Laboratoire de protection des droits numériques
Initiative « Bouclier des droits numériques »

GUIDE MÉTHODOLOGIQUE DES MINI-AUDITS ET PLANS DE SÉCURITÉ INDIVIDUELS



NAFASI
magamba
DEFEND DEFENDERS

🗺️ SOMMAIRE

Dans ce guide

01 📘 Présentation et contexte

02 🧭 Principes directeurs et éthique

03 🎯 Cadre conceptuel : comprendre le risque

04 🏠 Organisation du Laboratoire

05 🔎 Méthodologie du mini-audit en six étapes

06 🛡️ Domaines d'audit et points de contrôle

07 📝 Élaboration du plan de sécurité individuel

08 🚨 Gestion des incidents et orientation

09 💚 Protection des données et bien-être

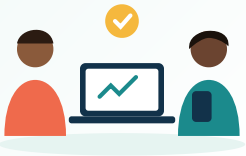
10 📊 Suivi, évaluation et indicateurs

11 🗂️ Annexes : modèles de fiches

💡 **Comment lire ce guide ?** Dans l'ordre à la première utilisation, puis comme référence grâce aux annexes. Les durées et seuils sont des repères à adapter au contexte local.

📘 SECTION 01

Présentation et contexte



Ce guide donne aux équipes du Laboratoire une méthode commune pour mener un mini-audit de sécurité numérique et produire un plan de sécurité individuel en **une à deux séances**.

Le Laboratoire de protection des droits numériques est une activité de l'initiative « Bouclier des droits numériques » du Projet NAFASI. L'ONG JeRestaure Bien-Etre le met en œuvre. Il accueille des personnes exposées à des risques numériques et les aide à mieux protéger leurs droits et leur bien-être.

🔓 Piratage de comptes · 😡 Harcèlement · 👁️ Surveillance · 📸 Diffusion non consentie · 📰 Désinformation

🎯 Objectifs du guide

Standardiser
Le déroulé des mini-audits, pour une qualité comparable d'un participant et d'un animateur à l'autre.

Rendre le plan réaliste
Un outil priorisé et porté par la personne elle-même.

Protéger
Participants et équipe, par des règles claires de consentement, de confidentialité et de bien-être.

Faciliter le suivi
Et l'évaluation des résultats du Laboratoire.

📖 Définitions

Mini-audit
Revue courte (60 à 90 minutes) des comptes, appareils et pratiques d'une personne, centrée sur ses risques réels.

Plan de sécurité individuel
Document de 1 à 2 pages listant les actions prioritaires, leur échéance, les ressources et les contacts d'urgence.

Participant
Personne accompagnée, qui reste propriétaire de ses données, de ses appareils et de ses décisions.

Public du guide : facilitateurs, auditeurs et référents bien-être du Laboratoire.

SECTION 02

Principes directeurs et éthique



Chaque mini-audit respecte **sept principes**. En cas de doute, la sécurité et l'autonomie de la personne priment sur la complétude de l'audit.

Ne pas nuire
Aucune action technique si elle peut exposer la personne (alerter un agresseur, perdre des preuves, couper un contact vital).

Consentement libre et éclairé
La personne sait ce qui sera examiné, noté et conservé, et peut refuser ou arrêter à tout moment.

Confidentialité
Rien ne sort de l'équipe, sauf danger grave et imminent, après échange avec la personne lorsque c'est possible.

Centré sur la personne
La personne décide. L'animateur conseille, explique les compromis et ne juge pas.

🌱 Sensibilité au traumatisme

Pas de récit détaillé des violences vécues ; la personne fixe le rythme et fait des pauses.

🌍 Genre, âge et inclusion

Les risques varient selon le genre, l'âge, le handicap, la langue, la littératie numérique et le statut.

⚖️ Proportionnalité

D'abord les risques les plus probables et les plus graves, pas toutes les failles possibles.

📜 Règles de conduite pour l'équipe

- ✓ 🔑 Ne jamais demander ni noter un mot de passe. Aider la personne à le changer elle-même.
- ✓ 📱 Ne pas accéder aux comptes ou appareils sans que la personne soit présente et d'accord.
- ✓ 🛡️ Ne pas promettre une sécurité totale ; parler de réduction des risques.
- ✓ 🙅 Ne pas intervenir sur des appareils appartenant à un tiers.
- ✓ 🧭 Orienter vers un avocat, un service de santé ou une ligne d'écoute dès que la situation dépasse le mandat du Laboratoire.

