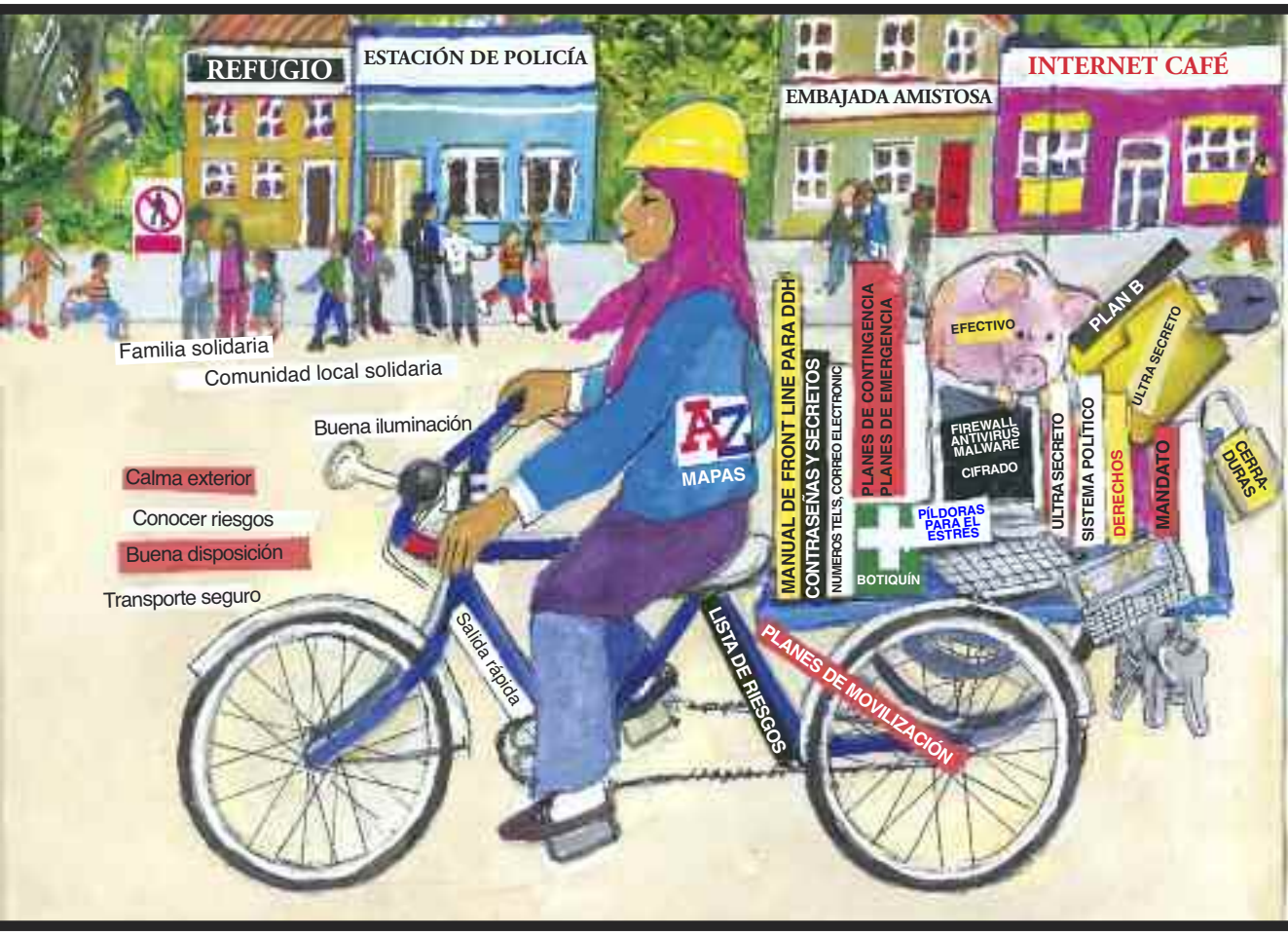
# MANUAL SOBRE SEGURIDAD:

## PASOS PRÁCTICOS PARA DEFENSORES/AS DE DERECHOS HUMANOS EN RIESGO




FRONT LINE DEFENDERS

## APÉNDICE 14

### Seguridad en los ordenadores y teléfonos

Esta lista de comprobación no intenta ser un modelo de seguridad. Tu contexto es un factor determinante. Considera los riesgos y amenazas que tú enfrentas y todas tus vulnerabilidades con el fin de suplementar y personalizar esta lista. Se trata solo de una lista de puntos importantes.

Visita Caja de Herramientas de Seguridad **https://security.ngoinabox.org/fr** para acceder a una información más detallada.

Esta información incluye una serie de consejos que pueden ser hallados en las Awareness Cards [tarjetas de concientización] de la Caja de Herramientas de Seguridad (ver el enlace en el párrafo anterior).

**1. Protege tu ordenador de malware y hackers**

- Instala software antivirus, anti espía y un cortafuegos.
- No utilices software pirata, te hace vulnerable debido a la falta de actualizaciones y a posibles acusaciones de posesión de software ilegal.
- Considera la utilización de software libre y de código abierto (Free Open Source software -FOSS) tales como el antivirus AVAST, el software antiespía Spybot y el cortafuegos Comodor.
- Considera utilizar un buscador como Firefox que cuenta con seguridad (Visita https://security.ngoinabox.org/es/chapter-1 para acceder a más información sobre cómo proteger tu ordenador).

