Renforcer la sécurité des responsables de la mise en œuvre des services VIH travaillant avec des populations clés

Une formation virtuelle pour une direction organisationnelle

avril 2021

PEPFAR USAID EpiC LINKAGES

Remerciement

Cette formation a été élaborée par Robyn Dayton (conseillère technique principale, FHI 360), et comprend un contenu adapté de l'Initiative Synergía pour les droits de l'homme et de la boîte à outils AMAN MENA : Security Protections for Organizations Working with Key Populations to Strengthen HIV Programming in the Middle East and North Africa (AMAN MENA : Protections sécuritaires pour les organisations travaillant avec les populations clés au renforcement de la programmation VIH dans la région du Moyen-Orient et de l'Afrique du Nord). Des itérations de cette formation virtuelle ont été réalisées avec le personnel de FHI 360 et des organisations partenaires dans le monde entier, notamment en Algérie, en Côte d'Ivoire, en Asie centrale, au Liberia, au Liban, au Kenya, au Malawi, au Mali, au Népal, au Sénégal et en Tanzanie. Leurs expériences de participation à la formation et de partage des enseignements avec leurs organisations, ainsi que leurs commentaires et leurs idées sur ce qui fonctionne ont pratiquement contribué à façonner le contenu final.

Ce travail est le fruit de la collaboration entre Chris Akolo, Meghan DiCarlo, Rose Wilcher de FHI 360 et Michael Marco de l'USAID qui ont veillé à la révision ; Stevie Daniels à l'édition et Lucy Harber à la conception graphique de ce contenu.

Ce document a été rendu possible grâce au généreux soutien du peuple américain à travers l'Agence des États-Unis pour le développement international (USAID) et du Plan d'urgence du Président des États-Unis pour la lutte contre le sida (PEPFAR). Le contenu est la responsabilité de FHI 360 et ne reflète pas nécessairement les opinions de l'USAID, du PEPFAR ou du gouvernement des États-Unis.

Citation suggérée : LINKAGES et EpiC. Renforcer la sécurité des responsables de la mise en œuvre des services VIH travaillant avec des populations clés : une formation virtuelle pour la direction organisationnelle. Durham (NC) : FHI 360 ; 2021.

Liens à travers le Continuum Services VIH pour les populations affectées par le VIH (LINKAGES) est financé par le Plan d'urgence du Président des États-Unis pour la lutte contre le sida (PEPFAR) et l'Agence des États-Unis pour le développement international (USAID). Le projet est un accord de coopération (#AID-OAA-A-14-00045) dirigé par FHI 360 en partenariat avec IntraHealth International, Pact et l'Université de la Caroline du Nord à Chapel Hill.

Le projet "Meeting Targets and Maintaining Epidemic Control" (EpiC), financé par l'Agence des Etats-Unis pour le développement international (USAID) et le Plan d'urgence du Président des États-Unis pour la lutte contre le sida (PEPFAR), est une initiative coopérative mondiale de cinq ans (7200AA19CA00002). Le projet est dirigé par FHI 360 avec des partenaires clés Right to Care, Palladium International, Population Services International (PSI), et Gobee Group.

Table des matières

Acronymes et abréviations

COVID-19 – La maladie du coronavirus de 2019

OSC – Organisation de la société civile

VFG – Violence fondée sur le genre

VIH – Virus de l'immunodéficience humaine

ONGI – Organisation non gouvernementale internationale

EX – Exécutant partenaire

PEPFAR – Le Plan d'urgence du président des Etats-Unis pour la lutte contre le Sida

PE – Exécutant partenaire

SOP – Procédures opérationnelles normalisées

IST – Infection sexuellement transmissible

USAID – Agence américaine pour le développement international

Aperçu de la formation

Audience et objectif

Ce kit de formation est destiné aux programmes de lutte contre le VIH offrant des services aux populations clés - hommes homosexuels et autres hommes ayant des rapports sexuels avec des hommes, usagers de drogues injectables, travailleurs du sexe et personnes transgenres. Il est conçu pour être dispensé à un groupe central comprenant des membres de la direction et du personnel des partenaires de mise en œuvre afin de les aider à identifier et à hiérarchiser les risques de sécurité auxquels leurs organisations sont confrontées, à répertorier leurs stratégies de sécurité pour identifier à la fois les lacunes et les points forts actuels, à élaborer des plans de sécurité pour combler les lacunes prioritaires et à déterminer une pleine mise en œuvre des plans de sécurité. Les équipes centrales de plusieurs partenaires de mise en œuvre doivent être réunies dans le cadre d'une même formation, car l'apprentissage inter-organisationnel est une stratégie de formation essentielle.

La formation peut se dérouler virtuellement, en personne ou sous la forme d'un hybride entre les deux. Après la formation initiale d'un groupe central de chaque partenaire de mise en œuvre, ceux qui ont été formés peuvent adapter les diapositives pour partager les conseils de sécurité avec l'ensemble de leur personnel afin de soutenir l'opérationnalisation complète des plans de sécurité.

Contenu

Le kit de formation contient :

1. Ce manuel de l'animateur avec un programme de formation des participants et de l'animateur, un pré/post-test, une clé de pré/post-test, des conseils sur la mise en œuvre efficace de la formation, des instructions détaillées sur les activités et des documents à distribuer pour la formation.
2. Des diapositives de formation avec des conseils clairs sur les endroits où les animateurs doivent ajouter ou remplacer du contenu, et des notes détaillées pour les intervenants.

Objectifs de l'atelier

L'équipe centrale de chaque partenaire de mise en œuvre sera formée à :

- Identifier les points forts et les lacunes en matière de sûreté et de sécurité et partager les points forts entre les responsables de la mise en œuvre.
- Classer par ordre de priorité les risques de sûreté et de sécurité auxquels le programme est confronté et déterminer les principales lacunes à combler par l'organisation de la société civile (OSC)
- Rédiger des plans de sécurité spécifiques à l'OSC qui traitent des risques prioritaires et de la manière de développer les compétences pour gérer ces risques.
- Planifier le déploiement du plan de sécurité

Temps et préparation nécessaires

Avant le début de la formation, ou au moins 24 heures avant le début de la deuxième session, tous les partenaires de mise en œuvre participants doivent remplir une liste de contrôle de leurs stratégies de sécurité actuelles. La liste de contrôle se trouve ici en arabe, français,et anglais. Les instructions sur la façon de remplir la liste de vérification se trouvent à l'annexe A.

La formation, lorsqu'elle est dispensée virtuellement, est conçue pour être donnée sur quatre périodes de deux heures, les participants devant faire leurs devoirs après la première et la deuxième session. Pour permettre aux participants de faire leurs devoirs entre les sessions, la formation devrait idéalement être mise en œuvre sur des jours non consécutifs. Elle doit être co-animée par deux personnes, l'une ayant une expertise et une expérience en matière de sécurité des personnes chargées de la mise en œuvre de la lutte contre le VIH, et l'autre connaissant bien les participants et pouvant suivre leurs progrès pour l'obtention d'un certificat.

Un exemple d'ordre du jour pour l'organisation virtuelle de la formation est fourni ci-dessous. La durée nécessaire pour le troisième jour dépendra du nombre d'organisations présentes et pourrait être supérieure ou inférieure à deux heures. La plupart des personnes qui organisent la formation en personne le font sur deux jours. Voir l'annexe B pour un exemple de programme de formation en présentiel. Cela donne plus de temps aux participants pour pratiquer et assimiler les compétences, y compris pour couvrir les devoirs à faire à la maison pendant la formation.

Programme virtuel des participants

Heure	Session	Objectifs
		JOUR 1
8:00	Bienvenue, introductions et contexte	▪ Accueil et présentation des participants. ▪ Parvenir à une compréhension commune du contenu, des objectifs et de la participation à la formation. ▪ Identifiez la sécurité des exécutants comme un domaine important et nouveau de la programmation du VIH.
8:45	Termes clés et recommandations majeures	▪ Définir les notions de sécurité, de risque, de menace, de capacité et de vulnérabilité, et discuter des principales recommandations relatives à la sécurité des exécutants des programmes des PC.
9:15	Identification et évaluation des menaces	▪ Identifier les menaces et déterminer leur gravité
9:55	Clôture de la première journée	▪ Evaluer la journée
		JOUR 2
8:00	Récapitulatif du premier jour et du Devoir #1	▪ Partagez les réponses du Devoir #1. ▪ Rappel des sujets abordés le premier jour.

Heure	Session	Objectifs
8:25	Limiter la capacité de nuire d'un agresseur	▪ Décrire ce qui peut être fait, et par qui, pour limiter la capacité d'un agresseur à causer du tort.
9:00	Sécurité numérique	▪ Décrire les vulnérabilités inhérentes aux plateformes numériques ; identifier les stratégies de réduction des risques au sein de chacune d'elles.
9:40	Revoir nos capacités et plan de partage des compétences	▪ Revoir les réponses collectives aux évaluations de la sécurité. ▪ Affecter chaque partenaire de mise en œuvre à une compétence qui sera présentée lors de la prochaine session.
9:55	Clôture du deuxième jour	▪ Compléter l'évaluation du jour 2
JOUR 3 – Session spéciale, Présentations du groupe		
Durée nécessaire	Présentations du groupe	▪ Partagez une stratégie de sécurité attribuée à votre OSC. ▪ Posez des questions sur toutes les stratégies présentées afin de comprendre la mise en œuvre, ainsi que les avantages et les inconvénients de la stratégie.
JOUR 4		
8:00	Récapitulatif du deuxième jour et réflexions sur la session spéciale	▪ Réfléchir aux stratégies présentées lors de la session spéciale ▪ Rappel des sujets abordés le deuxième jour
8:10	Utiliser ce que vous avez appris : études de cas sur les défis de sécurité	▪ Réfléchir à ce que pourrait faire votre organisation si elle était confrontée à divers problèmes de sécurité. ▪ Discutez si les "solutions possibles" après chaque scénario seraient appropriées dans le contexte local.
8:45	Formule d'évaluation des risques	▪ Se familiariser avec la formule permettant de déterminer la probabilité qu'un danger donné se produise.
9:05	Plan de sécurité	▪ Reconnaitre les éléments d'un plan de sécurité et s'entraîner à utiliser le modèle pour élaborer vos propres plans. ▪ Identifiez vos trois principaux risques et créez un plan de sécurité pour chacun d'eux en tenant compte des vulnérabilités, des capacités existantes et des capacités requises.
9:35	Prochaines étapes	▪ Discuter des possibilités suivantes : action immédiate sans frais ou à faible coût, apprentissage continu entre les OSC, liaison des activités de sécurité avec la prévention et la réponse à la violence en cours, et recherche d'un soutien international. ▪ Identifier les mesures à prendre pour finaliser et faire accepter les plans de sécurité par chaque OSC.
9:50	Réflexions et clôture	▪ Partage de vos réflexions et évaluation de l'atelier; formuler des réflexions de clôture.

Un programme pour les animateurs de la formation virtuelle se trouve à l'Annexe C.

Principe fondamental

Les organisations qui mettent en œuvre des programmes de lutte contre le VIH destinés aux membres des populations clés sont la cible de toute une série d'abus en raison de leurs efforts pour répondre aux besoins de santé des communautés marginalisées et, dans certains cas, criminalisées. Ces attaques - allant de la violence verbale de la part du grand public à l'isolement par leurs familles et leurs communautés, passant par les agressions physiques de la part des forces de l'ordre ou des groupes d'autodéfense, ou encore les atteintes à leur réputation par les médias locaux ou les institutions religieuses - sont souvent encore plus intenses lorsque les travailleurs sont eux-mêmes des membres des populations clés. Ces attaques ont des répercussions négatives et souvent extrêmes sur les individus, les organisations et les programmes de lutte contre le VIH. Il s'agit notamment de traumatismes à court et à long termes chez les travailleurs, d'atteinte à la réputation des individus et des organisations, de restriction des mouvements des travailleurs dans leur vie personnelle et professionnelle, de perte de biens (y compris de données), de désengagement des organisations, d'incapacité à fournir des services VIH efficaces et, dans certains cas, de perte de vie.

Le renforcement de la sécurité des exécutants est une exigence éthique et pratique pour un programme VIH efficace. Ceci est reflété dans le PEPFAR 2021 Country/Regional Operating Plan Guidance où une section spécifique sur la sûreté et la sécurité reconnaît la nécessité de "surveiller et suivre les progrès sur les questions relatives à la sûreté et à la sécurité..." et de "...déterminer les meilleures stratégies pour fournir un soutien dans la prévention et le traitement des cas de violence et de harcèlement contre les individus et les organisations communautaires"[1] dans le cadre de la programmation pour les populations clés

À la lumière du COVID-19, les formations à la sécurité pour les responsables de la mise en œuvre sont plus importantes que jamais - en particulier dans les cas où les mêmes organisations qui mettent en œuvre des programmes VIH mettent également en œuvre des efforts de prévention ou d'atténuation du COVID-19, les exposant ainsi à de nouvelles menaces - et doivent être disponibles virtuellement pour atténuer les risques liés au COVID-19.

Utilisation de ce manuel de l'animateur

Ce manuel de l'animateur offre des conseils pour vous aider à mener la formation de manière à susciter l'intérêt des participants, en particulier ceux qui se joignent virtuellement. Il fournit également des informations supplémentaires sur les sujets abordés dans la formation. Veuillez lire l'intégralité du manuel avant d'organiser et de mettre en œuvre une formation. Les instructions détaillées de la session, combinées aux notes de l'intervenant dans la présentation PowerPoint, fournissent des conseils pour la mise en œuvre.