🎯 SECTION 03

Cadre conceptuel : comprendre le risque



Le mini-audit repose sur un **modèle de menace simplifié** : on protège d'abord ce qui compte le plus pour la personne, contre les adversaires qui la menacent réellement.

🔑 Les notions clés

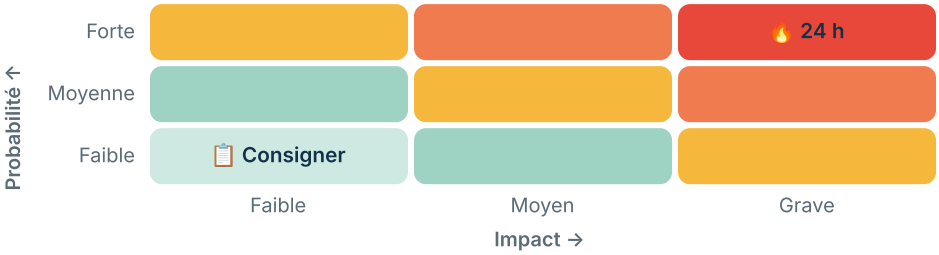
💎 **Actif**	**Qu'est-ce qui a de la valeur à protéger ?** Ex. : Photos privées, contacts, compte de messagerie, source de revenus, réputation, localisation
🕵️ **Adversaire**	**Qui pourrait vouloir y accéder ou nuire ?** Ex. : Ex-partenaire, proche, employeur, harceleur anonyme, escroc, acteur étatique
⚡ **Menace**	**Que pourrait-il faire ?** Ex. : Usurper un compte, publier des images, suivre les déplacements, voler l'appareil
🕳️ **Vulnérabilité**	**Quelle faille rend cela possible ?** Ex. : Mot de passe réutilisé, appareil partagé, absence de verrouillage, paramètres publics
💥 **Impact**	**Quelles conséquences si cela arrive ?** Ex. : Perte financière, atteinte physique, honte, perte d'emploi, isolement

❓ Le modèle de menace en cinq questions

1. Que voulez-vous protéger ?
2. De qui voulez-vous le protéger ?
3. Quelle est la probabilité que cela arrive ?
4. Quelles seraient les conséquences si cela arrivait ?
5. Quels efforts êtes-vous prêt à faire pour réduire ce risque ?

🌡️ Niveaux de risque

Chaque risque est noté selon sa **probabilité** (faible, moyenne, forte) et son **impact** (faible, moyen, grave).



🔥 **Forte probabilité + impact grave :** action prioritaire du plan, à traiter dans les 24 heures. Faible probabilité + impact faible : à consigner, sans action immédiate.

🏠 SECTION 04

Organisation du Laboratoire



Un mini-audit se déroule en tête-à-tête ou en binôme, dans un lieu calme et confidentiel, sur **60 à 90 minutes**, avec une séance de suivi courte.

🙋‍♀️ Public

En priorité, les personnes dont les droits numériques sont menacés :

🧑🏾 Jeunes · 👩🏾 Femmes et filles · ✊🏾 Militants · 🎙️ Journalistes · 🫂 Personnes en situation de vulnérabilité

🆓 **Accueil volontaire et gratuit.** Pour les mineurs, l'équipe applique la procédure de protection de l'enfance et d'autorisation parentale de JeRestaure Bien-Etre.

👥 Rôles

🤗 Facilitateur

Accueille, explique le cadre, anime l'entretien, garantit le rythme et le respect des principes.

💻 Auditeur numérique

Guide les vérifications techniques avec la personne, explique chaque paramètre.

💚 Référent bien-être

Repère la détresse, propose une pause ou une orientation psychosociale, assure le suivi.

📋 Coordinateur

Gère les rendez-vous, l'archivage minimal, les statistiques et les orientations juridiques.

⚠️ **Cumul de rôles :** possible pour deux rôles, mais **jamais** auditeur + référent bien-être sur un cas de violence grave.

