interior del edificio, y luego en el trayecto fuera del edificio hasta la caja de contactos en la banqueta de la calle, hasta la caja de pares, hasta la acometida de línea, y centralita.

c) Derivación de la línea mediante acoplamiento físico o por inducción de la misma y escucha directa (básicamente es un teléfono supletorio).

d) En estos dos casos generalmente se pone un emisor que es captado por un aparato dentro de un perímetro de 400 metros, donde se graba. Si el lugar de la intervención lo permite, se puede colocar una pequeña grabadora allí mismo. Luego, pasan las

[11] El artículo 24 de la Constitución Política de la República (CPRG) estipula que “se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otras procedentes de la tecnología moderna”. En virtud de la interpretación estricta de esa oración, la Corte de Constitucionalidad emitió una sentencia, contenida en el numeral 14 del expediente 296-94, la cual declara inconstitucional el artículo 205 del Código Procesal Penal (Libro Primero, Disposiciones Generales, Título III). De manera que, deicha sentencia declara ilegales todas las escuchas telefónicas, incluidas las realizadas por agentes o entidades del Estado.

personas periódicamente a cambiar las cintas, o bien puede haber personas escuchando directamente.

e) Desde la central telefónica (ver recuadro sobre El Salvador) también se puede intervenir. En estos casos se supone que para la recepción en sí de la información en las llamadas, existen desde personas que hacen la escucha directamente, o bien hay computadoras --activadas por la voz o por palabras clave –que graban la comunicación y la transcriben.

f) Las llamadas desde los teléfonos celulares se captan desde el mismo aire. Estas llamadas son más fáciles de interceptar pues para ello no se requiere realizar instalaciones previas: con una antena y el equipo adecuado se pueden captar y decodificar las llamadas solo con estar en las proximidades. Se hace mediante un simple scanner (explorador) que cualquiera puede comprar en Radio Shack, o bien con un aparato especial de intercepción de teléfono celular. La facilidad de esta intervención depende de, si uno de los dos teléfonos en la comunicación es analógico, o si ambos son digitales.

El Salvador: Intervención telefónica desde la central telefónica privatizada

Durante el curso de 2000 tuvo lugar en El Salvador un escándalo de magnas proporciones sobre el espionaje telefónico. Todo empezó cuando Jorge Zedán, presidente del Canal 12 y además de una compañía telefónica privada llamada SALNET, notó el problema de que muchas de sus llamadas o de sus colegas se tardaban demasiado en completarse o nunca se completaban. Al investigar los técnicos de SALTEL, encontraron que la docena de números en cuestión habría sido codificada como B-9 en el sistema de TELECOM (la anterior empresa estatal ahora propiedad de una empresa francesa). Con sorpresa, descubrieron que B-9 quiere decir "línea interceptada."

Las escuchas telefónicas son estrictamente prohibidas por la Constitución de El Salvador. Luego de una investigación inicial, en junio de 2000, la Superintendencia General de Energía y Telecomunicaciones (SIGET) multó a TELECOM por "haber violado el secreto de las comunicaciones mediante interferencia o intervención intencional de la misma," pero esta decisión luego fue revertida por la Junta de SIGET. El Congreso de El Salvador también hizo una investigación, en donde se determinó que el contrato de interconexión entre las compañías TELECOM, SALNET y las demás empresas telefónicas privadas, se detalla como parte de los protocolos de comunicaciones para Interfuncionamiento (específicamente en el apartado 2.2 Señales Hacia Atrás) una abreviatura ***B9*** *que significa* ***"Línea de abonado interceptada"****. Lo que todavía no se ha podido determinar, quién era el beneficiario o beneficiarios de este sistema de escuchas. Un exfuncionario de SIGET afirma que en 1997, todavía dentro del viejo ANTEL había un grupo de técnicos dedicados a las escuchas quienes fueron trasladados a la Presidencia. Por ende, la hipótesis común es que existe un convenio secreto entre TELECOM y el Organismo de Inteligencia del Estado (OIE), una entidad civil creada por los acuerdos de paz y ubicada en la Presidencia, para hacer las interconexiones que hagan posible este trabajo de espionaje estatal. Este supuesto se hace más probable tomando en cuenta que el jefe de la OIE de aquel entonces,*

Mauricio Sandoval, es ahora jefe de la PNC, y el ex-presidente de ANTEL, es actual secretario técnico de la Presidencia.

Conforme el escándalo creció, la prensa reportó ya más de 1,000 números que supuestamente tienen esta codificación. Algunos de los números ya identificados pertenecen a:

Residencia del Ministro de Economía
Residencia del Jefe de Prensa de Casa Presidencial
Residencia del coordinador general del FMLN
Residencia de un diputado (y ex-presidente del Corte de Cuentas)
Residencia del presidente del Banco Desarrollo
Residencia del ex-presidente del Banco Central de Reserva
Radio Corporación Salvadoreña
Redacción del Canal 12
Despacho del Fiscal General
Sociedad "Entre Amigos" (una asociación de homosexuales)
Residencia del Editor General del Diario de Hoy
Residencia de Jorge Zedán, Presidente de SALTEL
Federación de Asociaciones de Sindicatos Independientes de El Salvador (FEASIES)
Asociación de trabajadores del Ministerio de Obras Públicas
Comisión de Derechos Humanos

Actualmente, la investigación de las escuchas ilegales sigue a cargo del Ministerio Público, todavía sin los resultados anunciados, hace tiempo, para octubre de 2000. Puede tener relevancia notar además, que, en medio del escándalo, Jorge Zaldán sufrió un secuestro temporal y desde entonces ha bajado mucho su perfil público.

Tanto por la eventual complicidad de las empresas de teléfonos como por la facilidad de intervención de teléfonos celulares (de amplio uso también en zonas rurales), la intervención telefónica no se descarta fuera de las zonas urbanas. De hecho, los mismos teléfonos comunitarios pueden ser intervenidos aunque signifique manejo voluminoso de información para los escuchas ilegales.

II.4.1 Medidas de protección contra escuchas telefónicas

a) No hablar asuntos confidenciales por teléfono. En las organizaciones pueden utilizar medidas sencillas y baratas para recordar a todas los trabajadores tener cuidado con lo que dicen por teléfono. Por ejemplo, se puede poner etiquetas en el auricular, o rótulos en la pared cerca del teléfono. También recordarlo en las reuniones con el equipo de trabajo. Debe ser práctica de proceso de inducción de personal de nuevo ingreso.

b) Hablar por teléfono de manera indirecta utilizando códigos previamente acordados. Por ejemplo, si quiere avisar a su familia de la hora de su llegada sin que lo sepan posibles atacantes. También debería evitarse las palabras que podrían activar los programas de búsqueda que utilizan los servicios de inteligencia, pero esto es difícil mientras no se sabe cuáles son.

c) Encriptar el teléfono. Siempre y cuando no haya una escucha oculta en la habitación o el teléfono mismo, la encriptación de la conversación telefónica es una medida extremadamente eficaz ya que la voz se convierte en señales digitales encriptadas. Para ello es necesario que ambos interlocutores utilicen la encriptación y tengan el software PGP phone que es gratis. En cuanto al equipo necesario, es básicamente un micrófono con auriculares (headset), por lo que no es muy caro. Esta tecnología requiere de una computadora con sistema Windows 95/98, FaxModem 33./ 56.6 Kbps, diadema con auricular y micrófono (este aparato se llama PGPFone) y el software de PGP. (Igualmente hay en venta algunos teléfonos encriptados, como el STU-III, pero relativamente caros todavía, y muchas veces se permite su venta únicamente a entidades gubernamentales.)

d) Para que la encriptación de la conversación telefónica asegure la privacidad, es esencial hablar desde un lugar seguro. El **sitio seguro** para hablar asuntos confidenciales por teléfono encriptado debe cumplir los mismos requisitos que el sitio seguro para reuniones: es decir, un lugar protegido y barrido, o bien un lugar no usual donde no habrá, por tanto, escuchas.

e) Usar un fax encriptado. Este presenta el mismo problema del teléfono encriptado, es decir, requiere que en ambos extremos de la comunicación tengan el aparato fax especial. Por esto, generalmente resultará más fácil usar correo electrónico encriptado. La ventaja en ambos casos (fax y correo electrónico) es que no se necesita hablar, por lo que los micrófonos ocultos no representan una amenaza.

f) Tener especial cuidado con su teléfono celular. Es más fácil de intervenir que un teléfono normal. En este caso la regla de oro es no usar el celular para discutir asuntos delicados, ya que cualquiera, hasta su vecino aficionado, le puede oír cuando lo desee.

g) Se puede comprar un aparato llamado balanceador de tensiones, el cual detecta caídas inusuales de tensión en la red durante una conversación (los pinchos restan de energía de las líneas), además este aparato puede generar un ruido constante que bloquea la activación de grabadores por VOX (detección de sonido). Hay que tener cuidado, sin embargo, de que no alteren el sistema de tarifas ya que pueden resultar en cargos telefónicos estrafalarios.

II.5 Intervención de correo electrónico y redes locales

En condiciones de uso normal debemos considerar que todos los mensajes que enviamos por correo electrónico son como tarjetas postales: están abiertos a la observación de cualquiera que tenga los medios técnicos apropiados. Otro problema clave es el de la autenticidad de los mensajes. Un operador entrenado puede apoderarse de su dirección de correo electrónico para enviar mensajes apócrifos. Con ello puede causar grave daño al hacernos aparecer como portadores de opiniones o mensajes de cualquier tipo incluyendo aquellos que resulten contrarios a nuestros objetivos[12].

Es muy fácil controlar o intervenir las comunicaciones electrónicas, ya que estas se guardan en el servidor de la compañía privada que nos proporciona el buzón de correo (mailbox) y por eso, las personas de este servicio que tienen acceso a nuestra cuenta, palabra clave. las pueden ver en cualquier momento y reenviarlos a terceras personas o utilizarlos si laboran para un servicio que espía la actividad de la institución. Los sitios gratuitos son peligrosos por estar vigilados por agencias de seguridad.

II.5.1 Medidas de protección contra intervención del correo electrónico o en la red local

a) Debe usarse la encriptación. La información encriptada parece una sopa de alfabeto, no se entiende en absoluto para traducirla solo lo puede hacer la persona que tiene la clave para desencriptarla. En este caso, aunque la información fuera interceptada, no puede ser leída ni descifrada. La encriptación del correo electrónico protege las comunicaciones, mientras un disco encriptado, protege los archivos, textos y bases de datos. El programa de computación más común para la encriptación, PGP, es amigable y además gratuito (ver sección adelante).

b) Debe usarse un servidor de correo electrónico fuera del país. Si bien contrata su conexión con el Internet como local, es aconsejable que las personas que tengan bajo su cuidado y custodia su buzón de correo, no sean locales y por lo tanto, hay mucho menos posibilidad de que un empleado o la empresa misma venda o reenvíe sus mensajes a un interesado local. Ahora, los servidores internacionales siempre pueden ser intervenidos por los servicios de inteligencia norteamericana, pero a lo mejor éstos no se interesan en los detalles de vida de un guatemalteco.

c) Instale un programa FireWall. Los Firewalls son sistemas de protección contra la intrusión en nuestro sistema de computación, por ejemplo, los ataques de los hackers o interesados en robar nuestra información personal o financiera. Los firewalls nos protegen de intrusos que se meten a través de nuestra conexión con

[12] Esto se ha utilizado recientemente en Guatemala, mediante el envío de amenazas a periodistas por correo electrónico, utilizando direcciones de otras personas.

Internet; son aconsejables para todo el mundo que se conecta, e indispensables para quienes tengan una red interna con acceso permanente a Internet. En este caso, si no se usan es prácticamente el equivalente de publicar todos tus archivos en la Internet. Podemos bajar de Internet un Firewall gratuito aunque su instalación y operación requiere entrenamiento accesible por medio de un técnico en redes informáticas; igual se puede comprar un aparato con la misma función a un precio algo más elevado.

III. ACCIONES INTIMIDATORIAS

III.1 Allanamientos Ilegales

Según la Constitución de Guatemala, las viviendas particulares y las oficinas son inviolables. Se puede penetrar en ellas sólo con orden de juez competente y dentro del horario de las 6:00 AM a las 6:00 PM. A pesar de ello existen cuerpos de control que actúan en la ilegalidad y que han perpetrado una serie de allanamientos en oficinas de ONG y miembros de la oposición. Han utilizado este método tanto para buscar información confidencial como para enviar un mensaje político de amenaza e intimidación con impunidad.

III.1.1 Medidas de Protección contra allanamientos ilegales

Las medidas de protección contra allanamiento son parecidas a las medidas contra robo. Primero se busca la disuasión, bajo la perspectiva de que el ladrón o el allanador van a buscar primero presas fáciles, y tal vez desistan de penetrar a un lugar donde va a ser más difícil y complicado hacerlo. Por otro lado, sabemos que, cuando algún ladrón quiere meterse de verdad, es muy difícil obstaculizarle del todo el acceso. Por lo mismo, hay que tomar otras medidas puramente en la línea de minimizar el daño que esta intrusión pueda hacer.

En zonas urbanas

a) Ubique su vivienda u oficina dentro de un vecindario o edificio que exija identificación a quienes entran.

b) Para las noches, o cuando todos van a estar ausentes del lugar por un período de tiempo largo, contrate un guardián o como mínimo utilice una máquina para encender y apagar las luces y un radio o un televisor.

c) Desarrolle buenas relaciones con sus vecinos, y pídales que le informen si observan alguna persona extraña frente a su casa u oficina. Igual, pida a los empleados mantenerse atentos e informar sobre movimientos raros, incluso de vendedores, encuestadores, mensajeros, cobradores, o cualquier persona ajena. No es raro observar vigilancia previa a una acción de esta naturaleza.

d) Ubique su oficina o vivienda en un segundo o tercer nivel, para poder reconocer fácilmente a los visitantes y dificultar el acceso por las ventanas. Instale puertas reforzadas y balcones en las ventanas. Asegúrese de que la entrada al edificio sea

bien iluminada y despejada de arbustos u otros escondites donde un asaltante podría ocultarse.

e) Mantenga una lista restringida de personas que tienen copia de las llaves. Si alguien pierde sus llaves, cambie los registros de inmediato. Instale cerraduras o chapas nuevas en casas recién alquiladas y cuando tema que alguna copia se haya extraviado.

f) Instale intercomunicadores electrónicos en las áreas de ingreso para poder preguntar la identidad de los visitantes sin tener que abrir primero la puerta. Para mayor seguridad, se puede instalar, además una cámara de vigilancia para así poder ver directamente desde el área de recepción a las personas que tocan. (Si no se puede costear el gasto de una cámara real, un aparato falso que cueste sólo Q300.00 puede ser un buen disuasivo.) Las cámaras de puertas del más reciente modelo ya no requieren cableado para funcionar.

g) Un disuasivo particularmente efectivo es la instalación de un sistema de doble puerta, cada uno con cerraduras eléctricas, (tipo "Trampa de Ratas"), en la entrada principal o única. Este sistema no permite abrir la segunda puerta hasta tanto no se ha cerrado la primera. Algunos sistemas requieren que una persona adentro de la oficina accione dos botones diferentes desde adentro, tanto para permitir la entrada, como para permitir la salida. De esta forma aun si personas no deseadas lograran entrar en la oficina, no podrán salir sin dejar alguien adentro que les facilitara la escapada, a no ser que haya una salida alternativa que puedan usar. De lo contrario, al tratar de salir, quedan atrapados entre las dos puertas, si no hay quien les accione la segunda puerta para salir. No obstante, este sistema presenta un inconveniente y es que para garantizar su efectividad al cien por ciento debe ser construido en un espacio blindado. Si lo que se teme es un ingreso violento, el sistema no funciona si está construido con rejas o estructura metálica o de otro material vulnerable a las armas de fuego.

h) No deje entrar a personas no esperadas que dicen que vienen de una compañía de servicios (tales como Telgua, Empagua, EEGSA o cualquier otra). A cualquier persona sospechosa, exíjale identificación y llame a la empresa para confirmar, antes de dejarla entrar.

i) Suponiendo que las personas interesadas, de todas maneras van a lograr penetrar a su casa u oficina, de allí hay que tomar medidas para proteger su información, dinero o, valores. Para la protección de la información física, desde luego se recomienda mantener los archivos con llave. Para la protección de la información computarizada, se recomienda que se instale en sus computadoras un disco encriptado (PGP Disk, que se usa para encriptar tanto archivos en el disco duro como los disquetes), o un Scram disk. De esta forma, aunque alguien logre acceso a su máquina o incluso se la lleve, no podrá entender nada de estos archivos o no podrá ni siquiera encontrarlos. De esta forma, usted logra mantener la privacidad de su información[13].

[13] SEDEM puede apoyar en el uso de estos programas. Si su organización se interesa por ellos, puede ponerse en contacto con las oficinas de SEDEM

j) Contra el riesgo de **perder** su información ante el robo, extracción o destrucción de una máquina, también es necesario hacer una copia de respaldo de los archivos y correo de su computadora cada semana, y depositarla en un lugar seguro, tal como una caja fuerte, fuera de la oficina, o en una cajilla de seguridad bancaria. Para hacer las copias de seguridad se recomienda la compra de una quemadora de CD y el uso de discos regrabables o en todo caso la de un aparato WinZip que facilita enormemente esta tarea.

k) Otra opción es que el respaldo de los discos encriptados puede depositarse en sitios seguros en la Web. En este caso es conveniente contratar el servicio de Internet por cable que está disponible en algunas partes de la ciudad (por US$ 80.00 al mes).

l) Otra alternativa es la compra de una computadora con disco duro removible, junto con una caja fuerte empotrada, en donde se guarda el disco durante las noches o durante un allanamiento mismo. También es de notar que las computadoras portátiles ofrecen la opción de llevarlas a la casa en la noche, de esta forma se resguarda parcialmente la información, aunque ofrece otros riesgos ya que fácilmente se arruinan o se las roban.

m) Instale una caja fuerte empotrada en el piso para que sea muy difícil de sacar y llevar. Puede usarla para guardar chequeras, papeles legales y otra información confidencial. Un robo o allanamiento puede afectar no solo la seguridad de una ONG, sino además su contabilidad y seguridad financiera.

n) Pensando en la posibilidad de un allanamiento ilegal cuando haya personas presentes en la oficina o vivienda, se debe convertir parte de su casa u oficina en un refugio seguro, desde donde pueda protegerse de una agresión y pedir ayuda. Se refiere a un cuarto interior con puertas reforzadas, que cuenta con teléfono o celular. Igualmente pueden revisarse anticipadamente algunas posibles rutas de escape por puertas traseras, patios vecinos, etc.

o) Puede ocurrir un allanamiento subrepticio, es decir que la persona o la institución no se percaten de que alguien hayan entrado a su residencia u oficina, con el objetivo de registrar, copiar o llevarse información. En este caso, es aconsejable dejar señas que permitan detectar que alguien entró en nuestra ausencia. Igualmente, en la mañana deben revisarse la hora de creación y modificación de archivos, de conexión con Internet, para saber si alguien ingresó a las computadoras.

En zonas rurales

a) Trate de que su vivienda u oficina esté en un área que le permita control sobre visual sobre las personas que se acercan al lugar.

b) Para las noches, o cuando todos van a estar ausentes del lugar por un período de tiempo largo, contrate un guardián o como mínimo (si hay acceso a energía eléctrica), utilice una máquina para encender y apagar las luces y un radio o un televisor.

c) Desarrolle buenas relaciones con sus vecinos, y pídales que le informen si observan alguna persona extraña frente a su casa u oficina. Igual, pida a los empleados mantenerse atentos e informar sobre movimientos raros, incluso de vendedores, inspectores, turistas, encuestadores, mensajeros, cobradores, o cualquier persona ajena. No es raro observar vigilancia previa a una acción de esta naturaleza.

d) En la medida de las posibilidades, instale puertas reforzadas y balcones en las ventanas. Asegúrese de que la entrada sea bien iluminada y despejada de arbustos u otros escondites donde un asaltante podría ocultarse.

e) Mantenga una lista restringida de personas que tienen copia de las llaves. Si alguien pierde sus llaves, cambie los registros o candados de inmediato. Instale cerraduras o chapas nuevas en casas recién alquiladas y cuando tema que alguna copia se haya extraviado.

f) No deje entrar a personas no esperadas que dicen que vienen de una compañía de servicios (tales como Telgua, Empagua, EEGSA o cualquier otra). A cualquier persona sospechosa, exíjale identificación y llame a la empresa para confirmar, antes de dejarla entrar.

g) Suponiendo que las personas interesadas, de todas maneras van a lograr penetrar a su casa u oficina, de allí hay que tomar medidas para proteger su información, dinero o, valores. Para la protección de la información física, desde luego se recomienda mantener los archivos con llave. Para la protección de la información computarizada, se recomienda que se instale en sus computadoras un disco encriptado (PGP Disk, que se usa para encriptar tanto archivos en el disco duro como los disquetes), o un Scram disk. De esta forma, aunque alguien logre acceso a su máquina o incluso se la lleve, no podrá entender nada de estos archivos o no podrá ni siquiera encontrarlos. De esta forma, usted logra mantener la privacidad de su información[14].

h) Contra el riesgo de perder su información ante el robo, extracción o destrucción de una máquina, también es necesario hacer una copia de respaldo de los archivos y correo de su computadora cada semana, y depositarla en un lugar seguro, tal como una caja fuerte o fuera de la oficina. Para hacer las copias de seguridad se recomienda la compra de una quemadora de CD y el uso de discos regrabables o en todo caso la de un aparato Zip que facilita enormemente esta tarea.

i) Otra alternativa es la compra de una computadora con disco duro removible, junto con una caja fuerte empotrada, en donde se guarda el disco durante las noches o durante un allanamiento mismo. También es de notar que las computadoras portátiles ofrecen la opción de llevarlas a la casa en la noche, de esta forma se

[14] SEDEM puede apoyar en el uso de estos programas. Si su organización se interesa por ellos, puede ponerse en contacto con las oficinas de SEDEM.

resguarda parcialmente la información, aunque ofrece otros riesgos ya que fácilmente se arruinan o se las roban.

j) Instale una caja fuerte empotrada en el piso para que sea muy difícil de sacar y llevar. Puede usarla para guardar chequeras, papeles legales y otra información confidencial. Un robo o allanamiento puede afectar no solo la seguridad de una ONG, sino además su contabilidad y seguridad financiera.

k) Pensando en la posibilidad de un allanamiento ilegal cuando haya personas presentes en la oficina o vivienda, se debe convertir parte de su casa u oficina en un refugio seguro, desde donde pueda protegerse de una agresión y pedir ayuda. Se refiere a un cuarto interior con puertas reforzadas, que cuenta con teléfono o celular. Igualmente pueden revisarse anticipadamente algunas posibles rutas de escape por puertas traseras, patios vecinos, etc.

l) Puede ocurrir un allanamiento subrepticio, es decir que la persona o la institución no se percaten de que alguien hayan entrado a su residencia u oficina, con el objetivo de registrar, copiar o llevarse información. En este caso, es aconsejable dejar señas que permitan detectar que alguien entró en nuestra ausencia. Igualmente, en la mañana deben revisarse la hora de creación y modificación de archivos, de conexión con Internet, para saber si alguien ingresó a las computadoras.

III.2 Vigilancia y seguimiento

Los delincuentes y los agentes de los aparatos de control no siempre dan señales antes de actuar, al efectuar operativos de vigilancia que les sirven para preparar alguna intervención. Sin embargo, es posible percatarse de algunos movimientos previos a los que debe prestarse atención. Para estas operaciones es común usar agentes encubiertos que se disfrazan y se ubican alrededor de las oficinas o viviendas que vigilan, o dentro de ellas: vendedores ambulantes, encuestadores, personas desconocidas que solicitan su apoyo, personal de servicios, empleados de la compañía telefónica o de la luz eléctrica y otros.

Hay acciones de vigilancia que combinan ambas funciones, de recoger información pero también infundir miedo y preocupación, como una forma de acoso psicológico hacia las y los trabajadores de derechos humanos. Por ejemplo, hay una diferencia entre el impacto de la vigilancia realizada por parte de agentes encubiertos, y la vigilancia realizada por parte de un grupo de hombres fuertemente armados, quienes se estacionan frente a una oficina o una casa. En el segundo caso, a la vez de ser una actividad de espionaje, el grupo de acosadores tiene el objetivo concreto de intimidar a todas las personas que entran y salen del lugar.