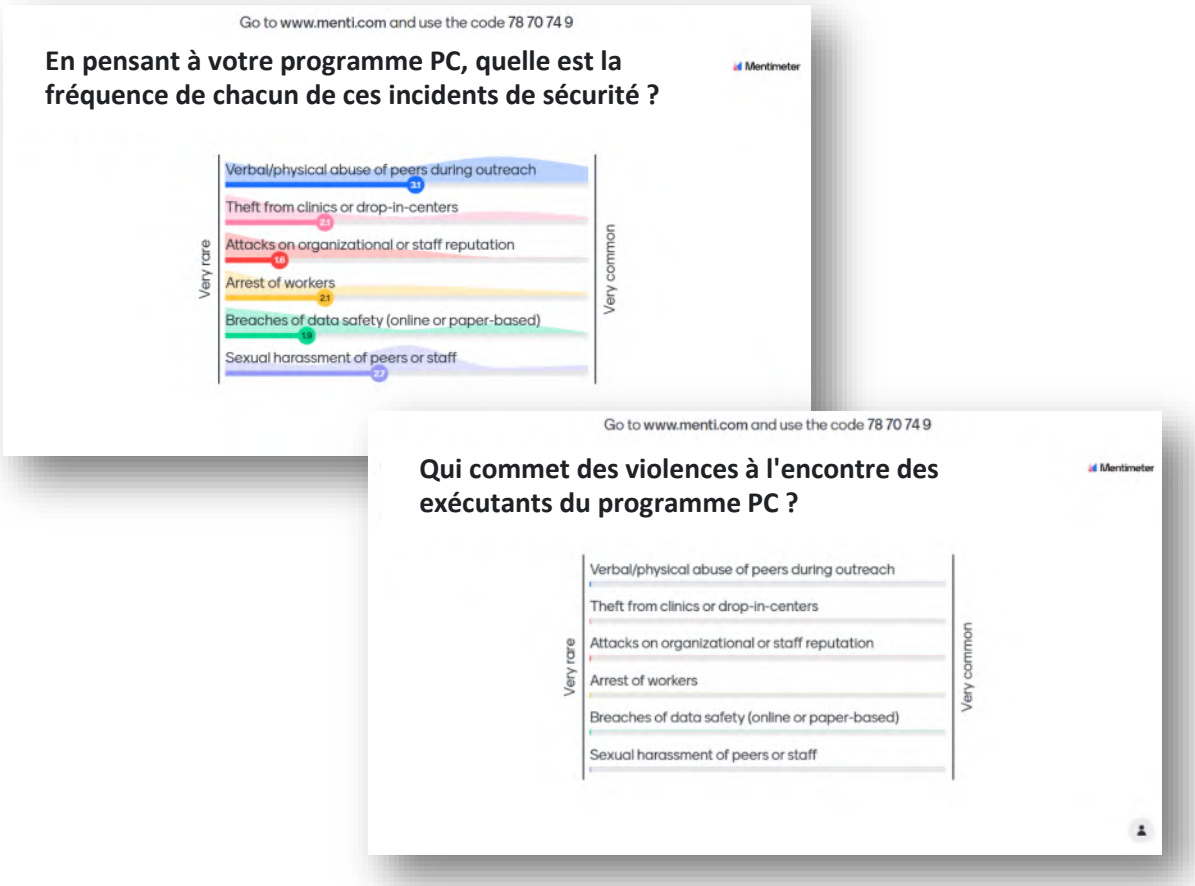
[1] PEPFAR. PEPFAR 2021 Country and Regional Operational Plan (COP/ROP) Guidance for all PEPFAR Countries. Washington (DC): PEPFAR; 2021. p. 419.

Connectivité

Si vous organisez cette formation virtuellement, veuillez-vous assurer que vous avez un plan en place pour les points suivants :

- **Quelle(s) plateforme(s) utiliserez-vous pour mener cette formation** ? Nous avons utilisé Microsoft Teams et Mentimeter pour la présentation et les enquêtes/quiz en temps réel. Mentimeter est une plateforme d'enquête/de questionnaire en ligne qui vous permet de poser des questions aux participants qui saisissent leurs réponses sur un ordinateur ou un téléphone intelligent. Leurs réponses sont ensuite visibles au fur et à mesure pour l'animateur - et pour les participants si l'animateur partage son écran. L'animateur a ainsi l'occasion de recueillir des informations auprès des participants, de vérifier leur compréhension et de clarifier tout ce qui n'est pas bien compris (voir la figure 1 pour les images de Mentimeter). Nous avons utilisé Google Forms pour le post-test et les évaluations quotidiennes. Quelle que soit la ou les plateformes que vous choisissez d'utiliser, assurez-vous que tous les participants peuvent y accéder et utiliser leurs fonctionnalités, telles que le chat et la possibilité de parler en "sourdine". Si nécessaire, prévoyez du temps supplémentaire avant la première session pour tester la capacité de chaque participant à utiliser les plateformes correctement, afin d'éviter toute frustration et une faible participation par la suite.

Figure 1 : Les images de Mentimeter



- **Comment allez-vous résoudre les inévitables problèmes de déconnexion dans les formations virtuelles ?** Lorsque l'on dispense des formations virtuelles, il y a presque toujours quelqu'un qui ne pourra pas assister à une partie en raison de problèmes de connectivité. Prévoyez une solution de rechange, comme enregistrer les formations pour les mettre à disposition des participants par la suite. Assurez-vous d'obtenir la permission avant d'enregistrer. Si vous souhaitez enregistrer, demandez aux participants s'ils ont des inquiétudes avant de commencer l'enregistrement. Si tel est le cas, vous pouvez soit éviter l'enregistrement, soit conseiller à ceux qui ne souhaitent pas être enregistrés lorsqu'ils prennent la parole de contribuer d'une autre manière. Par exemple, ils peuvent souhaiter envoyer leurs réflexions par e-mail après la formation.

  Réfléchissez également à adapter les exigences des participants pour ceux qui essaient de participer mais rencontrent des problèmes de connectivité. Par exemple, ceux qui manquent une session en direct peuvent envoyer leurs questions et observations par e-mail à l'animateur après avoir visionné l'enregistrement.

Si vous avez besoin de plus de ressources pour dispenser la formation dans un environnement à faible connectivité, veuillez voir ci-dessous.

- Le **Cluster CCCM** a organisé un webinaire sur les adaptations des approches de renforcement des capacités, de mentorat et de coaching pour les travailleurs humanitaires pendant la période du COVID-19. Bien qu'il soit destiné aux professionnels de la coordination et de la gestion des camps, les orateurs invités et les participants ont donné des indications utiles sur le renforcement des capacités opérationnelles lorsque la connectivité et l'accès sont limités. Un YouTube est disponible ici.
- **L'UNESCO** a compilé une liste de solutions d'apprentissage à distance par catégorie, y compris des systèmes dotés d'une forte fonctionnalité hors ligne.
- En dehors des secteurs du développement et de la santé, **TalentLMS** a élaboré un guide pour les modérateurs sur la façon d'adapter les possibilités d'apprentissage en ligne aux utilisateurs disposant d'une faible connectivité. **EdTech** fournit également des conseils sur l'accès hors ligne dans l'apprentissage à distance.

Langue et noms

Ce matériel de formation est actuellement disponible en anglais. Cependant, toutes les diapositives peuvent être éditées et traduites dans d'autres langues si nécessaire. Lors de la traduction ou de l'adaptation à un contexte local, veuillez également modifier les noms utilisés dans les scénarios afin qu'ils soient plus pertinents au niveau local. Cela peut éviter la confusion des participants qui ne sont pas familiers avec les noms actuellement utilisés dans les diapositives. Essayez d'éviter d'utiliser les noms des participants à la formation dans les scénarios.

En outre, en tant qu'animateur(s), vous pouvez ajouter des informations vous concernant pour rendre la formation plus intéressante. Par exemple, les diapositives 61, "Recherchez-vous", et 66, "Activité Q", contiennent des informations sur l'auteur de la formation. Envisagez de les remplacer par les mêmes informations sur vous-même.

Nombre de participants

Assurez-vous que les participants comprennent ce que l'on attend d'eux dès le début, y compris participation continue de leur part. N'invitez pas plus de 25 participants à chaque formation, même si elle est dispensée virtuellement ; cela permet à l'animateur d'impliquer chaque participant à tout moment de la formation. Comme nous l'avons mentionné, cette formation est conçue pour être donnée à des groupes de différents partenaires de mise en œuvre. Nous avons constaté que trois personnes de chaque partenaire de mise en œuvre et pas plus de huit partenaires de mise en œuvre sont présents lors d'une formation

Responsabilisation des participants et maîtrise des compétences

Partagez les attentes avec tous les participants avant la formation. Les attentes recommandées sont indiquées ci-dessous. Si un participant ne peut s'engager à respecter ces exigences, il ne recevra pas de certificat.

Nous recommandons à tous les participants de répondre à chacune des attentes ci-dessous.

- En groupe, remplissez à l'avance la liste de vérification de sécurité. Elle est disponible ici en arabe, français, et anglais. La liste de vérification doit être complétée et envoyée aux animateurs au moins 24 heures avant la deuxième session de la formation.
- Participer à toutes les sessions pendant toute la durée de celles-ci.
- Contribuez oralement (sur le fond) au moins deux fois par session.
- Contribuer à travers le chat au moins cinq fois par session.
- Effectuer les devoirs après les sessions 1 et 2.
    - Réfléchir aux recommandations de sécurité pour les EP
    - En groupe, préparez une présentation avec d'autres membres de votre OSC sur la stratégie de sécurité qui vous a été assignée.
- Obtenir un score de 85 % au post-test

Accéder à des ressources supplémentaires

Le contenu présenté ici s'appuie sur la ressource de sécurité 2020, AMAN MENA Protections sécuritaires des organisations travaillant avec les populations clés pour renforcer la programmation du VIH au Moyen Orient et en Afrique du Nord. La lecture de cette ressource aidera les animateurs et les participants à approfondir leur compréhension du sujet et permettra aux animateurs de se sentir plus à l'aise pour présenter ce sujet s'il est nouveau pour eux. La boîte à outils AMAN MENA est une adaptation et une mise à jour régionale de la ressource LINKAGES et Frontline AIDS de 2018 : la boîte à outils sur la sûreté et la sécurité : Renforcer la mise en œuvre des programmes VIH pour et avec les populations clés Safety and Security Toolkit: Strengthening the Implementation of HIV Programs for and with Key Populations.

Le renforcement de la sécurité des exécutants fait partie de tout programme efficace en faveur des populations clés, mais peut jouer un rôle particulièrement important dans les efforts, tels que le suivi communautaire, qui visent à améliorer la capacité du programme global à répondre aux

besoins holistiques des clients. L'intégration d'activités visant à renforcer la sécurité des exécutants dans le suivi communautaire permet de s'assurer que les voix et les préoccupations des exécutants des programmes sont prises en compte au même titre que celles des clients. Le fait d'aborder les deux à la fois permet de s'assurer que les changements adoptés pour améliorer l'accessibilité des services, par exemple des heures d'ouverture plus tardives, s'accompagnent de mesures, telles qu'une allocation de transport pour les prestataires, qui empêchent les adaptations des programmes de mettre en danger les exécutants par inadvertance. Pour en savoir plus sur l'ensemble du dispositif de suivi communautaire d'EpiC, veuillez consulter le site : https://www.fhi360.org/resource/community-led-monitoring-resources.

Rendre le contenu attrayant

Lors des formations virtuelles, il peut être particulièrement difficile de maintenir l'engagement des participants. Cette formation est conçue pour favoriser la participation dans les espaces virtuels. Toutefois, le maintien de l'intérêt des participants incombe également aux animateurs, dont le rôle consiste à appeler les participants en permanence et à les faire participer à travers le chat pour s'assurer que chacun acquiert les compétences présentées.

Si vous dispensez une présentation virtuelle, en raison des restrictions COVID-19, envisagez de réunir quelques petits groupes (par exemple, dans une formation de 15 personnes, elles pourraient se trouver à cinq endroits différents par groupes de trois). Vous trouverez ci-dessous un tableau contenant d'autres idées sur la manière de rendre différents types d'activités plus engageantes dans le cadre d'une formation en présentiel ou en virtuel.

Activité	Présentiel	Virtuel
Nécessite la réponse de tout le groupe	Cartes de note; vote par points	Mentimeter ; tapez dans le chat (réponse courte uniquement)
Pré-test/post-test	Sur papier ou en ligne	En ligne à l'aide des formulaires Google forms
Evaluation quotidienne	Vote par points pour indiquer l'activité favorite ; brainstorming ouvert sur ce qui s'est bien passé et ce qui peut être amélioré ; post-it pour une réponse anonyme sur ce qui s'est bien passé et ce qui peut être amélioré.	Formulaires Google ou Mentimeter
Activités en petits groupes	Répartir en groupes et donner à chaque groupe l'espace et le temps nécessaires pour formuler une réponse.	Assigner des travaux en petits groupes en dehors des sessions et désignez une personne dans chaque groupe pour veiller à ce que le groupe se réunisse ; demander aux participants de s'appeler sur leur téléphone portable pour de courtes conversations pendant

		la formation ; utilisez les fonctions de salle de réunion dans Zoom ou Teams.
Rendre la présentation plus attrayante	Si vous pouvez prolonger le temps nécessaire à la présentation, envisager de transformer les diapositives contenant beaucoup de texte en activités de petits groupes destinées à s'enseigner mutuellement le contenu. Par exemple, la diapositive 15, intitulée " Comment les défis de la sécurité affectent-ils les programmes des PC ? ", pourrait être transformée en une activité où les participants réfléchissent à l'impact potentiel dans chacun des sept domaines présentés.	Demander aux participants d'utiliser le chat pour discuter entre eux de ce qui est présenté et pour poser des questions au présentateur. Le présentateur doit résumer le chat et répondre aux questions qui y sont posées.

Préparation de la formation

Les étapes ci-dessous sont utiles pour préparer une formation virtuelle ou en présentiel, sauf indication contraire.

