PROTECTION INTERNATIONAL

LIGNES DIRECTRICES POUR LA SÉCURITÉ DES FEMMES DÉFENSEURES DES DROITS HUMAINS

PROTECTION INTERNATIONAL

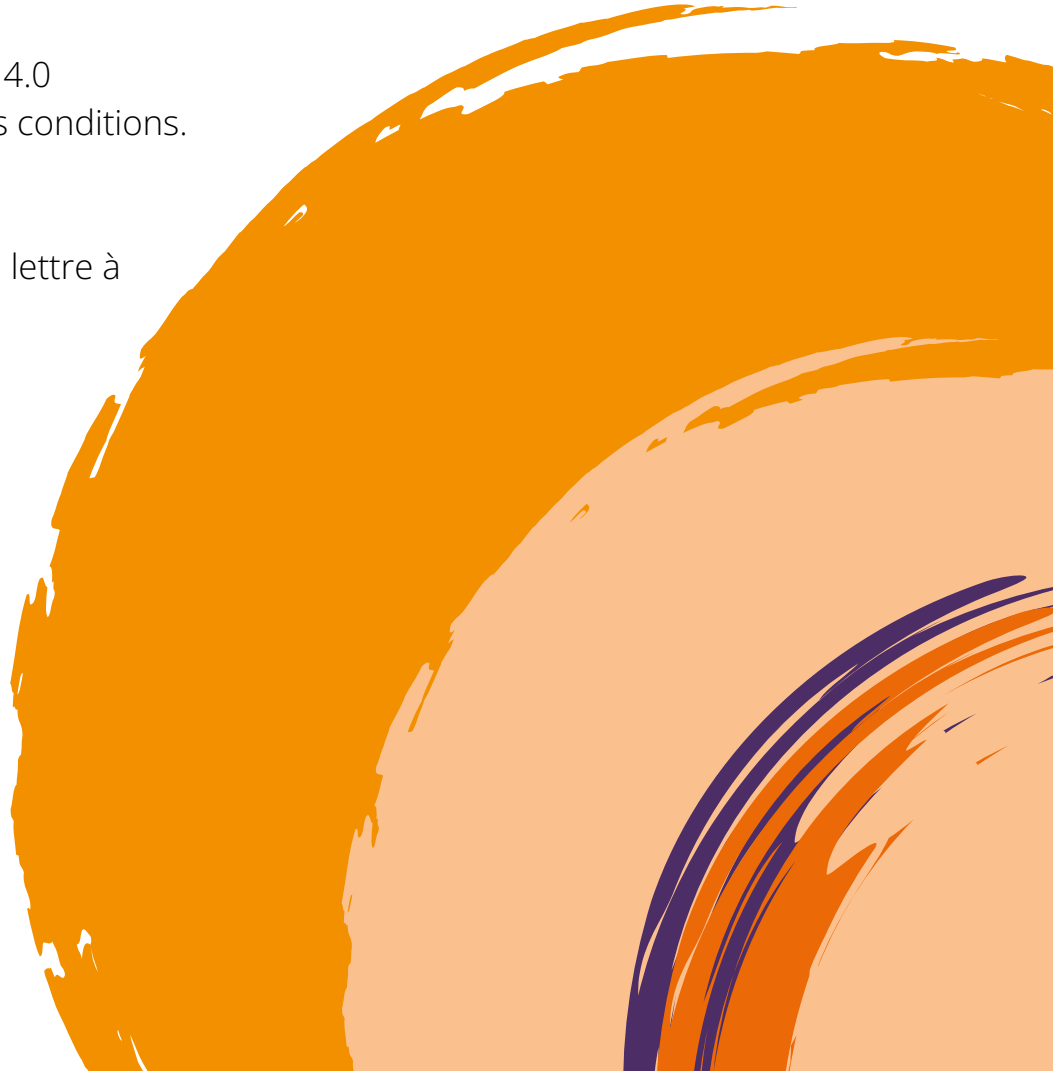
www.protectioninternational.org

Auteur·e·s
Protection International DRC

Conception graphique
Lucrecia Cisneros Rincón

ISBN : 978-2-931244-29-6
EAN : 9782931244296

Juin 2024



INTRODUCTION

Les femmes défenseures des droits humains (FDH) en République Démocratique du Congo (RDC) font face à des défis et des risques particuliers en raison de leur travail crucial en faveur de la justice et des droits humains. Elles sont souvent victimes d'intimidations, de harcèlement, de menaces, d'agressions physiques et même de meurtres en raison de leurs activités.