III.2.1 Medidas de protección contra vigilancia

Las medidas de protección contra la vigilancia externa incluyen, además de las medidas contra intervención de las comunicaciones, explicadas en secciones anteriores, las siguientes:

a) No proporcionar, ni usted ni las personas con las que se relaciona o trabaja, información acerca de sus horarios de llegada y salida, así como detalles que faciliten su vigilancia.

b) Coloque cortinas o persianas y no ubique teléfonos, computadoras o salones de reunión, cerca de ventanas desde donde puedan ser monitoreadas electrónicamente.

c) Esté alerta y tome nota de la presencia de personas sospechosas en el vecindario. Es conveniente que estas personas se den cuenta que usted se mantiene alerta. Si la vigilancia es obvia, puede tomar fotos y anotar una descripción detallada de las personas que le observan. Lo mejor es usar una cámara digital para permitir la reproducción de la imagen por computadora, y tener una lente telefoto para sacar las caras a distancia. Igual puede tomarse un video de todos los asistentes a algún evento donde se teme infiltración.

d) Tome nota inmediata (apúntelos), de los modelos y las placas de los carros que parecen sospechosos. Trate de identificar los patrones de conducta de los vigilantes. Tome nota de los carros que arrancan cuando usted pasa cerca. Utilice vías no rutinarias para confirmar si le están siguiendo. En la medida de lo posible, lleve a cabo un chequeo de seguimiento con alguien de su confianza. Póngase de acuerdo con alguien de su confianza, en cuanto a la ruta que seguirá y la hora que dará inicio su partida. Salga según lo convenido y llegue al punto establecido, permitiendo que la persona de apoyo chequee toda la ruta a fin de verificar si hubo o no seguimiento a su persona.

e) Si teme que su correspondencia esté siendo interceptada, omita el nombre del remitente en la enviada, y utilice códigos o nombres abreviados en lugar del nombre completo del receptor. También se pueden utilizar direcciones alternativas, que tienen menos posibilidad de ser controladas, para enviar y recibir material escrito. Es necesario ponerse de acuerdo con la otra persona antes de utilizar estos métodos.

f) Si decide mantener la confidencialidad de la dirección de su casa, hay que tomar varias medidas tales como: no debe dar su dirección a nadie fuera de su familia inmediata (y pedirles que no la den a nadie sin su consentimiento); establecer una dirección alternativa para recibir correspondencia; cuidar que nadie le esté vigilando al entrar y salir de su casa; debe solicitar que otra persona firme el contrato de alquiler y servicios. No pida servicio a domicilio o de taxi con su nombre, por ninguna circunstancia.

g) Se debe cuidar la basura:

- Destruya manual o mecánicamente todos los documentos sensibles de trabajo, utilizando una trituradora eléctrica de papel o la incineración.
- Destruya los diskettes que desea tirar, rompiéndolos o quemándolos
- Cuando elimina un archivo, haga una "wipe", limpieza, para asegurar su borrado definitivo de la computadora. Recuerde que hay programas especiales para reconstruir archivos eliminados.

III.3 Hostigamiento y amenazas

Las amenazas son aquellas acciones de abuso psicológico que dan a entender que la violencia u otro daño, como el encarcelamiento, la muerte o cargos criminales falsos, se ejecutarán si no se toman ciertas acciones. Pueden ser dañinas en sí mismas ya que provocan miedo, y también pueden preceder a actos violentos.

El recurso de la amenaza es la medida más barata que pueden usar los aparatos de control para neutralizar y obstaculizar nuestra actividad. Hay múltiples acciones que no parecen tener otro fin que asustar y hostigar a la persona afectada. De vez en cuando llevan a más, pero a la vez los líderes más destacados de los derechos humanos, así como periodistas y operadores de justicia, han convivido con amenazas constantes durante meses y años de su vida.

Aparecer en un listado de personas que van a ser asesinadas por un grupo que actúa en la clandestinidad, provoca distintas reacciones de temor no sólo en los afectados, sino en sus organizaciones, en sus familiares y en sus amistades. En Guatemala hay antecedentes de ejecuciones de personas que aparecieron en listados de amenazados de muerte. Entonces, un acontecimiento exterior a la vida normal, que viene a ser repentino e inesperado, perturba el sentido de control de cada uno, se percibe una amenaza a la vida y puede generar desequilibrios físicos o emocionales si no se enfrenta de manera organizada, para que las reacciones evolucionen con el tiempo.

III.3.1 Medidas de protección contra amenazas

a) Trate de determinar de dónde vino la amenaza, y hacia quien está orientada. Hay que saber si la amenaza tiene el fin de detener las actividades de una sola persona, o de toda la organización. Si la amenaza se dirige a una persona en particular, habrá que tomar medidas muy específicas para protegerla. Si se dirige a toda la organización, las medidas han de ser diferentes y más dispersas.

b) En casos de hostigamiento o amenazas telefónicas, puede ser útil un sistema de identificación de llamadas, -CALLER ID- en el cual el número de la persona que

hace la llamada aparece en el teléfono receptor (si no está bloqueado). Este servicio se puede contratar a través de Telgua, y se puede comprar un teléfono apropiado o el aparato especifico. Este servicio no está disponible en todos los lugares del país, únicamente donde operan redes alámbricas digitales. Averigue si también está disponible el servicio de protección contra bloqueo. Es decir que, si un número tiene bloqueada su identidad no puede completar la llamada a su línea, a menos que libere el bloqueo.

c) Mantenga un registro de todas las amenazas. Comparta esta información con otros grupos para entender qué puede estar pasando. Un aumento repentino en las amenazas hacia cierto grupo, o cierto sector, puede preceder actos violentos más severos. El registro de las amenazas requiere la anotación de fecha, hora, lugar y tipo de amenaza (escrita, oral directa, telefónica, otra). Recuerde que por cada tipo, debe anotar las características de la misma. Por ejem plo, si es telefónica, número en el que se recibe y número –si está disponible- desde el que se transmite. Tipo de voz, masculina, femenina, infantil, distorcionada o fingida, grve, aguda. Forma de habla, lenta, rápida, normal. Tipo de acento. Si es escrita, tipo de papel, tipo de letra, tipo de escritura, gramática, sintaxis y ortografía.

d) Si está recibiendo amenazas por teléfono, instale una máquina contestadora para revisar de quién es la llamada antes de responder. Algunas máquinas además permiten grabar la conversación, de esta forma si uno reaccionara con mucha rapidez, incluso podría grabar parte misma de la amenaza.

III.4 Ataques físicos y secuestros

Lamentablemente el secuestro económico en Guatemala es del todo común, igual el robo violento y el ataque físico, lo que incluye en no pocos casos, hasta la ejecución. Aunque uno espera que la actividad política, periodística o de derechos humanos no le cueste la vida, en este país siempre queda presente tal alternativa. Peor aún, aquí se encuentra la barbaridad del ataque a los familiares del blanco principal. Por lo tanto, es sensato que no sólo uno mismo, sino otros familiares cercanos, tomen medidas básicas de protección contra el ataque físico y el secuestro.

III.4.1 Medidas de protección contra ataques físicos y secuestros

A). En el vehículo:

a) Si al ir por la calle un vehículo se detiene para hacerle alguna pregunta, desconfíe y no se acerque. Aléjese en dirección contraria. No camine ni maneje solo o sola de noche.

b) Antes de entrar en su carro o en cualquier vehículo, compruebe que no se encuentre nadie escondido en el asiento de atrás. Trate de no dejar el vehículo estacionado en la calle, es preferible dejarlo en un parqueo vigilado y preste atención y compruebe que no haya vagabundos en los alrededores.

c) No le dé aventón a nadie en su carro ni se ofrezca para ayudar si parece que alguien sufrió una avería, ya sea un hombre o mujer.

d) Si viaja en su carro y nota seguimiento amenazante: 1) Aumente la velocidad y trate de no parar hasta llegar a un lugar seguro. 2) No permita que le fuercen a salir de las calles y caminos transitados; al entrar a una calle solitaria es más fácil que le ataquen con impunidad. 3) Si se encuentra en peligro, llame la atención gritando o haciendo sonar la bocina de su automóvil.

e) Cambiar de carro cuando sea posible (a través de la rotación en los automóviles institucionales). No use un carro que es muy identificado con su trabajo, para actividades familiares o personales.

f) Lleve consigo celular para llamar pidiendo auxilio en estos casos de emergencia

g) Conducir con los vidrios subidos y los seguros de las puertas puestos. Busque estacionar en lugares bien iluminados y no en la calle.

h) Mantener el vehículo en buen estado, con suficiente gasolina para un viaje largo. No quiere que falle justo cuando más lo necesita.

i) Evitar caminos oscuros y poco transitados tanto a pie como viajando en carro. Reconocer acontecimientos que pudieran preceder a un ataque, tales como: un bloqueo o una persona en el camino que le fuerce a parar el carro; desviaciones extrañas en el camino que le hagan tomar una ruta más aislada.

j) No permitir que su vehículo sea rodeado fácilmente; dejar por lo menos 4 metros de distancia entre su carro y el siguiente y mantener salidas de emergencia.

B). AL DESPLAZARSE

a) Si teme un ataque, manténgase atento a su entorno. Camine alejado de las paredes, pues en alguna puerta puede esconderse alguien y agredirlo, y si necesita abordar un taxi, utilice únicamente taxistas conocidos, o taxis de sitio que responden a su llamado telefónico y cuentan con localizadores y radio.

b) Si al ir por la calle un vehículo se detiene para hacerle alguna pregunta, desconfíe y no se acerque. Aléjese en dirección contraria. No camine ni maneje solo o sola de noche.

c) Si en la calle usted nota vigilancia y seguimiento, busque entrar a una tienda o lugar donde haya muchas personas (si va a pie), o a una gasolinera bien iluminada (si va

en vehículo). Espere adentro para ver si la persona desaparece. Y avise por teléfono a personas que le pueden prestar apoyo.

d) Lleve consigo celular para llamar pidiendo auxilio en estos casos de emergencia.

e) Si considera que está en mucho peligro de ser atacado, siempre vaya acompañado, no será blanco fácil entre varias personas. Evite viajar sin compañía cuando está bajo amenaza directa.

f) Variar sus rutas y rutinas. La mayor parte de los incidentes ocurren al salir o regresar a la casa. No realice actividades fijas a la misma hora todas las semanas. Varíe sus horarios.

g) Evitar caminos oscuros y poco transitados tanto a pie como viajando en carro. Reconocer acontecimientos que pudieran preceder a un ataque, tales como: un bloqueo o una persona en el camino que le fuerce a parar el carro; desviaciones extrañas en el camino que le hagan tomar una ruta más aislada.

C). CON EL TELÉFONO

a) Lleve consigo celular para llamar pidiendo auxilio en estos casos de emergencia.

b) No hablar por teléfono de los horarios de sus actividades y otra información que haría más fácil ubicarle en un lugar inseguro. Si es necesario dar información por teléfono cuando el riesgo es muy alto, establecer códigos con sus familiares y colegas.

D). ACCIONES DE PREVENCIÓN

a) Debe mantener un plan con su familia en caso de una separación por emergencia. Por ejemplo, los familiares deben tener todos sus datos personales importantes, información médica y dental, acceso a sus ahorros, información de contactos para sus colegas, entre otras.

b) Igualmente, mantenga sus asuntos en orden para la seguridad de su familia. Asegúrese de que todos sus negocios y papeles importantes estén al día, incluyendo: testamentos; certificados de nacimientos y de matrimonio; poderes legales sobre propiedades y otros bienes; contratos de seguros; recibos de impuestos; beneficios de alimentación; constancia de su membresía en grupos, planes de pensiones; datos precisos sobre deudas por pagar o por cobrar.

c) Mantenga un pasaporte vigente, con las visas necesarias para salir del país. En caso que no los tenga, puede viajar sin problemas a El Salvador y Honduras. Es útil desarrollar y mantener contactos en el extranjero. Se puede pedir que estas personas le proporcionen cartas de invitación que justifiquen una salida repentina si fuera necesario; igual podrían proporcionar vivienda para unas semanas o meses en caso necesario.

d) Mantener una tarjeta de crédito con saldo suficiente para comprar un boleto de salida o cubrir otros gastos de emergencia, es importante.

e) Trabajar en coordinación con otras personas e instituciones que tienen menos posibilidad de sufrir ataques. Por ejemplo, si se trata de una investigación de campo, en un lugar donde hay mucho peligro, se puede organizar una pequeña delegación para la visita, e invitar autoridades locales, acompañantes internacionales, y otras personas conocidas.

f) Crear una red de apoyo y/o de contactos en los lugares a donde se piensa viajar, que no sean cercanos a su organización. Estas personas pueden ayudar en el caso de una emergencia, o pueden dar información sobre la situación de seguridad cuando sea necesario. Si es posible, desarrollar relaciones con las autoridades locales, éstas también pueden ayudar en un momento de crisis o amenaza.

g) Tener a mano un listado de números de emergencia (es importante que todas las personas que trabajan en las organizaciones de DDHH tengan esta información, aunque no están bajo amenaza o control directo). Esta lista puede incluir números de observadores nacionales e internacionales, tales como la PDH y Minugua, personas de su red de apoyo, abogados y jueces solidarios, embajadas, autoridades del gobierno, e instancias gubernamentales, tales como la Policía Nacional Civil y el Ministerio Público.

h) Establecer y proporcionar medios de comunicación que sirvan de enlace entre las personas de su organización que trabajan en el campo y la ciudad. Por ejemplo: se puede definir un horario para enviar mensajes por radio; comprar teléfonos celulares y/o localizadores (*bipers*); desarrollar relaciones con otras ONG o grupos que tienen radios de comunicación directa.

i) En el caso de que otra persona en su organización sufra de un secuestro o una detención extrajudicial, es importante investigar para dar con su paradero, incluyendo un trámite escrito de habeas corpus (Exhibición personal).

j) Se pueden solicitar medidas cautelares a la OEA.

E). EN CASA U OFICINA

a) Observar bien su alrededor y las personas. Tome nota en particular de las personas (personal de servicios, vendedores ambulantes) que se encuentren alrededor de su casa u oficina, o en los lugares congestionados de su camino para confirmar que su labor sea real. Tenga cuidado con cualquier persona que no parezca genuina o cuya presencia es fuera de lo común.

b) Antes de salir del carro, residencia, u oficina se debe observar la calle para detectar personas sospechosas. Si siente inseguridad, es mejor utilizar otra salida o estacionar su vehículo en otro lugar.

c) No dar entrevistas en privado con personas desconocidas que dicen ser periodistas o que utilizan pretextos para verle a solas.

d) Tener a mano un listado de números de emergencia (es importante que todas las personas que trabajan en las organizaciones de DDHH tengan esta información, aunque no están bajo amenaza o control directo). Esta lista puede incluir números de observadores nacionales e internacionales, tales como la PDH y Minugua, personas de su red de apoyo, abogados y jueces solidarios, embajadas, autoridades del gobierno, e instancias gubernamentales, tales como la Policía Nacional Civil y el Ministerio Público.

IV. CÓMO ENFRENTAR EL ESPIONAJE Y LA INTIMIDACIÓN

IV.1 Medidas y equipos básicos de seguridad

Antes de proceder a la adopción de medidas o la compra de equipos de seguridad, es importante estudiar las amenazas específicas y la utilidad de las medidas propuestas para contrarrestarlas. Es necesario introducir el aspecto relativo a la seguridad y protección en las instituciones, tanto con el objeto de garantizar que existan elementos coordinados para la protección institucional como del personal.

Estas medidas generales tendrán que adaptarse a la situación de cada persona y servirán para elaborar un plan de seguridad que deberá cumplirse con disciplina, rigurosidad y creatividad en tiempos difíciles. Como regla general para preservar la seguridad, se debe evitar situaciones peligrosas, como trasnochar, frecuentar lugares donde la delincuencia es alta, intervenir en riñas en la calle o cualquier otra situación de riesgo innecesario a la labor que realizamos.

En el actual momento se considera una necesidad invertir parte de nuestro presupuesto institucional en el aspecto de la seguridad y protección. Debemos contemplar gastos que aunque pequeños, deben cargarse a nuestros Proyectos, tal el caso de una caja fuerte para documentos importantes, accesorios para encriptar la información en las computadoras, teléfonos celulares para emergencias, cambios de registros a las cerraduras de puertas de entradas y salidas, circuito cerrado de televisión, máquina trituradora de papel. En fin, aquellas cuestiones que mejoran nuestro nivel de seguridad en el trabajo y cuya adquisición no debe considerarse superflua.

En la sección de anexos encontrarán un listado de algunos equipos básicos que las instituciones podrían considerar en sus presupuestos de seguridad.[15]

IV.2 La seguridad informática

El uso de los medios electrónicos de información como el correo electrónico e Internet, entre otros. impone nuevos retos a la seguridad y privacidad de las comunicaciones.

[15] Ver sección V.Anexos.

Contrario a la aparente privacidad de estar uno sólo con la computadora, viendo la Internet o enviando y recibiendo mensajes, es muy fácil para cualquier intruso (hacker) o agente de inteligencia gubernamental penetrar en el sistema de correo electrónico o en nuestras computadoras vía su conexión con el Internet, y saber todo el contenido de nuestras comunicaciones y ficheros electrónicos.

El correo electrónico y la Internet también imponen el reto de cómo identificar con seguridad la autoría y la integridad de un mensaje. La Fundación Rigoberta Menchú tuvo una situación en el año 2,000, en donde personas desconocidas enviaron, a nombre de la Fundación, un mensaje falso en correo electrónico relacionado con el caso judicial en España. Otros hechos similares se han repetido en 2002. De manera que, asegurar la identidad del remitente, es fundamental.

Por lo tanto, no solo para proteger las comunicaciones sino toda la información electrónica, es necesario establecer en cada institución una política de seguridad informática.

Esta política, de obligatorio cumplimiento para el personal, incluirá los procedimientos, niveles de acceso y tipo de programas a utilizar. Incluirá inspecciones de prueba y efectividad de los procedimientos.

Dicha política debería contener, como mínimo, lo siguiente:

a) Inventario de equipo informático y periférico

b) Niveles de acceso a equipo (uso de password o passfrase)

c) Programas instalados, por equipo y, de ser el caso, licencias

d) Sistemas Firewall cuando haya red interna o internet permanente

e) Disco de seguridad

f) Programación de copias de respaldo de los archivos electrónicos

g) Medios de protección electrónica
    i. Discos virtuales
    ii. Encriptación

IV.2.1 La Codificación de la información

Codificar la información electrónica es emplear recursos informáticos que imposibiliten la lectura de los datos personales o institucionales, por parte de personas no autorizadas.

Puede hacerse por medio de la encriptación de los mensajes o textos o por medio de la creación de discos virtuales encriptados.

El programa más seguro para encriptación es el PGP, en tanto para discos virtuales es el Scramdisk. Aunque hay otros programas, en esta guía desarrollamos solo estas dos opciones.

IV. 2.2 Preguntas y respuestas frecuentes sobre seguridad. Algunas ideas[16].

Últimamente, por donde usted vaya, alguien está hablando de la seguridad de las computadoras. Proteja su red, proteja su información. ¿Qué es lo que realmente tiene que proteger?¿Tiene que preocuparse por sus usuarios? ¿Es usted vulnerable a los piratas informáticos (hackers)? ¿Quién debiera instalar qué? ¿Qué debe hacer? ¿Son realmente necesarias todas estas precauciones de seguridad?

La respuesta es un resonante SÍ.

Existen riesgos de seguridad asociados con las redes de área locales (LANs), servidores, acceso remoto, computadoras personales de casa, computadoras portátiles (laptops), el Internet, el correo electrónico y la lista continúa. ¿Qué puede usted hacer para asegurarse de que su red es lo más segura posible? El siguiente es un grupo de preguntas y respuestas frecuentes para responder a algunas de sus dudas.

1. ¿Qué es una buena codificación?

Ésta depende de su sistema y de sus actividades, pero generalmente, todo el mundo debiera tener:

- Una pared de fuego (firewall)
- Codificación del disco
- Codificación del correo electrónico que también realice firmas digitales – si usted no sabe qué más usar, utilice el PGP
- Programas de detección de virus
- Copia de seguridad segura – correo electrónico a un sitio seguro y copia de seguridad (backup) de todos los materiales en forma semanal al CDRW, luego guardarlo en un lugar separado y seguro.
- Grandes contraseñas que no puedan ser adivinadas
- Una jerarquía de acceso – no todo el mundo en la organización necesita tener acceso a todos los archivos.

[16] To9da esta parte es incluida en la guía por contribución de Privaterra, CPSR, de Canadá.

- Consistencia – ninguna de las herramientas funcionará si usted no las usa todo el tiempo.

2. ¿Cuál NO es una buena codificación?

Colocar un archivo en un ZIP no lo codifica. Ese archivo puede ser abierto y leído en unos pocos segundos.

3. ¿Cómo se elige cuál programa (software) de codificación usar?

Usted por lo general le pregunta a sus amigos… y lo confirma con nosotros. Necesita comunicarse con ciertas personas y grupos, de manera que si están utilizando un sistema específico de codificación, usted debiera utilizar el mismo sistema para facilitar las comunicaciones. Sin embargo, comuníquese antes con nosotros. Algunos programas simplemente no realizan un buen trabajo mientras que otros se ofrecen como los llamados "Ollas de Miel". Usted es seducido para utilizar los programas gratuitos y aparentemente excelentes que ofrecen precisamente quienes quieren espiarlo. ¿Cómo puede usted leer mejor sus comunicaciones más vulnerables que siendo el supervisor de su propio programa de codificación? Aun así, existen muchas marcas con buena reputación tanto de programas de propietario como gratuitos. Simplemente recuerde investigar antes de utilizarlos.

4. Si tengo una pared de fuego (firewall), ¿por qué necesito codificar mi correo?

Las paredes de fuego evitan que los "hackers" tengan acceso a su disco duro y a su red, pero una vez que usted envía un correo por el Internet, éste está abierto al mundo. Necesita protegerlo antes de enviarlo.

5. ¿Por qué necesitamos codificar el correo y los documentos todo el tiempo?

Si usted solamente utiliza la codificación para asuntos delicados, quienes lo están vigilando a usted o a sus clientes, pueden inferir cuándo está ocurriendo alguna actividad crítica…y probablemente tratarán de interferir en esos momentos. Aunque no puedan leer sus comunicaciones codificadas, pueden decir si los archivos están codificados o no. Un aumento repentino en su codificación podría provocar una redada. De hecho, es mejor asegurar que todo el tráfico de sus comunicaciones fluya en forma pareja. Mande correo electrónico codificado en intervalos regulares, aun cuando no haya nada nuevo sobre qué informar. En esta forma, cuando usted necesita enviar información delicada, será menos notorio.

6. Nadie está allanando esta oficina, de manera que ¿para qué necesito utilizar programas de privacidad?

En primer lugar, usted no sabe si alguien está allanando su sistema o si alguien está filtrando información. Sin comunicaciones codificadas, sin seguridad física, sin protocolos de privacidad, cualquiera puede estar teniendo acceso a sus archivos, leyendo su correo y manipulando sus documentos sin que usted lo sepa. Seguro, sus comunicaciones abiertas pueden poner a otros en riesgo en lugares donde es probable que ocurran redadas con

motivación política. Si usted cierra con llave sus puertas, usted debe codificar sus archivos. Así de simple.

7. ¿Cómo puedo saber si mi sitio en la Red ha sido intervenido?

Una pared de fuego le puede decir si alguien ha intentado ingresar a su sistema. Para mayor seguridad, no ponga información delicada en su sitio en la Red – aun en áreas protegidas por una contraseña.

8. No tenemos acceso a la Internet, de manera que tenemos que utilizar un Café Internet. ¿Cómo podemos proteger las comunicaciones que enviamos desde una computadora externa?

Todavía puede codificar su correo y sus archivos. Antes de ir al Café Internet, codifique cualquier archivo que desee enviar por correo electrónico y cópielo en forma codificada en su diskette o CD. En el Café Internet, suscríbase a un servicio de codificación tal como Hushmail.com o a un servicio de anonimato tal como Anonymizer.com, y utilícelos cuando envíe su correo. Asegúrese de que las personas que reciben sus comunicaciones también se hayan suscrito a estos servicios.