Étape 1. Examinez les diapositives et lisez intégralement ce manuel. Vous remarquerez que de nombreuses diapositives contiennent du texte en vert. Le texte en vert dans les diapositives doit être supprimé ou remplacé avant de dispenser la formation.

Si vous prévoyez de réviser les activités pour augmenter l'interaction entre les participants ou pour dispenser la formation en présentiel, apportez ces changements après examen du manuel et des diapositives.

Étape 2 (obligatoire si virtuelle, facultative si en présentiel). Préparez des sondages interactifs à l'aide de Mentimeter.com (ou une autre plateforme de votre choix) ainsi qu'un pré/post-test et une évaluation à l'aide de Google Forms (ou une autre plateforme de votre choix). Les sessions qui nécessitent l'utilisation de ces plateformes sont indiquées ci-dessous. Elles sont également indiquées dans le diaporama par du texte surligné qui doit être remplacé avant de mener la formation.

Étape 3. Passez en revue toutes les instructions relatives aux composantes participatives de la formation. Alors que la plupart des diapositives comprennent un script pour guider les propos de l'animateur, les activités marquées d'une étoile sont interactives et nécessitent une compréhension et/ou une planification préalable de la part des animateurs.

Étape 4 (si la formation est virtuelle). Créez un suivi de la participation virtuelle. Il doit comprendre les éléments suivants :

Organisation du participant	Nom du participant	Contributions Session 1		Contributions Session 2		Contributions Session 3		Contributions Session 4		Devoir #1 complété	Score au post-test
		# Chat	# Verbal	# Chat	# Verbal	Présentation donnée	Autres questions posées	# Chat	# Verbal		

Cela vous permettra de documenter la participation de chaque personne et de déterminer qui répond aux exigences minimales pour continuer et former d'autres personnes. Voir Responsabilité des participants et maîtrise des compétences pour en savoir plus.

Étape 5. Envoyez des invitations indiquant les dates de la formation, les attentes de tous les participants, les objectifs d'apprentissage, l'ordre du jour et des informations sur la manière dont la formation sera menée (par exemple, elle peut inclure un lien vers Zoom si elle sera menée de cette manière). Si les participants n'ont jamais utilisé ces plateformes auparavant, prévoyez du temps à l'avance pour s'entraîner à les utiliser. N'utilisez pas le temps prévu pour la formation pour résoudre des problèmes technologiques. Vous pouvez également rechercher des vidéos d'instruction sur la manière d'utiliser les technologies dont vous vous servirez. Par exemple, en recherchant sur YouTube une vidéo "comment faire" dans la langue de vos participants. Ces liens peuvent ensuite être partagés à l'avance afin de soutenir l'utilisation des technologies par les participants.

Étape 6. À la fin de chaque journée de formation, vous pourrez partager les diapositives étudiées et un enregistrement de ces diapositives (le cas échéant). Tous les participants doivent accepter l'enregistrement avant que cette option ne soit utilisée.

Instructions détaillées pour la session

Jour 1

Time	Session	Objectifs
8:00	Bienvenue, introductions et contexte	▪ Accueil et présentation des participants. ▪ Parvenir à une compréhension commune du contenu, objectifs de la formation et de la participation à la formation. ▪ Identifiez la sécurité des exécutants comme un domaine important et nouveau de la programmation du VIH.
8:45	Termes clés et recommandations majeures	▪ Définir les notions de sécurité, de risque, de menace, de capacité et de vulnérabilité, et discuter des principales recommandations relatives à la sécurité des exécutants des programmes des PC.
9:15	Identification et évaluation des menaces	▪ Identifier les menaces et déterminer leur gravité
9:55	Clôture de la première journée	▪ Evaluer la journée

Préparation en ligne pour le premier jour

- Utilisez Mentimeter.com pour créer deux questions d'enquête. Vous les montrerez quand vous arriverez à la diapositive de l'activité C.

  Question 1. En pensant à votre programme PC, quelle est la fréquence de chacun de ces incidents de sécurité ?

  - Violence verbale/physique à l'égard des pairs pendant les activités de sensibilisation
  - Vols dans les cliniques ou les centres d'accueil
  - Atteintes à la réputation de l'organisation et/ou du personnel
  - Arrestation de travailleurs
  - Violation de la sécurité des données (en ligne ou sur papier)
  - Harcèlement sexuel des pairs ou du personnel

  Question 2. Qui commet des violences à l'encontre des exécutants du programme PC ?

  - La police
  - Les chefs religieux
  - Les médias
  - Le grand public
  - Bénéficiaires des PC
  - Autres

- Utilisez Mentimeter ou Google Forms pour recueillir des informations sur le déroulement de la première journée. Ceci est pertinent pour l'activité I. Les questions doivent vous fournir, à vous les animateurs, des informations sur la façon de procéder. Voici quelques exemples de questions :
    - Cette session était intéressante pour moi. (de pas du tout d'accord à tout à fait d'accord, échelle)
    - Cette session m'aidera à faire mon travail. (de pas du tout d'accord à tout à fait d'accord, échelle)
    - L'animateur était bien informé. (de pas du tout d'accord à tout à fait d'accord, échelle)
    - J'ai eu l'occasion de partager mes opinions. (de pas du tout d'accord à tout à fait d'accord, échelle)
    - Je recommanderais cette session à d'autres personnes. (de pas du tout d'accord à tout à fait d'accord, échelle)
    - Quels changements souhaiteriez-vous voir lors de la prochaine session (question ouverte) ?

Instructions pour les activités du Jour 1

Utilisez les diapositives pour encadrer la formation ; les diapositives et les notes de l'intervenant résument les messages clés ou fournissent des instructions pour les activités. Toutes les diapositives basées sur des activités sont marquées d'une étoile. Cette notation signifie que l'animateur ne doit pas se contenter de présenter les informations figurant sur la diapositive, mais qu'il doit inciter les participants à générer des réponses. Chaque diapositive d'activité est décrite plus en détail ci-dessous.

- **Activité A. Introductions.** Il est essentiel de donner aux gens la possibilité de s'exprimer au début de toute formation. Cela les encourage à participer tout au long de l'activité. Prenez le temps nécessaire pour que chaque personne se présente, même si l'activité se prolonge légèrement. Dans une formation en ligne, il peut être difficile pour les personnes de savoir quand se présenter. Personne n'aime interrompre ou être interrompu. Vous pouvez faciliter ce processus en ayant le tableau de l'activité A déjà rempli. Il suffit ensuite de demander à chaque personne de se présenter afin de partager les informations demandées. Si vous n'avez pas ces informations à l'avance, demandez à ceux d'une organisation spécifique de commencer, puis passez à l'organisation suivante jusqu'à ce que tout le monde ait la possibilité de se présenter.
- **Activité B. Normes du groupe.** Nous voulons nous assurer que les participants comprennent ce que l'on attend d'eux au cours de la formation. Ils doivent également savoir ce qu'ils attendent les uns des autres, notamment en ce qui concerne la confidentialité des informations ; après tout, nous discutons de questions de sécurité. Vous pouvez modifier les normes suggérées à l'avance. Assurez-vous simplement que tout ce qui est listé concerne l'enregistrement (si un enregistrement est prévu). Les normes

doivent également préciser si les expériences personnelles relatées pendant la formation peuvent être partagées avec d'autres personnes en dehors de l'espace de formation.

- **Activité C. Quoi, qui, pourquoi ?** Utilisez Mentimeter pour créer à l'avance des questions qui vous permettront de comprendre les types d'incidents les plus courants et de savoir qui en sont les auteurs. Si vous avez connaissance d'autres défis de sécurité non décrits dans les diapositives, n'hésitez pas à les ajouter. Les questions nécessaires sont décrites dans la section "Préparation en ligne obligatoire pour le jour 1".

  Après avoir obtenu des réponses à ces questions, demandez aux personnes de se "débloquer" et de réfléchir aux réponses sur l'écran. Des exemples précis sont utiles. Pendant les réflexions, demandez à ceux qui partagent leurs idées de réfléchir non seulement ce qui se passe, mais aussi pourquoi ils pensent que cela se passe.

- **Activité D. Définitions** Cette activité couvre les cinq définitions. Lisez la question et les réponses possibles à voix haute (ou demandez à un participant de les lire). Ensuite, demandez aux participants d'inscrire leur choix de réponses dans le chat. Laissez plusieurs secondes pour leur donner le temps de répondre. Demandez ensuite à une personne qui a répondu correctement dans le chat d'activer le microphone pour expliquer sa réponse. Après sa réponse, avancez la diapositive pour montrer la bonne réponse. Puis, avancez à nouveau la diapositive pour montrer un texte d'explication supplémentaire. Lisez ce texte à voix haute.

- **Activité E. Travail à domicile** : Recommandations majeures - Cette activité sera réalisée en tant que devoir à la maison, mais il est important de l'expliquer clairement pendant la session. Elle demande aux groupes (décrits pendant l'activité A) d'examiner chacun une recommandation de la liste. La lettre de leur groupe figure à côté du numéro de la recommandation concernée. Chaque groupe doit faire ce qui suit avant la prochaine session :

  - Passer en revue leur recommandation, y compris les informations supplémentaires figurant sur l'aide-mémoire.
  - Discuter la manière dont leur organisation utilise déjà cette recommandation et pourrait l'utiliser.
  - Etre prêt à partager la recommandation et son utilisation actuelle et potentielle avec tous les participants lors de la prochaine session. Vous devrez notamment choisir une personne pour parler au nom de son groupe.
  - Les groupes auront besoin de l'aide-mémoire de la formation à la sécurité", disponible à l'annexe D, pour réaliser ce travail. On l'appelle "aide-mémoire" car elle résume toutes les informations qu'ils devront retenir de la formation pour passer le post-test. La leur envoyer par courriel immédiatement après la session.

- **Activité F. Étiquetez chaque menace.** Les participants s'exercent à utiliser les classifications qu'ils viennent d'apprendre. Lisez chacune d'entre elles, puis demandez aux participants d'écrire "menace indirecte, menace directe ou incident de sécurité" dans le

chat. Lorsque de nombreux participants ont répondu, demandez à l'un d'entre eux qui a répondu correctement d'activer le son et d'expliquer sa réponse. Ensuite, avancez la diapositive et montrez la bonne réponse.

Après avoir fait cela pour tous les incidents, demander s'il y a des questions.

Notez que si de nombreuses réponses incorrectes sont saisies dans le chat, il est important de prendre plus de temps pour les clarifier.

- **Activité G. Évaluer les menaces en fonction de leur impact.** Dans cette activité, vous demandez aux participants d'évaluer le degré de dangerosité de l'exemple de menace. Ils doivent indiquer un chiffre dans le chat. Demandez à quelques personnes d'expliquer leur choix. Si plusieurs personnes ont choisi des réponses différentes, demandez à ceux qui ont des réponses différentes d'expliquer leur raisonnement.

  Il n'y a pas une seule bonne réponse. Tant que les participants peuvent justifier leur réponse, tout va bien. Si des opinions différentes sont exprimées, c'est l'occasion de souligner que l'appétit du risque est différent selon les personnes et que les mesures de sécurité sont déterminées en fonction du contexte. Dans certains endroits, cette menace peut causer beaucoup de dommages. Dans d'autres, elle peut être facilement neutralisée.

- **Activité H. Considérer nos propres menaces.** Cette activité est l'occasion pour le groupe de faire sa propre analyse des menaces. Demander à l'un des participants de se lever et de répondre à chacune des questions. Si personne ne se porte volontaire, repensez aux menaces décrites dans Menti, et demandez à quelqu'un qui s'est déjà exprimé de décrire plus précisément ce qu'il a vécu.

  Passez de l'affichage présentation à l'affichage édition, puis tapez sur la diapositive au fur et à mesure que le participant contribue, en capturant les parties importantes de ce qu'il dit. Posez des questions de clarification si nécessaire afin de comprendre ce qui est dit. Une fois qu'ils ont répondu aux cinq questions, demandez-leur dans quelle mesure la menace est dangereuse sur une échelle de 1 à 5. Demander si d'autres participants ont des commentaires sur le chiffre attribué. Encore une fois, il n'y a pas une seule bonne réponse. Il s'agit d'utiliser ce que vous savez pour donner un sens à l'importance du danger de manière systématique.

- **Activité I. Menti, clôture du jour 1.** L'évaluation quotidienne peut être faite publiquement à l'aide de Menti en montrant votre écran au fur et à mesure que les résultats de l'enquête arrivent. Vous pouvez également laisser l'enquête ouverte à la fin de la session, puis vérifier les réponses par vous-même sans partager l'écran. Des exemples de questions sont inclus dans la section "Préparation en ligne pour le Jour 1".

- **Activités de récapitulatif.** A la fin de la première session, l'animateur doit envoyer les diapositives par e-mail à tous les participants, un lien vers l'enregistrement (si disponible), ainsi que les documents relatifs à l'aide-mémoire (Annexe D) et au journal des incidents de sécurité (Annexe E). L'e-mail doit également rappeler le devoir à domicile. Voir l'annexe F pour un exemple d'e-mail à envoyer à la fin du premier jour.

Jour 2

Heure	Session	Objectifs
8:00	Récapitulatif du premier jour et du Devoir #1	▪ Partagez les réponses du Devoir #1. ▪ Rappel des sujets abordés le premier jour.
8:25	Limiter la capacité de nuire d'un agresseur	▪ Décrire ce qui peut être fait, et par qui, pour limiter la capacité d'un agresseur à causer du tort.
9:00	Sécurité numérique	▪ Décrire les vulnérabilités inhérentes aux plateformes numériques ; identifier les stratégies de réduction des risques au sein de chacune d'elles.
9:40	Revoir de nos capacités et plan de partage des compétences	▪ Revoir les réponses collectives aux évaluations de la sécurité. ▪ Affecter chaque partenaire de mise en œuvre à une compétence qui sera présentée lors de la prochaine session.
9:55	Clôture du deuxième jour	▪ Compléter l'évaluation du jour 2

Préparation en ligne du 2e jour

- Pour l'activité K, utilisez Menti.com pour poser la question suivante. Notez que "***" indique la bonne réponse et ne doit pas être inclus dans la question d'enquête elle-même.