PI se propose d'édicter des mesures pour leur protection. Ces mesures seront importantes pour les FDDHs afin de renforcer leur sécurité et leur bien-être car, en acquérant des connaissances et des compétences en matière de sécurité physique, numérique et psychologique, les FDDH pourront mieux se protéger contre les risques et les menaces auxquels elles sont confrontées. Cela leur permet de travailler plus efficacement en toute sécurité en vue de mieux poursuivre leurs activités de protection au sein de la communauté. Ces mesures les aideront aussi à développer des stratégies d'autoprotection : apprendre à bien analyser le contexte, à identifier les risques potentiels, à évaluer les situations dangereuses et à mettre en place des stratégies efficaces pour se protéger.

Cet outil est produit dans le cadre du projet intitulé *« Protéger et Sécuriser les Femmes et les Filles pour une Participation Efficace au Processus de Paix et Promotion Des Droits Humains en RDC »* mis en œuvre par Protection International (PI) et SOFEPADI, avec l'appui financier de ONU Femmes.

Protocoles prévus pour la sécurité

BUREAU

- Effectuer une évaluation approfondie des risques pour identifier les menaces potentielles, telles que les intrusions, les vols, les incendies ou les attaques physiques.
- Sécurité des locaux: Assurer la sécurité des locaux en installant des portes et serrures robustes, des systèmes de surveillance vidéo si possible, des alarmes et des contrôles d'accès, fils barbelés.
- Planification d'urgence: Élaborer un plan d'urgence clair et accessible à toutes les personnes qui fréquentent le bureau, définissant les procédures à suivre en cas d'incident.
- Définir les horaires de travail et ne pas rester au bureau après les heures de travail ou arriver avant les heures prévues si la situation n'est sécuritaire n'est pas bonne.
- Veiller à ce que le bureau (notamment les placards, les fenêtres et les portes) soit bien fermé avant de quitter les lieux.
- Briefer régulièrement tous les gardiens afin qu'ils ne fassent rentrer que les personnes autorisées et qu'elles suivent toutes les procédures établies pour l'accessibilité du bureau.
- Créer un registre pour consigner toutes les visites (mentionner les identités sur base d'une pièce d'identité valable/ Carte d'électeur, passeport ou tout autre document valable avec photo du visiteur)
- Créer un cahier ou un registre pour y consigner les incidents de sécurité. Suivre les procédures d'admission aux visites du bureau.
- S'assurer que les montants en cash présents au bureau soient limités.
- Signer une décharge lorsque du matériel de bureau est emporté à la maison.
- Constituer une malle de sécurité avec des bidons d'eau, des bouteilles d'eau potable et de la nourriture en veillant sur la date de péremption pour les périodes d'hibernation forcée.
- S'assurer que tous les objets de valeur soient bien gardés et assurés en cas de pillage.
- Promouvoir une culture de bien-être au sein du bureau en encourageant des pratiques saines, telles que la gestion du temps, la pratique d'exercices physiques et des techniques de relaxation.

COMMUNICATION

- Utiliser un code PIN ou un mot de passe fort et unique pour verrouiller l'écran du téléphone et protéger l'accès aux données.
- Activer la fonction de localisation du téléphone pour permettre son suivi en cas de perte ou de vol.
- Utiliser des plateformes de communication sécurisées pour les échanges confidentiels, comme les logiciels de messagerie instantanée chiffrés ou les appels téléphoniques cryptés (wire, signal ...)
- Avoir à tout moment une réserve de crédit sur son portable, ou si possible un abonnement.
- Installer un logiciel de sécurité mobile réputé pour protéger contre les malwares, les virus et les tentatives d'intrusion.
- Dans la mesure du possible, avoir deux cartes SIM de deux réseaux différents. Tous les numéros devraient être disponibles auprès d'une personne de confiance.
- Avoir suffisamment de crédit sur des modem/USB internet comme moyen alternatif de communication.
- S'informer continuellement, en particulier par les radios, sur la situation quotidienne dans sa zone et les environs.
- Toute nouvelle alarmante et crédible devrait être partagée avec les collègues.
- Les numéros de téléphone des membres de la famille de tous les collègues devraient être communiqués à une personne de confiance (de préférence un point focal de sécurité dans votre organisation).
- Le numéro de la personne de confiance devrait être communiqué aux proches. Les membres de la famille doivent être informés sur les lignes de conduite de votre organisation et doivent avoir connaissance des comportements à adopter en cas de problème.
- Verrouiller les applications sensibles, telles que les messageries instantanées, les réseaux sociaux et les applications bancaires, avec des mots de passe supplémentaires.
- Télécharger des applications uniquement depuis des sources officielles, comme les magasins d'applications légitimes.
- Examiner attentivement les autorisations demandées par les applications avant de les installer.