9. Si es tan importante asegurar nuestros archivos y comunicaciones ¿por qué no todo el mundo lo hace?

Esta tecnología es relativamente nueva pero su uso se está difundiendo. Los bancos, las empresas multinacionales, las agencias de noticias y los gobiernos la usan, reconociendo que es una inversión sana y un costo necesario al hacer negocios. Las ONGs se encuentran en mayor riesgo que las empresas a quienes la mayoría de los gobiernos aceptan con gusto. Las ONGs probablemente sean blancos de vigilancia de manera que deben ser mucho más ágiles y activos en implantar la tecnología. El enfoque para quienes trabajan en derechos humanos es proteger a individuos y grupos que son perseguidos. Para hacerlo, mantienen archivos con información que los identifica y con su ubicación. Si estos archivos son allanados, estos individuos podrían ser asesinados, torturados, secuestrados o “convencidos” para que no ayuden más a la ONG. La información de estos archivos también puede ser usada como evidencia contra la ONG y sus clientes en persecuciones políticas.

10. Uno de nuestros principios es la apertura. Estamos cabildeando para tener mayor transparencia de parte del gobierno. ¿Cómo podemos usar la tecnología de privacidad?

La privacidad es consistente con la apertura. Si el gobierno desea pedirles abiertamente sus archivos, puede hacerlo a través de procedimientos apropiados y reconocidos. La tecnología de privacidad evita que las personas tengan acceso a su información en una forma clandestina.

11. Seguimos todos los protocolos de privacidad y de seguridad y aun así nuestra información se está filtrando -- ¿qué pasa?

Puede ser que usted tenga un espía dentro de su organización o puede tener a alguien que simplemente no puede mantener la información confidencial. Reorganice su jerarquía de información para asegurarse de que menos personas tengan acceso a la información delicada –y mantenga un ojo especialmente vigilante sobre esas pocas personas.

Algunas ideas:

Aquí hay once maneras de protegerse usted y la privacidad y la seguridad de su organización en la línea. Ponga en práctica tantas de ellas como usted y su organización puedan y siéntase en libertad de llamar a Privaterra para que le ayude con cualquier cosa que usted no pueda hacer.

1. No conteste correos no solicitados y nunca abra adjuntos de correo electrónico que no haya solicitado, sin antes verificar al remitente. Si usted no lo estaba esperando, no lo descargue. Muchos virus y troyanos se diseminan como "gusanos" y los gusanos de los modems a menudo parecen ser enviados por alguien que usted conoce. Los gusanos inteligentes revisan su libreta de direcciones y la replican disfrazándose como adjuntos legítimos de contactos legítimos. El PGP – firmar sus correos, tanto con adjuntos como sin ellos, puede reducir en gran medida la confusión sobre adjuntos libres de virus que usted envíe a sus colegas.

2. Instale los dispositivos de seguridad más recientes para todos los programas que utilice, especialmente Microsoft Office, Microsoft Explorador de Internet y Netscape. La amenaza más grande a la seguridad se encuentra dentro de los programas y los equipos entregados con vulnerabilidad conocida. Mejor aun, considere cambiarse a unos programas de Fuente Abierta, que no descansen en el modelo "Seguridad por medio de la Obscuridad", pero que acepta a los expertos en seguridad y a los "hackers" por igual para verificar rigurosamente todos los códigos.

3. Asegúrese de mantener y probar con regularidad las copias de seguridad (backups). Asegúrese de que éstos están seguros, manteniéndolos en un disco duro codificado, con una organización de copias de seguridad de los datos que sea segura, o bien que estén asegurados por cerraduras físicas sofisticadas.

4. Ponga en práctica programas de detección de virus y asegúrese que los mismos sean actualizados con frecuencia, como mínimo cada mes, en cada componente de la red. Constantemente están siendo creados o descubiertos nuevos virus (refiérase a la Biblioteca de Información de Virus (vil.nai.com). Debiera incorporar actualizaciones mensuales en el calendario de su organización si usted no tienen un administrador de la red a tiempo completo que maneje las actualizaciones del antivirus. La biblioteca VIL también le da detalles sobre cómo eliminar un virus de su computadora, una vez que ésta haya sido infectada.

5. Confíe solo en profesionales capacitados y certificados para que se hagan responsables de asegurar su red. Si no conoce a ninguno, Privaterra puede ayudarle directamente o buscando a alguien en su área local que sea competente y confiable.

6. Actualice a todos los navegantes en la red para que soporten la codificación de 128 bits. Esto ayudará a salvaguardar cualquier información que usted desee pasar con seguridad a través de la red, incluyendo contraseñas y otros datos sensibles presentados en formularios.

7. Si usted no desea proporcionar información en un formulario en línea, con la cual usted no se sentiría cómodo proporcionándola por teléfono, no lo haga.

8. Asegúrese que todos sus accesorios y aparatos tales como las impresoras sean seguros – pueden ser usados para acomodar a "hackers" y sus ataques en su red.

9. Elabore una política fuerte para las computadoras, hacia todos los usuarios que manejan material de trabajo en su organización, en su casa y en el camino. Esto debe incluir políticas para las contraseñas, el uso del Internet, el correo electrónico, seguridad de los datos, paredes de fuego, programas antivirus y más.

10. Usted necesita una pared de fuego: Las personas que usted puede conocer o no conocer, en cualquier parte del planeta, pueden ingresar a su computadora aun ahora. Pueden estar leyendo, alterando o borrando cualquiera de sus archivos. Existen numerosos paquetes de programas con paredes de fuego disponibles. La red de su oficina puede ya estar protegida, pero no se olvide de su computadora portátil (laptop) cuando usted sale de viaje o la computadora de su casa. Para los usuarios novatos, sugerimos Zone Alarm de los Laboratorios Zone (www.zonelabs.com). Para usuarios más experimentados, sugerimos "Tiny Personal Firewall" de Tiny Software (www.tinysoftware.com). Estos ya han sido probados extensamente por administradores de redes de computación y por lo general se consideran buenos. Adicionalmente, son gratis para usos no comerciales.

11. No use líneas de asunto en el correo electrónico codificado que pueda dar un indicio sobre el contenido del correo. La línea de asunto no se encuentra codificada y puede mostrar la naturaleza del correo codificado, y provocar ataques.

No subestime el valor de la infraestructura electrónica de su organización. Las amenazas contra su patrimonio más valioso, su información, la base de sus conocimientos, continuará. UN FALSO SENTIDO DE SEGURIDAD ES PEOR QUE ESTAR INSEGURO.

Aquí hay unas cuantas ideas más, las cuales le dan un conocimiento que puede armarle contra posibles atacantes, maliciosos o no, tomados de Winfosec (www.winfosec.com)

¡El sentido común es la mejor defensa! Prevéngase de infecciones con virus y mantenga su computadora libre de troyanos, practicando una computación sana.

Un buen programa antivirus y una buena pared de fuego le llevarán lejos en cuanto a mantener a su computadora segura, pero al final, la seguridad de su máquina depende de usted. Sobre todo, la mejor defensa contra programas maliciosos y gente maliciosa es el sentido común. Además de las cosas importantes que hemos cubierto, aquí hay algunas ideas rápidas de sentido común para ayudarle a mantenerse protegido.

Permita que haya extensiones de archivos en Explorer. Mientras se encuentre en el Explorador, vaya al menú de Herramientas y elija “Opciones de Archivo”. Haga un click en la opción de Ver, luego asegúrese de que no haya un marcador al lado de “Ocultar extensiones para tipos de archivos conocidos”. El hecho de poder ver las extensiones de archivo le evitarán marcar accidentalmente, por ejemplo, picture.vbs en vez de picture.jpg.

Elimine el dejar que corran automáticamente los archivos bajados. Si su correo o programa de noticias está automáticamente programado para que automáticamente corra los archivos que usted descarga, está buscando problemas. La mayoría del correo común y programas de noticias le permiten apagar las características de correr automáticamente. Le sugerimos Becky como cliente de correo, y Agent como un lector de noticias. No sólo puede usted apagar las características de correr automáticamente en estos programas, sino que incluso puede elaborar una lista de extensiones de archivo para que éstos le avisen cuando los encuentre.

Conozca sus tipos de archivo. Muchas personas no se dan cuenta que los archivos EXE no son los únicos tipos de archivo que pueden correrse en una máquina, COM, SCR, SHS, VBS, PIF y BAT son sólo algunas de las extensiones de archivo que pueden ser ejecutados por su sistema. ¡Tenga cuidado con estos archivos, no importa de donde vengan, puesto que pueden contener algo indeseado! Si usted no reconoce un tipo de archivo, ejerza precaución antes de hacer un doble click en el mismo. Quienes fabrican virus dependen de intentar engañarlo para que abra un virus o un gusano.

Evite los archivos ejecutables como si fueran una plaga. Si usted recibe un correo electrónico de un amigo que dice “Aww, tienes que correr esto, es tan lindo” con algo ejecutable adjunto, ALÉJESE! Muchos programas indeseables se adjuntan a otros programas – como el gusano Happy 99, que llegó con fuegos artificiales – y son inadvertidamente diseminados por personas que creen que el programa que lo lleva es muy bonito o divertido.

Evite los Archivos VBS como si fueran dos plagas. Pocos usuarios necesitarán alguna vez correr un archivo VBS, y si usted necesita correr uno, lo sabrá de antemano. Hay cientos – tal vez miles de virus y gusanos VBS flotando en el ambiente. Los gusanos VBS son tan fáciles de crear, que incluso existe un programa que le permite hacer sus propios gusanos. Si recibe un archivo VBS, bórrelo inmediatamente sin abrirlo.

Desactive la codificación insegura y Active X. Esto difiere de un navegador a otro, pero debiera estar en el área de preferencias de su navegador. Haga que su navegador le avise cuando un sitio en la red desee correr una codificación o control de Active X. Si usted confía en ese sitio, puede dejar que corra el control. Toma un par de segundos más, pero vale la pena la seguridad que usted gana.

Si parece ser demasiado bueno para ser verdad, probablemente lo sea. ¡Esto habla por sí mismo! No confíe en los correos electrónicos que dicen contener fotos al desnudo de su artista favorita, cartas de amor de fuentes desconocidas u ofertas maravillosas sobre cómo hacerse millonario o de varios miles sin esfuerzo. Piense antes de dar el click, y sabrá lo que está abriendo. Estará mucho mejor.

IV.2.3 El programa de encriptación PGP

Frente a estas situaciones, existen tecnologías fácilmente accesibles y algunas gratuitas, para poder encriptar (o codificar con claves) los mensajes de correo electrónico, parte del disco duro de la computadora o cualquier otra información electrónica. El programa más común usado para este fin, se llama Pretty Good Privacy (PGP), la que en español quiere decir, Privacidad Bastante Buena.

PGP permite cifrar archivos y mensajes electrónicos de forma que solo puedan acceder a ellos quienes usted determine, adicionalmente estos archivos y/o mensajes pueden ser firmados para asegurar su procedencia y la no-alternación de los mismos.

Para hacer uso de la encriptación de parte del disco duro basta instalar y configurar el software PGP y haber escogido una frase clave segura. Ahora bien, si se desea compartir información cifrada es necesario que las demás personas tengan instalado este programa.

Para las comunicaciones PGP utiliza una tecnología de dos llaves interrelacionadas, una privada y una pública. Es necesario que cada una de las personas que desean comunicarse haya generado su par de llaves y luego hayan intercambiado solamente sus claves públicas.

Este programa de software tiene una historia muy interesante. Durantes la década de los 70 la encriptación de las comunicaciones electrónicas fue inventada por matemáticos y expertos en computación de los Estados Unidos. Ya que la Agencia de Seguridad Nacional opinaba que podría afectar su capacidad de monitorear las comunicaciones internacionales y por el otro lado, el FBI, sus capacidades de intervenir las comunicaciones de los criminales, el gobierno de Estados Unidos durante años quiso regular su uso y sobre todo, su exportación. Los matemáticos del mundo opinan que este método de encriptación es tan seguro que no lo pueden romper ni las supercomputadoras de las agencias de seguridad norteamericana.

Frente a esta oposición gubernamental al libre desarrollo de esta nueva tecnología -- indispensable para la privacidad en el Internet y por ende para el comercio electrónico -- las empresas trasnacionales Norteamericanas comenzaron a desarrollar tecnologías fuera de su país, y se organizó un movimiento social en los EEUU que defendía la absoluta privacidad de las comunicaciones ciudadanas. En 1991 un estadounidense llamado Phil Zimmerman confrontando las restricciones sobre la exportación, creó PGP y lo colocó en la Internet, al alcance de todo el mundo, por lo que, el movimiento de Encriptación se volvió internacional.

Finalmente, las cortes estadounidenses defendieron la capacidad de encriptación como parte de los derechos constitucionales de libertad de expresión y privacidad, y en 1999 – con la tecnología ya extendida por todo el mundo-- se levantó la prohibición norteamericana a la exportación, aunque con limitaciones.

En Guatemala, la Constitución garantiza la privacidad de las comunicaciones y no hay ninguna ley que restrinja el uso de los métodos de encriptación, por lo que su uso por las personas es completamente legal. Ese no es el caso de las comunicaciones del Gobierno, ya que existe un requisito constitucional de publicidad de los actos de la administración, siendo las comunicaciones uno de ellos[17].

¿Como obtener e instalar el software PGP?

El software de PGP tiene un tamaño de 10 megabytes y es de distribución libre y gratuita. Puede distribuirse en CD o como sea, siempre y cuando no se cobre más que el costo de los materiales. También puede copiar el software de las máquinas de otras personas que tengan el programa.

PGP se puede bajar libremente y sin costo alguno del sitio web en inglés para PGP internacional, localizado en Noruega y en varios idiomas, cuya dirección es: http://www.pgpi.org/pgpi.

Otro buen recurso es el sitio web en idioma español, del grupo Kriptópolis, de España, cuya dirección es: http://www.kriptopolis.com/pgp. También se recomienda comunicarse con la organización Computer Professionals for Social Responsibility (CPSR), cuyo sitio web es: www.cpsr.org. Ellos ofrecen apoyo técnico gratuito en la seguridad de las comunicaciones, a ONG de derechos humanos.

¿Cómo prepararse para usar PGP?

Para hacer uso del PGP luego de su instalación, es necesario definir su frase secreta y además hacer que la computadora le genere sus llaves públicas y privadas. Estas llaves son secuencias únicas de números generadas por la computadora, que contengan las formulas matemáticas para la encriptación y desencriptación de la información. Para las comunicaciones entonces las personas intercambian solamente sus llaves públicas.

Frase secreta, frase contraseña

Su frase secreta es su primer y más importante nivel de defensa de su privacidad. Es una combinación compleja de letras, números y símbolos, mayúsculas y minúsculas, que debe inventar y que le va a permitir acceder a su información encriptada o a la información encriptada que otros le manden. Es importante tratar de pensar en una frase suficientemente compleja para que no sea fácil adivinar pero también sencilla de recordar para que no se le vaya a olvidar. Si se le llegara a olvidar esta frase, NO PODRÁ ACCEDER A LA INFORMACIÓN QUE YA TIENE ENCRIPTADA. Unos buenos consejos son: 1) nunca se debe escribir en otro lugar y 2) usted no lo va a olvidar nunca.

La primera vez que usted use PGP es necesario definir e ingresar su frase secreta, luego será necesario ingresarla cada vez que desea firmar o desencriptar un mensaje. Si alguien llegara a obtenerla, junto con su clave privada electrónica, esta persona podría proceder a

[17] El derecho a la privacidad y la publicidad de los actos de la administración, los regulan los artículos 24 y 30 de la Constitución Política de la República, respectivamente.

desencriptar toda su información así como firmar mensajes y archivos como si usted lo hiciera.

La clave pública

Cada usuario de PGP tiene una llave pública. El programa PGP requiere que al momento que usted encripte información, le indique la lista de las llaves públicas (electrónicas) de los destinatarios del mensaje. Así, sólo estos destinatarios tendrán la posibilidad de desencriptar y leer el mensaje. Si no tiene la llave pública de alguna persona, no podrá enviarle información encriptada. Entonces, antes de poder mandarle información encriptada a alguien, es necesario haber obtenido su llave pública, ya sea porque se la haya dado en un disquete, se la haya mandado por correo electrónico, o porque la haya publicado en un directorio de Internet al cual PGP tiene acceso. También hay "plug-ins" para programas de correo como Outlook (Outlook Express) que seleccionan las llaves para encriptar automáticamente.

Por lo mismo, para que otras personas puedan enviarle mensajes encriptados, es necesario que usted haya generado su llave pública y que la socialice, por medio de disquete, mensajes electrónicos, o poniéndolo en un directorio público. No hay peligro al distribuir su clave pública ampliamente pues, nadie puede desencriptar su información con ella, pero sí la necesita para enviarle cualquier mensaje encriptado.

El riesgo de este sistema de llaves públicas es que algunos usuarios podrían dar nombres falsos al momento de generar sus claves públicas, fingiendo ser otros. Sobre esta posibilidad, se tienen dos controles. En primer lugar, existen unos códigos de comprobación de cada llave pública que usted puede pedir que la persona en cuestión le lea, personalmente o por teléfono. En segundo lugar, las llaves públicas pueden ser firmadas por otras llaves, de tal forma que la persona A da constancia que constató la identidad real de la persona B.

La clave privada

La clave privada electrónica, uno lo mantiene siempre en reserva. Sirve para firmar y encriptar mensajes y archivos. La clave privada es una secuencia tan larga de números que no puede ser quebrada ni con computadoras que prueban todas las posibles combinaciones. Al generar su clave privada, debe escoger la extensión máxima ofrecida.

Al generarse su clave privada, una copia queda en su computadora, por lo que debe protegerla a fin de que no sea robada ni copiada. Igual debe guardar otra copia aparte, por si perdiera la primera versión, ya que sin ella no podrá jamás desencriptar un mensaje o un disco duro encriptado.

PGP para correo electrónico

El uso del PGP es muy sencillo. Cuando reciba un mensaje encriptado, solamente tiene que seleccionar el texto de interés, pedir a PGP que lo desencripte e ingresar su frase clave. Proceso parecido es la encriptación para el envío. En cuestión de segundos el texto se transforma desde algo completamente incomprensible a un texto como cualquier otro.

Para las instrucciones exactas de cómo proceder, consulte uno de los sitios web indicados arriba.

El uso del PGP es un poco más difícil para los que tengan Netscape Messenger, pero existen adaptaciones que lo hacen posible, o bien se puede encriptar y desencriptar vía el clipboard.

(Hushmail: Una alternativa al uso del software PGP es volverse usuario del servicio de correo electrónico llamado "hushmail" el cual encripta automáticamente todas las comunicaciones entre dos usuarios de esta red. Servicio parecido tiene la empresa canadiense www.freedom.net)

¿Como usar PGP en el disco duro?

Para encriptar una porción del disco duro, se crea un disco adicional E: y luego desde el Explorador de Windows se puede cifrar y firmar ficheros, descrifrar y verificar sus ficheros, y además borrar de forma segura cualquier elemento en su computadora. Esta facilidad podría convertirse en un método crucial de protección de información sensible, frente a la posibilidad de allanamientos, robo de disquettes, o intrusión de piratas informáticas en su sistema.

IV.2.4 El Scramdisk[18]

ScramDisk es un programa que proporciona un disco cifrado virtual en máquinas bajo Windows 95 y 98. Básicamente, se crea un archivo (contenedor) que es montado por el programa ScramDisk. Este programa crea una nueva unidad lógica de disco mediante la cual se da acceso al disco. Lo importante es que cualquier dato escrito a la nueva unidad lógica queda cifrada con el algoritmo que usted escoja.

Existen programas que ya proporcionan esta función bajo Windows 95 y NT, pero ScramDisk es en la actualidad único por diversos motivos:

1. Es un cifrado basado en un disco virtual completamente funcional que funciona bajo Windows 95 y Windows 98.

2. Su uso es libre, sin restricciones en absoluto.

3. El código fuente esta disponible para revisión y ulterior desarrollo del programa, con muy pocas condiciones.

[18] Esta parte ha sido tomada del manual de usuario del Scramdiosck, contenido en el programa de instalación. En dicho programa está disponible el manual completo.

4. Ha sido desarrollado en el Reino Unido y, por el momento al menos, puede ser exportado electrónicamente desde el Reino Unido. Aunque la ley cambie en el futuro, es de esperar que para entonces ScramDisk estará bien diseminado.

5. Es imposible demostrar que un archivo grande contenido en un disco es un contenedor de disco virtual ScramDisk sin conocer la frase de contraseña. Los archivos contenedores de ScramDisk no tienen una extensión de archivo estándar y no contiene encabezados de archivo que indiquen que el archivo es algo más que datos aleatorios. Use el programa DieHard para comprobar la 'aleatoriedad' de un disco virtual ScramDisk.

6. Puede verse como un trabajo en curso. Es de esperar que otras personas con las habilidades correctas tomen el programa y aumenten sus funciones añadiéndole nuevas características y nuevos algoritmos de cifrado. El programa incluye una arquitectura extensible, que permite que se añadan nuevos algoritmos con mínimos problemas.

7. Los archivos ejecutables del programa son muy pequeños y caben en un disco de 3 ½".

8. El programa permite ocultar un sistema de archivos en un archivo WAV. Esto se conoce como esteganografía.

9. Es mucho más difícil montar ataques de diccionario o de fuerza bruta contra ScramDisk que contra cualquiera de sus competidores.

10. Una "Pantalla Roja" para entrada de contraseñas que evita que las contraseñas sean capturadas por programas como Skin98 o Back Orifice.

Requisitos de Sistema

Para funcionar, los requisitos de ScramDisk son muy discretos:

- Un PC capaz de correr bajo Windows 95 o 98.

- Al menos 1Mb de espacio libre en disco para la instalación de ScramDisk.

- Espacio para crear los archivos de unidad de ScramDisk. Puede ser espacio en una unidad FAT16 o FAT32, una partición en blanco o un archivo WAV grande en el caso de esteganografía.

Instalación de ScramDisk

ScramDisk se distribuye como un archivo ZIP llamado Sdisk.zip, descargable desde la página de ScramDisk (http://www.scramdisk.clara.net/). Una vez el archivo zip a sido descargado, necesitará usted extraer el archivo en un directorio adecuado (por ejemplo: 'c:\scramdisk\').

Problema conocido: No intente instalar ScramDisk en el mismo directorio en el que fue extraído.

Ahora ejecute el archivo 'installdir\sdinstal.exe' y siga las instrucciones. Una vez la instalación haya terminado, el sistema se reiniciará. Cuando el sistema se haya reiniciado podrá usted usar el programa ScramDisk para crear y acceder a unidades cifradas.

En el muy probable caso de un fallo completo del sistema justo tras la instalación, haga esto:

1. Arranque en modo DOS usando las teclas de función adecuadas.

2. Borre el archivo "c:\Windows\system\oisubsys\sd.vxd".

3. Reinicie Windows. ScramDisk no funcionará, sin embargo, ya que el driver ha sido eliminado.

La ruta de directorios mostrada arriba supone que el directorio de Windows es "C:\Windows\"; si no lo es, use el directorio correcto de Windows.

Desinstalación de ScramDisk

Ejecute ScramDisk y escoja la opción de menú 'File | Uninstall ScramDisk...'[Archivo \ Desinstalar ScramDisk]. Se le preguntará si realmente desea eliminar el programa ScramDisk, y el programa reiniciará el sistema.

Ataques Teóricos contra ScramDisk

Hay dos tipos de ataques que pueden aplicarse a la mayoría de los criptosistemas modernos:

I) Ataque de Diccionario: esto implica probar cada entrada de un diccionario contra el contenedor. Si la contraseña está en el diccionario, el atacante ha "tenido suerte".

II) Ataque mediante Fuerza Bruta. Esto significa probar todas las posibles contraseñas contra un contenedor ScramDisk. Este es un tiro muy largo, como veremos más abajo.

¿Es más débil que PGPDisk / BestCrypt, etc.?

No. De hecho, esto reafirma nuestra sospecha de que SD es más resistente frente a un ataque de fuerza bruta que esos programas. Cada intento de introducir una contraseña en ScramDisk lleva aproximadamente 0.5 segundos (en un Pentium 166) – esta es una tasa muy lenta para un ataque de fuerza bruta.

¿Por qué afirma que esos ataques son "difíciles" contra SD?

Las unidades ScramDisk no desencriptadas no contienen indicadores del tipo de cifrado usado para encriptar el disco. Cada vez que se intenta desmontar un disco, ocurre (como mínimo) lo siguiente:

a) SHA-1 de la contraseña (una vez).
b) Y, por cada uno de los algoritmos de cifrado (en la actualidad, hay 9):
   i) Una iniciación del cifrado.
   ii) Dos desciframientos.