  Question 1. "Vous êtes un pair éducateur. Vous apprenez que deux autres pairs éducateurs de votre province ont été arrêtés lors d'une action de sensibilisation. Quel type de menace cela représente-t-il pour vous ?"

  - Menace directe
  - Menace indirecte***
  - Incident de sécurité

- Pour l'activité O, utilisez Menti.com pour poser les questions suivantes. Il n'y a pas de réponses correctes.

  Question 1. "Lequel de ces appareils utilisez-vous ?"

  - Non-smartphone
  - Smartphone
  - Ordinateur portable
  - Ordinateur de bureau
  - Tablette
  - USB/Charge USB

Question 2. "Que pourrait apprendre quelqu'un sur vous s'il accédait à votre appareil ?"

- Où je travaille
- Les noms des membres de ma famille
- Mes informations financières (telles que mes informations bancaires et mes numéros de carte de crédit)
- Les sites web que je visite
- Les noms et coordonnées de mes amis

Instructions pour les activités du 2 jour

Toutes les diapositives basées sur des activités comportent une étoile. Cela signifie que l'animateur ne doit pas se contenter de présenter les informations, mais qu'il doit inciter les participants à trouver les réponses. Chaque diapositive d'activité est décrite plus en détail ci-dessous.

- **Activité J. Réflexions sur les recommandations**. Cette activité est l'occasion pour les petits groupes ou les individus de partager leurs réponses au premier devoir à domicile (décrit à l'activité E). L'un des animateurs doit appeler chaque groupe par son nom (par exemple, "Marie et Jean, vous avez fait la recommandation n° 1, l'un d'entre vous pourrait-il partager ses réflexions ?") et leur accorder un maximum de deux minutes pour partager leurs réponses. Pour rappel, le devoir demandait à chaque groupe de : (1) de décrire cette recommandation, (2) de partager comment votre programme utilise déjà cette recommandation, et (3) comment le programme pourrait utiliser cette recommandation.
- **Activité K. Menti Récapitulatif du premier jour**. Utilisez Menti pour élaborer une question d'enquête à l'avance. Cette procédure est décrite dans la section "Préparation en ligne pour le Jour 2". Lorsque vous affichez la question, fournissez le lien vers Menti et le code dans le chat.

  Pendant que le groupe répond, demandez à quelqu'un d'activer le son et d'expliquer sa réponse. Soulignez que cette menace est indirecte parce qu'elle ne vous vise pas, mais qu'elle vise directement une personne de la même profession ou organisation que vous, de sorte que vous êtes également susceptible de vous sentir menacé. Si de nombreux participants donnent une mauvaise réponse, revenez à la diapositive 27, "Types de menaces", pour rappeler au groupe les définitions de chaque type de menace.
- **Activité L. De quoi un attaquant potentiel a-t-il besoin** ? Cette activité demande aux participants de réfléchir à ce dont un attaquant pourrait avoir besoin pour nuire à une cible. Cela peut être dans un espace virtuel ou physique. Demandez aux participants de taper leurs réponses dans le chat. Ensuite, demandez aux participants de clarifier ou de développer leurs réponses. Par exemple, si quelqu'un écrit que l'attaquant a besoin d'une "cause", vous pouvez préciser qu'il s'agit d'un motif.

- **Activité M. Scénarios.** Cette activité permet aux participants de réfléchir à la manière dont ils pourraient utiliser leur connaissance de ce qu'il faut pour empêcher les attaques de se produire. Pour chaque scénario, vous lirez (ou demanderez à un participant de lire) le scénario. Ensuite, demandez à trois ou quatre volontaires d'expliquer ce qui pourrait être fait. Les personnes qui ne sont pas appelées sont invitées à taper dans le chat. Après avoir obtenu leurs réponses, passez à la diapositive suivante et examinez certaines des options.
- **Activité N. Qu'est-ce que ces solutions ont en commun ?** Cette activité est l'occasion pour les participants de constater l'importance pour l'organisation de prendre l'initiative en matière de sécurité des travailleurs. Montrez la diapositive avec les quatre images et demandez à un volontaire d'expliquer ce que ces quatre solutions au scénario ont en commun. Si un indice est nécessaire, dites que vous recherchez des points communs en termes de qui a le plus grand rôle à jouer dans la limitation de l'accès, de l'information, du mobile et de l'impunité.

  Lorsqu'un volontaire répond, avancez la diapositive pour montrer les cercles rouges. Expliquez que le point commun de chaque cas est que c'est l'organisation qui a le plus grand rôle à jouer.

  Présenter à nouveau et revoir le texte de la diapositive
- **Activité O. Quels appareils utilisez-vous et que disent-ils de vous ?** Cette occasion de réflexion donne aux participants l'opportunité de penser aux appareils qu'ils utilisent et à ce que les autres pourraient apprendre sur eux à partir de cette utilisation. Demandez aux participants d'utiliser l'enquête Menti.com pour répondre aux questions de la rubrique "Préparation en ligne pour le 2e jour". Une fois qu'ils ont répondu aux deux questions, notez que nous utilisons tous une série d'appareils chaque jour et que de plus en plus de nos informations les plus privées sont disponibles en ligne si d'autres personnes savent comment y accéder. Il nous appartient donc d'utiliser ces appareils de la manière la plus sûre possible, et c'est ce dont nous allons parler maintenant.
- **Activité P. Que partageons-nous sur les médias sociaux ?** Ce bref brainstorming se fait par chat. Demandez aux participants de réfléchir aux plateformes de médias sociaux qu'ils utilisent et à ce qu'ils partagent. Demander à quelques personnes qui écrivent dans le chat d'activer le son et de développer leurs réponses. Terminer la conversation en notant à quel point nous partageons en ligne.
- **Activité Q. Que pourrait-on apprendre sur moi à partir de ces publications sur les médias sociaux ?** Cette activité demande aux participants d'analyser les publications Facebook pour déterminer quels types d'informations pourraient être obtenus sur la personne qui les publie. Les diapositives du jeu de diapositives génériques comprennent des publications de la page Facebook de l'auteur de la formation. Les animateurs doivent les remplacer par leurs propres publications sur les médias sociaux (en veillant à ne pas partager des informations qu'ils ne souhaitent pas connaître). L'animateur doit demander à quelques volontaires de noter ce que l'on peut apprendre sur la personne à partir de ses messages. Ceux qui se trouvent dans le paquet générique pourraient indiquer :

- que la personne qui poste a voté en 2020 et où le vote a lieu (ce qui pourrait donner des informations sur son lieu de résidence) ;
- que la personne a des enfants et à quoi ressemblent ces enfants ;
- que la personne qui poste soutient les droits des LGBT.
- Si vous cliquez sur le lien GoFundMe, vous pouvez savoir combien la personne a fait de dons, à moins qu'elle ne l'ait fait anonymement.

Terminer en soulignant qu'il est important de réfléchir de manière critique à ce que vous partagez, en particulier parce que cela pourrait être partagé beaucoup plus qu'avec ceux que vous vouliez initialement.

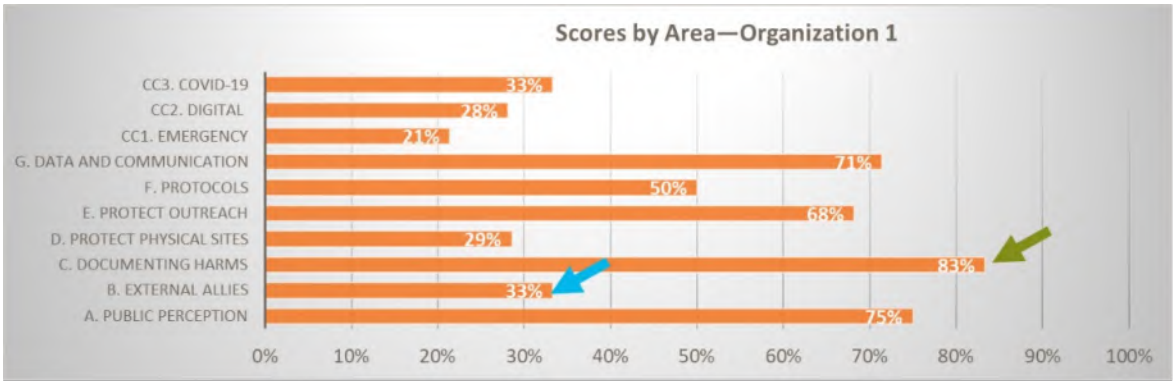
- **Activité R. Avez-vous utilisé l'une de ces méthodes ?** S'il y a du temps pour la réflexion, une activité importante consiste à écouter les expériences des personnes qui utilisent ces différentes options pour faire face au harcèlement en ligne. Demander si quelqu'un souhaite partager ces informations, sans les obliger. Si quelqu'un prend la parole, remerciez-le de sa volonté de partager cette expérience avec le groupe. Insister sur le fait qu'il ne méritait pas d'être traité de la sorte et que des expériences comme la sienne peuvent être très difficiles.
- **Activité S. Relier les problèmes aux solutions**. Cette activité permet aux participants de réfléchir à des options de haute et de basse technologie pour résoudre leurs problèmes de sécurité numérique. Lisez le problème n° 1 et demandez aux participants d'utiliser le chat pour suggérer laquelle des "options de solution" serait la plus appropriée. Choisissez quelques participants pour expliquer leur choix. Ensuite, avancez la diapositive pour montrer les solutions. Faites de même pour le problème n°2 et le problème n°3.

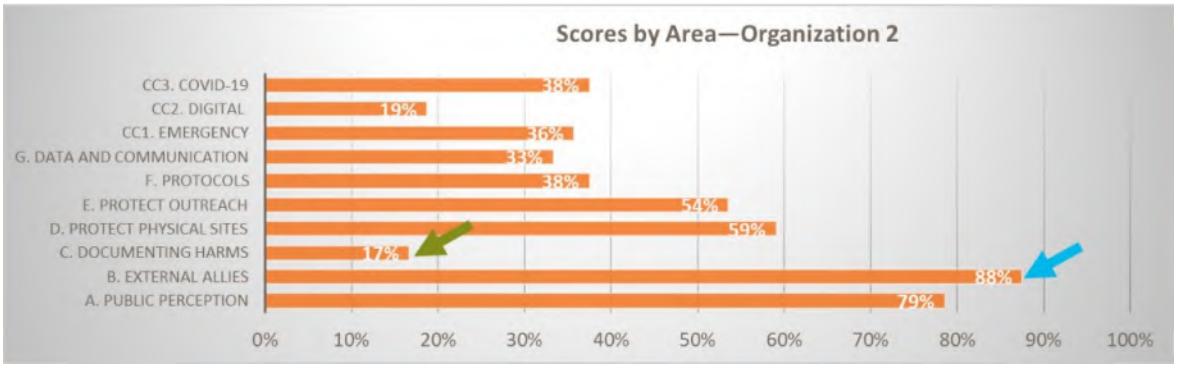
  Après avoir terminé, notez que de nombreuses solutions peuvent contribuer à atténuer ou à résoudre plusieurs problèmes. Par exemple, pour le problème n°3 :

  - Si les pairs ne partagent pas leur photo, leur nom ou leur lieu de résidence, ils sont difficiles à identifier (ce qui rend le chantage plus difficile).
  - Si les pairs ont des scripts qui les aident à répondre aux avances sexuelles, ils ne risquent pas de mettre les clients en colère, ce qui pourrait supprimer une motivation pour le chantage.
  - Si vous utilisez un groupe Facebook fermé, l'impunité est moindre car tout le monde est connu d'au moins un autre membre du groupe. Vous pouvez également faire plus attention à qui est invité au départ.
  - Le partage des photos et l'identification des harceleurs habituels signifient que moins de pairs s'occuperont de ces personnes, ce qui limite les risques.
  - Le fait d'avoir une politique claire sur ce sujet peut empêcher le début de relations amoureuses, limitant ainsi la motivation pour le chantage si la relation ne fonctionne pas.

- **Activité T. Missions d'enseignement de l'EP**. Ceci est un autre devoir pour le groupe. Veuillez copier le graphique récapitulatif des scores de chaque organisation dans la présentation. "Activité T (partie 1)" est la diapositive d'exemple. Si vous devez utiliser plusieurs diapositives pour intégrer tous les graphiques, veuillez le faire. En fonction des sensibilités du groupe, vous pouvez décider d'afficher ces graphiques sans les noms des organisations.

  Vous auriez dû sélectionner, à l'avance, les EP qui enseigneraient chaque compétence en examinant leurs points forts comparés sur les listes de vérification. Par exemple, si vous effectuez cette formation pour les organisations 1 et 2 ci-dessous, vous confierez à l'organisation 1 l'enseignement du domaine C en raison de son score relativement élevé (à la fois par rapport à ses autres scores et par rapport au score de l'organisation 2 dans le domaine C). Vous confieriez le domaine B à l'Organisation 2, là encore parce qu'il s'agit de l'un de ses domaines les plus forts et d'une grande faiblesse pour l'Organisation 1.





Au cours de cette session, partagez les devoirs et donnez des instructions sur la façon dont ils doivent être accomplis. Pour affecter chaque EP à un domaine, ajustez le texte vert sur la diapositive "Activité T (partie 2)".