⏳ Déroulé type en quatre phases

1. Accueil

10 min

Présentation, consentement, règles de confidentialité

2. Cadrage

15–20 min

Entretien et modèle de menace

3. Audit

30–40 min

Vérifications guidées des comptes, appareils et paramètres

4. Plan

15–20 min

Priorisation, plan de sécurité, remise du document

🧰 Matériel et environnement

- ✓ 🚪 Salle fermée, sans passage, avec possibilité de pause et d'eau.
- ✓ 📱 Appareil du participant uniquement ; l'équipe ne branche aucune clé USB inconnue dessus.
- ✓ 💻 Ordinateur de l'équipe à jour, utilisé uniquement pour des notes minimales ou afficher des guides.
- ✓ 🖨️ Fiches imprimées : consentement, grille d'audit, plan de sécurité (voir annexes).
- ✓ 📇 Liste à jour des services d'orientation : juridique, médical, psychosocial, signalement.

🔎 SECTION 05

Méthodologie du mini-audit en six étapes



Six étapes dans un **ordre fixe**, pour que la personne comprenne ce qui se passe et garde le contrôle à chaque moment.

1

🤝 Accueil et consentement

⏱ 10 min

Présenter le Laboratoire, expliquer ce qui sera examiné, noté et conservé, faire signer ou confirmer oralement le consentement. Rappeler que la personne peut arrêter à tout moment.

2

🗣️ Entretien de cadrage

⏱ 15–20 min

Poser les cinq questions du modèle de menace. Demander si la personne se sent en sécurité maintenant, si quelqu'un d'autre a accès à ses appareils ou comptes, et ce qui l'inquiète le plus. Ne pas forcer le récit.

3

🗺️ Cartographie

⏱ 10 min

Lister avec la personne ses appareils, ses comptes principaux (messagerie, réseaux sociaux, banque, mobile money) et les personnes qui y ont accès.

4

🔧 Vérifications techniques

⏱ 20–30 min

Parcourir les domaines de la section 6, appareil en main, en laissant la personne manipuler. L'auditeur explique chaque paramètre et son effet.

5

⚖️ Analyse et priorisation

⏱ 10 min

Classer les constats par probabilité et impact. Retenir 3 à 5 actions maximum pour ne pas décourager.

6

🎤 Restitution

⏱ 10 min

Présenter les constats en langage simple, valoriser ce qui est déjà bien fait, valider les actions retenues et passer à la rédaction du plan.

🚧 Points de vigilance

⚠ 👀 Si la personne est suivie ou surveillée par un proche, ne pas modifier brutalement les paramètres : un changement visible peut alerter l'agresseur. Évaluer d'abord les risques pour sa sécurité physique.

⚠ 🧪 Si un appareil est soupçonné d'être compromis, ne pas le réinitialiser avant d'avoir discuté de la conservation de preuves.

⚠ 💚 Si la personne montre de la détresse, interrompre l'audit et passer la main au référent bien-être.

⚠ ✍ Noter uniquement les constats et actions, jamais les contenus personnels vus à l'écran.

🛡 SECTION 06

Domaines d'audit et points de contrôle



Huit domaines couvrent l'essentiel des risques courants. L'auditeur ne traite que ceux qui correspondent aux risques identifiés pendant le cadrage.

1 Comptes et mots de passe 🔐

- Mot de passe unique par compte important
- Gestionnaire de mots de passe ou phrase de passe longue
- Vérification en deux étapes activée
- Adresse et numéro de récupération à jour et contrôlés par la personne

2 Appareils 📱

- Verrouillage par code ou empreinte
- Mises à jour installées
- Applications inconnues ou inutiles supprimées
- Permissions sensibles (localisation, micro, caméra) vérifiées
- Absence de partage involontaire avec un proche

3 Messagerie et réseaux sociaux

- Appareils connectés au compte vérifiés
- Confidentialité du profil
- Qui peut voir, contacter ou identifier la personne
- Messages éphémères et chiffrement de bout en bout si pertinent

4 Navigation

- Navigateur à jour
- Extensions limitées
- Méfiance envers liens et pièces jointes (hameçonnage)
- Sessions fermées sur appareils partagés