Para algunos algoritmos (p. Ej. BlowFish) el coste de una inicialización es muy grande. En la mayoría de los programas de cifrado, la unidad encriptada contiene indicaciones del tipo de algoritmo de cifrado usado – de ese modo se hacen más fáciles los ataques de fuerza bruta.

¿Son (in)viables esos ataques?

Depende de lo chiflado que sea usted con los passwords. Si ha usado una contraseña razonable (¡ver pregunta siguiente!), este ataque no tiene absolutamente ninguna posibilidad de funcionar.

Algunos ejemplos simples:[19]:

Ataque de diccionario:

100,000 palabras contra 1 línea de contraseña = 1 segundo.
100,000 palabras contra 2 líneas de contraseña = 1 día.
100,000 palabras contra 3 líneas de contraseña = 300 años
100,000 palabras contra las 4 líneas de contraseña = 3 millones de años

Ataques de fuerza bruta (con una sola línea):

7 caracteres (la longitud mínima de la contraseña) con alfabeto a..z = 22 horas
7 caracteres (la longitud mínima de la contraseña) con alfabeto completo = 7 años
11 caracteres con alfabeto completo = 3 millones de años

Parece obvio que, incluso con hardware a niveles masivos, un ataque contra una contraseña bien escogida es inviable.

¿Qué tipo de contraseñas encontrarán estos ataques?

[19] Los números del ejemplo suponen 10000x chips PII 450Mhz funcionando en paralelo, y que cada uno puede realizar 100 tests/segundo (muy optimista - ¡un P166 solo puede hacer 2 tests/sgundo!).

Contraseñas cortas, contraseñas formadas de palabras en el diccionario y contraseñas construidas a partir de un alfabeto pequeño.

Preguntas Frecuentes sobre Scramdisk (FAQ)

¿Qué puedo almacenar en mi ordenador con Scramdisk?
Cualquier cosa que pueda almacenarse en otro disco de Windows, aparte de imágenes de un archivo ScramDisk. Un disco ScramDisk no puede almacenarse en otro disco ScramDisk. Todo lo demás sí.

¿Qué significa la licencia, en cristiano?

Hay varias cuestiones relativas al significado preciso de la licencia. Lo siguiente debería ayudar a dejarlo claro. Los individuos y empresas pueden usar ScramDisk para proteger datos con las siguientes guías:

- El programa no se ofrece comercialmente por parte de ningún individuo o empresa a ningún individuo o empresa.

- El programa no se usará para cifrar datos comerciales ofrecidos en venta al público al por menor, como DVD, otras películas, música, programas o datos informáticos.

- No nos responsabilizamos por pérdidas de datos, u otras pérdidas, al margen de cómo se causen.

- IDEA necesita una licencia para uso comercial.

Básicamente, no queremos que la gente haga dinero gracias a nuestro duro trabajo, o el duro trabajo de algunos de los diseñadores / implementadores de los algoritmos de cifrado.

¿Cómo saber si ScramDisk está instalado?

Se hacen en el sistema los siguientes (y necesarios) cambios:

- Se añade el archivo “c:\windows\system\iosubsys\sd.vxd”.

- Se añade el archivo “c:\windows\scramdisk.ini”. Este es el archivo que guarda la configuración de SD.

- Se añade el archivo “ruta_de_instalación\scramdisk.exe”. Este es el ejecutable principal.

¿Qué algoritmo de cifrado es mejor?

¡No lo sé! En realidad, nadie lo sabe. Algunos algoritmos se conocen que son “débiles” (esto es, sucumben ante ataques publicados). El que un algoritmo aguante todos los ataques conocidos no significa que se haya “demostrado” su fortaleza – solamente que es relativamente fuerte comparado con los algoritmos “débiles”. Se cree improbable que la fortaleza de un algoritmo de cifrado en bloque pueda ser demostrado en el futuro próximo[20].

Dicho esto, creo apropiado ofrecer aluna guía al usuario:

- Se piensa que 3DES es extremadamente fuerte, pero puede que sea demasiado lento para todos los discos cifrados.

- IDEA y Blowfish son buenas elecciones – ambos se cree son seguros contra todos los ataques conocidos.

- Personalmente prefiero Blowfish debido a su mayor longitud de clave, velocidad muy razonable, ausencia de problemas de licencia y robustez contra ataques.

- IDEA precisa de una licencia para su uso comercial.

- Summer es débil.

- TEA, Square y MISTY1 están bien, pero son relativamente nuevos.

- DES es ciertamente débiles frente a un adversario decidido (debido a su longitud de clave).

¿Qué es esa horrible “pantalla roja” en la que tengo que teclear contraseñas?

Esa pantalla es un mecanismo de muy bajo nivel, proporcionado en Windows 95, que se usa habitualmente para mensajes criticos de error. Al introducir una contraseña en esa pantalla, en lugar de en una pantalla de dialogo convencional, se evita que ciertos programas “husmeadores” como Skin98 puedan leer las teclas que forman la frase de contraseña.

¿Qué clase de “disco” ve Windows en un disco ScramDisk?

Windows “ve” un disco estándar FAT16 en todos los casos. Los datos pueden de hacho estar almacenados en una partición o en un archivo con FAT32 o FAT16, en un archivo CD en CDFS, incluso en otro lugar de una red.

Si creo un disco virtual con ScramDisk, ¿puedo desfragmentarlo y repararlo como los otros discos FAT?

[20] Del artículo de TowFish: “Cualquier demostración razonable de la seguridad general de un cifrado en bloque debería también demostrar que P ≠ NP”.

Se puede desfragmentar un disco “ScramDisk” como cualquier otro disco estándar. Puede usarse Scandisk para reparar cualquier estructura DOS que falle, como un disco estándar. De hecho, ¡el sistema no sabe que no es un disco estándar!

¿Qué hay de soporte para FAT32

Hay soporte limitado para FAT32 en ScramDisk, es posible crear un archivo de unidad ScramDisk en un disco FAT32, pero no es posible crear una unidad FAT32. Todos los contenedores ScramDisk tienen que ser formateados con el sistema de archivos FAT16 – esto restringe las unidades ScramDisk a un máximo de 2 GB de tamaño.

¿En qué parte del disco se almacenan las contraseñas?

No se almacenan. El disco se monta estadísticamente, no mediante comparación de contraseñas. Hay dos sectores con los mismos datos (derivados aleatoriamente) que tienen diferentes claves de sector. Los datos de esos sectores, con una contraseña incorrecta, tienen diferente aspecto. Solamente cuando se suministra la contraseña correcta, creando el par de claves correcto (una clave para cada sector) mostrarán ambos sectores los mismos datos, y la contraseña se acepta como correcta.

Cuándo está inaccesible, ¿puede alguien ver los nombres de los archivos que he guardado en el disco?

No. El sector de arranque, tabla de partición y datos son todos cifrados usando el algoritmo de su elección.

¿Cómo puedo hacer una copia de seguridad de mis archivos, cuando éstos están guardados en discos ScramDisk?

Igual que de costumbre. Sin embargo, si han de permanecer seguros, necesitará copiarlos en una segunda unidad ScramDisk. Simplemente abra ambas unidades y arrastre los archivos mediante Windows desde una unidad a la otra. Otra opción es hacer una copia de seguridad de toda la unidad cifrada.

¿ScramDisk no funciona con x?

ScramDisk debería funcionar con todas las aplicaciones, pero hay problemas con algunas, por ejemplo JBN. 9 de cada 10 veces, los usuarios que informan de problemas con ScramDisk están realmente haciendo algo mal, por ejemplo:

1. Intentar crear demasiados archivos en el directorio raíz de una unidad.

2. Intentar hacer algo con un archivo de sólo lectura.

Obviamente, esos errores pueden suceder en cualquier tipo de disco. Por favor, informe de cualquier problema de aplicación al autor.

¿ScramDisk funciona con DOS ?

ScramDisk es un sistema bajo Windows con driver VxD, con una utilidad de aplicación Win32. Funcionará perfectamente bien en una ventana DOS bajo Windows, y permite el uso de las aplicaciones DOS para acceder al disco de forma normal, pero por supuesto no funcionará a menos que Windows 95 sea el sistema operativo subyacente. Hay una versión de ScramDisk para DOS, pero solamente leerá particiones ScramDisk y no archivos cifrados.

¿Tengo que usar el programa de utilidad "Scramdisk.exe" ejecutándolo cuando estoy usando mis discos ScramDisk?

No. El driver VxD "SD.vxd" instalado en el directorio "..\system\iosubsys" hace todo el trabajo. A menos que desee cerrar discos o abrir discos nuevos, puede cerrar el programa de utilidad cuando haya acabado con él.

¿Por qué no funciona con Windows NT?

Windows NT usa un modelo completamente diferente de drivers, llamado Kernel Mode Driver (KMD) que requiere una base de conocimiento al programa diferente. Windows 95/98 usa "VxDs" y el "IOS" para los drivers de discos. Son completamente diferentes, e incompatibles. Espero que algún alma caritativa ayude a la causa echando una mano en la versión NT. El nuevo Windows Driver Model que viene con NT v5 y Windows 98 no ayudará tampoco, ya que solamente cubre drivers de presentación y multimedia.

¿Y si olvido mi frase de contraseña?

!Hágase a la idea de que ha perdido sus datos! Si yo pudiese mostrarle cómo recuperarlos, no sería un sistema muy seguro, ¿no?

¿Cómo se hace una buena frase de contraseña?

Pueden darse algunos consejos a los usuarios que tienen la tarea de elegir una frase de contraseña:

1. Haga la frase lo más larga posible. La frase puede tener 39 caracteres por línea y hay 4 líneas – así que una frase de contraseña puede tener hasta 156 caracteres.

2. Haga uso de letras mayúsculas y minúsculas.

3. Incluya números y signos de puntuación como ; : , . ! " £ Etc.

4. No escoja una sola palabra o una frase bien conocida en la literatura – eso haría posible un ataque de diccionario contra el sistema.

Con ScramDisk, montar un ataque de diccionario es una tarea muy lenta – para cada contraseña probada sin éxito hace falta lo siguiente: ejecutar un SHA-1 una vez, seguido por una inicialización y dos desciframientos en bloque para cada algoritmo -- esto es así porque el algoritmo usado para cifrar el disco no está almacenado.

!Socorro! !Aparecen partes de mi frase de contraseña en la unidad cifrada!

Estadísticamente, es de esperar. Por ejemplo, si crea una unidad cifrada de 100 Mb, es de esperar que cada combinación de 3 caracteres (p. ej. AAA, AAB, AAC etc.) aparecerán aproximadamente 16 veces: (100*1024*1024)/2563. De ese modo, la frase de contraseña del usuario aparecerá en la unidad cifrada en bloques de 3 letras, lo más probable.

Esto sucede porque los datos cifrados tienen el mismo aspecto que los números aleatorios – sería posible que ScramDisk comprobase y se asegurase de que no aparecen partes de la contraseña – pero eso haría posible un análisis.
Puesto que (16*1024*1024)/2563 = 1, es de esperar en promedio ver cada combinación de 3 caracteres en un archivo de 16 Mb.

Sí debe preocuparse si trozos de 5 letras de su contraseñan aparecen en la unidad cifrada – la probabilidad de que esto suceda accidentalmente es extremadamente pequeña.

¿Cómo es que cada disco que creo tiene diferente aspecto, incluso si creo el disco usando la misma contraseña y algoritmo y pongo los mismos datos en él?

Nunca podrá generar la misma tabla de clave maestra. Las probabilidades de hacerlo son astronómicamente remotas. Es dicha tabla de clave maestra la que es cifrada con la contraseña, y es la tabla no cifrada la que descifra los datos del disco. No hay dos tablas de clave maestra iguales a no ser que copie usted un archivo hospedador de ScramDisk en otro lugar.

¿Hay algo que no debería hacer?

No copie archivos hospedadores de ScramDisk (los que “contienen” un disco ScramDisk) para a continuación usarlos separadamente. Para cada nuevo disco que desee crear, debería usar la instalación de creación o formateado de partición proporcionados en el programa de utilidad. Esto asegura una mayor seguridad. Si copió usted un archivo hospedador y continuó usando el anterior, ambas unidades operarán con los mismos valores de IVs y de pre-blanqueamiento (ya que tienen los mismos datos aleatorios al comienzo del disco), lo que podría favorecer el criptoanálisis.

¿Por qué se produjo el programa?

¿Por qué se produjo PGP? ¿Por qué no? Si creyésemos honradamente que los productos criptográficos fuertes fuesen a costar vidas o a amenazar la seguridad

nacional, estaríamos moral y éticamente obligados a no desarrollar o facilitar el programa. Pero la verdad es que no ha habido una argumentación convincente, por parte de cualquier grupo político o legislador, sobre por qué la criptografía fuerte no debería ser producida, usada, distribuida y vendida.

Personalmente me gusta la analogía de las 'llaves'. No tenemos que dar al gobierno copia de las llaves de nuestra casa u oficina, así que ¿por qué deberíamos permitirles el mismo privilegio con las "llaves" a nuestros datos? La policía está invitada a acceder a mis datos con una orden judicial válida, de igual forma que pueden entrar en mi casa con una orden de registro válida.

También me gusta el argumento de 'postal' de Phil Zimmerman. Cuando la gente envía cartas, usa sobres para asegurarse cierto grado de seguridad, no envían cartas sin sobres porque no tienen por qué hacerlo. Enviar cartas dentro de un sobre se considera aceptable porque todo el mundo lo hace. Todo el mundo debería tener derecho a usar criptografía fuerte.

La verdadera razón por la que el gobierno norteamericano (¿y del Reino Unido?) se opone a la criptografía fuerte es porque obtienen demasiada información mediante interceptación de comunicaciones para permitir la proliferación de criptografía fuerte, lo que haría su trabajo necesariamente más difícil. !Lea Puzzle Palace y For the President's Eyes Only si no nos cree!

Tanto el autor del programa como yo mismo somos profesionales del ramo, sin antecedentes penales (¡ni siquiera una multa de tráfico!). No somos "transgresores de la ley" ni "anarquistas" – simplemente creemos que la privacidad debería ser un derecho y que la criptografía fuerte debería estar a disposición de cualquier persona que desee usarla.

No excusamos el uso de ScramDisk por fines ilegales en su jurisdicción de uso.

¿Qué otros programas similares existen?

Bestcrypt (de Jetico) y PGPDisk de PGP. Son, por supuesto, incompatibles mutuamente, y usan diferentes algoritmos de cifrado. BestCrypt usa Blowfish / GOST/ DES, PGPDisk usa CAST. ScramDisk (gratuito) es el más barato. Jetico rehúsa mostrar el código fuente de BestCrypt.

¿Hay asuntos "internacionales"

Sólo este: la Pantalla Roja de bajo nivel debe evitarse si está usando usted otro teclado que no sea el QWERTY.

¿Qué puertas traseras hay en ScramDisk

Hasta donde nosotros sabemos, ninguna. No tenemos motivos para producir un programa defectuoso, así que saque usted sus propias conclusiones. Y si lo desea, ¡inspeccione el código fuente!

ScramDisk no es totalmente seguro (¡cómo no lo es ningún programa de seguridad!). Hay diversas maneras en que un atacante puede infiltrarse en su sistema:

1. Buscar aplicaciones que filtren datos. Un procesador de textos muy conocido tiene un fallo interesante que filtra partes de los contenidos en bruto del disco cuando guarda un Documento Compuesto OLE.

2. Buscar datos que no han sido borrados de forma segura. Vale, todo el mundo sabe que se puede des-borrar un archivo con facilidad. Pero ¿sabía que incluso un archivo que ha sido "machacado" {wiped} pueden en teoría ser recuperados mirando la superficie del disco? Los archivos borrados deben ser machacados de forma segura usando un programa apropiado (PGP v6 contiene un programa de borrados seguro de archivos – los usuarios de PGP v5.x deben tener cuidado, pues la función de borrado posiblemente sea insegura).

3. Buscar datos que hayan sido filtrados de otro modo. Los archivos temporales y el archivo de intercambio saltan a la mente. Ambos necesitan también ser borrados de forma segura.

4. Usar un ataque tipo "Tempest". Básicamente, las emisiones eléctricas del monitor, disco duro e incluso teclado pueden ser detectadas y registradas a distancia. Esto puede permitir a un fisgón ver lo que hay en la pantalla y detectar la frase de contraseña cuando es tecleada.

5. Fuerza bruta. Esto puede suceder de diversas maneras: pueden atacar mediante fuerza bruta la frase de contraseña o el algoritmo. Para contrarrestar el primer ataque es importante usar una frase de contraseña larga y difícil de adivinar; ayuda el usar mayúsculas y minúsculas, así como números. El segundo ataque es trabajo duro (y llevaría unas 2127 operaciones con la mayoría de los algoritmos incluidos en ScramDisk – DES y Summer son excepciones).

6. Algunos de los algoritmos de cifrado pueden ser vulnerables a ataques desconocidos en público. Puede que la NSA/GCHQ tenga un mecanismo más rápido que la fuerza bruta para atacar los algoritmos. No hemos incluido ningún algoritmo débil en la distribución original (aparte de Summer, que se incluye por motivos de compatibilidad), pero ¿quién puede detectar lo que las Agencias de Inteligencia pueden hacer con Blowfish, IDES, 3DES, etc.?

7. Instalar una versión alterada de ScramDisk en su ordenador que almacene de forma secreta la frase de contraseña, de forma que un agente de la CIA pueda luego leerla (¡o usar un programa como Skin98 para hacerlo!) ¿Rebuscado? Tal vez, pero hay que estar al tanto de que este tipo de ataques

existe. No hay manera real de defenderse de este ataque. Compruebe las firmas PGP de los archivos de ScramDisk, pero ¿acaso no puede su copia de PGP haber sido asimismo alterada?

8. Golpearle a usted hasta que confiese la frase de contraseña. Aparentemente, las drogas de la verdad también funcionan.

IV.3 Medidas de apoyo psicológico

Los hostigamientos y ataques, afectan nuestra forma de pensar y actuar. Se puede decir que casi todas las amenazas tienen un componente psicológico, ya que pretenden paralizar o interrumpir el trabajo de la persona afectada.

El trauma, un estado psicológico que tiene efectos a largo plazo, puede resultar cuando un acontecimiento que es intrusivo, es severo y puede cambiar o poner en peligro su vida. Igualmente puede ocurrir trauma cuando el hostigamiento es continuo, o cuando toca puntos especialmente sensibles como nuestro sentido de responsabilidad para con la familia.

Casi siempre, la primera defensa que tenemos en el caso de un trauma es la negación y la insensibilidad depresiva. Es por eso que a veces las personas parecen no reaccionar ante un hecho muy fuerte, o se aíslan de otras personas en vez de buscar ayuda. Pero aunque niegan la importancia o impacto de su situación, igual les puede ocurrir una gama de otros síntomas del estrés pos-traumático. Estas incluyen sentimientos de: choque, enojo, culpabilidad, aislamiento, temor, ansiedad, preocupación constante, confusión, depresión, irritabilidad, impaciencia, frustración, e impotencia. También pueden presentarse: problemas para dormir (tales como insomnio, pesadillas, dificultades para despertarse); problemas para comer, problemas sexuales, pensamientos y recuerdos intrusivos, llanto frecuente, uso de drogas o alcohol y dolor de cuerpo así como algunas enfermedades.

Hay ciertos factores que pueden intensificar y empeorar nuestras reacciones ante un trauma, por ejemplo si la persona:

- Ha sufrido traumas o pérdidas anteriores (especialmente si no ha resuelto sus sentimientos en torno a este acontecimiento).
- Ha sufrido anteriormente de abuso físico, sexual o emocional
- Está pasando por otra crisis en su vida personal (como la muerte de un ser querido, el divorcio, los problemas económicos).
- Tiene una posición de responsabilidad en la organización (bajo la cual tiene que cuidar a otras personas, además de sí mismo).

En el proceso de recuperación de un trauma, siempre hay altibajos. Es difícil saber cuánto tiempo sufrirá de los efectos psicológicos, dado que cada persona es diferente y reacciona de diferente forma. Sin embargo, hay cosas que podemos hacer para favorecer el proceso de recuperación, especialmente importante es recordar que no estamos solos y que podemos y, debemos buscar el apoyo de otros.

IV.3.1 Medidas de protección ante el trauma pos-estrés

a) Hablar de lo que pasó. Es sano e importante hablar sobre lo acontecido, así como sus sentimientos, emociones, pensamientos, y reacciones. Es bueno incluso hablar sobre lo mismo con muchas personas diferentes, porque la repetición puede ayudar a disminuir la intensidad de los sentimientos.

b) Reconocer y explicar sus necesidades. Prestar atención a sus reacciones y tratar de identificar las cosas que le ayuden y las cosas que más estrés le causan. Comentar sus reacciones con las personas a su alrededor. Si las reacciones de varias personas al mismo hecho son distintas, esto es normal también. Cada cual tendrá una forma diferente de reaccionar.

c) Aprender y utilizar técnicas de relajación progresiva o deliberada, cuando se hace un esfuerzo conciente para centrarse mentalmente y relajarse físicamente.

d) Para algunas personas, la espiritualidad y la religión también es importante en un momento de crisis. Asimismo, el juego, la recreación, y el humor pueden ayudar a aliviar el estrés.

e) Tratar de no pensar en “lo peor que puede pasar.” Esto sólo crea más ansiedad y puede llegar a paralizar a las personas. Esto no quiere decir que uno no debe ponerle atención a los peligros reales, pero después de tomar las medidas apropiadas para protegerse es necesario tratar de pensar en términos positivos.

f) Preparar un plan de respuesta institucional anticipadamente. Por ejemplo, puede ser útil formar un equipo de tres a cinco terapeutas (fuera de la organización) quienes pueden preparar una metodología sencilla de trabajo con anticipación, para ponerlo en acción cuando sea requerido.

g) Solicitar cartas de apoyo de otros grupos y personas solidarias, y compartirlas con todas las personas afectadas por el hecho. Es importante aumentar el nivel de contacto entre la persona afectada y otras personas dispuestas a apoyarle, y que sepan darle un acompañamiento desarrollando empatía para contribuir a procesar y superar la situación.

h) Tomar acciones para defenderse y denunciar lo que pasó. A veces la acción para denunciar es la mejor terapia que existe. Pedir que otras personas le callen si quiere hablar.

i) Compartir información sobre lo sucedido entre todas las personas que trabajan en la organización. Esto es una de las funciones de la dirección en tiempos de crisis. La falta de información crea más ansiedad, y puede contribuir a rumores que pueden ser aún peores que la realidad. Cuando tenemos información sobre lo que pasa, sentimos que tenemos más control sobre la situación. La información también crea

confianza entre los miembros del equipo, para que pueda confrontar conjuntamente el problema.

j) Informar a todo el equipo de las medidas de protección que la organización ha tomado, para que puedan sentirse con más seguridad en su participación. Recuerde también informar al nuevo personal de estas medidas.

k) Crear una red de apoyo (gente con quien hablar, personas que pueden dar apoyo logístico y moral en caso de una emergencia, personas que pueden asumir el trabajo concreto de la organización si hubiese una crisis). Es mejor que esta red sea la más amplia posible, para evitar que se desgasten una o dos personas únicas de apoyo.

l) Conseguir apoyo para otras personas cercanas a usted. Es normal que ellos y ellas también reaccionen a la crisis de diferente forma. Algunos de sus síntomas pueden incluir: mucha ansiedad y temor; regresión en las etapas de desarrollo por parte de los niños y las niñas; enojo y violencia hacia usted y otras personas; deseo de "tapar" lo que pasó e impaciencia con los efectos del trauma; y la generación de críticas y un sentimiento de culpabilidad, con el fin de lograr que usted deje su trabajo. Si los miembros de su familia pueden manejar sus propias emociones, podrán darle más apoyo en el momento de la crisis.

m) El apoyo psicológico es especialmente importante para los dirigentes por su responsabilidad de guiar a los demás.

n) En caso de síntomas severos, o solamente como una medida preventiva de salud mental, busque apoyo profesional. Sufrir estas situaciones de tensión y angustia provoca un estrés muy fuerte, y no es recomendanble que nadie lo sufra a solas. En esta guía se incluye un listado de profesionales de la psicología que ofrecen estos servicios a defensores de derechos humanos y otras personas afectadas por el estrés postraumático. [21]

IV.4 Descripción y documentación de los hechos

Cada persona que sufra problemas de vigilancia, intervención de las comunicaciones hostigamientos o allanamientos, debe decidir si es pertinente hacer una denuncia a las autoridades, un comunicado de prensa, u otro tipo de presión hacia las autoridades. Como mínimo, se recomienda a las personas documentar los hechos ocurridos. Reunir y anotar en forma sistemática toda la información pertinente, ayuda a las personas a procesar los hechos y analizarlos. Igualmente, es útil por si más adelante se repiten los hechos o las situaciones van de mal en peor.

