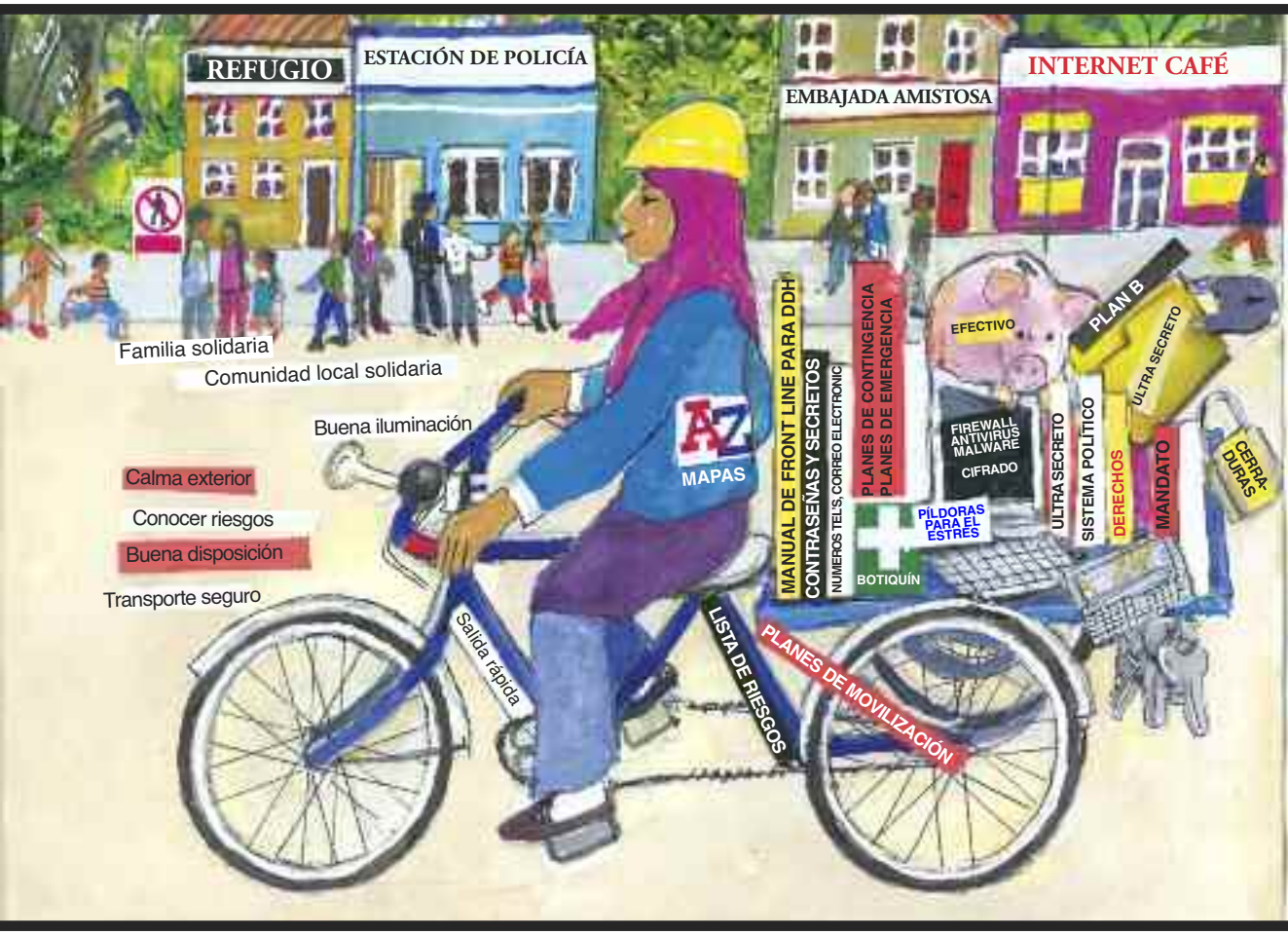
MANUAL SOBRE SEGURIDAD:

PASOS PRÁCTICOS PARA DEFENSORES/AS DE DERECHOS HUMANOS EN RIESGO



FRONT LINE DEFENDERS

APÉNDICE 5

Lista de comprobación: seguridad en la oficina

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.