5 Wi-Fi et réseaux

- Éviter les opérations sensibles sur Wi-Fi public
- Mot de passe du routeur personnel changé
- Partage de connexion protégé

6 Données et sauvegardes

- Sauvegarde des documents essentiels
- Chiffrement du téléphone
- Suppression sécurisée des données sensibles
- Gestion des photos et documents d'identité

7 Identité et vie privée en ligne

- Recherche de son nom et de ses informations publiques
- Suppression ou limitation de ce qui expose (adresse, école, lieu de travail)
- Paramètres de géolocalisation des publications

8 Harcèlement et désinformation

- Savoir bloquer, signaler et documenter (captures horodatées, liens)
- Réflexes de vérification d'une information
- Contacts utiles en cas de menace

Règle d'utilisation — chaque point est noté : ✅ Conforme 🛠️ À améliorer ➖ Non applicable

Les points « à améliorer » alimentent l'analyse de l'étape 5 — **jamais plus de trois actions par domaine**.

📝 SECTION 07

Élaboration du plan de sécurité individuel



Une à deux pages, dans la langue de la personne, avec des actions **concrètes, datées et réalisables** par elle seule ou avec un soutien identifié.

🧱 Structure du plan

- 💎 **Ce que je protège en priorité** — 2 à 3 éléments, dans les mots de la personne
- ⚠️ **Les risques principaux identifiés**
- ✅ **Mes actions, classées par échéance**
- 🆘 **Mon plan d'urgence**
- 🤝 **Mes personnes et services de confiance**
- 📅 **La date de mon prochain point de suivi**

📆 Actions par échéance

⚡ 24 heures

Risques forts et gestes simples

- Changer le mot de passe du compte de messagerie principal
- Activer la vérification en deux étapes
- Verrouiller le téléphone

🗓️ 30 jours

Habitudes et paramétrage

- Installer un gestionnaire de mots de passe
- Revoir la confidentialité des réseaux sociaux
- Sauvegarder les documents importants

🌳 90 jours

Changements durables

- Migrer les comptes secondaires
- Former un proche
- Réévaluer le modèle de menace

🏅 Critères d'une bonne action

🎯 Précise	👍 Réaliste	📅 Datée	📏 Mesurable	🙋 Choisie
quoi	faisable	quand	c'est fait ?	par la personne

> 💬 *« D'ici vendredi, j'active la vérification en deux étapes sur mon compte de messagerie. »*

🆘 Plan d'urgence

La personne note ce qu'elle fait en premier si son compte est piraté, son téléphone perdu ou volé, ou si elle est menacée en ligne, et qui elle prévient. Elle garde ce plan hors de l'appareil concerné (papier, ou confiance d'un proche) lorsque c'est plus sûr.

🤝 **Personnes de confiance**

1 à 3 personnes ou services, avec leur moyen de contact préféré. Ne jamais inscrire une information qui pourrait mettre la personne en danger si le document était découvert ; adapter le support (version courte, codée ou orale).

🚨 SECTION 08

Gestion des incidents et orientation



L'équipe applique d'abord les **gestes de protection immédiate**, puis oriente vers le bon service, sans jamais agir à la place de la personne.

🔓 Compte piraté

⚡ RÉFLEXES

Changer le mot de passe depuis un appareil sûr ; fermer les sessions ouvertes ; activer la vérification en deux étapes ; prévenir les contacts ; documenter

➡️ ORIENTATION

Service d'assistance de la plateforme ; référent juridique si usurpation ou chantage

📵 Vol ou perte d'appareil

⚡ RÉFLEXES

Verrouiller ou effacer à distance si possible ; changer les mots de passe des comptes connectés ; prévenir l'opérateur mobile

➡️ ORIENTATION

Déclaration aux autorités selon le contexte local et le souhait de la personne

😠 Harcèlement ou menaces en ligne

⚡ RÉFLEXES

Ne pas répondre ; capturer avec date et lien ; bloquer et signaler sur la plateforme ; limiter la visibilité du profil

➡️ ORIENTATION

Référent juridique, service d'écoute, organisation de protection des femmes ou de l'enfance

🖼️ Diffusion non consentie d'images

⚡ RÉFLEXES

Documenter ; demander le retrait à la plateforme ; ne pas supprimer les preuves avant avis