[21] Ver Listado de Psicólogos que trabajan Estrés Postraumático en sección V.Anexos.

La decisión de denunciar o no los hechos a las autoridades o al público, es algo que cada persona afectada tiene que tomar, sobre la base de consideraciones como las siguientes:

a) En la mayoría de casos se cree que la publicidad nos protege, pero hay ocasiones en que puede promover más violencia. Lo que buscan ciertos grupos es la publicidad a raíz de sus acciones, en esas situaciones es mejor no hacer una denuncia pública.

b) Se debe consultar con todas las personas afectadas antes de hacer la denuncia, y conseguir el permiso de todas las víctimas. Hay personas que deciden no hacer público un ataque por razones personales, y es importante respetar su decisión.

c) Antes de hacer una denuncia pública, se debe averiguar todos los hechos, y considerar los posibles motivos del ataque. Si es una emergencia de vida o muerte, hay que actuar inmediatamente, pero en otros casos menos críticos puede ser útil realizar una investigación interna primero.

d) Si usted cree que la amenaza proviene de estructuras políticas y militares, hay que pensar en los puntos débiles de estas instancias para ejercer presión sobre ellas desde afuera. La presión internacional es más efectiva en estos casos. De igual manera, cuando la amenaza surge de una disputa local, o cuando proviene de un grupo que no tiene vínculos gubernamentales, la presión internacional es menos efectiva.

IV.4.1 Lista de control para amenazas telefónicas

Para facilitar la tarea de llevar un control sistemático de los hechos, a continuación se presenta una variedad de formatos para tomar descripciones de llamadas amenazantes, de personas y de vehículos. Se recomienda a las instituciones sacar copias de estas hojas y tenerlas a la mano para facilitar el registro inmediato de cualquier hecho sospechoso.

Si usted recibe una amenaza personal por teléfono, por favor observar lo siguiente y notificar inmediatamente a la policía:

Información básica:

1. Número del teléfono en que recibió la amenaza: _____
2. Número del teléfono que hace la llamada: _____
3. Fecha y hora exacta de la llamada: _____
4. Palabras exactas de la persona que llamó: _____

5. Preguntar lo siguiente:

   ¿Cuál es su nombre? _____

   ¿Cuál es el teléfono a donde se le puede llamar? _____

   ¿Cuál es su dirección? _____

   ¿De dónde llama? _____

   ¿Cuál es el motivo de esta amenaza? _____

6. Notar en especial lo siguiente:

   Sexo y edad aproximada de la persona que llama (por la voz): _____

   ¿Le pareció conocida la voz? _____

   ¿Ha recibido usted llamadas similares? _____

   ¿Hay alguna razón por la que usted cree que se le amenazó?

   _____

Características de la Voz que Llama:

____ calmada	____ susurrada	____ disfrazada
____ normal	____ carraspeante	____ risa
____ tartamudeante	____ ceceante	____ áspera
____ nerviosa	____ lenta	____ rápida
____ definida	____ con acento	____ arrastra palabras
____ agitada	____ llorosa	____ entrecortada
____ profunda	____ opaca	____conocida
____ suave	____ fuerte	
____ nasal	____ enojada	

Sonidos de Fondo

____ ruido de calle	____ cabina	____ ruidos de casa
____ loza	____ maquinaria fábrica	____ motor
____ voces	____ ruidos de animales	____ máquinas oficina
____ altoparlantes	____ claridad	____otros
____ música	____ estática	
____ local	____ larga distancia	

Lenguaje de la Amenaza

____ educado

____ obsceno

____ incoherente

____ grabado

____irracional

_____poético

IV.4.2 Amenazas por correo electrónico

1. Notificar inmediatamente y enviar a su servidor una copia de la amenaza recibida por correo electrónico.

2. Si utiliza Microsoft Outlock, seleccione el mensaje y haga click en ver, luego en opciones y, en opciones de mensaje vaya a encabezado de internet. Seleccione ese texto y cópielo a un archivo de texto para enviarlo a su proveedor de correo y a las autoridades.

3. Guardar el mensaje, **NO BORRARLO**.

4. Guardar el mensaje en su disco duro e imprimir una copia.

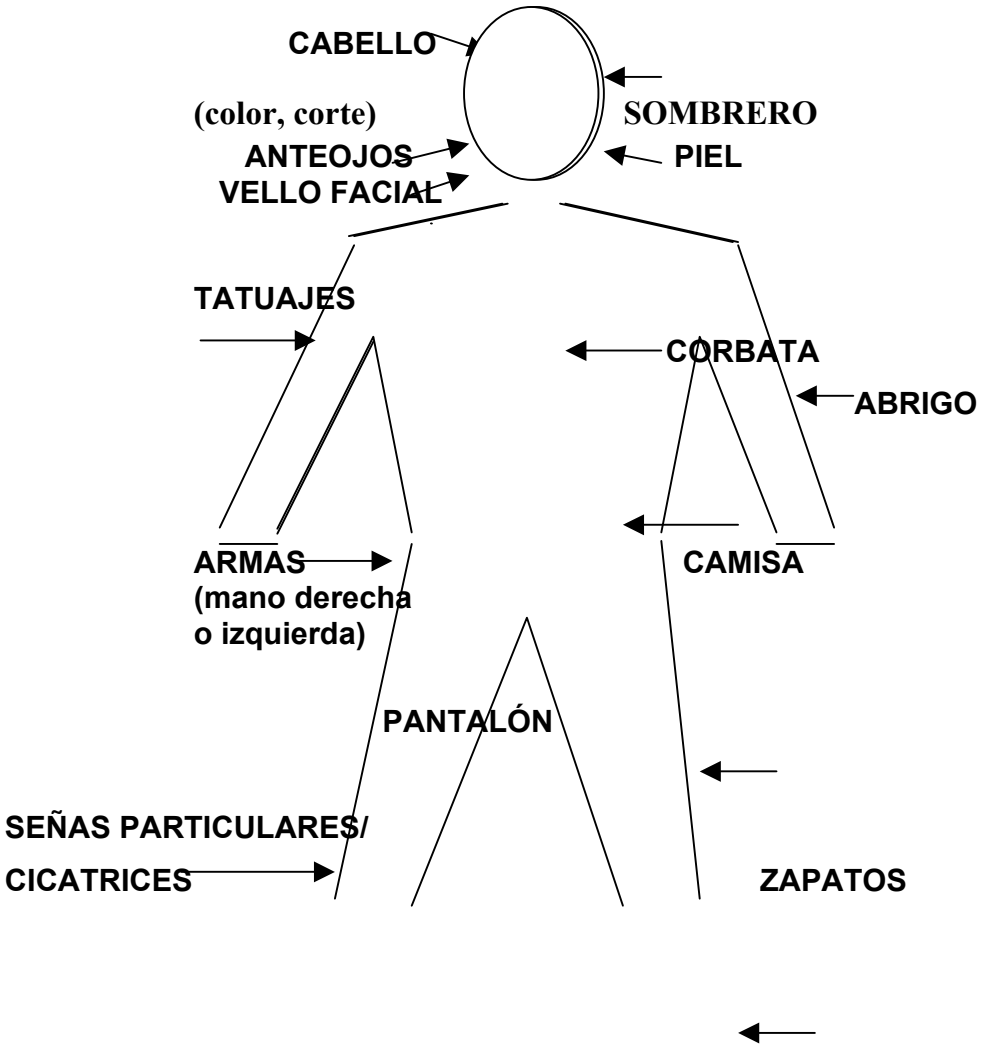
4. Reportar todas las amenazas recibidas por correo electrónico.

5. Notificar a la policía y al Ministerio Público.

IV.4.3 Descripciones de personas

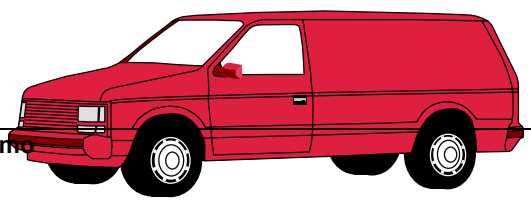
La información más importante es:

1) Descripción física del atacante lo que incluye datos aproximados sobre edad, peso, estatura.
2) Color y tipo del cabello, largo o corto, liso, ondulado, murusho
3) Color y tipo de los ojos (claros, oscuros, negros, café, verdes, grises, rasgados, redondos)
4) Descripción de la ropa, los zapatos
5) Señas particulares inusuales, cicatrices, tatuajes, anillos, aretes, etc.



IV.4.4 Guía para la descripción de vehículos

Llene este formulario inmediatamente después del incidente:



VISTA LATERAL

Año _____ Marca _____

Placa _____ Color _____

Estilo: Sedán____ panel____ pick up____ camionetilla_____

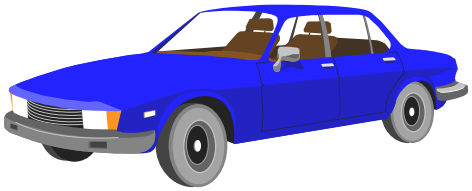
Número de puertas_____

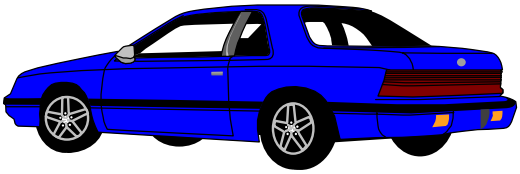
Señas: Modelo reciente(nuevo)_____ antiguo(viejo)_____

chocado_____ pintura original_____

Características principales: Vidrios polarizados_____ vidrios claros_____

PARTE DELANTERA **PARTE TRASERA**





Número de luces _____

Forma de las luces traseras _____de las luces delanteras_____

¿Qué rumbo traía el vehículo?

_____

¿Cuántas personas viajaban en él? _____

¿Qué rumbo tomó el vehículo cuando desapareció?

_____

IV.5 Denuncias a la prensa

Un medio importante para dar a conocer las amenazas e intimidaciones lo constituye la prensa: radiofónica, televisiva y escrita. Esto es posible mediante la emisión de comunicados y la realización de las conferencias de prensa. El éxito en la difusión del hecho dependerá de cuán importante sea la noticia para el medio en cuestión. (con relación al o los personajes o la magnitud del hecho en sí, así como la oportunidad en la presentación de ésta). De lo que se trata es asegurar que no se cubra como una noticia de sucesos sino que exista una cobertura en función del hecho como tal.

Para mantener una cobertura de prensa adecuada, tanto para el comunicado como para la conferencia de prensa, se requiere de acciones constantes tales como:

a) Desarrollar relaciones con periodistas simpatizantes. En todos los medios siempre hay reporteros e incluso editores, con un alto grado de sensibilidad con respecto a los temas de derechos humanos. Cultivar ese vínculo es trabajo permanente y lo único que exige es una relación mutua de respeto.

b) Al momento de dar a conocer el hecho, explicar por qué la noticia es importante. Un simple hecho de impunidad o de violencia en Guatemala no basta para tener prioridad en los medios. Explicar lo que se cree que es el motivo, para que tenga más peso la denuncia.

c) Promover la cobertura de la prensa por medio de actividades creativas. En el 2000 se hizo este tipo de actividades con relación al Guategate (chilqueado[22] del congreso). En estas actividades se puede lograr que la prensa escuche las denuncias de varias acciones de intimidación y violación a los derechos humanos.

d) Organizar grandes eventos o marchas es otra forma de lograr la publicidad. En este caso, definir quiénes pueden hablar en nombre de la organización y asegurar que el mensaje sea claro y conciso.

e) Evaluar bien cómo hacer la denuncia a la prensa. Dado que los medios de comunicación en Guatemala no siempre actúan con absoluta independencia, a veces es mejor hablar con un periodista simpatizante en vez de hacer un comunicado para distribuir ampliamente. En el caso en que se divulgue un comunicado es mejor acompañarlo, de una vez, con la nota de prensa ya escrita. Es decir, se envían las dos cosas: el comunicado y una nota redactada en estilo periodístico en alusión al comunicado.

f) Premios y eventos internacionales también generan cobertura de prensa (a veces pueden ser una fuente de apoyo e interés constante). Son particularmente útiles para lograr que haya publicidad internacional que protege a trabajadores de

[22] Chilca es una planta medicinal, que usan algunas personas para alejar malas influencias, golpeándose con las ramas todo el cuerpo, a ese acto se le llama chilqueado. En el Congreso, los manifestantes golpearon las paredes para alejar las malas influencias.

derechos humanos en situaciones particularmente vulnerables (por ejemplo, personas que trabajan en el campo en zonas donde hay mayores niveles de conflictividad social, o las personas que están promoviendo casos ejemplares contra militares u otras personas con mucho poder).

g) Si se convoca a una conferencia de prensa, debe asegurarse que inicie con la mayor puntualidad posible. Los reporteros suelen tener poco tiempo para cubrir varias actividades y luego regresar a su sede y escribir las notas. Entonces, además de hacer breve la conferencia de prensa, vale la pena distribuir material escrito que amplíe la información proporcionada en la actividad.

h) Nunca olvidar que muchos reporteros también buscarán tener exclusividad en alguna nota o entrevista. Si ha hecho este tipo de compromiso, manténgalo como forma de garantizar un nivel profesional en la relación con el periodista.

i) Si tiene necesidad de llamar a un medio en horario no hábil, pida hablar con el reportero o reportera de turno e, incluso, con el editor o editora de turno.

Les sugerimos mantener una lista completa y actualizada de los medios con direcciones y teléfonos, así como el correo electrónico de los periodistas, para una comunicación permanente.[23]

IV.5.1 Cómo generar publicidad protectora[24]

La publicidad puede proporcionar protección. Hay muchas maneras de atraer la atención de las medios de prensa. Sin embargo, primero debemos desarrollar relaciones con los periodistas simpatizantes. La prensa pondrá a veces más atención a una violación de derechos humanos si la víctima pertenece a una ONG legítima. Pero será necesario convencer al periodista de que la noticia es importante, ya sea porque el grupo sea prominente, porque la violación demuestra una tendencia más general, porque indica que el grupo ha hecho trabajo eficaz, o porque tiene algún significado similar.

Como un medio de promover la legitimidad y credibilidad de los grupos locales de derechos humanos, la cobertura creativa de los medios publicitarios puede proveer protección mediante el aumento del conocimiento general sobre derechos humanos. Esto se puede hacer al descubrir los eventos públicos que conmemoren días simbólicos, visitas guiadas de las oficinas de las ONG a personas prominentes internacionales, patrocinio del trabajo en pro de los derechos humanos por medio de conciertos o exhibiciones de arte, y campañas publicitarias directas para la defensa de los miembros de las organizaciones de derechos humanos. El alcance de los medios publicitarios deberá incluir medios alternativos tales como periódicos de la comunidad y otra prensa local; publicaciones de los gremios y sindicatos; publicaciones electrónicas; radiodifusión de onda corta; y otros similares.

[23] Ver listado de teléfonos de la redacción de algunos medios periodísticos en la sección V.Anexos.
[24] Este apartado fue tomado en gran parte de, Estrategias prácticas para grupos pro Derechos Humanos, del Centro para la acción sostenible en Derechos Humanos.

Pero la pregunta sobre si se debe de involucrar a los medios publicitarios en un caso particular depende del contexto local, y el grado de la independencia de los medios. En ambientes en donde es posible y deseable involucrar a la prensa, varios escenarios pueden desarrollarse: un comunicado de prensa puede ya sea ser distribuido ampliamente, o dado exclusivamente a un sólo periodista simpatizante; o se puede convocar una conferencia de prensa en el momento debido.

Como Se Difundió La Vigilancia De Un Bando

En México, a mediados de 1990, en una temporada cuando Amnistía Internacional registró un aumento dramático en ataques y amenazas de muerte contra los defensores mexicanos de derechos humanos, un grupo asediado llamado Centro de Derechos Humanos, Miguel Agustín Projuárez, invitó a la prensa para cambiar la situación. Después de un creciente patrón de amenazas de murete y difamación, la oficina de dicho centro había sido "vigilada" por casi una semana, por un grupo de hombres armados vestidos de civiles. Para aliviar la tensión que se dio como resultado, el grupo convocó a una conferencia de prensa en la que se describió la situación a los reporteros. Los fotógrafos y periodistas inmediatamente corrieron hacia afuera para tomar fotos y entrevistar a dichos hombres, quienes se dispersaron. La policía entonces acusó públicamente sl Centro por poner en peligro una investigación, pero la vigilancia cesó, no obstante. Al final la Comisión Interamericana de Derechos Humanos (vea la página 65) investigó el problema del Centro y desde ese entonces las amenazas y el hostigamiento parecen haberse terminado.

IV.5.2 Cómo responder campañas de descrédito[25]

Algunas veces el hostigamiento se convierte en intentos para desprestigiar a los grupos locales de derechos humanos. Esto les dificulta sus funciones si sus colegas o el público en general, o ambos, empiezan a dudar de su credibilidad, aislándolos o paralizándolos de esta manera; o si las demandas infundidas agotan sus recursos financieros.

Los métodos comunes usados para desacreditar a los grupos de derechos humanos incluyen acusaciones falsas en los medios de comunicaicón o en los tribunales,

[25] Este apartado fue tomado en gran parte de, Estrategias prácticas para grupos pro Derechos Humanos, del Centro para la acción sostenible en Derechos Humanos.

declaraciones públicas locales e internacionaes, y declaraciones privadas hechas a aliados claves tales como funcionarios de las embajadas o donodares. Se les acusa a los grupos de “afiliación a la guerrilla”, “inclinaciones políticas”, “terrorismo”, “traición”, “colaboración con gobiernos extranjeros, u otras formas de “subversión”. Algunos grupos están incluidos en las listas de “organizaciones extremas”, causando así un aumento en la vigilancia de éstos por parte de los Estados, y la exclusión social. Otros son acusados de conspirar con los regímenes opresores, lo que acarrea represalias de los agentes armados no gubernamentales.

Como respuesta, algunas organizaciones trabajan discretamente para poner fin a dichas tentativas para desacreditarlos a través de discusiones privadas con aquellos que formularon los cargos.

Otros actúan más públicamente. Estos se reúnen con agencias relevantes, publican artículos, organizan el respaldo de otra ONG y aliados, buscan reparación en los tribunales, y convocan a la opinión pública por medio de la publicación de comunicados de prensa o al llevar a cabo ruedas de prensa, o ambas a la vez. Ya sea si la respuesta del grupo es privada o pública dependerá de la situación local, pero de cualquier manera, es esencial para los grupos que no recurran al silencio mientras observan los intentos para desacreditarlos.

El Líder De Una ONG Lucha Contra El Estigma

La prensa puede ser un instrumento devastador para desacreditar las organizaciones de derechos humanos. A menudo, los medios de información, ya sean pribados o del Estado, son controlados por intereses poderosos. Un grupo local que trabaja en una sociedad altamente conflictiva, encontró una manera de responder a tal hostigamiento después que su dirigente fuer difamado en dos periódicos locales como agente de las fuerzas guerrilleras. Él demandó a los periódicos por daños y perjuicios, y ganó el caso. Esto fue posible ya que el poder judicial, que a su vez es también el blanco del ejército y los grupos guerrilleros, procedió con valentía y tomó una decisión inusualmente independiente.

La decisión del juez, fue muy justa al adjudicar la retracción de las declaraciones de los dos periódicos que habían publicado la difamación. Las retracciones tenian que ser del mismo tamaño que los artículos originales para que llegaran al mismo público. Uno de los redactores culpables cumplió con la sentencia, pero el segundo se négo y fue encarcelado.

Un grupo entrevistado expresó que, a pesar de que todavía existe una guerra de palabras entre ejército y las organizaciones locales de derechos humanos, esta victoria del tribunal ha contribuido a una prensa más

responsible. Hay menos posibilidades ahora que los periódicos nacionales obliguen declaraciones tergiversadas o editadas selectivamente sobre los grupos de derechos humanso, y es más posible que cubran el tema de los derechos humanos en general.

Para casos en donde se use los tribunales para desacreditar a las organizaciones locales legítimas, vea la sección sobre observadores de procesos.

Otro método utilizado muy frecuentemente en Guatemala es la circulación de anónimos con falsas informaciones sobre la vida privada de algunos líderes. Dichos anónimos se hacen circular entre organizaciones colegas y en medios de prensa. De igual modo, se ha recurrido al rumor esparciendo también informaciones falsas sobre relaciones de líderes o supuestos complots de los líderes con organismos represivos, a fin de aislar a un grupo de dirigentes o a una organización en particular.

Como mecanismo de respuesta a campañas de difamación, algunos grupos buscan la fortaleza en números al crear coaliciones locales, como se hizo en Perú. Allí, en una coalición compuesta de 50 organizaciones de derechos humanos del país, los miembros hablan en favor de cada uno con una voz unida.

Sin embargo, la reacción de otros al ser desacreditados es la de invitar a la solidaridad regional e internacional, de manera que haga resaltar el valor de su trabajo. Este se puede llevar a cabo al publicar comunicados de prensa, invitar a observadores de procesos, involucrarse en campañas conjuntas y organizar actividades públicas tales como discursos, conferencias, cenas para presentar premios, y reuniones con otros activistas y responsables de tomar decisiones locales e internacionales. Dichas actividades pueden ser publicadas para reforzar la credibilidad de los grupos locales y para subrayar la importancia de su trabajo. Las ONG internacionales también pueden exhortar a sus propios gobiernos a que hablen en favor de los grupos locales legítimos cuando éstos estén siendo desprestigiados. Las autoridades simpatizantes de las embajadas (vea página 57) pueden ser invitadas a asistir a actividades públicas patrocinadas por los grupos asediados, ser fotografiado con miembros y, en los peores casos, ofrecer refugio en el suelo de la embajada.

Algunos grupos invitan a los ciudadanos locales influyentes a que sean miembros de su junta directiva, cabildear en su nombre, y aparecer en público para ofrecer de esta manera su solidaridad. Los jueces, abogados, autoridades religiosas, académicos, médicos y empresarios pueden todos influenciar a la opinión pública y política. Todos estos pueden ofrecer experiencia única, y, hasta cierto punto, protección por medio de la asociación si aquellos grupos locales a quienes se está desprestigiando los consideran de alta estima. En Tailandia, algunas ONG invitan a académicos a que cumplan este papel. En la India, Pakistán y Bangladesh, dicho papel lo juegan más a menudo exjueces de la Corte Suprema. En las Filipinas, puede ser más fácil recurrir a las autoridades religiosas y abogados prominentes.

Y en algunos ambientes hostiles, tales como la ex-Yugoslavia, las figuras públicas que se expresan abiertamente han sido objeto de arresto, detención o ejecución sumaria. A mediados de los años noventa en el territorio controlado por los bosnios-serbios, durante la

guerra pero a menudo atrás de las lineas de combate, los líderes no serbios, incluso los médicos, jueces y dueños de negocios fueron amenazados. Los serbios que se opusieron abiertamente a la política serbia también fueron amenazados, y varios fueron asesinados por tratar de proteger a los no serbios. Aunque muchos ofrecieron ayuda, y tal vez más hubiesen podido ser exhortados a ayudar si los serbios prominentes, quienes no estaban de acuerdo con la política central, hubiesen dicho claramente que los serbios tenían la responsabilidad de proteger a sus vecinos de toda la vida, amigos y colegas.

IV.6 Denuncias a Minugua

La Misión de Naciones Unidas para Guatemala (MINUGUA) mantiene vigilancia y verificación en las violaciones a los Derechos Humanos por parte del Estado Guatemalteco. Se puede acudir a denunciar situaciones de acoso, amenazas o allanamientos con el objetivo de que contribuya a esclarecer los hechos y encauzar su tratamiento en las instancias del Estado que correspondan. Las denuncias se hacen en forma verbal y son atendidas por un oficial acreditado por la Misión, quien tomará nota y de acuerdo con la gravedad de los planteamientos, procederá a realizar la investigación a su alcance.

En la actualidad Minugua mantiene oficinas en la ciudad capital y en algunos departamentos y municipios, aunque ha anunciado su disminución paulatina, en vista de que su mandato está por concluir, en diciembre del 2003. Es probable que continúe su presencia un año más pero no hay certeza de ello.[26]

IV.7 Denuncias a la Procuraduría de los Derechos Humanos (PDH)

A la Procuraduría de Derechos Humanos también se pueden presentar denuncias sobre las amenazas e intimidaciones que sufren personas o instituciones que se dedican al tema de los derechos Humanos. La PDH realizará su propia investigación con los datos que los denunciantes aporten. Deberán hacerlo de manera verbal y un oficial de la institución se encargará de tomar nota para proceder a analizar la información y proceder de acuerdo a la gravedad del caso.