1. Contactos de emergencia
¿Cuentas con una lista actualizada y a mano con números telefónicos y domicilios de otras ONG locales, salas de emergencia en hospitales, policía, bomberos y ambulancias?

2. Límites técnicos y físicos (externos, internos y en el interior)
- Controlar en qué estado se encuentran y cómo funcionan los portones externos/cercas, puertas hacia el edificio, ventanas, paredes y techos.
- Controlar en qué estado se encuentran y cómo funcionan la iluminación exterior, alarmas, cámaras de seguridad o porteros eléctricos en el ingreso.
- Controlar todo lo relativo a cerrojos, incluyendo si las llaves están guardadas en lugar seguro y codificadas, asignación de responsabilidades en el control de llaves y sus copias, y que las copias de las llaves funcionen bien. Asegurarse de que los cerrojos sean cambiados cuando se pierden las llaves o si son robadas, y que esos incidentes queden registrados.
- ¿Cuentas con un "cuarto seguro" especial?
- ¿Es posible retirar el cartel con tu nombre de la oficina en tiempos de mayores amenazas para reducir la vulnerabilidad en caso de agresión?

3. Personal en la oficina
- ¿Contratan solamente personal confiable, entre ellos guardias, y verifican sus referencias?
- ¿Está todo el personal capacitado en cuando a los planes de seguridad que les son relevantes?
- ¿Cuentan con un plan en el caso de que la oficina sea allanada por las autoridades u otros grupos?
- ¿Mantienen un buen diálogo con todo el personal, especialmente si saben que tienen problemas financieros o están bajo algún otro tipo de presión? (Personal disgustado puede constituirse en el enemigo más peligroso).
- Cuando alguien deja la organización: ¿cambian las medidas de seguridad, contraseñas y llaves que sean necesarias?

4. Procedimientos y "filtros" para la admisión de visitas
- ¿Están operando procedimientos de admisión para todo tipo de visitantes? ¿Está todo el personal familiarizado con ellos?
- ¿ Preguntan al personal que normalmente desarrollan los procedimientos de admisión si éstos funcionan adecuadamente y qué mejoras habría que hacer?
- ¿El personal sabe qué hacer si llega un paquete que no están esperando? (por ejemplo: aislarlo, no abrirlo, llamar a las autoridades).
- ¿Tomas nota de los nombres de los visitantes (incluyendo a quienes asisten a reuniones en su oficina)? En caso afirmativo, ¿esta información es sensible? y ¿cómo la protegen? (por ejemplo mediante códigos y archivos encriptados).

5. Seguridad de la información (ver también Apéndice 14, Seguridad en los teléfonos y ordenadores)
- ¿Realizas habitualmente una copia de seguridad (back-up) y la mantienes en un lugar seguro fuera de la oficina?
- ¿El personal sabe que no debe dejar información sensible en sus escritorios?
- ¿Cuentan con un sistema de seguridad para registrar información confidencial, por ejemplo sobre clientes o testigos?
- ¿Le otorgan a los archivos de información más sensible (físicos o electrónicos) nombres seguros de modo que no sean identificados fácilmente?

6. Seguridad en caso de accidentes
- Controlar el estado de los extinguidores de incendio, válvulas de gas, cañerías y grifos de agua, conexiones eléctricas y cables y generadores eléctricos (cuando corresponda).

7. Responsabilidad y capacitación
- ¿Han sido asignadas las responsabilidades de la seguridad en la oficina? ¿Es efectiva?
- ¿Cuentan con un programa de capacitación en seguridad de la oficina? ¿Cubre todas las áreas incluidas en este análisis? ¿Están entrenados todos los integrantes del personal? ¿Esta capacitación es efectiva?