SÉCURITÉ NUMÉRIQUE

Téléphone

- Supprimer régulièrement les applications inutilisées pour réduire les risques de sécurité.
- Installer régulièrement les mises à jour du système d'exploitation du téléphone pour corriger les failles de sécurité et se protéger contre les menaces émergentes.
- Activer une messagerie vocale sécurisée avec un code PIN pour protéger les messages vocaux contre les écoutes indiscrètes.
- Utiliser des méthodes de sauvegarde chiffrées pour protéger les données sensibles contre les accès non autorisés.
- Pour les smartphones, utiliser des applications sécurisées pour la communication (Signal/ Wire ou à défaut WhatsApp) au lieu des SMS ou appels normaux. Utiliser le navigateur Orfox (navigateur TOR sur le smartphone).
- Utiliser un numéro de téléphone alternatif pour les communications sensibles, comme les conversations confidentielles ou les messages importants.
- Crypter tout le smartphone en gardant à l'esprit que les données ne sont pas nécessairement cryptées sur les serveurs. Avoir connaissance des données sauvegardées.
- Pour remettre à zéro et effacer toutes les données sensibles et personnelles stockées sur vos applications, vider les données et le cache des applications régulièrement.
- Dans les situations confidentielles ou sensibles, utiliser un nouveau smartphone et une nouvelle carte SIM non associés payés en liquide.
- Limiter l'utilisation du numéro principal aux communications quotidiennes et éviter de le partager sur des sites Web ou des réseaux sociaux publics.

Ordinateurs

1. Sécuriser l'appareil

- Mot de passe fort et unique: Utiliser un mot de passe fort et unique pour le compte administrateur et activer l'authentification à deux facteurs pour une protection supplémentaire.
- Verrouillage de l'écran: Activer le verrouillage automatique de l'écran lorsqu'il n'est pas utilisé et exiger un mot de passe pour le déverrouiller.
- Logiciel de sécurité: Installer un logiciel de sécurité réputé, comprenant un antivirus, un anti-malware et un pare-feu, et maintenir ses définitions à jour.

2. Protection des données

- **Sauvegardes régulières:** Effectuer des sauvegardes régulières des données importantes sur un disque dur externe ou un service de stockage cloud sécurisé.
- **Chiffrement des données:** Chiffrer les données sensibles sur l'ordinateur pour les protéger en cas de vol ou de perte de l'appareil.
- **Contrôle d'accès aux fichiers:** Limiter l'accès aux fichiers sensibles aux utilisateurs qui en ont réellement besoin.

3. Utilisation prudente d'Internet

- **Naviguer sur des sites Web de confiance:** Éviter les sites Web suspects ou non sécurisés et faire attention aux liens et pièces jointes provenant de sources inconnues.
- **Mettre à jour le navigateur et les logiciels:** Maintenir le navigateur Web et les logiciels à jour pour bénéficier des derniers correctifs de sécurité.
- **Utiliser un VPN sur les réseaux Wi-Fi publics:** Utiliser un VPN (réseau privé virtuel) pour chiffrer les communications et protéger la confidentialité lors de la connexion à des réseaux Wi-Fi publics.

4. Logiciels et applications

- **Téléchargement à partir de sources fiables:** Télécharger des logiciels et des applications uniquement à partir de sources officielles, comme les sites Web des développeurs ou les magasins d'applications légitimes.
- **Mettre à jour les logiciels:** Mettre à jour régulièrement les logiciels et les applications installés sur l'ordinateur pour corriger les failles de sécurité et bénéficier des nouvelles fonctionnalités.
- **Supprimer les logiciels inutiles:** Désinstaller les logiciels et applications inutilisés pour réduire les risques de sécurité.

5. Sensibilisation et formation

- **Formation à la sécurité numérique:** Dispenser des formations régulières aux femmes défenseures des droits humains sur les risques numériques, les bonnes pratiques de sécurité et l'utilisation des ordinateurs.
- **Partage d'informations et de ressources:** Partage des informations et des ressources sur la sécurité numérique avec les femmes défenseures, y compris des guides, des tutoriels et des conseils pratiques.
- **Encourager une culture de sécurité numérique:** Promouvoir une culture de sécurité numérique au sein des communautés de défenseurs des droits humains, en encourageant le partage d'expériences sur l'évolution de technologies.