[26] Ver listado de direcciones de Minugua en la sección V.Anexos.

Las denuncias se pueden presentar en las oficinas centrales situadas en la 12 avenida 12-72 de la zona 1. Los teléfonos son 230 08 74 al 76. Y en todos los departamentos del país hay oficinas de la PDH que cuentan con un representante del Procurador donde le dará curso a la denuncia presentada. Existen auxiliaturas en cinco regiones del país, a donde también se puede acudir a presentar una denuncia porque se cuenta con un representante del Procurador en cada una de ellas. Algunas axiliaturas son móviles, lo cual significa que se desplazan a las comunidades del área para conocer las denuncias que se presentan y recopilar la información que se considere necesaria.[27]

IV.8 Denuncias a la Policía Nacional Civil (PNC)

En las Comisarías de la Policía Nacional Civil se deben presentar las denuncias sobre cualquier hecho que atente contra la seguridad de las personas. Con el objetivo de abrir las investigaciones y apoyar en su conducción, es aconsejable presentar todos los datos que se tengan, tales como número de placas, descripción de personas, características de las amenazas o intimidaciones, así como toda la información que ayude en las pesquizas.

Cuando se presente la denuncia a la PNC, la persona debe llevar su cédula de vecindad y relatar verbalmente los hechos que ha enfrentado, de tal manera que un oficial escribe el parte que al terminarlo se lo leerá, y se le podrán hacer correcciones. Esta denuncia es trasladada en un lapso de 24 horas al Ministerio Público, y citarán a la persona para que ratifique la denuncia y proceder a abrir la investigación.

Las Oficinas Centrales están ubicadas la 6ª avenida 13-71 zona 1, en el Palacio de la Policía Nacional. También hay varias Comisarías de la PNC en diferentes zonas de la ciudad capital y en los Departamentos del país.[28]

IV. 9 Denuncias al Ministerio Público (MP)

Las denuncias también deben hacerse ante el Ministerio Público al igual que en la PNC. Es aquí donde se desarrollarán la investigaciones de la situación presentada por las personas e instituciones que están siendo amenazadas y hostigadas. De obtener resultados dictarán las medidas legales contra quienes se encuentren responsables.

[27] Ver listado de Auxiliaturas de la PDH en la sección V.Anexos.
[28] Ver listado de las Comisarías y Subestaciones de la PNC en la sección V.Anexos.

Los denunciantes deben presentar un relato verbal de los hechos, y aportar todas las características y pruebas que tengan para posibilitar la investigación. La persona denunciante debe presentar su cédula de vecindad para que se inicien las acciones pertinentes.

Las oficinas del área metropolitana se encuentran en la avenida 8ª Avenida 10-57 zona 1y existen fiscalías distritales y municipales en todos los departamentos del país[29].

IV.10 Acciones urgentes

Las acciones urgentes se producen cuando alguien activa una red de personas en el extranjero. Cada una de ellas envía una comunicación al Gobierno de Guatemala manifestando preocupación por su caso. Se utiliza sobre todo cuando está en peligro la seguridad de la persona, como una medida de protección.

Amnistía Internacional es uno de los grupos de derechos humanos más importantes, ya que tiene una base de membresía personal enorme de individuos quienes se comprometen con la defensa de los derechos humanos. Por ende, **Amnistía Internacional** es el grupo más conocido por sus acciones urgentes, pero también hay otras tales como la **Red de Apoyo**, que tiene contacto con grupos de solidaridad alrededor del mundo.

Sirve tener contacto y comunicación regular con las instituciones que manejan acciones urgentes para que sepan qué tipo de trabajo hacen las instituciones en Guatemala, qué hace la institución donde trabaja. Así podrán responder rápidamente y con conocimiento previo del contexto de la situación.

También, es útil conseguir copias de Acciones Urgentes (por ejemplo de la página de web de Amnistía Internacional) para poder ver el tipo de información incluida.

Una vez se ha decidido optar por este tipo de reacción, la persona puede preparar su solicitud:

- Asegurarse que tiene toda la información sobre el hecho, corroborada con otras personas presentes

- Preparar un breve relato de los hechos y agregar información sobre qué trabajo realiza la persona o personas afectadas

- Especificar a los receptores de la Acción Urgente a quién deberían dirigir sus cartas o peticiones, por ejemplo: al Presidente, Ministerio de la Defensa, Ministerio

[29] Ver listado de fiscalías distritales y municipales del Ministerio Público en la sección V. Anexos.

de Gobernación, Jefe la PNC, Jefe de Destacamento X, incluidas direcciones, números de fax, teléfono y correo electrónico.

- Especificar quién recibirá copias de las cartas: normalmente la organización / ONG donde trabaja la persona afectada

- Detallar qué otras medidas se van a tomar o ya se han tomado: denuncias ante otras instancias, peticiones a otras organizaciones internacionales, aviso a embajadas

El costo: Es bajo. Gastos de llamadas telefónicas, correo electrónico. Poco tiempo necesario de preparación y comunicación.

¿A dónde dirijo mi solicitud?

La Sede de Amnistía Internacional (la Secretaría Internacional) está en Londres. Es allí donde se toma la decisión sobre la emisión de Acciones Urgentes:

Amnistía Internacional:
Sección de Guatemala,
Encargada: Tracy Ulltveit -Moe
International Secretariat,
1 Easton Street,
LONDON WC1X 8DJ
Tel: 0044 207 413 5500
Fax: 0044 207 956 1157
Email: tulltvei@amnesty.org

También la red de Acción Urgentes de Amnistía Internacional se activa enviando un correo electrónico explicando la situación a: amnestyis@amnesty.org, y luego en la línea de referencia se pone: ATENCIÓN: GUATEMALA RESEARCH TEAM. Si fuera muy urgente, se puede llamar al teléfono 303-258-1170 para avisar de la entrada de este correo.
Además de comunicar la situación de peligro, debe dar direcciones y formas para ser contactado, para que un investigador de AI que hable español lo localice para verificar la denuncia.

Red de Apoyo Internacional:
Coordinación de Acompañamiento Internacional en Guatemala
Amaya de Miguel
Coordinadora
2ª Calle, 4-42,
Zona 2,
Ciudad de Guatemala
Telefax: 232 3181
Email: acoguate@gmx.net

IV. 10.1 Situaciones de emergencia[30]

A pesar de las fuentes de respaldo y solidaridad, los grupos locales de derechos humanos, siguen enfrentando emergencias. Estos grupos deberían prestar especial atención a las siguientes consideraciones de seguridad. Los miembros del personal no deben viajar solos a las jefaturas de policía o a las bases militares y deberían notificar a otros de sus planes de viaje y los lugares en donde se encuentren en todo momento. Sugerimos que se tomen los pasos siguientes cuando surja una situación de emergencia, particularmente una detención extrajudicial en la que el captor está identificado.

1. Ponerse en contacto personal o en grupo, por teléfono o a través de intermediarios, con las personas (militares, policías, u otros) que se cree tienen bajo custodia al detenido o están poniendo en peligro al grupo. Si no está claro quiénes son estas personas, será necesario ponerse en contacto con varias jefaturas de policía o bases militares.

2. Las preguntas que deben hacerse incluyen, ¿Cuál es la localidad exacta en donde se encuentra el detenido? ¿Quién lo tiene bajo su custodia? ¿Cuál es el estado de salud del detenido? ¿Cuál es la razón de su detención?

3. Una ONG debería hacer todo lo posible para enviar grupos a visitar a la persona en detención, acompañada de testigos objetivos, si es posible. Se debe entrevistar a los detenidos (lejos de los oídos de los guardias), y se debe obtener, tanta información como sea posible sobre el caso, incluso cómo están siendo tratados, y su condición física.

4. Si el grupo cree que los detenidos han sufrido daños físicos, se debe llevar a un médico al lugar de detención, o se debe hacer demandas para que las autoridades proporcionen atención médica.

5. Se le debe hacer saber a las autoridades que las ONG están siguiendo de cerca el caso. El grupo de una ONG debería visitar el centro de detención tan a menudo como sea posible.

6. Un grupo tiene que decir si debe buscar la atención pública local o internacional, o ambas. Cada caso es diferente. Algunas veces la publicidad puede aumentar la intransigencia en vez de salvar vidas.

   Algunas veces la situación será tan peligrosa que no existe alternativa para los individuos excepto salir del país, disolver el grupo u operar clandestinamente. Esto puede ser difícil por muchas razones (personales, monetarias y prácticas). Pero si se sale del país, se debe considerar lo siguiente:

[30] Este apartado fue tomado en gran parte de, Estrategias prácticas para grupos pro Derechos Humanos, del Centro para la acción sostenible en Derechos Humanos.

1. *Documentación Apropiada:* Los viajeros necesitan pasaportes válidos y las visas necesarias. Si fuera posible, se debe hacer estos preparativos antes que cualquier emergencia ocurra.

2. *Buena disposición para marcharse:* Los activistas prominentes con un historial largo de haber sufrido hostigamiento compran típicamente pasajes de avión por adelantado, y los mantienen (junto con sus pasaportes) a la mano todo el tiempo. También es aconsejable tener un plan de reserva (por ejemplo, si viajar por avión no es una opción, se debe planificar una ruta por tierra fuera del país.

3. *Contactos internacionales:* Las organizaciones internacionales pueden a veces arreglar salidas de emergecia de individuos a través de sus propios concactos con los gobiernos y agencias extranjeras.

4. *Cartas de invitación:* Los individuos que temen llegar a ser el objeto de hostigamiento deben obtener ofertas permanentes de las universidades o instituciones extranjeras para dar clases o realizar investigaciones. Esto facilitará los problemas con la visa y podría cubrir los gastos de esatadía mientras se encuentra en el extranjero.

5. *Destinos:* Algunos activistas de derechos humanos tienen a huir a países lejanos, porque piensan que tendrán más libertad de continuar con su trabajo. Sin embargo, los países más cerca del propio pueden proveer lugares menos costosos para vivir y más oportunidades de trabajo.

   En casos tales como desaparición o temor de ser torturado, la acción rápida es principal. A pesar de que esto es una fuente de debate, en casos extremos, algunos grupos se oponen a la espera de verificación de hechos si esto resulta en fatalidades. Estos piensan que es más importante actuar rápidamente para salvar vidas. Cuando se sospecha que ha habido una ejecución, tortura, o detención extrajudicial, las campañas de acciones urgentes juegan un papel muy importante. Se describen algunas más abajo.

Los grupos locales pueden enviar información de naturaleza urgente a Amnistía Internacional en Londres, teléfono: 44 171 413 5500, Fax: 44 171 956 1157, dirección electrónica: uateam@amnesty.org. Cuando envíe mensajes por correo electrónico, incluya el nombre del país involucrado en el espacio del “asunto”, por ejemplo, “atención: investigación en Bolivia”. En caso que no se consiga comunicaicón con la oficina de Londres, los grupos pueden ponerse en contacto con una sección de Amnistía de Estados Unidos, Teléfono: 303 258 7886, Fax: 303 258 7881, dirección electrónica: sharriso@aiusa.org.

Aunque las misiones de las ONG Internacionales son diferentes, incluso Amnistía Internacional, el Article 19, el comité para proteger a los Periodistas, Human Rights Watch, International League for Human Rigths y el Comité de Abogados para los derechos Humanos producen alertas con respecto a los grupos locales de derechos humanos y otros que se encuentra en peligro.

En 1997, además de su otro trabajo, la International Feration of Human Rigth y la Organización Mundial contra la Tortura formaron una alianza llamada Observatory. El objeto es comunicar sistemáticamente a la comunidad internacional (90.00 entidades, incluso gobiernos, organismos intergubernamentales, ONG y medios de comunicación) sobre actos atroces de hostigamiento y represión de los defensores, particularmente cuando en casos específicos se requiere intervensión inmediata. Una línea para emergencias especiales ha sido establecida para comunicaciones urgentes (dirección electrónica: observatoire@iprolink.ch; fax en Francia: 33 (0) 1 4039 2242). El Observatory también lanza misiones de investigación en situaciones de extrema necesidad para proporcionar apoyo directo a los defensores a un nivel nacional. Además, publica un informe anual que puede ser usado como un documento de acción para el reconocimiento internacional y como protección de los defensores.

El Human Rights Internet publica regularmente, en su sitio de la web (http//www.hri.ca/urgent) alertas, acciones, campañas y comunicados de prensa urgentes de los grupos de defensa de los derechos humanos alrededor del mundo. Se enfoca en la situación en vez de casos individuales, por ejemplo, grupos en peligro, países en crisis, acciones dentro de las Naciones Unidas y otras arenas internacionales o regionales.

Además los comunicados dirigidos a la oficina de procedimientos especiales de las Naciones Unidas (incluso los relatores especiales) ocasionalmente contienen información sobre una violación seria de derechos humanos que está a punto de ser cometida (por ejemplo, ejecusiones extrajudiciales inminentes, o tortura) en dichos casos, el relator especial relevante o director de un grupo de trabajo pueden dirigir un mensaje a las autoridades pertinentes y solicitar que clarifiquen la situación. Estos mensajes no prejuzgan una situación pero son preventivos. Las solicitudes especificas para dicha intervensión urgente pueden ser dirigidas a los relatores especiales relevantes o un grupo de trabajo c/o la Oficina del Alto Comisionado para los Derechos Humanos –UNOG, 1211 Ginebra 10, Suiza, el fax en Ginebra: 4122 917 9003; dirección electrónica: webadmin.hchr@unog.ch. Las palabras “Acción Urgente” deben ser escritas en el comienzo de la comunicación para poder facilitar una transmisión inmediata a la parte correcta.

La Oficina del Alto Comisionado para los Derechos Humanos ha establecido una Línea de emergencia para facsímiles sobre derechos humanos en Ginebra: 4122 917 0092, disponible las 24 horas del día. El objetivo de esta línea de emergencia es ayudar a la Oficina del Altro Comisonado a controlar y reaccionar rápidamente a las emergencias de derechos humanos. Esta línea de emergencia está disponible a las víctimas de violaciones a los derechos humanos, sus familiares y las ONG.

Finalmente, el sistema interamericano cuenta con un mecanismo de acciones urgentes para individuos que pueden demostrar una amenaza seria de daños irreparables. Para obtener Medidas de Precuación, los demandantes pueden aplicar a la Comisión Interamericana; y para obtener Medidas Provisionales que

requieren que el estado acusado haga el máximo esfuerzo para prevenir la transgresión, se puede aplicar a la Corte Interamericana.

Algunas ONG internacionales han establecido un fondo para ayudar a los grupos locales asediados que se encuentren en situaciones de emergencia. Algunas han exhortado a que se establezcan más fondos como éstos, incluso establecer líneas telefónicas las 24 horas del día, cuyas llamadas por cobrar las contesten personas reales en vez de una máquina contestadora. Dichas iniciativas pueden incluir a las ONG, periodistas o figuras públicas, o ambas, quienes acuerden estar de guardia las 24 horas del día en situaciones en donde vidas humanas se encuentran en peligro inmediato.

IV.11 Protección internacional

Es aquella protección ofrecida por gobiernos o entidades internacionales. En los casos extremos, como el asilo político, requieren de una serie de trámites que es necesario realizar para asegurar que el estatus de tal es otorgable. Aquí encontrará algunas ideas, de acuerdo con la legislación vigente, que pueden orientar a este respecto.

IV. 11.1 Pidiendo estado de refugiado o asilo político en otros países o embajadas

A diferencia de las Acciones Urgentes y Medidas Cautelares, se sugiere que para esta medida se busque el apoyo de un abogado con experiencia en el tema. De esta manera se podrá conocer las posibilidades reales de éxito y redactar la solicitud en una forma que pueda maximizar dichas posibilidades.

El marco legal:

Asilo político es una figura basada en el derecho internacional y en las relaciones internacionales entre países. Hay dos maneras en que un país puede brindar protección a una persona:

Primero, bajo la Convención de 1951 sobre el Estado de Refugiados (“la Convención”) y segundo bajo el poder soberano que tiene cualquier Estado de permitir la presencia de extranjeros en su territorio nacional. Esta segunda opción es menos común.

Los requisitos que dispone la Convención son bastantes rígidos y exigentes. Desafortunadamente hoy día la tendencia internacional es de interpretarla de una forma restringida. Dice en Artículo 1(2):

"Para los propósitos de la presente Convención, el término "refugiado" aplicará a cualquier persona quien, debido a un miedo fundamentado de ser sujeto de persecución por razones de raza, religión, nacionalidad, o porque pertenece a un grupo social o político, está afuera de su país de origen y no puede, o debido a dicho miedo no está dispuesto a, aprovechar de la protección de dicho país..."

Por lo tanto, la regla general es que la persona tiene que estar afuera de su país de origen ANTES de pedir asilo bajo la Convención. Muchos países exigen que la persona que pide asilo, lo solicite en el momento de llegar, ya sea en el aeropuerto o en el puesto de migración de la frontera. Incluso, esperar hasta que la persona esté dentro del país puede perjudicar su petición: unos países lo toman como un pretexto para negar la petición. Sin embargo, la persona muchas veces va a querer estar lo más lejos posible de su país y va a querer evitar la posibilidad de deportación inmediata. Entonces, si es posible y si hay tiempo, lo mejor es averiguar anticipadamente, las reglas legales de asilo del país al cual se va y con base en ellas tomar la decisión sobre a dónde se va a presentar la solicitud.

Una excepción en la práctica de la regla, dice que se debe estar afuera del país antes de pedir asilo, entonces se puede ir a una Embajada dentro de Guatemala. Si no hay manera de poder salir, y la persona está considerando ir a una Embajada, es aconsejable averiguar qué embajadores están dispuestos a recibir solicitudes, ya que algunos tendrán una política interna o práctica dependiendo del país. Otro consejo es no agotar la buena voluntad de la Embajada, pidiendo asilo cuando no se tiene preparado un buen argumento o evidencias convincentes para la petición. La peor pesadilla de muchas Embajadas es tener una multitud de personas solicitando asilo, que después no dan seguimiento a la petición o quienes no llevan suficiente información con ellas. Con estas debilidades solo se posibilita a la Embajada un pretexto para negar la solicitud.

La Petición:

Puede ser verbal o escrita, dependiendo de las reglas internas de procedimiento del país donde se solicita protección. Junto con la petición inicial o poco después, se tendrá que presentar pruebas. Lo que se está haciendo en la petición es intentar demostrar a las autoridades la probabilidad de que en el futuro, si la persona se queda en su país, es probable que vaya a sufrir persecución por las razones especificadas. En pocas palabras, la evidencia que se tiene que proporcionar es de dos categorías: a) Evidencia sobre la propia situación personal y b) Evidencia sobre la situación del país que afectaría su seguridad. La persona tiene que demostrar que lo que teme es persecución. La definición legal de persecución varía entre países, pero es más exigente que comprobar acoso. Además, no es suficiente decir que se tiene temor de persecución: se tiene que demostrar que se puede comprobar ese temor objetivamente por las condiciones del país.

Finalmente la persona tiene que comprobar que la persecución está basada en una de las cinco razones mencionadas en la Convención: raza, religión, nacionalidad, grupo social o político.

La persona debe presentar su propio testimonio, especialmente sobre eventos en el pasado que pueden tener una posibilidad real de que puedan repetirse. Si hay declaraciones de otros testigos o documentos que pueden corroborar su testimonio, hay que conseguirlos. También ayuda presentar documentos tales como informes sobre la situación actual de derechos humanos en su país en cuanto a personas con trabajo parecido o una situación parecida a la suya. Se tiene que ofrecer alguna evidencia de la probable fuente del riesgo de persecución: ya sea el Estado u otra.

¿Qué hago si temo persecución no estatal?

Algunos estados como Alemania han interpretado la Convención de una manera en que nadie puede lograr asilo si tiene miedo, aunque fundamentado, de actores no estatales. Otros países aceptan peticiones así, por ejemplo de personas perseguidas por la mafia, crimen organizado o grupos insurgentes, cuando el Estado no es capaz de brindar suficiente protección. Si el riesgo de persecución viene de una fuente no formalmente estatal (por ejemplo, ex patrulleros), se puede ofrecer evidencias de complicidad con el Estado, con su aquiescencia, falta de voluntad o simplemente incapacidad del Estado de protegerle. Sin embargo – otra vez -, hay que demostrar que el riesgo de persecución existe no importa en qué parte de país se esté.

¿Qué pasa si rechazan mi petición?

Si no se logra convencer al país extranjero de que se reúne todos los requisitos de la Convención, ese país todavía puede darle permiso de permanecer allá, usando su poder soberano general (opción dos, mencionada al principio). Normalmente esto se llama “Permiso Extraordinario”. El Estado puede proporcionar esta medida por razones humanitarias y por un período determinado, por ejemplo un año, y se puede solicitar su renovación. Si durante el período la situación empeora – se puede pedir asilo político otra vez, sobre la base de las nuevas circunstancias de riesgo de persecución.

Siempre hay que tomar en cuenta que si no se logra asilo político, ni una especie de permiso extraordinario – existe el riesgo que le deporten y que las autoridades de gobierno estén informadas de su llegada. Si intenta ir a un tercer país, después del rechazo de su solicitud, este tercer país muchas veces le enviará ya sea al país que rechazó su solicitud o directamente a su país.

¿Quién puede ayudarme?

Hay ONG en varios países que brindan asesoría legal después de su llegada: sirve averiguar con anticipación, a través de ACNUR o Amnistía Internacional, qué organizaciones hay en los países a donde iría en estas circunstancias. En Guatemala, el Centro de Acción Legal en Derechos Humanos (CALDH), también tiene abogados con experiencia en representación de personas pidiendo asilo.

Se puede obtener mucha información de la página de web de ACNUR:
www.unhcr.ch

Costos: Alto, especialmente si no se tiene asesoría legal gratis. Gastos de viaje. Mucho tiempo invertido en la preparación.

¿A dónde dirijo mi solicitud?

A las autoridades de migración del país extranjero o a la embajada del país relevante (si se pide protección bajo la Convención o asilo afuera del ámbito de ello).
ACNUR tiene oficinas en varios países. Sin embargo solo pueden decidir sobre peticiones para asilo en dos circunstancias: una, si el país ha invitado ACNUR a su territorio con el propósito de tramitarlas o dos, si es indispensable para su función de protección que las tramiten.

IV.12 Tribunales internacionales

En términos regionales, se puede llevar un proceso normal de Petición ante la Comisión Interamericana de Derechos Humanos (CIDH). No habrá un resultado rápido y puede ser costoso. Información y guías escritas sobre cómo llevar casos a la Comisión estan disponible en la página web www.cidh.org o en las oficinas de CALDH (251 4157). La dirección para enviar peticiones está detallada en el apartado de esta guía sobre "Medidas Cautelares". Aparte del sistema Interamericano, en el ámbito internacional, hay varios Comités y Comisiones que tratan de distintas violaciones de los derechos humanos y ofrecen distintas medidas.

Acudir a estas instancias, no sería una medida de prevención de hostigamiento o amenazas a corto plazo, ya que cualquier proceso ante ellas será largo y costará mucho esfuerzo. No es fuera de lo normal esperar tres o cuatro años para una determinación. Además, antes de acudir a estas instancias es necesario agotar los recursos legales del sistema interno de Guatemala o estar en condiciones de alegar uno de las excepciones de esta regla.

Por lo tanto, la idea de usar estas instancias es lograr reconocimiento posterior de las violaciones estatales, conseguir reparaciones y castigo para el gobierno internacionalmente. Son más útiles para casos paradigmáticos, o grupos de casos parecidos que muestran prácticas sistemáticas.

Dentro del sistema de las Naciones Unidas hay tres órganos competentes que reciben denuncias de individuos víctimas de violaciones de derechos humanos:

1. El Comité de Derechos Humanos
2. El Comité contra la Tortura
3. El Comité sobre la Eliminación de Discriminación Racial

Generalmente, el más útil para denuncias de acoso / amenaza u hostigamiento sería el Comité de Derechos Humanos. Por razones de espacio, esta sección de la guía se

concentrará en el Comité, ya que es un ejemplo de una instancia internacional muy útil y ahora accesible para los Guatemaltecos.