➡️ ORIENTATION

Appui juridique et psychosocial en priorité

💧 Fuite ou vol de données

⚡ RÉFLEXES	➡️ ORIENTATION
Identifier les comptes touchés ; changer les mots de passe ; surveiller les comptes financiers	Banque, opérateur, autorité de protection des données si elle existe

⚖️ Arrestation ou saisie d'appareil

⚡ RÉFLEXES	➡️ ORIENTATION
Préparer à l'avance : sauvegardes, verrouillage, contact d'un avocat à connaître	Avocat ou organisation de défense des droits

🧭 Principes d'orientation

- ✓ 📇 Avoir une liste locale à jour des services et la vérifier tous les trimestres.
- ✓ ✋ Demander l'accord de la personne avant tout transfert d'information à un tiers.
- ✓ 🚑 En cas de danger physique imminent, appliquer la procédure d'urgence de JeRestaure Bien-Etre et faciliter l'accès aux services de protection.
- ✓ 🗒️ Tracer chaque orientation (date, service, résultat) sans détails personnels superflus.

💚 SECTION 09

Protection des données et bien-être



Le Laboratoire collecte le **strict minimum** de données et protège autant le bien-être des participants que celui de l'équipe.

🔒 Gestion des données du Laboratoire

✂️ Minimisation

Uniquement un code participant, la date, les domaines examinés, les actions décidées et les orientations. Aucun mot de passe, contenu de message ou image.

🎭 Anonymisation

Statistiques agrégées, ne permettant pas d'identifier une personne.

Stockage

Fiches numériques chiffrées, accès restreint, authentification forte. Fiches papier dans un meuble fermé.

Durée de conservation

Fixée avec la direction de JeRestaure Bien-Etre, conforme à la loi ; suppression sécurisée à l'échéance.

Droits des participants

Consulter, corriger ou faire supprimer sa fiche sur simple demande.

Bien-être des participants

- Prévenir au début que l'on peut faire une pause ou arrêter.
- Écouter sans minimiser ni dramatiser ; valider l'inquiétude sans promettre l'impossible.
- Proposer un contact avec le référent bien-être quand la situation est lourde, sans l'imposer.

Bien-être de l'équipe

- Débriefing court après chaque séance difficile.
- Supervision régulière par un professionnel psychosocial.
- Limite de cas lourds par semaine et alternance des rôles contre l'épuisement.
- Séparation des comptes perso/pro ; conduite à tenir en cas de menaces reçues.

SECTION 10

Suivi, évaluation et indicateurs



Chaque participant bénéficie d'un point de suivi à **30 jours** et, si possible, à **90 jours**, pour mesurer la mise en œuvre du plan et ajuster les actions.

Suivi individuel

J+30 — Appel court, message ou rencontre : actions faites, blocages, nouveaux risques.

J+90 — Réévaluation du modèle de menace et mise à jour du plan.

🕐 **Discrétion :** le suivi respecte le canal et l'horaire choisis par la personne, pour ne pas l'exposer.

📐 Indicateurs proposés

Dimension	Indicateur	Source
📣 Portée	Nombre de mini-audits réalisés, ventilés par sexe, âge et profil	Fiches codées
⭐ Qualité	Part des participants repartant avec un plan signé	Fiches codées
✅ Résultat J+30	Part des actions prioritaires réalisées	Point de suivi
🔐 Résultat J+90	Part des participants ayant activé la vérification en deux étapes sur leur compte principal	Point de suivi
🛡️ Protection	Nombre d'incidents traités et d'orientations effectuées	Journal des orientations
😊 Satisfaction	Sentiment de sécurité avant et après (échelle de 1 à 5)	Questionnaire court anonyme

🎓 **Apprentissage :** chaque trimestre, l'équipe analyse les constats récurrents, les obstacles et les incidents, puis met à jour le guide, les fiches et la liste d'orientation. Les cibles chiffrées sont à fixer avec les responsables du Projet NAFASI.

🗂️ SECTION 11

Annexes : modèles de fiches



Cinq modèles **à adapter** à la langue, au contexte et à la charte de JeRestaure Bien-Etre avant usage.