**2. Creación y mantenimiento de contraseñas seguras**

- Cuanto más largas son las contraseñas, más seguras. Tus contraseñas deben contener más de 12 caracteres, mayúsculas y minúsculas, números y caracteres especiales, y – de ser posible – un espacio.
- En lo posible no incluyas en la contraseña palabras que figuran en el diccionario y/o información pública disponible sobre ti mismo/a tales como la fecha de nacimiento o el nombre de un amigo/a, mezcla las palabras o reemplace palabras con caracteres especiales o números, o mezcla idiomas.
- Considera utilizar como contraseña una frase: puede ser el título de un libro, o una línea de una canción (con algunos caracteres o números sustituidos por letras).
- Cambia la contraseña a menudo.
- Establece distintas contraseñas para distintos servicios, actualízalas de manera regular y no las compartas (considera utilizar KeePass para guardar todas las contraseñas), (ver https://security.ngoinabox.org/es/chapter-3 para acceder a más información sobre contraseñas seguras).

**3. Cómo proteger archivos sensibles en tu ordenador**

- Crea una copia de seguridad regularmente y guárdala en un lugar seguro.
- Esconde archivos de información sensible bajo nombres inocuos.
- Considera el cifrar tus archivos (aunque el cifrado/encriptado es ilegal en algunos países y podría llamar la atención hacia ti).
- Una aplicación FOSS denominada TrueCrypt puede cifrar y esconder tus archivos.
- Un experto puede rastrear los archivos eliminados en tu ordenador, evalúa la utilización de herramientas seguras para la eliminación tales como CCleaner (para eliminar archivos temporales) y Eraser.
- De ser posible, chequea la reputación de tu ISP o la ubicación desde donde planeas conectarse a internet, tal como cibercafés.
- Asegúrate de que las personas con las que te comunicas también están atentas a la privacidad y la seguridad. La comunicación es un proceso de ida y vuelta. No tiene sentido si una sola de las partes se preocupa de la privacidad y seguridad. (Para acceder a más información, visita https://security.ngoinabox.org/es/chapter-4" y https://security.ngoinabox.org/es/chapter-6

**4. Mantén privacidad en tu comunicación de Internet**

- Muchas cuentas de correo electrónico con interfaz web (webmail) son inseguras (entre ellas Yahoo y Hotmail) y proveen tu dirección IP en los mensajes que envías. Gmail y Riseup son servicios que

brindan cuentas de correo electrónico más seguras (aunque Google ha hecho concesiones en el pasado ante las exigencias de algunos gobiernos que han restringido la seguridad digital).
- Utilizar cibercafés puede exponerte a ser vigilado, estate muy atento a los riesgos y a quién estás contactando con qué información. Elimina tu contraseña e historial después de usarlo.
- Utiliza "https" en lugar de "http" cuando te conectas a los servicios on line, siempre que sea posible, de modo que tu nombre de usuario, contraseña y otra información se transmita de manera segura.
- No abras adjuntos de correo electrónico enviado por alguien que no conoces, o que parece sospechoso.
- Mantente especialmente atento/a al enviar, recibir o ver información sensible a través de Internet.
- Considera la utilización de un servicio o aplicación proxy que te ofrezca anonimato en Internet. Esto te permite acceder y comunicarte en la red haciendo uso de la dirección IP de otro ordenador.
- Los mensajes instantáneos (chat) normalmente también son seguros, aunque Skype es, probablemente, más seguros que otros.

(Para más información visita https://security.ngoinabox.org/es/chapter-7
y https://security.ngoinabox.org/es/node/328)

**5. Redes sociales**
- Piensa cuidadosamente qué información compartes sobre ti mismo/a, tus amigos/as, movimientos, etc.
- Si publicas información, documentos, fotografías y lugares de otros, solicita su consentimiento.
- Asegúrate de mantener las contraseñas seguras y cámbialas regularmente.
- Sé cuidadoso/a al acceder a tu cuenta de una red social en espacios públicos de Internet, utilízalos solamente si estás seguro de que son confiables. Elimina tu contraseña y el historial del navegador después de utilizar un ordenador y buscador público.
- Lee y comprende la licencia de uso (End User License Agreement – EULA), Condiciones de uso y/o Directivas de privacidad. Estos documentos podrían cambiar en el futuro, de modo que es importante volver a visitarlos regularmente.
- Asegúrate de que conoces la configuración de privacidad de la cuenta de la red social que utilizas. No confíes en la configuración por defecto, cambia la tuya y revísala regularmente ya que podría ser necesario introducir cambios.
- Se cauteloso al instalar aplicaciones sugeridas por los servicios de las redes sociales. Utilízalas solamente si confías en la fuente, comprendes qué información expondrán y si puedes controlar el flujo de tu información personal.

(Ver https://security.ngoinabox.org/es/chapter-10)

**6. Seguridad para teléfonos móviles**
- La tecnología actual y la forma en que están configurados los teléfonos móviles hoy día (incluyendo SMS y llamadas de voz) es insegura, pueden rastrear tu ubicación e interceptar tus comunicaciones, de modo que siempre evalúa cuál es la forma más segura para comunicar información importante.
- El teléfono móvil más seguro es el más económico, no registrado, "paga lo que usas"(pay-as-you-go) que puedes descartar después de usarlo.
- Activa la contraseña o código PIN en tu móvil.
- No guardes información sensible en tu teléfono, o si debes hacerlo, cífrala.
- Mantente siempre atento al lugar donde utilizas el teléfono móvil y abstente de usarlo en situaciones y lugares riesgosos.
- Asegúrate de que toda tu información fue eliminada de tu móvil antes de venderlo o llevarlo a reparar.
- Destruye teléfonos que ya no sirven y tarjetas SIM viejas antes de descartarlas.
- Cuando trabajas con organizaciones y personas que transmiten información sensible, considera la posibilidad de tener distintos teléfonos y SIMs para el trabajo y el uso personal.

(Ver https://security.ngoinabox.org/es/chapter-9)