El Comité fue establecido bajo el Pacto Internacional de Derechos Humanos y Civiles. El Estado de Guatemala ratificó el Protocolo Opcional en noviembre del año 2000 y entró en vigor para Guatemala el 28 de Febrero de 2001. Quiere decir que Guatemaltecos víctimas de abusos de los derechos humanos que tienen lugar después de esa fecha y que son nombrados en el Pacto pueden acudir al Comité.

Las decisiones del Comité, en la rama del derecho internacional de los derechos humanos, tienen mucha legitimidad y fuerza, por la historia del órgano y sus integrantes judiciales.

La Comunicación al Comité

La comunicación al Comité debe incluir la siguiente información:

- nombre,
- dirección,
- nacionalidad de la víctima,
- asesor de la víctima si hay,
- identificación de Estado acusado,
- la fecha de presentación y la firma de la víctima o su representante
- detalles sobre los artículos del Pacto violados según la alegación
- pasos que se han tomado para agotar los recursos internos
- una declaración al efecto si el asunto está conocido por otra instancia internacional y
- la descripción detallada de los hechos.

La comunicación se dirige al:

Comité de Derechos Humanos

Centro de Derechos Humanos de las Naciones Unidas,
Palais des Nations
8 – 14 Avenue de la Paix
1211 Geneva, Ginebra 10
Switzerland, Suiza
Tel: 22 734 6011
Fax: 22 733 9879

También se puede contactar a la sub oficina en Nueva York para información o avisar de casos urgentes:
Naciones Unidas
New York, Nueva York 10017,
Tel. 212 963 5930

IV:13 Medidas cautelares de la OEA

IV.13.1 Solicitando medidas cautelares ante la Comisión Interamericana de derechos humanos

Hay tres posibles acciones que se pueden tomar ante la Comisión:

a) Una solicitud para medidas cautelares
b) Una Petición incluyendo una solicitud para medidas cautelares
c) Una Petición

Una solicitud para medidas cautelares se trata de intentar prevenir una violación grave a la vida o integridad personal. Una Petición se trata de responsabilizar al Estado y pedir reparaciones para una violación ya consumada. Las medidas pueden ser varias: protección de la persona por la policía, investigación sobre la fuente de la amenaza. Si ya ocurrió una violación de derechos humanos y se pretende prevenir una repetición, se puede juntar la solicitud y una Petición formal, o sea, enviar una Petición que incluye una solicitud para medidas cautelares. Sin embargo, lleva tiempo preparar una Petición, correctamente con los documentos o anexos necesarios. Y si la necesidad urgente es la protección, se debería enviar la solicitud de inmediato. Más tarde se puede interponer la Petición.

Las provisiones legales relevantes son:

Artículo 29 del Reglamento de la Comisión incisos 1 y 2 y
Artículo 41 de la Convención Interamericana sobre Derechos Humanos.

Artículo 29, Inciso 2 del Reglamento dice:

"En casos urgentes, cuando se haga necesario para evitar daños irreparables a las personas, la Comisión podrá pedir que sean tomadas medidas cautelares para evitar que se consume el daño irreparable, en el caso de ser verdaderos los hechos denunciados".

El proceso normal es que la Comisión, al recibir la solicitud decidirá si está fundamentada y de ser así, dirigirá inmediatamente una comunicación al Ministro de Relaciones Exteriores de Guatemala, alertándole del riesgo al daño irreparable y pidiendo que tome las medidas cautelares necesarias para evitarlo. La práctica de la Comisión es que normalmente da al gobierno 30 días para iniciar las medidas, pero puede imponer un plazo más corto dependiendo de la situación. En unos casos se ha puesto un plazo de dos días por ejemplo.

Si el gobierno no toma las medidas necesarias, la Comisión puede enviar el asunto a la Corte, la cual después puede ordenar que el Estado las tome.

La forma de la solicitud no es muy formal e incluso, se puede hacer en forma de una carta. Si la persona no tiene asesoría legal que la haga sin cobrar, puede hacerlo sola. Igual que en todos los procesos de la Corte Interamericana de Derechos Humanos (CIDH), no es necesario usar papel oficio, timbres, sellos o tener la firma de un abogado. La idea es que el sistema sea útil para el público y que la víctima tenga acceso fácil y barato. En términos generales, seguirá la siguiente forma para una solicitud:

El **título** (opcional) Organización de Estados Americanos
Comisión Interamericana de Derechos Humanos
Solicitud para Medidas Cautelares
Nombre y dirección del solicitante
(Se puede poner la dirección de su asesor legal u otra persona).
Nombre y dirección del asesor legal si hay.
Fecha de presentación.

Entonces, los apartados serán:

- **Introducción**: quién es el solicitante, dónde trabaja, que pretende evitar una violación de tal naturaleza. Debe escribirse un párrafo muy breve.
- **Antecedentes:** Hechos que son pertinentes y relevantes pero que no constituyen la amenaza / violación / riesgo de violación de derechos humanos, pero que le dan contexto al hecho actual.
- **Hechos**: aquí se incluye detalles sobre los eventos que demuestran el posible daño irreparable.
- **Provisiones legales pertinentes.** Además de las partes de la Convención y Reglamento ya mencionado, vale la pena relacionar a la Convención qué podría pasar: por ejemplo, hay riesgo de que se viole el derecho la vida, protegido por artículo 4...
- **Petición:** qué se quiere: (Por ejemplo) que la Comisión pida al Estado de Guatemala que tomen las medidas cautelares necesarias para evitar que XX pase a la señora XX

NOTA:
Hay un nuevo reglamento que entró en vigencia en mayo de 2002 y para solicitudes después de abril, se debe hacer referencia al Artículo 25 del nuevo Reglamento:

"En caso de gravedad y urgencia y toda vez que resulte necesario de acuerdo a la información disponible, la Comisión podrá, a iniciativa propia, o a la petición de parte, solicitar al Estado de que se trata, la adopción de medidas cautelares para evitar daños irreparables a las personas".
Entonces, la Comisión podrá tomar acción después de mayo sin haber recibido una solicitud.

Además, hay un nuevo inciso 3 que dice:

“La Comisión podrá solicitar información a las partes interesadas sobre cualquier asunto relacionado con la adopción y vigencia de las medidas cautelares”.
Quiere decir que fortalece el poder de la Comisión de hacer cumplir con sus recomendaciones al Estado.

Más información:

Todos los documentos, incluyendo la Convención y Reglamento están disponibles en la página web de la Comisión:

www.cidh.org
Además, los abogados que trabajan en la sección de Guatemala estarán dispuestos a ayudarle con cualquier duda.

Costo: Medio, si no se paga un abogado. Gastos de fax, llamadas telefónicas. Más tiempo en preparación que una Acción Urgente.

¿A dónde dirijo mi solicitud?

Pablo Saavedra
Encargado sección: Guatemala
Comisión Interamericana de Derechos Humanos
1889 F Street N.W.
Washington D.C.
Tel: 202 458 3423
Fax: 202 458 3992
Email: psaavedra@oas.org

V. ANEXOS

V.1 Listado parcial de psicólogos que trabajan con estrés post-traumático

Dra. Elvira Ariano Jeréz
Calzada Roosevelt 36-48, zona 7
Clínica 8, Hospital de Día Itzamná
Tel. 5913666

Licda. Ligia Barrascout de Piedra Santa
10ª. Ave. 16-71, zona 14
Tel. 3683296

Licda. Guisela Cárcamo Duarte
Boulevard Liberación 2-68, zona 13
Tel. 4713578

Licda. Anaité de la Cruz Calderón
17 ave. 3-05, zona 15, Col. Jardines de Minerva
Tel. 3692655 y 3658115

Lic. Marco Antonio Garavito,
Director
Liga Guatemalteca de Higiene Mental
Tel. 232-6269, fax 238-3739
liga@concyt.gob.gt

Dr. Jorge Aldana
6 Ave. "A" 10-36, zona 9, 3er nivel
Tel. 362-2754/5/6

M.A. Edgar Alfonso Rodríguez Castillo
Tel. 405-7740 y 4721162

Olga Alicia Paz, Felipe Sarti, y Susan Navarro
ECAP (Equipo de Estudios Comunitarios y Acción Psicosocial)
Tel. 363-5270 y 5403
ecap@guate.net

V.2 Algunos equipos básicos de seguridad[31]

EQUIPO	PRECIO	DISTRIBUIDORA	UBICACIÓN
Caja con llave para disquetes	$ 20.00	Supermercados, librerías y otros.	
Programa PGP de encriptación	Gratis	Sitio web:	Internet
Programa firewall	Gratis o muy barato, asistencia técnica para su instalación y uso.		
Disco zip	$ 218.00	Tiendas de accesorios de computadoras como Microsys	6 Av. Y 4 calle Zona 9
Programa para borrar disco duro	Dentro dePGP y otros		
Celular para una persona	Variable y muchas ofertas en el mercado	PCS, Comcel,Telefónica, Bell South y otras.	Diferentes lugares en todo el país.
Caja Fuerte (p/empotrar pared)	$ 900.00 a $ 2,500.00	Alarmas y Servicios de Seguridad.	23 Calle. 1-05 Zona. 1 3er. Nivel.
Caja Fuerte Gde. (p/empotrar pared).	$ 700.00	PRICE SMART	Periférico, zona 11; Zona 4 y Zona 10.
Alarmas o luces que se encienden con movimientos	$ 20.00	Simex	
Alarmas contra robo y asalto.	$ 230.00	Alarmas De Occidente, S.A. 7ª. Calle. “A” 5-31	Zona 3 (Mixco) Col. Nueva Montserrat. Telefax: 5942215
Abridor electrónico de puertas	Diferentes precios de acuerdo a características de las puertas. Puede estimarse arriba de. $ 2,500.00	Lugares especializados	
Circuito cerrado de televisión, C.C.T.V. B/N 1 cámara.	$ 770.000	Alarmas y Servicios de Seguridad.	23 Calle. 1-05 Zona 1 3er. Nivel.
C.C.T.V. B/N 2 Cámaras.	$ 1,100.00	Ídem.	Ídem.
C.C.T.V. Color 2 cámaras.	$ 2,500.00	Idem.	Idem.

[31] Los precios se colocan en dólares debido a las fluctuaciones del mercado.

C.C.T.V. Color 4 cámaras.	$ 4,800.00	Idem.	Idem.
C.C.T.V. B/N 4 Cámaras	$ 1, 730.00	Idem.	Idem.
C.C.T.V. B/N 1 cámara.	$ 270.00	PRICE SMART	Periférico, Zona 11; Zona 4 y Zona 10.
Cámaras adicionales.	$ 90.00	Idem.	Idem.
Cable extra p/cámaras.	$ 28.00	Idem.	Idem.
Cámara digital con telefoto	$.500.00 y más	Mivrosys, Canella, Kodack, Quick	
Máquina trituradora de papel.	$ 25.00 o más, según la capacidad	Idem.	Idem.
Construcción de una caja de ratones en la entrada	Depende del edificio		
Cortinas o persianas	Depende del edificio		
Puertas reforzadas	Depende del edificio		
Mantener membresía en asociaciones profesionales claves	Depende de la profesión		
Mantener pasaportes y visas vigentes	Q.100.00 por persona. Visas depende del país, para Estados Unidos, $ 100.00	Migración	
Cambio periódico de registros y chapas.	Entre $ 30.00 y $ 40.00	Cerrajerías de prestigio y de antigüedad	

(*) La mayoría de empresas ofrece precios especiales si varias instituciones se organizan para comprar de manera global o por paquetes. En el caso de las alarmas, depende de la observación visual que el personal de estas empresas realice en cada una, para determinar el área a proteger de cada una de las instituciones; y, brindan asesoría como parte del servicio de venta de equipo.

V.3 Listado de medios de prensa en Guatemala.

A continuación, facilitamos los teléfonos de la redacción de algunos medios periodísticos. La lista completa es mucho mayor y sugerimos a su institución, mantener una lista completa y actualizada, no sólo de los medios sino también de teléfonos celulares de los periodistas.

Preferentemente mantener listas de reporteros de sección nacional o política y seguridad.

Medio	Teléfonos	Fax
Prensa Libre	2301384, 2301383, 2301670,	2518768
ElPeriódico	3321578, 3347036, 3620242 al 45	3329761
Nuestro Diario	3321578, 3347036, 3620242 al 45	3329761
Siglo XXI	3607004	3319145
La Hora	2321903	
Al Día	3397430	3397435
El Quezalteco	7674331	7670850
Emisoras Unidas	4405139, 4405140, 4405133 al 38	4405159
Radio Punto	3799595	3799560
Corporación Nacional (RCN)	3352030	3352005
Radio Sonora	3693970	
Guatemala Flash	2206543 al 46, 2327219	2513915
Comando Informativo	2382233	2382233
Notigrupo Alius	3799595, 3799559	3799560
Noti7	4347001, 4347246, 4347707	4346744
Telediario	4347493	4347491
Club de prensa extranjera	2210301, 2210306, 2329034	2329034

V.4 Oficinas de Minugua en Guatemala.

OFICINA	DIRECCION	TELEFONOS
Guatemala, sede central	Blvd. Los Próceres 18-67 Zona 10, Edificio Torre Granito	279 3333 445 3333
Guatemala, oficina regional	1ª Calle 1-53 Zona 2, Ciudad	2453332, 2793332
Quetzaltenango	3a. Calle 15A-20, Zona 1	761 4321, 763 0688, Fax 763 0750
Huehuetenango	2a. Avenida 2-25, Zona 1	764 2860, Fax 764-2551
Coatepeque, Quetzaltenango	5a. Avenida 4-55, Apto. B, Nivel 2, Zona 1	445 3565, 445 3566, 279 3565, 279 3566 Fax: solicitar señal
Sololá	4a. Avenida 12-05, Zona. 1, Barrio El Carmen	762 3623, Fax: solicitar señal
Quiché	7a. Calle 8-39, Zona 5	755 1011, 755 1006, Fax 323 3524
Nebaj, Quiché	4a. Calle 1-15, Cantón Vipila	755 1222, 755 1228 Fax: solicitar señal.
Cobán, Alta Verapaz	3a. Calle 5-29, Zona 3	952 1719, 952 1726 Fax: 952 3544
Cantabal, Quiché	Complejo ONU, Playa Grande, Ixcán	2793127 , 9513313 Fax.2793121
Petén	1a. Avenida 4-67 Zona 1 Santa Elena	926 0651, 52, 57, 58 Fax: solicitar señal
Zacapa	Bosques de San Julián	941 2727, 2746, Fax: 941 2058

V.5 Auxiliaturas de la Procuraduría de los Derechos Humanos.

Región Central		
Oficina	**Dirección**	**Teléfono**
Sacatepéquez	Calle del Manchén No. 3	8323369
Chimaltenango	Km. 55 carretera Los Aposentos. Chalet Villa Nieves	8391562
Escuintla	2 Calle 4-67 Zona 1	8881972

Región Norte		
Alta Verapaz	1 Calle 6 Av. Zona 4, Cobán	9513248
Baja Verapaz	7 Av. 4-50 Zona 1, Salamá	9400207
Petén	1 Av. 5-81 Zona 1, Flores	9260704 9260652 Minugua
Poptún, Petén (Municipal)	8 Calle 2-06 Zona 1	9277063

Región Nororiente		
Izabal	Lote110 de la 4 Av. y 11 Calle esquina. Puerto Barrios	9480028
El Progreso	Barrio El Golfo, El Progreso	9451591 9451370
Zacapa	8 Calle 15-23 Zona 1	9410744
Chiquimula	7 Av. 5-78 Zona 1	9422333

Región Suroccidente		
Suchitepéquez	2 Av. 3-31 Zona 2 Cantón Santa Cristina, Mazatenango	8725641
Retalhuleu	7 Calle 6-46 Zona 1,	7713252 - 7710248
Coatepeque	5 Av. 8-34 Zona 1 Barrio Las Casas	7755476
Quetzaltenango	8 Av. 3-20 Zona 1	7652176
San Marcos	5 Calle 7-34 Zona 2	7608087
Totonicapán	3 Calle y 16 Av. Zona 2	7661081. 7661412
Sololá	5 Av. 8-20 Zona 1	7623642 – 7137458

Región Noroccidente		
Santa Cruz, El Quiché	3 Calle 2-42 Zona 1, Auxiliatura Móvil. Victoria 20 de enero	7550344 - 7551181
Nebaj, El Quiché	Santa María Nebaj, Chaju, Cotzal	7554828 – Minugua 7551222 - 7551228
Ixcán, El Quiché	Playa Grande	9513313 – 9513309
Huehuetenango	8 Av. 1-81Zona 1	7641789
Nentón. Huehuetenango, Auxiliatura Móvil	Lado oriente de la Plaza Pública	7642343
Barillas, Huehuetenango	Perímetro urbano de la cabecera municipal de Santa Cruz Barillas	

Región Suroriente		
Jutiapa	4 Av. y 5 Calle 3-24 Zona 3 Barrio La Federal	8441686
Jalapa	3 Av. Barrio Chipilapa 0-30 Zona 6	9224347
Santa Rosa	4 Calle 2-09 Zona 3	8865541 8865179
Santa Rosa Regional	2 Av. Sur Barrio Santiago , Chiquimulilla	7134686- 8850600

V.6 Comisarías y sub estaciones de la Policía Nacional Civil.

OFICINA	DIRECCIÓN	TELÉFONO
Comisaría 11 (zonas 1, 3, 4, 8, 9)	11 Av. 4-01 zona 1	2380794, 2327524/19
Subestación. Estación 112, 113, 114	Av. Bolívar y 40 calle zona 3	4718533, 4712799, 4712899
Comisaría No. 12 (zona 6, 2, 17 y 18.)	16 Av. 14-00 zona 6	2886849, 2544239
Subestación Santa Luisa	Jocotales zona 6	2888059
Subestación Lomas del Norte	Zona 17	2582466
Comisaría 13 (zonas5,10,13,14.15 y 16)	29 calle 13-36 zona 5	3310203, 3621225
Subestación Villa de Guadalupe	Zona 10	3370487
Subestación zona 13	Frente aeropuerto	4405867
Subestación Sn. José Pinula	San José Pinula	6343264
Comisaría No. 14 (Zonas 7, 11, 12 y 21)	31 Av. Zona 7 Col. Centro América	5927097 5930235
Subestación El Mezquital	Zona 12	4772004
Su estación Col Justo Rufino Barrios	Zona 21	4499078, 4499080
Subestación El Carmen	Zona 12	4423406- 07
Subestación 142	Zona 11	4424723 4420678
Comisaría 15 Villa Nueva	3 Av. 1-14 zona 4	3369779 6313910
Subestación Amatitlán	Amatitlán	6332077
Subestación Boca del Monte	Boca del Monte	4480132
Subestación Vista Hermosa	Zona 15	3656969-70
Subestación Villa Canales	Villa Canales	3650267
Subestación Villa Hermosa	Villa Hermosa zona 12	4482045
Subestación Mixco	Mixco	5985736
Subestación San Juan	San Juan Sacatepéquez	6302305

Sacatepéquez		
Comisaría No.21	Jutiapa	8441120 8441438
Subestación Asunción Mita	Asunción Mita	8457373
Subestación El Progreso	Jutiapa	8434449
Subestación Atescatempa	Atescatempa Jutiapa	8428119
Comisaría No.22	Jalapa	9224261
Comisaría 23	Chiquimula	9420120
Subestación Esquipulas	Esquipulas	9432074
Comisaría 24	Zacapa	9410504
Comisaría No.31	Escuintla	8881120
Subestación Sta. Lucía Cotz.	Sta. Lucía cotzumalguapa	8825032
Subestación Puerto	Puerto San José	8811333
Subestación tiquizate	Tiquizate	8847205
Subestación La Gomera	La Gomera	8800627
Subestación Siquinalá	Siquinilá, Escuintla	8802045
Subestación La Democracia	La Democracia Escuintla	8803455
Comisaría No.32	Cuilapa Santa Rosa	8865479
Subestación Barberena	Barberena	8870259
Comisaría No.33	Mazatenango	8723999 8722460
Subestación San Antonio Suchitepéquez.	San Antonio Suchitepéquez	8704011
Comisaría No.34	Retalhuleu	7710120
Comisaría No.41	Quetzaltenango	7654994 – 95
Subestación Coatepeque	Coatepeque	7751370
Subestación Salcajá	Salcajá, Quetzaltenango	7689508
Comisaría 42	San Marcos	7601296
Subestación San Pablo	San Marcos	7771159
Subestación Tejutla	San Marcos	7600169
Comisaría No. 43	Huehuetenango	7641150
Comisaría No.44	Totonicapán	7661131
Comisaría No.51	Cobán	9521225
Comisaría No.52	Salamá Baja Verapaz	9400050
Comisaría No.53	Guastatoya, El Progreso	9451026
Subestación Sanarate	Sanarate	9252315
Subestación San Agustín Acasaguastlán	San Agustín Acasaguastlán	9451540
Comisaría No.61	Izabal	9487643
Subestación Morales	Izabal	9478045
Comisaría No. 62	Flores, Petén	9261152
Comisaría No.71	El Quiché	7550237
Subestación Chichicastenango	Chichicastenango	7561355
Comisaría NO.72	Sololá	7624129
Subestación Panajachel	Panajachel, Sololá	7621120
Comisaría No.73	Chimaltenango	8396005
Comisaría No.74	Antigua, Sacatepéquez	8320251

V.7 Fiscalías distritales y municipales del Ministerio Público

OFICINA	DIRECCIÓN	TELÉFONO
Área Metropolitana	8 Av. 10-57 zona 1	2305762
Antigua, Sacatepéquez	1 Calle del Cajón, Plazuela San Sebastián No. 5	8320377, 8322095
Amatitlán	5 Av. Prolongación Norte 00-45, Frente a las canchas	6320574, 6337521
Coatepeque, Quetzaltenango	6 calle 5-65 zona 2, Barrio El Rosario.	7755549, 7755618,7751645
Cobán, Alta Verapaz	6 Av. 5-14 zona 3	9514607, 9521017
Chimaltenango	2 Av. 4-30 zona 1	8392571, 8392655
Chiquimula	8 Av. y 6 calle esquina zona 1	9420669, 9420719, 9420007
Cuilapa, Santa Rosa	1 Av. 3-40 zona 3, Barrio La Parroquia	8865220, 8865594,8880437
Escuintla	4 Av. 2-39 zona 1	8880437, 8894198,8894199
Guatatoya, El Progreso	Barrio El Calvario	9450181, 9451848
Huehuetenango	4 Av. 6-54 zona 1	7642667, 7646702
Izabal, Puerto Barrios	8 calle y 9 Av. Esquina	9481193, 9487969
Jalapa	5 Av. 2 calle zona 1	9222077, 9222088
Jutiapa	2 Av. 4-20 zona 1	8441571, 8442620
Malacatán San Marcos	4 Av. Entre 4 y 5 calle z. 1	7769311, 7770841
Mazatenango Suchitepéquez	5 Av. 9-22 zona 1 frente mercado central	8723202m 8723182
Mixco, Guatemala	7 valle 3-24 zona1, edificio Plaza Centro	5985420, 5985426
Nebaj, El Quiché	Cantón Simocoj	2534256
Poptún, Petén	5 Av. 8-10 zona 1	9274382, 9278444
Quetzaltenango	Diagonal 11 7-20 zona 1	7654849, 7655305
Retalhuleu	1 calle 4-05 zona 4	7713138, 7714381
San Benito, Petén	1 Av. 11-30 zona 1	9263157, 9263405
Santa Elena, Petén	C. Limítrofe zona 2	9263405,9260940
Santa Cruz del Quiché	3 Av. 4-35 zona 1	7551357, 7552011
San Juan Sacatepéquez	4 calle 5-14 zona 3	6302017,6302451
La Libertad, Petén	La Libertad	9261088
Salamá, Baja Verapaz	4 Av. 3-70 zona 2	9400248, 9402023
San Marcos	7 Av. 8-06 zona 1	7604350, 7604355
Santa Eulalia, Huehuetenango	Edificio Municipal	7806152
Santa Lucía Cotzumalguapa, Escuintla	Av. 15 septiembre 5-18 zona 1	8825070, 8825482
Sololá	7 Av. 7-02 zona 2	7624153, 7623388
Totonicapán	7 calle 13-34 zona 3	7664149, 7664152
Villa Nueva, Guatemala	6 Av. 5-55 zona 1	6356555, 6356518

V.8 Herramientas en seguridad informática

Codificación de Disco

Disco PGP
Puede obtenerse en www.pgpi.com herramientas libres versión 6.01

Pros: confiable, la versión más antigua puede ser gratis.