- **A** ✍️ Formulaire de consentement
- **B** 🗣️ Fiche d'entretien de cadrage
- **C** 🔎 Grille de mini-audit
- **D** 📝 Modèle de plan de sécurité individuel
- **E** 🔁 Fiche de suivi (30 et 90 jours)

A

ANNEXE A

✍️ Formulaire de consentement

Code participant : ..... Date : .....

J'ai compris que :

- ✓ le mini-audit examine mes comptes, appareils et pratiques, avec ma participation ;
- ✓ l'équipe ne note ni mes mots de passe ni le contenu de mes messages ;
- ✓ seules des informations minimales sont conservées : code, date, actions, orientations ;
- ✓ je peux arrêter à tout moment et demander la suppression de ma fiche ;
- ✓ l'équipe peut rompre la confidentialité uniquement en cas de danger grave et imminent, en m'en informant si possible.

Je consens librement : ☐ **Oui** ☐ **Non**

Signature ou accord oral noté par : .....

Signature

B

ANNEXE B

🗣️ Fiche d'entretien de cadrage

Question	Réponse (mots de la personne)
💎 Que voulez-vous protéger en priorité ?	
🕵️ De qui ou de quoi ?	
🔑 Quelqu'un a-t-il accès à vos appareils ou comptes ?	
🫶 Vous sentez-vous en sécurité en ce moment ?	
📌 Quels incidents avez-vous déjà vécus ? (sans détails)	
💪 Quels efforts pouvez-vous fournir ?	

C

ANNEXE C

🔎 Grille de mini-audit

Domaine	Point de contrôle	État	Priorité
🔐 Comptes	Vérification en deux étapes active	☐ Conforme ☐ À améliorer ☐ N.A.	☐ Haute ☐ Moyenne ☐ Basse
🔐 Comptes	Mots de passe uniques	☐ Conforme ☐ À améliorer ☐ N.A.	☐ Haute ☐ Moyenne ☐ Basse
📱 Appareils	Verrouillage et mises à jour	☐ Conforme ☐ À améliorer ☐ N.A.	☐ Haute ☐ Moyenne ☐ Basse
💬 Réseaux sociaux	Confidentialité du profil	☐ Conforme ☐ À améliorer ☐ N.A.	☐ Haute ☐ Moyenne ☐ Basse
💾 Données	Sauvegarde des documents essentiels	☐ Conforme ☐ À améliorer ☐ N.A.	☐ Haute ☐ Moyenne ☐ Basse
		☐ Conforme ☐ À améliorer ☐ N.A.	☐ Haute ☐ Moyenne ☐ Basse
		☐ Conforme ☐ À améliorer ☐ N.A.	☐ Haute ☐ Moyenne ☐ Basse

➕ À compléter avec les autres points de la section 6 selon les risques du participant.

D

ANNEXE D

📝 Modèle de plan de sécurité individuel

Rubrique	Contenu
💎 Ce que je protège	
⚠️ Risques principaux	
⚡ Actions sous 24 heures	
🗓️ Actions sous 30 jours	
🌳 Actions sous 90 jours	
🔓 Si mon compte est piraté	
📵 Si mon téléphone est perdu ou volé	
😠 Si je suis menacé(e) en ligne	
🤝 Mes personnes et services de confiance	
📅 Date de mon prochain point de suivi	

E

ANNEXE E

🔁 Fiche de suivi (30 et 90 jours)

Action du plan	Faite ?	Obstacle rencontré	Nouvelle action
	☐ Oui ☐ Non ☐ En cours		
	☐ Oui ☐ Non ☐ En cours		
	☐ Oui ☐ Non ☐ En cours		
	☐ Oui ☐ Non ☐ En cours		
	☐ Oui ☐ Non ☐ En cours		

🌡️ **Sentiment de sécurité (1 à 5)**

Avant (1) (2) (3) (4) (5)

Après (1) (2) (3) (4) (5)

🆕 Nouveau risque identifié : .....

➡️ Orientation proposée : .....



Protéger ses droits numériques, c'est protéger son bien-être.

Laboratoire de protection des droits numériques
Initiative « Bouclier des droits numériques » · Projet NAFASI

Mis en œuvre par l'ONG JeRestaure Bien-Etre