Au cours de la session, expliquez que tous les EP sont affectés à un domaine spécifique. Ils doivent retourner dans la liste de contrôle et regarder ce domaine. Il y a un exemple de ceci sur la diapositive "Activité T (partie 3)". Ils verront que tous les domaines comprennent plusieurs stratégies. Le EP doit choisir au moins une stratégie dans le domaine qui lui a été attribué pour l'enseigner au groupe. Cela inclut le développement de diapositives et la planification d'une présentation de 10 minutes.

En tant qu'animateur, assurez-vous que la date et l'heure de la session du jour 3, au cours de laquelle ces présentations seront faites, figurent également sur la diapositive.

- **Activité U. Clôture du jour 2**. L'évaluation quotidienne peut être faite publiquement en utilisant Menti, en montrant votre écran au fur et à mesure que les résultats de l'enquête arrivent. Vous pouvez également laisser l'enquête ouverte à la fin de la session, puis vérifier les réponses par vous-même sans partager l'écran. Des exemples de questions sont inclus dans la section "Préparation en ligne pour le premier jour".

  A la fin de la session, partagez les diapositives avec tous les participants et rappelez-leur leurs devoirs. Un exemple de courriel à envoyer après le Jour 2 se trouve à l'Annexe G.

Jour 3 - Session spéciale

Heure	Session	Objectifs
Durée nécessaire	Présentations du groupe	▪ Partagez une stratégie de sécurité attribuée à votre OSC. ▪ Posez des questions sur toutes les stratégies présentées afin de comprendre la mise en œuvre, ainsi que les avantages et les inconvénients de la stratégie.

Préparation en ligne du jour 3

Aucune préparation en ligne n'est requise avant le jour 3. Les participants peuvent souhaiter partager leurs présentations avec l'animateur afin que ce dernier puisse les projeter pendant les présentations.

Instructions pour les activités du 3ème jour

- **Activité V. Présentations des partenaires de mise en œuvre.** Cette session est consacrée aux présentations de chaque partenaire de mise en œuvre, suivies des questions des autres participants. L'animateur doit surveiller le temps pour s'assurer que chaque organisation aura la possibilité de faire une présentation d'environ 10 minutes, suivie de cinq minutes de questions et réponses. L'animateur doit proposer de projeter à partir de son propre écran si les groupes qui présentent ont des difficultés de connexion. Pour cela, l'animateur doit disposer des diapositives avant la session. Si l'animateur ne dispose pas de toutes les diapositives avant le début de la session, il doit les récupérer à la fin de la session. À moins que des problèmes de sécurité ne se posent, toutes les diapositives collectées doivent être distribuées au groupe.

  À la fin de la session, l'animateur doit mentionner les ressources incroyables que nous sommes les uns pour les autres alors que nous renforçons tous notre capacité de sécurité. Après la session, l'animateur doit partager toutes les diapositives des partenaires de mise en œuvre. Un exemple de courriel pour la fin de la troisième journée figure à l'annexe H.

Jour 4

Heure	Session	Objectifs
8:00	Récapitulatif du deuxième jour et réflexions sur la session spéciale	▪ Réfléchir aux stratégies présentées lors de la session spéciale ▪ Rappel des sujets abordés le deuxième jour
8:10	Utiliser ce que vous avez appris : études de cas sur les défis de la sécurité	▪ Réfléchir à ce que pourrait faire votre organisation si elle était confrontée à divers problèmes de sécurité. ▪ Discutez si les "solutions possibles" après chaque scénario seraient appropriées dans le contexte local.
8:45	Formule d'évaluation des risques	▪ Se familiariser avec la formule permettant de déterminer la probabilité qu'un danger donné se produise.
9:05	Plan de sécurité	▪ Reconnaitre les éléments d'un plan de sécurité et s'entraîner à utiliser le modèle pour élaborer vos propres plans. ▪ Identifiez vos trois principaux risques et créez un plan de sécurité pour chacun d'eux en tenant compte des vulnérabilités, des capacités existantes et des capacités nécessaires.
9:35	Prochaines étapes	▪ Discuter des possibilités suivantes : action immédiate sans frais ou à faible coût, apprentissage continu entre les OSC, liaison des activités de sécurité avec la prévention et la réponse à la violence en cours, et recherche d'un soutien international. ▪ Identifier les mesures à prendre pour finaliser et faire accepter les plans de sécurité par chaque OSC.
9:50	Réflexions et clôture	▪ Partage de vos réflexions et évaluation de l'atelier; formuler des réflexions de clôture.

Préparation en ligne du 4ème jour

- Créez deux questions sur Menti. Notez que les étoiles indiquent les bonnes réponses et doivent être supprimées.

  Question 1. "De quoi un attaquant a-t-il besoin pour nous nuire ?" (sélectionner toutes les réponses qui s'appliquent)

  A. Motif**
  B. Ressources**
  C. Soutiens
  D. Pour nous voir en face à face

  Question 2. "Que pouvons-nous faire pour nous protéger en ligne ?"

  A. Ne pas partager les informations que nous ne voulons pas qu'un attaquant potentiel ait.**
  B. Utiliser des mots de passe forts.**
  C. Utiliser des applications de texto plus sûres, comme Signal plutôt que WhatsApp.**
  D. Mettez à jour les logiciels de sécurité, comme les programmes de protection antivirus.**

- Créer un post-test à l'aide de Google Forms (exemple de post-test à l'annexe J ; clé de réponse au post-test à l'annexe K).
- Créez une évaluation à l'aide de Google Forms (exemple à l'annexe L).

Instructions pour les activités du jour 4

Toutes les diapositives basées sur des activités comportent une étoile. Cela signifie que l'animateur ne doit pas se contenter de présenter les informations, mais qu'il doit inciter les participants à trouver les réponses. Chaque diapositive d'activité est décrite plus en détail ci-dessous.

- **Activité W. Principaux points à retenir**. Cette activité permet aux participants de réfléchir à la manière dont ils vont appliquer ce qu'ils ont appris de leurs collègues. L'animateur doit demander à deux ou trois volontaires de partager ce qu'ils ont appris lors de la dernière session et, surtout, comment ils vont utiliser ce qu'ils ont appris dans leur propre organisation.

  Après le partage, l'animateur doit souligner à nouveau que nous apportons tous beaucoup de connaissances pratiques à ce travail, et que nous pouvons toujours apprendre les uns des autres. En fonction des besoins du projet, l'animateur peut également aider à organiser un groupe Signal pour discuter des défis de sécurité et des solutions à venir.

- **Activité X. Rappel du 2e jour**. Cette diapositive permet de rappeler rapidement au groupe ce qui a été abordé au cours de la deuxième journée. Les questions se trouvent dans "Préparation en ligne pour le Jour 4".

  Demander à chacun d'aller sur Menti.com (mettre le lien et le code dans le chat). Après avoir répondu à la première question, demander à un volontaire d'expliquer son raisonnement. Montrer ensuite les bonnes réponses.

  Au cours de la discussion sur les réponses correctes à la première question sur les besoins d'un attaquant, noter que C n'est pas correct car un individu peut agir seul, et que D n'est pas correct car les attaques peuvent également se produire en ligne.

  Passer ensuite à la question suivante sur les protections en ligne. Encore une fois, demandez à chacun de répondre au questionnaire en ligne, puis demandez à un volontaire d'expliquer sa pensée. Mentionnez ensuite que toutes les réponses sont correctes. Chacune d'entre elles peut contribuer à assurer notre sécurité en ligne.

- **Activité Y. Utiliser ce que vous avez appris**. Dans cette activité, les petits groupes travailleront ensemble soit dans des salles de réunion, soit par téléphone, soit en personne (s'ils sont réunis en petits groupes). Chaque organisation doit être affectée à une étude de cas (scénario). Coller toutes les études de cas dans le chat pour pouvoir les consulter facilement. S'il y a moins de groupes que d'études de cas, sélectionner les études de cas qui vous semblent les plus pertinentes pour le contexte. Par exemple, vous pouvez assigner des EP uniquement aux études de cas 3, 5, 7 et 8.

Dire au groupe qu'il doit prendre son étude de cas et se poser deux questions. Premièrement, que peut faire cette organisation maintenant ? Deuxièmement, qu'aurait-elle pu faire - avant que ce problème ne se produise - pour atténuer ou prévenir le préjudice causé ?

Leur expliquer qu'ils auront cinq minutes pour discuter, puis vous demanderez à chaque groupe de partager ses réflexions. Après cela, vous, en tant qu'animateur, partagerez quelques solutions possibles à leurs commentaires.

Après cinq minutes, passez à la diapositive suivante sur le scénario 1 et demandez au premier groupe de faire sa présentation. Si aucun groupe n'a été chargé du scénario 1, répondez vous-même à la question en passant à la diapositive suivante pour passer en revue les réponses possibles. Faites la même chose pour chaque scénario.

À la fin, félicitez toutes les équipes et soulignez qu'elles ont des réponses à des problèmes délicats. Toute sécurité est contextuelle, et ils connaissent leurs contextes mieux que quiconque.

- **Activité Z. Réflexions sur les scénarios.** Cette activité aide les participants à comprendre que ce n'est pas seulement ce que vous faites, mais aussi le moment où vous le faites qui affecte la sécurité. Lire la question sur la diapositive, et demander à quelques volontaires de se lever et de répondre. Après avoir reçu plusieurs réponses, avancer la diapositive et examiner les réponses.
- **Activité AA. Exemple d'évaluation des risques**. Les formules d'évaluation des risques semblent complexes car elles ressemblent à des problèmes mathématiques compliqués. Cependant, cette formule est un outil pour aider les participants à réfléchir aux relations qui existent entre les vulnérabilités et les capacités et ne doit pas être utilisée avec des chiffres réels. La formule est également un outil permettant de rassembler tout le contenu qui a été présenté tout au long de la formation. Cette activité rend l'évaluation des risques plus concrète en présentant un exemple spécifique et en permettant aux participants de générer leurs propres idées sur la manière de réduire la vulnérabilité et d'augmenter la capacité.

  Sur la première diapositive de l'activité AA, la question "Que pourriez-vous faire pour réduire les vulnérabilités et augmenter les capacités ?" apparaît en bas. Donner aux participants quelques minutes pour y réfléchir, puis demander à deux ou trois personnes de répondre. Après avoir reçu les réponses, passer à la diapositive suivante de l'activité AA. La deuxième diapositive montre les solutions possibles pour supprimer les vulnérabilités en rouge et ajouter des capacités en bleu. Comme une seule vulnérabilité a été supprimée, un "-1" apparaît à côté des vulnérabilités. Il y a quatre façons d'augmenter la capacité, donc un "+4" apparaît à côté des capacités.

  Si les participants suggèrent que certaines vulnérabilités, comme le travail de sensibilisation durant la nuit, devraient également être supprimées, faites-leur savoir que chaque programme devra décider de ce qui est approprié en fonction de son contexte. Dans cet exemple, le programme a peut-être estimé que le fait de mener des actions de

proximité uniquement pendant la journée était trop restrictif ou limiterait trop l'accès des bénéficiaires du programme aux services.

- **Activité BB. Exemple local.** Dans cette activité, l'animateur guidera le groupe à travers un exemple concret. Demandez à un volontaire de partager un risque qui le préoccupe. Une personne (ou une organisation) remplira la majeure partie de ce tableau, car toutes les informations doivent être liées au risque initial. Remplissez la diapositive en utilisant les informations qu'ils ont fournies sur le risque, les menaces, les vulnérabilités et les capacités existantes. Lorsque vous en arrivez aux capacités requises, demander à la personne ou à l'organisation qui a rempli le tableau de donner quelques idées initiales sur ce qui pourrait être fait. Puis demander au groupe d'ajouter ses propres idées.

  Noter que la personne ou l'organisation ne souhaitera peut-être pas utiliser toutes les idées de la rubrique "capacités requises", mais cela leur donne un menu d'options parmi lesquelles choisir lorsqu'ils créent leur propre plan de sécurité.

- **Activité CC. Vos risques prioritaires**. Dans la formation virtuelle, cette activité est susceptible d'être assignée comme travail post-formation en petits groupes organisationnels. C'est l'occasion pour les organisations de décider quels sont les risques qu'elles jugent les plus urgents à traiter. La formule d'évaluation des risques peut être utilisée pour prendre cette décision. Après avoir décidé des trois risques les plus importants à traiter, ils doivent élaborer un plan de sécurité pour ceux-ci. Le modèle de plan de sécurité sera partagé dans le courriel qui sera envoyé après le Jour 4. Voir l'annexe I pour un exemple.

  Si vous animez cet atelier en présentiel, l'idéal est de laisser aux organisations le temps de travailler sur leur plan de sécurité pendant que tout le monde est réuni. Elles pourront ensuite les présenter aux autres participants pour obtenir leurs commentaires et améliorer encore leur produit final.

- **Activité DD. Planification des actions**. Cette étape permet aux organisations de convertir leurs plans de sécurité en plans d'action. Une fois que vous avez examiné leurs plans de sécurité et fourni un retour d'information, demander à chaque EP de remplir le tableau (communiqué dans le courriel après la dernière session) et de vous le renvoyer par courriel. Vous pourrez alors suivre leurs progrès et les aider à respecter le calendrier. Vous pouvez également utiliser les informations sur les ressources requises pour mettre en évidence les besoins en matière de sécurité lors des conversations avec le donateur.

  Les notes de l'orateur pour cette diapositive soulignent également un point extrêmement important : si les personnes formées souhaitent partager ce qu'elles ont appris avec d'autres, elles doivent d'abord apporter des changements substantiels à la formation elle-même. La formation est conçue pour aider les responsables organisationnels à faire de leur organisation un lieu de travail plus sûr. Cela se fait en grande partie en créant des protocoles et des politiques que les travailleurs doivent suivre, puis en sensibilisant les travailleurs à ces documents. Ainsi, si les personnes formées souhaitent partager le contenu de la formation avec d'autres, elles ne doivent le faire qu'après que les

responsables de l'organisation aient créé les politiques pertinentes. Ensuite, la formation doit être révisée pour refléter ces politiques/protocoles et être utilisée pour aider les travailleurs à comprendre les politiques et la manière dont les politiques/protocoles devraient influencer leurs actions.