Contras: no tiene apoyo, no es completamente intuitivo y las versiones gratuitas no trabajan con sistemas operativos modernos y actualizados; la versión comercial ya no está disponible, la versión gratuita más antigua requiere de una conexión provisional o de un parche (*patch*) separado para instalarla.

Drive Crypt – www.drivecrypt.com

Pros: apoyado, confiable, tiene más características que el Disco PGP

Contras: $40.

BestCrypt – www.bestcrypt.com

Pros: Trabaja con Windows y Linux, está apoyado, tiene muchas características incluyendo el Wipe, versión gratis de prueba.

Contras: No trabaja con Macintosh, tiene propietario, de manera que no es tan gratis.

Codificación de Correo Electrónico

PGP – www.pgpi.com

Pros: es confiable, gratis, relativamente fácil de usar, con plataforma transversa, puede importar y exportar archivos de la Red, el sistema estándar de codificación es usado por la mayoría de la industria.

Contras: No tiene apoyo, la instalación no es totalmente intuitiva, tiene dos diferentes implementaciones una de NAI y la otra es GnuPG desarrollada por FSF. El sistema de clave puede ser confuso.

Bóveda de Correo (MailVault) – www.mailvault.com

Pros: es gratis, tiene apoyo, es confiable (debido al contacto personal), fácil de usar, no está limitado a los usuarios de MailVault, basado en la Red de manera que la plataforma no es problema, puede usarse en los cafés internet.

Contras: Genera claves PG en el servidor más que en su propia máquina, de manera que se requiere confiar en el servidor.

Hushmail – www.hushmail.com

Pros: versión ligera gratis, apoyado, confiable (debido al contacto personal), fácil de usar, basado en la Red, puede usarse en los cafés Internet, generación de clave segura.

Contras: limitado a los usuarios de Hushmail, para la versión ligera, debe utilizarse cada tres semanas o se borra la cuenta. Se encuentra disponible su compra sin limitaciones por $30 al año. No trabaja con computadoras Macintosh. Algunos problemas que se han reportado al cargarlo lo hacen ser inconsistente.

CryptoHeaven – www.cryptoheaven.com

Muy Nuevo de manera que no ha sido probado por la comunidad de codificación (*crypto*); tiene propietario de manera que es requerido comprarlo - $30 al año. Privaterra estará monitoreando esta herramienta y con el tiempo recopilará los Pros y Contras.

Reenvío de correo anónimo

Anonimatizador – www.anonymizer.com

Pros: El autor es muy creíble dentro del campo de la seguridad. Privaterra ha asegurado un número limitado de cuentas gratuitas para ser usadas por grupos de derechos humanos.

Contras: Propietario, debe confiar en el autor, no hay revisión de compañeros.

Sistema de boletines

Martus – www.martus.org
Pros: muy fácil de usar, fuente confiable será fuente abierta, también puede usarse para copia de seguridad.
Contras: aún no se encuentra disponible, funcionalidad limitada.

Copia de seguridad (Backup)

CDRWs (CD Lectura/Escritura)

Pros: Económico y fácil de usar

Contras: Se basa en el usuario, de manera que debe recordarse de realizar una copia de seguridad. La copia debe guardarse en un lugar separado y seguro.

Dispositivo extra para disco en la computadora

Pros: Fácil de usar y siempre disponible, relativamente económico

Contras: Una redada o rajadura resultaría en la destrucción tanto del original como de la copia de seguridad; puede escribirse encima por accidente.

Compañía de seguridad en línea
(novastore.com, bitstore.com, virtualbackup.com y muchas más)

Pros: Fácil de usar

Contras: costo, debe enviar todos los documentos codificados puesto que la fuente no es necesariamente confiable.

Software de Copia de Seguridad
Retrospect.com (NovaStore, Symantec Norton Ghost y muchas más son similares)

Pros: Plataforma transversal, versiones de escritorio y de servidor pueden ser automatizadas para ahorrar tiempo, relativamente fácil de usar, colocación sólo una vez y luego es transparente al usuario, puede copiarse en múltiples medios – disco, internet.

Contras: código del propietario, cuesta dinero.

USB, Memoria compacta de luz o barra de memoria

Pros: Extremadamente portátil, puede esconderse fácilmente en una inspección casual, puede sostener hasta 512 MB.

Contras: Debe comprarse el aparato (*hardware*) basado en el usuario, de manera que debe recordarse de realizar una copia de seguridad (*backup*). Usa consumo de batería de manera que agotará más rápidamente la batería de una computadora portátil (*laptop)*.

Protección contra virus

Lo mejor: Precauciones generales y una pared de fuego; use un proveedor confiable que utilice un filtro de virus y manténgase actualizado en cuanto a los últimos virus (refiérase a la Biblioteca de Información de Virus – vil.nai.com). Permita las extensiones de archivos para ver lo que es un archivo antes de abrirlo, y no permita que los archivos bajen automáticamente.

Elija un cliente de correo electrónico sin un menú de vista previa, tal como Mulberry. El menú de vista previa puede cerrarse al utilizar Eudora. El Microsoft Access es el más vulnerable porque es el más popular y porque tiene un menú de vista previa.

Si borrar todos los archivos no deseados no es una opción, elija un sistema popular, tal como Norton o Symantec. Estos son relativamente económicos y fáciles de usar. Vienen tanto en versiones para el Cliente y para el Servidor.

Contras: Los usuarios deben actualizar regularmente sus programas de software para tener protección nueva contra los virus. La actualización en vivo puede no ser una opción en áreas con ancho de banda muy lento.

Seguridad Física

Identificación Biométrica (Huellas dactilares)

Siemens y otras compañías ahora fabrican ratones USB que tienen características de reconocimiento de las huellas dactilares incorporadas, evitando que usuarios no autorizados utilicen su computadora.

Cámaras

Hay cámaras pequeñas y económicas que pueden montarse de manera discreta para controlar quién entra por su puerta y/o ventana, cuando sus computadoras se encuentran totalmente desatendidas.

Cerraduras, etc.

El uso juicioso de cerraduras, personal de seguridad y la colocación de las computadoras lejos de las ventanas proporciona una mejor protección.

Otros

PGP SDA (Archivo autodescodificado)

Pros: Le permite enviar un documento codificado PGP a un usuario que no tenga PGP instalado en su computadora. Se encuentra en paquete con las versiones de PGP 6.5 y mayores.

Contras: Debe obtenerse una frase de contraseña descodificadora, para que el usuario final lo obtenga en una forma un tanto segura.

Destructor virtual

Pros: Empaquetado con PGP, el Diskwipe destruye los archivos.

Contras: El simple hecho de borrar un documento no lo elimina de su sistema – debe recordarse de eliminarlo (*wipe*).

Salto del teclado

"Escriba" su frase de contraseña en un teclado en su pantalla, cuando sospeche que las emisiones de sus golpes de teclado están siendo espiadas. Esto se encuentra incorporado en el software de CryptoHeaven, pero no conocemos otros que tengan esta característica incorporada.

Tempestad

El uso de fuentes con escudos de "tempestad" en su cliente de correo electrónico (incorporado en el PGP que utiliza "visión segura") y otros, lo protegerán si usted sospecha que está siendo espiado en emisiones no intencionales que produce la mayoría de equipo electrónico. Véase www.tempest-inc.com/ para ver ejemplos o información adicional.

V.9 Preguntas y respuestas sobre la codificación

1. ¿Qué es la codificación?

La codificación es cifrar datos en un código secreto que no puede ser descifrado excepto por la parte a quien van dirigidos.

En términos sencillos, la codificación es una forma en la que usted puede asegurar sus archivos y sus correos electrónicos de ojos que lo espíen. Sus archivos se traducen a un código que no tiene sentido para nadie que lo vea. Aparentemente es una colección al azar de números y letras. Para codificar un archivo, usted lo "cierra" con una llave, representada por una frase de contraseña. Para codificar un mensaje, usted lo encierra con un par de llaves que utilizan su frase de contraseña. Sólo puede ser abierto por el receptor a quien va dirigido, quien usa su propia frase de contraseña.

2. ¿Por qué deben los grupos de derechos humanos utilizar la codificación?

Todos debieran usar la codificación porque las comunicaciones digitales son inherentemente inseguras. Sin embargo, los trabajadores en derechos humanos se encuentran en un mayor riesgo que la mayoría de los individuos, así como sus archivos y comunicaciones son más sensibles. Es imperativo que quienes trabajan en derechos humanos utilicen la codificación en sus comunicaciones digitales para protegerse a sí mismos y a las personas a quienes están tratando de ayudar.

La tecnología digital es un beneficio para los grupos de derechos humanos, permitiéndoles comunicaciones más fáciles, mayor eficiencia y mayores oportunidades. Sin embargo, con el beneficio vienen ciertos riesgos. Usted no conduciría un carro sin cinturones de seguridad aun si usted probablemente no va a tener un accidente cada vez que conduzca. Si usted está conduciendo en una situación más peligrosa, como puede ser una carrera, es más probable que usted utilice las herramientas que se encuentren disponibles para tener mayor seguridad.

De manera similar, los trabajadores en derechos humanos son blancos conocidos para ser vigilados. Sabiendo que el correo no codificado puede ser visto por casi cualquier persona desde muchos puntos distintos de acceso, hace casi inevitable que su correo no codificado será visto en algún punto. Sus mensajes pueden estar ya siendo controlados por sus adversarios y usted nunca lo sabrá. Los enemigos de sus beneficiarios son sus adversarios.

3. ¿Es ilegal usar la codificación?

A veces. Es perfectamente legal utilizar la codificación en los Estados Unidos, Canadá y otros países occidentales. En efecto, es legal en la mayoría de países del mundo. Sin embargo existen algunas excepciones particulares – tal como en China- que usted debe saber antes de enviar a sus trabajadores de campo a esas partes del mundo.

En China, por ejemplo, las organizaciones deben solicitar un permiso para utilizar la codificación y todos deben informar sobre cualquier tecnología de codificación que tengan en sus computadoras portátiles a su ingreso al país. Singapur y Malasia tienen leyes que requieren que cualquier persona que desee utilizar la codificación debe reportar su contraseña privada. Leyes similares se encuentran pendientes en India. También hay otras excepciones.

El Centro de Información sobre Privacidad Electrónica (EPIC) proporciona un Estudio Internacional sobre Política de Codificación en el cual discuten las leyes de la mayoría de países en http://www2.epic.org/reports/crypto2000/, sin embargo, esta lista se actualizó por última vez en el año 2000. Antes de utilizar la codificación en un país en particular, consulte con nosotros.

4. ¿Qué programas (software) se encuentran disponibles?

Existe la codificación del correo electrónico, codificación del disco duro, *re-mailers* anónimos, sistemas de copia de seguridad, protección contra virus, paredes de fuego y más.

Pero el hecho de contar con los programas adecuados no es toda la solución. Los eslabones más débiles por lo general son los individuos y no la tecnología. La codificación no funciona si los individuos no la utilizan en forma consistente, si comparten sus contraseñas o las dejan en lugares visibles tales como en una nota pegada en sus monitores. Los programas de copia de seguridad no lo salvarán en el caso de un incendio o una redada si usted no se asegura que la copia de seguridad (backup) se encuentra guardada en un lugar separado y seguro. La información sensible debe tratarse sobre una base de “necesito saber” en vez de compartirla con todos en la organización, de manera que es necesario que comience a formular sus jerarquías y protocolos. En general es importante tener conciencia en cuanto a la privacidad y seguridad en sus actividades cotidianas.

5. ¿De dónde se pueden bajar estos programas?

Vea nuestra hoja de herramientas para URLs individuales.

6. Lo que debe y no debe hacerse con el uso de la codificación.

Muchas ideas sobre privacidad y seguridad se encuentran disponibles en nuestros documentos, pero aquí presentamos un resumen específicamente sobre codificación.

SI, utilice la codificación constantemente. Si usted solamente codifica material sensible, entonces cualquiera que esté controlando su tráfico de correo electrónico sabrá que va a suceder algo importante. Un aumento repentino del uso de la codificación puede conducir a una redada.

NO coloque material sensible en las líneas del asunto. Por lo general no quedan codificadas, aunque el mensaje lo esté.

SI, utilice una frase de contraseña que contenga letras, números, espacios y puntuación que sólo usted pueda recordar. Algunas técnicas para la creación de contraseñas seguras son la utilización de un diseño en su teclado, utilizando una frase en inglés traducida a un idioma oscuro con números y puntuación entre cada palabra; y colocando en mayúscula, la segunda, la de en medio o la última letra de cada palabra.

NO use una palabra única, nombre, frase popular o dirección de su libreta de direcciones para su contraseña. Estas pueden averiguarse en minutos.

SI, haga una copia de seguridad de su clave privada en un lugar seguro, tal como codificada en una minúscula barra de memoria Sony, removible, o en un disco compacto con luz.

NO responda con material sensible a alguien, sólo porque le enviaron un correo codificado y utilizaron un nombre reconocible. Cualquiera puede “falsear” un nombre haciendo que su dirección de correo electrónico se parezca a la de alguien que usted conoce. Siempre verifique una identidad antes de elegir que usted confía en la fuente –comuníquese en persona, por teléfono o revise las huellas dactilares con una fuente confiable.

SI enséñele a otros a utilizar la codificación. Mientras más gente la utilice, estaremos más seguros.

NO se olvide de firmar el mensaje así como la codificación. Usted quiere que su receptor sepa si su mensaje ha sido alterado en el camino.

7. Recursos adicionales.

Estos enlaces se encuentran disponibles en el sitio de la red Privaterra.

Bert-Jaap Koops-Estudio de la Ley de Codificación
http://www.kub.nl/-frw/people/koops/lawsurvy.htm

Privacidad y Derechos Humanos 2000: Un Estudio Internacional de las Leyes de Privacidad y Sucesos
http:www.epic.org/phr/

Criptografía y Libertad 2000: Un Estudio Internacional de la Política de Codificación
(EPIC)
http:/www2.epic.org/reports/crypto2000/

Noticias BBC – Revelada la red de espionaje Echelon
La BBC descubre el sistema de espionaje que permite a los gobiernos leer sus correos electrónicos y escuchar sus llamadas telefónicas.
http://newssearch.bbc.co.uk/cgi-bin/results.pl?tab=news&scope=news&q=echelon

El Escudo Dorado de China
Las Empresas y el Desarrollo Global de la Tecnología de Vigilancia en China
http://go.openflows.org/
http://go.openflows.org/CGS_ENG.PDF

Proyecto de Vigilancia – Universidad de Queen
Vigilancia, Manejo de Riesgos & Ordenamiento Social en la Información Global Sociedades. Este proyecto de investigación está diseñado para mejorar el conocimiento sobre cómo funciona la vigilancia y también cómo se genera la resistencia o contención, en el nivel internacional, institucional, tecnológico y social-personal.
http://qsilver.queensu,ca/sociology/Surveillance/intro.htm

Sitio de Programas (Software) de Criptografía y de Archivo
http://www.zedz.net/

Herramientas:

Martus.org – Sistema de Boletines de Derechos Humanos
http://www.martus.org/

Haxial NetFone es un teléfono de Internet codificado para múltiples usuarios
http://www.haxial.com/roducts/netfone/

Remailers Anónimos Basado en la Red
http://security.lao.ca/www.shtml

Bandeja de Privacidad de Windows
http://www.winpt.org/

WinPT (la Bandeja de Privacidad de Windows) es una instalación de la barra de tareas para realizar codificación o descodificación de datos. WinPT es un llamado “Extremo Frontal” para el GnuPG. El programa actúa en forma muy similar a otro programa del paquete PGP.

Buscador de claves PGP Experimental

http://the.earth.li/noodles/pathfind.html

Página Pública para Ver Claves de PGP
http://www.openpgp.net/pgpsrv.html
http://www.keyserver.net

Recursos en otros idiomas:

Español:

Curso Sencillo de PGP
http://www.ugr.es/-aquiran/cripto/cursopgp.htm

Kriptopolis – Seguridad en Internet
http://www.kriptopolis.com/

Francés:

Bugbrother.com está dedicada a ayudar a los ciudadanos de la red a proteger su privacidad. El sitio….

V.10 Manifestaciones en masa[32]

Durante los años sesenta, en la lucha por la igualdad racial en el sur de Estados Unidos, las organizaciones de derechos civiles desarrolaron métodos para mejorar la seguridad de las manifestaciones públicas. Debido a que la policía tomaba represalias tan violentas contra los manifestantes, al usar perros agresores, mangueras de agua de alto poder, y otras armas tales como bastones y artefactos para golpearlos, las manifestaciones a menudo terminaban abruptamente con la dispersión de los manifestantes horrorizados. Por consiguiente, con el fin de prepararse para la marcha, los grupos empezaron a simular el anticipado abuso físico y verbal. Las simulaciones tenían el proposito de "endurecer" a los manifestantes de antemano, al pasarlos por una prueba de abuso físico y verbal simulados.

Asimismo, algunas organizaciones publicaron directrices y consejos para planificar las manifestaciones en masa. Por ejemplo, el National Lawyers Guild ha desarrollado estrategias sobre cómo las organizaciones pueden proteger a sus miembros, y a otros, durante las marchas de protesta. A pesar de haber sido desarrollado en un contexto democrático, algunas de las siguientes estrategias puden generar ideas para trabajar en clima menos abiertos.

Ya que el National Lawyers Guild ha definido a manifestantes que se oponen a la guerra y a activistas de derechos civiles en un período de más de treinta años, ha adquirido un caudal de experiencias sobre manifestaciones en masa. Esto incluye directrices para los observadores legales (quienes no necesitan ser abogados) para proteger a los manifestantes de varias maneras descritas abajo. Las marchas de protestas pueden ser caóticas, y han sido explotadas por las fuerzas hostiles para desacreditar a los organizadores de dichas marchas, incluso a los grupos locales de derechos humanos. Esto se lleva a cabo de muchas maneras, incluso al hacer que los agitadores sean partícipes de los disturbios y del vandalismo a lo largo de la ruta de la marcha. Los daños que resulten entonces se atribuyen a los organizadores. En reacción a esto, entonces, y para ayudar a proteger a los miembros del personal de las ONG y a otros, algunos grupos organizaron equipos de observadores muy bien entrenados, descritos más abajo.

V.10.1 Observadores legales.

Esencialmente, los observadores legales son testigos entrenados. Su trabajo principal es el de observar y registrar tanto las actividades de la policía como las actividades en contra de las manifestaciones. Algunos grupos creen que la presencia de los observadores legales minimiza la mala conducta de la policía, ayuda a averiguar las necesidades especiales de aquellos que han sido arrestados (tales como condiciones de salud, u objeciones a los cargos legales excesivos), y produce información que puede ser usada más tarde en los tribunales. Los observadores

[32] Este apartado fue tomado en gran parte de, Estrategias prácticas para grupos pro Derechos Humanos, del Centro para la acción sostenible en Derechos Humanos.

legales no son como los monitores que se involucran en el control de la multitud, resolución de conflictos o la interacción con la policía. Los observadores legales deben desviar las solicitudes de la policía a los monitores, por ejemplo, envío de mensajes. Esto dejará libre a los observadores para actuar como testigos.

Los deberes de los observadores legales incluyen grabar (en casette, fotografía o por escrito) quiénes son los policías presentes y si éstos están identificados adecuadamente. Una anotación por escrito podría ser "SDPD insignia #123, mujer, 1m 70 cm. de altura, cabellera castaña y rizada, anteojos para el sol, de raza blanca". Se debe anotar también los nombres de los policías y de los líderes de la manifestación; cuáles sobre avisos se hicieron; el tamaño de la multitud; las rutas que tomaron; los números de placas de los vehículos privados de los policías aparcados en los alrededores; las circunstancias de cualquier arresto; los nombres de los arrestados (incluso las necesidades médicas o de cuidado de niños, si se conocen) y a dónde serán llevados, así como también los nombres y descripción de los testigos, especialmente, las partes que portaban cámaras y otros aparatos para grabar. Los acontecimientos en las manifestaciones a menudo suceden rápidamente, así es que si no queda tiempo para nada más, las personas arrestadas deben ser exhortadas a que griten sus nombres a los observadores para que éstos los anoten. Las notas deben ser legibles, firmadas, fechadas y dadas al coordinador del equipo de los observadores legales.

Es también importante para los observadores anotar qué representantes de los medios de difusión estuvieron presentes. En algunos países, las secuencias de las noticias que se filman vulven a ser usadas, o se graba encima de ellas, dentro de 24 horas, así es que se deben solicitar inmediatamente copias de la filmación relevante.
Y por muchas razones, es importante conocer las ordenanzas locales tales como las siguientes: En algunos casos, la policía debe dar una orden para dispersarse y sólo después de haberla dado pueden arrestar a los manifestantes si no la obedecen.
Los observadores legales deben reunirse antes de la manifestación para recibir entrenamiento sobre sus deberes y técnicas, para asignar un coordinador del aréa, para acordar un brazal uniforme para propósitos de identificación, y para ponerse de acuerdo a permanecer muy visibles, para disuadir la violencia de la policía. También se debe acordar de antenamo la hora y lugar para reunirse después de la manifestación, y la dirección (y número de teléfono) debe ser distribuida para enviar por correo las notas tomadas durante la demostración. Las anotaciones y las fotos pueden ser requeridas si se inicia una demanda, y algunos entrenadores de observadores aconsejan que se documenten sólo las actividades de la policía y las actividades en contra de la manifestación para no implicar así a los manifestantes de ninguna manera.

Se informó además que los observadores legales deben poner sus deberes primero antes de cualquier deseo de participar en la manifestación. Deben declinar responder a solicitudes en cuanto a participación en acciones particulares. En otras palabras, no deben influenciar la dirección de la marcha de ninguna manera. Si un observador legal conoce las consecuencias legales de una acción, dicha información debe ser proporcionada de manera individual, pero no como miembro de un equipo de observación legal. Cualquier consejo legal debe ser dado por su abogado o bajo la dirección explícita de un abogado. Los observadores legales no deben

responder ninguna pregunta de la policía. Al contrario, con amabilidad deben referir los policías a los organizadores del evento o a los monitores. Y no deben darse la información personal para ponerse en contacto con los observadores mismos.

Finalmente, se deben distribuir imparcialmente en las manifestaciones tarjetas impresas de “conoce tus derechos” en nombre de la organizaciones que financian a los observadores. Estas tarjetas pueden indicar qué hacer en caso de arresto (por ejemplo, pedir ver a un abogado, no hablar con ninguno excepto con un abagado), o mientras se encuentra detenido (no discutir qué sucedió ni someterse a exámenes, hasta que su abogado esté presente; demande su derecho de hacer una llamada telefónica gratis). Estos derechos pueden variar según las leyes locales.

Bibliografía

Alexander, Sylvia

- Estrategias prácticas para grupos pro Derechos Humanos. Center for Sustainable Human Rights Action (CSHRA), New York, 1999.

Asamblea Nacional Constituyente

Constitución Política de la República de Guatemala, decretada por la Asamblea Nacional Constituyente el 31 de mayo de 1985 y reformada por Consulta Popular acuerdo legislativo 18-93. Guatemala, 1994.

Comisión para el Esclarecimiento Histórico (CEH)

- Guatemala memoria del silencio. Informe de la Comisión para el Esclarecimiento Histórico. Oficina de Servicios para Proyectos de las Naciones Unidas (UNOPS). Guatemala, 1999. Tomos I, II y III.

Equipo de Estudios Comunitarios y Acción Psicosocial (ECAP)

- El sistema de vigilancia de la salud mental comunitaria. Guía para el facilitador y el promotor de Salud Mental Comunitaria. Equipo de Estudios Comunitarios y Acción Psicosocial (ECAP). Guatemala 1998.

- Nuestras molestias. Técnicas participativas de apoyo psicosocial. Guía para el facilitador y el promotor de Salud Mental Comunitaria. Equipo de Estudios Comunitarios y Acción Psicosocial (ECAP). Guatemala 1998.

- Técnicas de Escucha Responsable. Equipo de Estudios Comunitarios y Acción Psicosocial (ECAP). Guatemala, 2001.

MINUGUA

- Décimo informe sobre derechos humanos de la Misión de Verificación de las Naciones Unidas en Guatemala (MINUGUA). Guatemala, 2000.

Naciones Unidas

- Seguridad sobre el terreno. Información para los funcionarios del sistema de Naciones Unidas. Oficina del coordinador de medidas de seguridad de las Naciones Unidas. Naciones Unidas, Nueva York, 1998.

National Security Archives

- El Ejército de Guatemala, lo que revelan los archivos de los Estados Unidos. National Security Archives, George Washington Universitu, Washington-Guatemala 2000.