6. Assistance et soutien spécialisés

- **Mise en place d'un service d'assistance dédié:** Mettre en place un service d'assistance dédié pour fournir aux femmes défenseurs des droits humains un soutien technique et des conseils en matière de sécurité informatique.
- **Collaboration avec des experts en sécurité:** Collaborer avec des experts en sécurité informatique pour effectuer des audits de sécurité des systèmes informatiques et fournir des conseils personnalisés.
- **Accès à des outils et à des ressources spécialisées:** Donner accès aux femmes défenseures des droits humains à des outils et à des ressources spécialisés pour améliorer leur sécurité informatique, tels que des logiciels de chiffrement et de communication sécurisée.

7. Protection contre les malwares et les ransomware

- **Mettre à jour le système d'exploitation et les logiciels:** Installer régulièrement les mises à jour du système d'exploitation et des logiciels pour corriger les failles de sécurité et se protéger contre les menaces émergentes.
- **Utiliser un logiciel anti-malware:** Installer un logiciel anti-malware réputé et maintenir ses définitions à jour.
- **Être prudent avec les pièces jointes et les liens:** Ne pas ouvrir de pièces jointes ou cliquer sur des liens provenant de sources inconnues ou suspectes, car ils peuvent contenir des malwares.

8. Protection contre les attaques de phishing et d'ingénierie sociale

- **Se méfier des emails et messages suspects:** Ne pas répondre aux emails ou messages provenant de sources inconnues ou suspectes, et ne pas cliquer sur les liens ou pièces jointes qu'ils contiennent.
- **Vérifier l'authenticité des sites Web:** Avant de saisir des informations personnelles ou financières sur un site Web, vérifier l'authenticité du site et l'URL.
- **Ne pas divulguer d'informations personnelles sensibles.**

Interdits en matière de sécurité numérique pour les femmes défenseures des droits humains

1 ÉVITER LES RÉSEAUX WI-FI PUBLICS NON SÉCURISÉS

- Les réseaux Wi-Fi publics, tels que ceux dans les cafés, les aéroports et les gares, ne sont souvent pas sécurisés et peuvent être facilement piratés.
- Évitez d'utiliser ces réseaux pour des activités sensibles, comme la connexion à des comptes bancaires ou l'envoi d'emails confidentiels.

2 NE PAS CLIQUER SUR DES LIENS OU PIÈCES JOINTES SUSPECTES

- Les emails, SMS et messages sur les réseaux sociaux provenant de sources inconnues ou suspectes peuvent contenir des liens malveillants ou des pièces jointes infectées par des virus.
- Ne cliquez jamais sur ces liens et n'ouvrez jamais ces pièces jointes, car elles pourraient compromettre votre sécurité.

3 NE PAS PARTAGER D'INFORMATIONS PERSONNELLES SENSIBLES EN LIGNE

- Évitez de partager des informations personnelles sensibles, telles que votre adresse personnelle, votre numéro de téléphone ou vos informations bancaires, sur des sites Web ou des réseaux sociaux publics.
- Soyez prudent quant aux informations que vous partagez en ligne et limitez-vous aux plateformes et aux personnes de confiance.

4 NE PAS UTILISER LE MÊME MOT DE PASSE POUR PLUSIEURS COMPTES

- Si un pirate informatique obtient votre mot de passe pour un compte, il pourrait l'utiliser pour accéder à d'autres comptes si vous utilisez le même mot de passe partout.
- Utilisez des mots de passe forts et uniques pour chaque compte en ligne et changez-les régulièrement.

5 NE PAS DÉSACTIVER LES MISES À JOUR DE SÉCURITÉ

- Les mises à jour de sécurité des systèmes d'exploitation et des logiciels sont essentielles pour corriger les failles de sécurité et protéger contre les menaces émergentes.
- Activez les mises à jour automatiques ou installez-les dès qu'elles sont disponibles.

6 NE PAS IGNORER LES AVERTISSEMENTS DE SÉCURITÉ

- Si votre ordinateur ou votre appareil vous avertit d'une menace de sécurité, prenez-le au sérieux.
- N'ignorez pas ces avertissements, car ils pourraient indiquer un problème réel qui nécessite votre attention.

7 NE PAS UTILISER DE LOGICIELS PIRATÉS OU ILLÉGAUX

- Les logiciels piratés ou illégaux peuvent contenir des malwares ou des virus qui peuvent compromettre votre sécurité et vos données.
- Téléchargez uniquement des logiciels provenant de sources officielles et payez pour les licences si nécessaires.