- **Activité EE**. Utilisez les formulaires Google que vous avez créés à l'avance, à partir du contenu de l'annexe J et de l'annexe L, pour donner aux participants la possibilité d'évaluer la formation et de montrer leurs connaissances.
- **Activité FF**. **Dans vos propres mots**. En utilisant Menti.com, demandez aux participants de saisir quelques mots décrivant ce qu'ils ressentent à la fin de la formation. Si vous le souhaitez, demandez à un représentant de chaque organisation de donner une réponse plus approfondie sur le contenu de la formation et sur la manière dont elle influencera leur réflexion et leurs actions futures.

  Une fois l'atelier de la dernière journée terminé, envoyer un courriel au groupe (un exemple figure à l'annexe I). Le courriel doit inclure les pièces jointes Annexe M (plan de sécurité) et Annexe N (plan d'action).

Annexe A : Instructions pour remplir la liste de vérification

Qui doit remplir la liste de vérification ?

La liste de vérification doit être remplie par les membres du partenaire de la mise en œuvre qui assisteront à la formation sur la sécurité. La liste de vérification doit être remplie dans un espace sûr et privé où il est possible de parler ouvertement. Étant donné que la liste de vérification est conçue pour informer les politiques et les procédures régissant les activités partout où la conception, la mise en œuvre et le suivi du programme ont lieu, l'équipe qui remplit la liste de vérification doit visiter ou parler à des représentants de ces sites afin de mieux comprendre les défis et les besoins uniques des différents environnements.

Lorsque vous remplissez la liste de vérification, reportez-vous à chaque titre de section pour déterminer le type d'organisation qui doit remplir cette partie. Par exemple, certaines sections doivent être remplies par les organismes chefs de file (tels que les bénéficiaires principaux du Fonds mondial ou les organisations non gouvernementales internationales [ONGI] qui coordonnent les activités de plusieurs partenaires de mise en œuvre) ainsi que par les organisations qui mettent en œuvre des activités (telles que les sous-récipiendaires du Fonds mondial et les partenaires de mise en œuvre de l'USAID). D'autres sections, comme la section D, qui traite de la sécurité dans les lieux physiques, ne doivent être remplies que par ceux qui mettent directement en œuvre les activités et doivent être faites individuellement pour chaque site plutôt qu'au niveau de l'organisation. Ce point est abordé plus en détail dans l'encadré **Comment les organisations partenaires et les réseaux régionaux peuvent-ils travailler ensemble pour remplir utilement la liste de vérification ?**

Comment les organisations partenaires et les réseaux régionaux peuvent-ils travailler ensemble pour remplir utilement la liste de vérification ?

La raison pour laquelle différentes organisations remplissent différentes sections de la liste de vérification repose dans le fait que tous les types de stratégies ne sont pas pertinents pour toutes les organisations, et que les organisations travaillant ensemble peuvent se compléter. En particulier dans le contexte d'une organisation cadre et de plusieurs partenaires de mise en œuvre travaillant tous sur les mêmes objectifs, la manière dont une organisation remplit la liste de vérification peut dépendre des approches de ses collaborateurs en matière de sécurité. Par exemple, si une organisation chef de file a demandé à tous les partenaires de mise en œuvre d'adresser les questions des journalistes au ministère de la Santé, alors chaque partenaire de mise en œuvre cochera simplement des questions telles que "L'organisation a-t-elle un membre désigné pour parler aux médias ?" avec "non applicable" parce qu'ils n'ont pas besoin d'avoir une personne désignée pour parler aux médias selon l'approche utilisée par l'organisation chef de file.

Les réseaux régionaux peuvent être incertains quant aux éléments de la liste de vérification à remplir. La direction centrale de ces réseaux régionaux aura probablement intérêt à remplir les sections indiquées pour "l'organisation qui dirige le projet", tandis que les agences membres souhaiteront peut-être remplir les composantes indiquées pour "les organisations qui mettent en œuvre les activités". Ils pourront ensuite examiner leurs résultats collectifs pour déterminer où le réseau souhaite concentrer ses énergies pour combler les lacunes et partager les bonnes pratiques entre les organisations.

Comment remplir la liste de vérification ?

Pour tous ceux qui remplissent les différentes sections de la liste de vérification, veuillez lire chaque question dans la colonne B. Si la question nécessite des précisions, reportez-vous à la colonne C. Après chaque question, mettez un "1" sous "oui", "non", "plutôt" ou "sans objet" pour indiquer la réponse qui correspond le mieux à la réalité de votre organisation.

- **Oui** : Cette réponse indique que l'organisation met régulièrement en œuvre cette stratégie. Par exemple, à la question 1 - "L'organisation prend-elle des mesures pour être visible aux yeux du public et donner une image positive ?", si l'organisation mène une campagne permanente pour être visible de manière positive, elle mettra un 1 sous "oui".
- **Non** : Cette réponse indique que l'organisation ne s'est jamais engagée dans cette stratégie et ne l'applique pas actuellement. Par exemple, à la question 1 - "L'organisation prend-elle des mesures pour être visible par le public et lui donner une image positive ?", si l'organisation n'a jamais mené d'activités pour avoir une visibilité publique positive, elle mettra un 1 sous "non".
- **Un peu** : Cette réponse indique que l'organisation a utilisé cette stratégie par le passé mais ne l'utilise pas actuellement, ou que la stratégie n'est que partiellement utilisée. Par exemple, à la question 1 - "L'organisation prend-elle des mesures pour être visible du public, en donnant une image positive ?" - si l'organisation ne fait des activités publiques que dans certains sites où elle met en œuvre ou a déjà eu une campagne de publicité qui n'est plus opérationnelle, elle mettra un 1 sous "un peu".

- **Ne s'applique pas :** Cette réponse indique que cette stratégie n'est pas pertinente ou utile pour l'organisation. Par exemple, à la question 1 - "L'organisation prend-elle des mesures pour être visible du public, en donnant une image positive ?" - certaines organisations ne souhaitent pas être visibles de quelque manière que ce soit, car elles estiment que la visibilité peut être préjudiciable. Dans ce cas, éviter la visibilité publique est un choix mûrement réfléchi, et ils choisiraient "sans objet" parce que cette stratégie ne leur est pas utile. Les activités qui ne sont pas pertinentes, comme les questions sur la sensibilisation d'une organisation qui ne fournit des services que dans une clinique, seraient également marquées comme "sans objet".

Dans la colonne qui suit les réponses "oui/non/un peu/non applicable", il y a de la place pour que la ou les personnes qui remplissent la liste de vérification expliquent leur réponse sous "notes". Pour en savoir plus, consultez l'encadré "Notes".

Notes

Bien qu'il ne soit pas nécessaire qu'une organisation remplisse la colonne "notes" après chaque question, le fait de la remplir aidera à prendre des décisions sur les prochaines étapes, en particulier si vous sélectionnez "un peu" comme réponse et souhaitez fournir des détails expliquant votre choix.

Comment les scores peuvent-ils être interprétés ?

Chaque réponse "oui" donne un point à l'organisation, "un peu" donne un demi-point, "non" donne zéro point. La réponse "non applicable" n'affecte pas le score de manière positive ou négative. Outre les sections A à G, il existe des scores transversaux pour la préparation aux situations d'urgence, la sécurité numérique et le COVID-19. Lorsque vous remplissez la liste de vérification, n'oubliez pas que cet outil est conçu pour votre usage personnel et que vos scores ne seront partagés que si vous choisissez de les mettre à la disposition des autres**. Consultez l'encadré Tirer le meilleur parti de la liste de vérification** pour obtenir des informations supplémentaires.

Tirer le meilleur parti de la liste de contrôle

Cette liste de vérification est conçue pour être utile aux personnes chargées de la mise en œuvre. Si une stratégie n'est pas utile ou pertinente pour votre organisation, le fait de la marquer comme "non applicable" n'aura pas d'impact sur votre score et vous permettra de vous concentrer uniquement sur les stratégies dont l'emploi vous semble bénéfique. Ce que vous marquez comme "non" ou "un peu" n'est pas non plus le reflet d'un échec. Nombre de ces éléments importants de la sécurité n'ont pas été envisagés ou financés dans les programmes VIH. Vous pouvez utiliser les scores faibles (qui résulteront de la sélection de "non" et "un peu") pour travailler avec votre bailleur de fonds et votre organisation afin de souligner les domaines à développer, tandis que les scores élevés peuvent indiquer que votre organisation pourrait fournir une assistance technique ou des conseils à d'autres qui se lancent dans ce nouveau domaine.

Vos scores sont présentés sous forme de graphique dans le deuxième onglet du document Excel, "Graphique des réponses".

Annexe B : Exemple d'ordre du jour pour les participants en présentiel

Veuillez noter que l'ordre du jour des participants en personne n'est pas accompagné d'un ordre du jour correspondant pour les animateurs en présentiel, car les modifications apportées pour accueillir cette formation en personne doivent être déterminées localement. Cet exemple d'ordre du jour est fourni à titre d'illustration. Il permet aux personnes qui envisagent d'organiser un événement en présentiel de prévoir du temps pour les activités conçues comme devoirs dans la formation virtuelle et qui pourraient être réalisées en petits groupes lors des réunions en présentiel. Par exemple, dans la version virtuelle, il est demandé aux participants de discuter des principales recommandations en guise de devoir et de présenter leurs commentaires le deuxième jour. Dans ce programme, du temps est prévu pour que cette activité ait lieu pendant la session "Termes clés et recommandations majeures" plutôt que comme devoir.

Heure	Session	Objectifs
	JOUR 1	
8:00	Bienvenue, introductions et contexte	▪ Accueil et présentation des participants. ▪ Parvenir à une compréhension commune du contenu, objectifs de la formation et de la participation à la formation. ▪ Identifiez la sécurité des exécutants comme un domaine important et nouveau de la programmation du VIH.
8:45	Termes clés et recommandations majeures	▪ Définir les notions de sécurité, de risque, de menace, de capacité et de vulnérabilité, et discuter des principales recommandations relatives à la sécurité des exécutants des programmes des PC.
10:15	Pause	
10 :45	Identification et évaluation des menaces	▪ Identifier les menaces et déterminer leur gravité
12:30	Déjeuner	
1:30	Limiter la capacité de nuire d'un agresseur	▪ Décrire ce qui peut être fait, et par qui, pour limiter la capacité d'un agresseur à causer du tort.
2:15	Sécurité numérique	▪ Décrire les vulnérabilités inhérentes aux plateformes numériques ; identifier les stratégies de réduction des risques au sein de chacune d'elles.
3:15	Revoir de nos capacités et plan de partage des compétences	▪ Revoir les réponses collectives aux évaluations de la sécurité. ▪ Affecter chaque partenaire de mise en œuvre à une compétence qui sera présentée lors de la prochaine session.
4:00	Clôture	▪ Compléter l'évaluation du jour 1
	JOUR 2	
8:00	Récapitulatif du premier jour	▪ Revoir le contenu du premier jour
8:30	Présentations du groupe	▪ Partagez une stratégie de sécurité attribuée à votre OSC.

		▪ Posez des questions sur toutes les stratégies présentées afin de comprendre la mise en œuvre, ainsi que les avantages et les inconvénients de la stratégie.
10:00	Pause	
10:30	Continuer les présentations du group (durée nécessaire)	▪ Partagez une stratégie de sécurité attribuée à votre OSC. ▪ Posez des questions sur toutes les stratégies présentées afin de comprendre la mise en œuvre, ainsi que les avantages et les inconvénients de la stratégie.
11:00	Utiliser ce que vous avez appris : études de cas sur les défis de la sécurité	▪ Réfléchir à ce que pourrait faire votre organisation si elle était confrontée à divers problèmes de sécurité. ▪ Discutez si les "solutions possibles" après chaque scénario seraient appropriées dans le contexte local.
12:30	Déjeuner	
1:30	Formule d'évaluation des risques	▪ Se familiariser avec la formule permettant de déterminer la probabilité qu'un danger donné se produise.
2:00	Plan de sécurité	▪ Reconnaitre les éléments d'un plan de sécurité et s'entraîner à utiliser le modèle pour élaborer vos propres plans. ▪ Identifiez vos trois principaux risques et créez un plan de sécurité pour chacun d'eux en tenant compte des vulnérabilités, des capacités existantes et des capacités nécessaires. ▪ Présenter votre plan de sécurité au groupe pour avoir des retours (facultatif en fonction du temps)
3:45	Prochaines étapes	▪ Discuter des possibilités suivantes : action immédiate sans frais ou à faible coût, apprentissage continu entre les OSC, liaison des activités de sécurité avec la prévention et la réponse à la violence en cours, et recherche d'un soutien international. ▪ Identifier les mesures à prendre pour finaliser et faire accepter les plans de sécurité par chaque OSC.
4:15	Réflexions et clôture	▪ Partage de vos réflexions et évaluation de l'atelier; formuler des réflexions de clôture.