8 NE PAS CONNECTER DES PÉRIPHÉRIQUES INCONNUS À VOTRE ORDINATEUR

- Ne connectez jamais des clés USB, des disques durs ou d'autres périphériques inconnus à votre ordinateur, car ils pourraient contenir des malwares ou des virus.
- Soyez prudent avec les périphériques que vous utilisez et assurez-vous qu'ils proviennent d'une source fiable.

9 NE PAS PARTAGER VOS APPAREILS PERSONNELS AVEC D'AUTRES

- Si vous partagez votre ordinateur ou votre téléphone avec d'autres personnes, définissez des comptes utilisateurs distincts et protégez votre compte par un mot de passe.
- Soyez prudent quant aux informations que vous stockez sur ces appareils et évitez de les utiliser pour des activités sensibles si vous les partagez.

10 NE PAS NÉGLIGER VOTRE BIEN-ÊTRE

- Prenez des pauses régulières lorsque vous utilisez des appareils numériques et évitez de passer trop de temps devant les écrans.
- Soyez conscient de l'impact potentiel des technologies numériques sur votre santé mentale et votre bien-être.

Situations d'urgence

AVANT L'URGENCE

- Rester attentif aux questions de sécurité en suivant les informations et les rapports d'organisations ou institutions chargées de la sécurité, comme l'INSO ou la MONUSCO.
- Établir un calendrier des dates stratégiques des événements politiques à haut risque ou les moments d'insécurité.
- Les rapports réguliers doivent être préparés à l'intérieur de votre organisation pour partager les informations sur l'évolution politique, électorale et sécuritaire.

APRÈS L'URGENCE

- Obtenez de l'aide médicale et psychologique: Si vous avez été blessée ou traumatisée pendant l'urgence, cherchez une aide médicale et un soutien psychologique appropriés.
- Contactez vos contacts de soutien: Renouez le contact avec vos contacts de soutien pour obtenir du réconfort, des conseils et de l'assistance.
- Documentez l'incident: Soumettez un rapport détaillé de l'incident aux autorités compétentes et aux organisations de défense des droits humains.
- Évaluez votre plan de sécurité: Réexaminez votre plan de sécurité et apportez les modifications nécessaires pour tenir compte de l'expérience vécue.

PENDANT L'URGENCE

1. Restez calme et évaluez la situation:

- Prenez une profonde respiration et essayez de rester calme pour analyser la situation et prendre des décisions réfléchies.
- Identifiez la nature de la menace, le niveau de risque immédiat et les options disponibles.

2. Si vous êtes en danger immédiat:

- **Quittez la zone dangereuse:** Si vous pouvez le faire en toute sécurité, quittez immédiatement la zone où vous vous sentez menacée.
- **Appelez à l'aide:** Contactez vos contacts d'urgence, les autorités locales ou les organisations de défense des droits humains pour obtenir de l'aide.
- **Rendez-vous dans un lieu sûr:** Si vous ne pouvez pas quitter la zone, trouvez un endroit sûr où vous cacher, comme un commissariat de police, un refuge pour femmes ou une maison de confiance.

3. Si vous ne pouvez pas quitter la zone immédiatement:

- **Protégez-vous:** Essayez de vous protéger en trouvant un endroit sûr à l'intérieur d'un bâtiment, en verrouillant les portes et en restant à l'écart des fenêtres.
- **Contactez vos contacts de soutien:** Informez vos contacts de confiance de votre situation et demandez-leur de vous aider ou d’alerter les autorités.
- **Documentez l'incident:** Si possible, recueillez des preuves de l'incident, telles que des photos, des vidéos ou des témoignages, pour les partager avec les autorités ou les organisations de défense des droits humains.

Protocoles de secours

Au sein de votre organisation, élaborer des plans de sécurité et de contingence, des protocoles pour traiter les violations flagrantes contre le personnel (au cas d'une arrestation arbitraire, une disparition forcée, une perquisition par la police ou un enlèvement).

Ces protocoles doivent indiquer:

- Qui est responsable de la mise en œuvre du protocole.
- Les coordonnées de la famille de chaque membre du personnel.
- Quels facteurs externes peuvent intervenir pour assister.
- Comment mobiliser une assistance judiciaire.
- Comment la victime peut plaider auprès les autorités locales, nationales et les acteurs internationaux.

PROTECTION
INTERNATIONAL