Annexe C : Programme de l'animateur pour la formation virtuelle

Time	Session	Objectives	Matériel
		JOUR 1	
8:00	Bienvenue, introductions et contexte	▪ Accueil et présentation des participants. ▪ Parvenir à une compréhension commune du contenu, objectifs de la formation et de la participation à la formation. ▪ Identifiez la sécurité des exécutants comme un domaine important et nouveau de la programmation du VIH.	▪ Diapositives ▪ Menti ▪ Document : Instructions pour compléter la liste de contrôle (Annexe A)
8:45	Termes clés et recommandations majeures	▪ Définir les notions de sécurité, de risque, de menace, de capacité et de vulnérabilité, et discuter des principales recommandations relatives à la sécurité des exécutants des programmes des PC.	▪ Diapositives ▪ Document : aide-mémoire (Annexe D)
9:15	Identification et évaluation des menaces	▪ Identifier les menaces et déterminer leur gravité	▪ Diapositives ▪ Document: Journal d'incident de sécurité (Annexe E)
9:55	Clôture de la première journée	▪ Evaluer la journée	▪ Diapositives ▪ Menti
		JOUR 2	
8:00	Récapitulatif du premier jour et du Devoir #1	▪ Partagez les réponses du Devoir #1. ▪ Rappel des sujets abordés le premier jour.	▪ Diapositives ▪ Menti
8:25	Limiter la capacité de nuire d'un agresseur	▪ Décrire ce qui peut être fait, et par qui, pour limiter la capacité d'un agresseur à causer du tort.	▪ Document : Aide-mémoire (Annexe D)
9:00	Sécurité numérique	▪ Décrire les vulnérabilités inhérentes aux plateformes numériques ; identifier les stratégies de réduction des risques au sein de chacune d'elles.	▪ Diapositives
9:40	Revoir de nos capacités et plan de partage des compétences	▪ Revoir les réponses collectives aux évaluations de la sécurité. ▪ Affecter chaque partenaire de mise en œuvre à une compétence qui sera présentée lors de la prochaine session.	▪ Diapositives ▪ Excel checklists
9:55	Récapitulatif du premier jour et du Devoir #1	▪ Partagez les réponses du Devoir #1. ▪ Rappel des sujets abordés le premier jour.	▪ Diapositives ▪ Menti

JOUR 3 – Session spéciale, Présentations du groupe			
Durée nécessaire	Présentations du groupe	▪ Partagez une stratégie de sécurité attribuée à votre OSC. ▪ Posez des questions sur toutes les stratégies présentées afin de comprendre la mise en œuvre, ainsi que les avantages et les inconvénients de la stratégie.	▪ Diapositives des OSC
JOUR 4			
8:00	Récapitulatif du deuxième jour et réflexions sur la session spéciale	▪ Réfléchir aux stratégies présentées lors de la session spéciale ▪ Rappel des sujets abordés le deuxième jour	▪ Diapositives ▪ Menti
8:10	Utiliser ce que vous avez appris : études de cas sur les défis de la sécurité	▪ Réfléchir à ce que pourrait faire votre organisation si elle était confrontée à divers problèmes de sécurité. ▪ Discutez si les "solutions possibles" après chaque scénario seraient appropriées dans le contexte local.	▪ Diapositives
8:45	Formule d'évaluation des risques	▪ Se familiariser avec la formule permettant de déterminer la probabilité qu'un danger donné se produise.	▪ Diapositives ▪ Document : Aide-mémoire (Annexe D)
9:05	Plan de sécurité	▪ Reconnaitre les éléments d'un plan de sécurité et s'entraîner à utiliser le modèle pour élaborer vos propres plans. ▪ Identifiez vos trois principaux risques et créez un plan de sécurité pour chacun d'eux en tenant compte des vulnérabilités, des capacités existantes et des capacités nécessaires.	▪ Diapositives ▪ Document : Modèle de plan de sécurité (Annexe M)
9:35	Prochaines étapes	▪ Discuter des possibilités suivantes : action immédiate sans frais ou à faible coût, apprentissage continu entre les OSC, liaison des activités de sécurité avec la prévention et la réponse à la violence en cours, et recherche d'un soutien international. ▪ Identifier les mesures à prendre pour finaliser et faire accepter les plans de sécurité par chaque OSC.	▪ Diapositives ▪ Document : Modèle de plan d'action (Annexe N)
9:50	Réflexions et clôture	▪ Partage de vos réflexions et évaluation de l'atelier; formuler des réflexions de clôture.	▪ Diapositives ▪ Menti

Annexe D : « Aide-mémoire » pour la formation à la sécurité

Recommandations majeures en matière de sécurité

1. Faire des principes et des approches du programme VIH le fondement des efforts de sécurité.

Les réponses à la sûreté et à la sécurité doivent suivre les mêmes principes et approches de bonnes pratiques que les autres aspects de la programmation du VIH. En voici quelques exemples :

- *Ne pas nuire* - Donner la priorité au bien-être des exécutants du programme et veiller à ce que les actions n'aggravent pas les situations, en particulier pour ceux qui ont déjà été lésés, à court ou à long terme.
- *Rien sur nous, sans nous* - S'assurer que les efforts de sécurité sont informés et dirigés par les personnes chargées de la mise en œuvre des programmes, y compris les membres des populations clés qui mettent en œuvre les programmes.
- *Approche fondée sur les droits* - S'assurer que les droits et la dignité des personnes chargées de la mise en œuvre des programmes sont protégés et respectés et que les réponses ne les forcent pas, comme par exemple, à cesser d'être fidèles à eux-mêmes pour rester en sécurité.
- *Approche dirigée par le pays/appartenant au pays* - S'assurer que les décisions sont prises par des organisations locales/nationales (lorsque cela est approprié et utile, avec le soutien de parties prenantes régionales et internationales).

2. Faire de la sécurité une priorité et y consacrer des ressources de manière explicite

La sûreté et la sécurité des programmes destinés aux populations clés ne doivent jamais être présumées ou laissées au hasard. Idéalement, elles devraient être envisagées dès le stade de la proposition d'un projet, dans la partie d'évaluation des risques, sous forme de "budgétisation de la sécurité".

Il est beaucoup plus facile et rentable d'investir dès le départ dans la planification et la prévention que de devoir prendre des mesures réactives (comme le déménagement d'un bureau). Réserver des fonds pour soutenir les travailleurs de proximité ou d'autres personnes qui subissent des préjudices, par exemple pour couvrir les frais d'hospitalisation en cas de violence. Cela permet d'agir immédiatement en cas de crise et démontre aux travailleurs que l'organisation s'engage pour leur bien-être.

Les mesures de sécurité doivent être une priorité de l'organisation et une composante essentielle de tous les programmes de lutte contre le VIH pour et avec les populations clés.

À ce titre, les activités de sécurité doivent faire l'objet de postes budgétaires spécifiques. Ces mesures de protection ne sont pas un luxe ou un supplément, mais une nécessité. Lorsque les activités visant à promouvoir la sûreté et la sécurité ne sont pas explicitement incluses dans les demandes de propositions des donateurs, il est important de faire pression pour qu'elles soient incluses dans les budgets et les plans de travail. L'intégration de la sécurité dans les budgets soutient les recommandations des orientations normatives - telles que les directives et les outils de mise en œuvre pour les populations clés de l'Organisation mondiale de la santé - selon lesquelles la prévention et l'action en réponse à la violence à l'encontre des populations clés est un facteur essentiel de l'efficacité des réponses au VIH.

La santé mentale des travailleurs revêt une importance particulière pour les efforts de sécurité organisationnelle et devrait faire l'objet de ressources et de programmes explicites. La mise en œuvre d'activités dans le cadre d'un programme de lutte contre le VIH s'accompagne d'un ensemble unique de

contraintes en matière de santé mentale. Au-delà de la violence et des abus qui peuvent être perpétrés contre les exécutants pour leur travail, ils rencontrent quotidiennement des bénéficiaires dont les besoins dépassent souvent de loin les capacités de l'organisation. L'incapacité à répondre aux besoins de base, tels qu'un logement sûr et une aide alimentaire, a un impact négatif sur la santé mentale des travailleurs. Les organisations doivent investir dans la santé mentale des travailleurs pour éviter l'épuisement professionnel et les conséquences négatives, telles que la toxicomanie.

3. Faire de la sécurité du lieu de travail la responsabilité de l'employeur

De nombreuses lacunes doivent être comblées pour garantir un environnement sûr et sécurisé aux personnes chargées de la mise en œuvre des programmes destinés aux populations clés, que ce soit dans les bureaux et cliniques établis ou sur le terrain. De nombreux donateurs ne financent pas d'activités liées à la sûreté et à la sécurité dans le cadre de leurs programmes de lutte contre le VIH et, dans certains cas, les organisations qui cherchent à fournir une assurance à leurs employés constatent également que les structures locales - comme les plans d'assurance disponibles - ne répondent pas à leurs besoins. Il en résulte trop souvent que les travailleurs sont laissés responsables de leur sûreté et de leur sécurité personnelle.

Pourtant, les normes mondiales exigent que les employeurs assument un devoir éthique de diligence pour assurer la sécurité de leurs employés (par exemple, les directives fournies par l'Organisation internationale du travail). Dans le cas des OSC dont les ressources sont limitées, les donateurs doivent plaider plus fermement en faveur de la sûreté et de la sécurité dans la programmation et fournir aux organisations de mise en œuvre les moyens de budgétiser et de planifier la sûreté et la sécurité afin qu'elles puissent respecter leur devoir de diligence envers leurs employés. En présentant les organisations performantes et responsables comme des exemples positifs, on peut non seulement leur donner les honneurs qu'elles méritent, mais aussi influencer le terrain.

4. Planifier à l'avance et s'assurer que tout le monde connaisse le plan (en maintenant la flexibilité).

Les mesures de prévention et d'intervention en matière de sûreté et de sécurité doivent être soigneusement identifiées et tracées dans le cadre d'un plan de sécurité organisationnel qui est élaboré, connu et détenu par l'ensemble de l'organisation ou de l'institution. Le plan doit être rationalisé, systématique et fondé sur des preuves dans le contexte local pertinent. Il doit identifier les menaces et les risques critiques pour la sûreté et la sécurité et fournir un guide clair, étape par étape, des actions à entreprendre, par qui et quand. Un plan efficace complète les plans d'urgence des partenaires clés, tels que les cliniques VIH adaptées aux populations clés.

Le plan doit également tenir compte des menaces les plus graves et inclure des actions visant à limiter la capacité d'un agresseur à commettre des violences.

Enfin, un bon plan de sécurité exige de décider systématiquement quelles menaces spécifiques sont prioritaires en identifiant celles qui comportent le plus de risques pour l'organisation (par exemple, non seulement celles qui sont graves mais aussi celles qui auront le plus grand impact). Comme il ne sera pas possible de prendre toutes les mesures souhaitées pour améliorer la sécurité en une seule fois, répondez d'abord aux défis les plus pressants en matière de sécurité et de sûreté.

5. Discuter explicitement le niveau de risque acceptable pour l'organisation et l'individu.

Les activités visant à améliorer la sûreté et la sécurité doivent être fondées sur l'appréciation du fait que chaque individu, organisation et programme a un niveau différent de confort et de tolérance vis-à-vis du risque. Le plan de sécurité d'une organisation ne doit pas, par exemple, être basé uniquement sur le goût du risque du directeur, qui peut, personnellement, être plus habitué ou préparé à faire face aux menaces.

De manière réaliste, dans des environnements hostiles, il est probable que tout travail avec des populations clés sera associé à un certain degré de risque.

Cependant, personne ne doit se sentir obligé de prendre des risques qui le mettent mal à l'aise. Tous les travailleurs doivent avoir - de préférence avant qu'un incident de sécurité ne se produise - la possibilité de réfléchir et de dire ce qu'ils sont personnellement prêts à faire. Parmi les options possibles, citons l'acceptation du niveau de risque, la réduction du niveau de risque, le partage du risque ou l'évitement du risque. Une fois que les niveaux individuels d'appétit pour le risque sont compris, les individus et leurs organisations peuvent prendre des décisions éclairées sur la façon de répondre aux risques réels qui sont identifiés.

Lorsque les environnements changent, les risques changent aussi. Cela signifie que les conversations doivent être permanentes pour identifier les risques, discuter des niveaux de risque acceptables et aider les travailleurs à comprendre ce que l'organisation fera pour aider à atténuer les risques. Par exemple, durant le COVID-19, le risque lié à la participation aux efforts de sensibilisation a changé de façon spectaculaire. Les personnes les plus susceptibles de souffrir de complications graves dues à l'infection - comme celles souffrant de problèmes de santé sous-jacents - couraient désormais un plus grand risque lors des activités de sensibilisation que les personnes sans problèmes de santé sous-jacents. Ces risques étant nouveaux, il était important que les organisations aident les travailleurs à évaluer leurs propres risques et à décider ensuite du niveau de risque qu'ils se sentaient prêts à assumer, idéalement avec le soutien de leur organisation, pour être affectés à d'autres tâches si le travail de sensibilisation était jugé trop risquée.

6. Opérer avec une connaissance des risques effectifs et de leurs causes profondes (y compris les cadres juridiques)

Les réponses aux incidents de sûreté et de sécurité doivent tenir compte non seulement des causes immédiates (le déclencheur) mais aussi des facteurs d'influence à plus long terme (les causes profondes). De même, les réponses doivent être adaptées au contexte spécifique (culturel, politique, juridique, etc.) dans lequel les problèmes surviennent. Quelque chose peut être faisable et efficace dans un contexte (par exemple, le dialogue avec la police) alors qu'il cause des dommages dans un autre.

Pour comprendre les risques et leurs causes, il est important d'examiner le cadre juridique d'un pays afin de déterminer quelles activités, le cas échéant, peuvent faire l'objet d'un examen minutieux de la part des forces de l'ordre et de comprendre et de pouvoir articuler vos droits en tant que responsables de la mise en œuvre d'un programme. Ces informations doivent être largement partagées avec les travailleurs qui bénéficient également d'un renforcement des capacités sur la manière d'exprimer ces droits aux autorités locales ou à d'autres personnes qui pourraient avoir des questions sur leurs activités.

7. Reconnaitre les différentes vulnérabilités et capacités de chaque travailleur dans la planification de la sécurité.

Les réponses en matière de sûreté et de sécurité doivent ne permanence prendre en compte le fait que le personnel et les volontaires des programmes VIH qui sont eux-mêmes des membres de la population clé sont confrontés à une double vulnérabilité, dans leur vie professionnelle et dans leur vie personnelle. C'est également le cas des personnes vivant avec le VIH et de celles qui sont sans papiers ou font partie de communautés de réfugiés. Toutes les personnes travaillant dans les programmes pour les populations clés ont des vulnérabilités et des capacités distinctes qui doivent être prises en compte au lieu d'utiliser une approche unique. Il est particulièrement important de prendre en compte les questions liées à :

▶ **Genre.** Par exemple, dans certains contextes, les membres du personnel qui sont des femmes cis-genres, transgenres ou des hommes cis-genres avec des expressions de genre plus féminines peuvent être

particulièrement vulnérables à la violence fondée sur le genre (VBG) dans le cadre de la mise en œuvre des programmes VIH et, à leur tour, peuvent avoir besoin de mesures de prévention et de réponse plus nombreuses et/ou différentes par rapport à d'autres collègues. La dynamique de pouvoir au sein des organisations peut également être impactée par le sexe, et une attention particulière doit être accordée à garantir un lieu de travail exempt de harcèlement sexuel.

▶ **Age.** Par exemple, il peut y avoir une dynamique de pouvoir au sein de l'organisation qui favorise les travailleurs plus âgés ou plus jeunes. L'âge d'un travailleur est également susceptible d'avoir un impact sur les menaces auxquelles il est confronté lors de son travail de proximité ; les travailleurs plus jeunes font l'objet d'une plus grande surveillance de la part de la police dans certains contextes, en particulier pendant les périodes de troubles politiques**.**

▶ **Différents groupes et sous-groupes des populations clés**. Il y a des problèmes à prendre en compte :

- **Entre les groupes de populations clés.** Par exemple, les membres du personnel travaillant avec des groupes spécifiques (tels que les usagers de drogues injectables) auront besoin de réponses de sûreté et de sécurité adaptées aux préoccupations relatives aux surdoses, aux interactions médicamenteuses et aux pratiques d'injection sûres. De même, certains membres des populations clés peuvent être confrontés à des défis uniques dans le cadre des réponses aux incidents (par exemple, les personnes transgenres peuvent manquer de documents officiels et ne pas être en mesure de déposer une plainte officielle).
- **Au sein des programmes destinés aux populations clés**. Par exemple, les questions de sécurité peuvent être différentes selon que l'on s'adresse à des hommes ayant des rapports sexuels avec des hommes dans des points chauds, dans des résidences ou en ligne.
- **Vulnérabilités multiples**. Par exemple, les travailleurs qui soutiennent des personnes appartenant à plusieurs groupes peuvent être vulnérables à de multiples problèmes de sûreté et de sécurité et nécessiter un ensemble de réponses spécifiques. Par exemple, les travailleurs qui interagissent avec des travailleurs du sexe qui s'injectent des drogues peuvent avoir besoin de transporter toute une série de produits (seringues, préservatifs, etc.) qui peuvent augmenter le risque d'arrestation et de détention.

▶ **Un statut juridique différent**. Il s'agit notamment de prendre en considération les personnes qui se trouvent dans un pays sans documents légaux ou celles qui ont un casier judiciaire et qui risquent de se voir infliger des peines plus sévères en cas d'interaction avec le système judiciaire.

8. Apprendre à connaitre toutes les parties prenantes, pas seulement les alliés évidents.

Il est essentiel d'essayer d'entrer en contact avec les individus et les institutions qui sont directement ou indirectement à l'origine des problèmes de sûreté et de sécurité. Cela peut impliquer l'établissement de relations avec des groupes de parties prenantes tels que les forces de l'ordre, les chefs religieux et les dirigeants communautaires. De tels partenariats peuvent prendre du temps et demander beaucoup de patience, mais ils peuvent apporter des récompenses importantes. Par exemple, lorsque ces parties prenantes deviennent des membres des équipes locales d'intervention d'urgence, plutôt que des adversaires. Prendre le temps d'établir des liens personnels et d'apprendre des autres groupes travaillant avec différentes communautés, est une tactique utile.

9. Identifier les menaces (physiques, numériques et psychologiques) et les stratégies de sécurité holistiques.

Les problèmes de sûreté et de sécurité au sein de la communauté des populations clés et dans les programmes de lutte contre le VIH sont rarement unidimensionnels. Ils évoluent également au fil du temps. En tant que tels, les réponses doivent être :

▶ **Holistiques** : aborder la sûreté et la sécurité physiques, psychosociales et numériques comme le suggère le Tactical Technology Collective. Les réponses doivent impliquer à la fois des initiatives tournées vers l'intérieur (par exemple, l'élaboration et la communication d'un plan d'urgence) et des initiatives tournées vers l'extérieur (par exemple, l'établissement de relations avec les parties prenantes locales).

▶ **Complets** - Utilisation d'une approche à plusieurs niveaux et facettes.

▶ **Flexibles**— Avoir la possibilité de modifier les plans et de s'adapter rapidement et efficacement, par exemple en réponse à un changement soudain de l'environnement de sécurité.

10. Etre ensemble, travailler en coalition, et apprendre les uns des autres.

Soyez conscient de la sûreté et de la sécurité en tant que collectif. Bien que chaque programme de population clé ou organisation de mise en œuvre ait des défis distincts à relever en matière de sûreté et de sécurité, des chevauchements existent. Le partage des défis, des succès et des questions permet d'apprendre et de réfléchir de manière critique sur les expériences, les stratégies et les ressources qui peuvent ensuite être exploitées pour renforcer les réponses en matière de sûreté et de sécurité.

Définitions clés

- **Sécurité** : l'état d'être exempt de risques ou de dommages provenant d'une violence intentionnelle
- **Risque :** la probabilité que quelque chose de nuisible se produise
- **Menace** : indication/signe que quelqu'un veut nous faire du mal, nous endommager, nous punir ; elle vient de l'extérieur.
    - **Menace directe** - Indication que quelqu'un veut me faire souffrir ou me nuire spécifiquement, par exemple : "Je vais t'attaquer parce que tu es une travailleuse du sexe".
    - **Menace indirecte** - Indication que quelqu'un veut faire souffrir ou nuire à un groupe plus large de personnes dont je fais partie, mais pas à moi/mon organisation en particulier, par exemple, un autre travailleur du sexe se sent menacé par la menace ci-dessus même si elle ne lui a pas été adressée.
    - **Incident de sécurité** - Situations que nous voyons se produire, mais dont nous ne sommes pas certains qu'elles constituent une menace ou qu'elle constitue une coïncidence, par exemple, votre ordinateur est volé. Est-ce qu'on vous vise pour obtenir des informations sur ce que vous faites ou pour voler vos contacts ? Ou s'agit-il simplement d'un vol opportuniste ?

- **Capacité** : toute ressource (financière, compétence, contacts, infrastructure, personnalité, etc.) que nous pouvons utiliser pour améliorer notre sécurité.
- **Vulnérabilité** : tout ce qui augmente notre exposition à ceux qui veulent nous faire du mal.

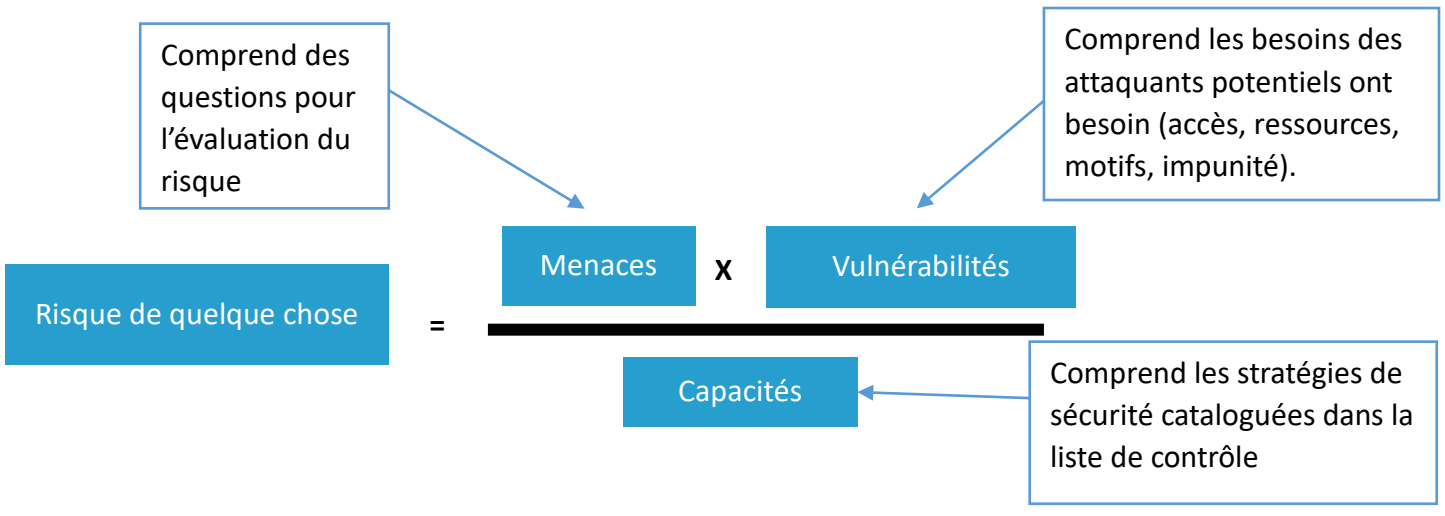
Questions pour évaluer le danger d'une menace

1. Quels sont les faits entourant la menace ?
2. La menace fait-elle partie d'une série qui est devenue plus systématique ou plus fréquente au fil du temps ?
3. Qui est la personne qui profère les menaces ?
4. Quel est l'objectif de la menace ?
5. Pensez-vous que la menace soit sérieuse ?

De quoi un attaquant a-t-il besoin pour réussir ?

- **Accès** : à vous physiquement ou électroniquement
- **Ressources** : tout ce qui peut être utilisé pour mener à bien l'attaque - informations sur l'emplacement de la victime, ses faiblesses ; arme ; transport ; argent.
- **Impunité** : absence de conséquences, juridiques et/ou sociales, pour l'agresseur.
- **Motif** : une raison de faire du mal.

Formule pour calculer le risque



Protocole de sécurité

- La mise en œuvre des plans de sécurité prend du temps. Nous devons trouver des mesures à prendre dès maintenant pour faire face aux problèmes lorsqu'ils surviennent. La solution aux besoins à court terme est un protocole de sécurité.
- Tout d'abord, nous devons définir des niveaux - vert (normal), orange ou ambre (indications qu'une attaque pourrait être menée), rouge (probabilité extrême d'une attaque) - puis réfléchir aux mesures à prendre en ce qui concerne le personnel, les programmes et les locaux.

Voici un exemple de protocole de sécurité.

	Personnel	Programmes	Locaux
Vert	Aucune restriction	Aucune restriction	Procédures de sécurité normale
Ambre	1. Le personnel jugé le plus à risque (défini/déterminé à l'avance) ne se rend pas au travail ou ne travaille pas dans les espaces publics. 2. Rappeler l'ensemble du personnel des personnes à informer en cas d'urgence. 3. Alerter les voisins et alliés de confiance de la situation ("hey, nous pensons que tout va bien, mais faites-nous savoir si vous voyez quelque chose d'étrange") 4. Alerter les avocats de l'organisation	1. Les activités extrêmement sensibles ou celles qui se déroulent dans des environnements hostiles (déterminées à l'avance) sont mises en attente 2. Les activités non sensibles se poursuivent normalement 3. Alerter les donateurs 4. Avertir les bénéficiaires de la situation et s'assurer qu'ils respectent les mesures de sécurité requises (par exemple, nous n'accueillerons plus de grands événements jusqu'à nouvel ordre).	1. Engager un agent de sécurité à court terme pour la surveillance pendant les heures de bureau. 2. Les visiteurs doivent faire l'objet d'un contrôle préalable pour accéder aux locaux (pas de visiteurs inopinés). 3. Il est rappelé au personnel de vérifier qu'aucune information sensible ne soit facilement accessible (numérique ou physique). 4. Déplacez les fonds d'urgence de manière à ce qu'ils soient facilement accessibles (peut-être sur des cartes bancaires, peut-être dans Western Union).
Rouge	1. Le personnel jugé "le plus à risque" sera temporairement relocalisé (le personnel et les sites de relocalisation étant définis à l'avance). 2. Les autres membres du personnel ne viennent pas au bureau 3. Les alliés de l'organisation sont informés et mobilisés 4. Les avocats de l'organisation sont alertés	1. Suspendre temporairement toutes les activités du projet 2. Informer les donateurs organisationnels que les projets ont été suspendus 3. Communiquer les suspensions aux bénéficiaires	1. Verrouiller le bureau (le personnel responsable de la fermeture du bureau a été déterminé à l'avance). 2. Engager un agent de sécurité pour la surveillance pendant et après les heures de bureau 3. Aucun visiteur n'est autorisé dans les locaux

Annexe E : Journal des incidents de sécurité

Journal des incidents de sécurité de l'exécutant			
	Question	**Comment répondre**	**Réponse**
1	Numéro de l'incident de sécurité	Commencez par le numéro 1 et continuez ; la numérotation permet de relier les incidents de sécurité les uns aux autres (voir la question 14).	
2	Date de l'incident	Tapez –JOUR-MOIS-ANNEE (par exemple, 17-02-2019 pour le 17 février 2019) pour organiser ce journal des événements de sécurité par date.	
3	Heure de l'incident	Heure précise de la journée (si elle est connue), ou plus générale (matin, après-midi, soir, nuit)	
4	Auteur de l'attaque	S'il est connu et qu'il est sûr de le lister , ou utiliser un terme plus général tel que "agent des forces de l'ordre".	
5	Organisation affectée	Nom du partenaire de mise en œuvre du programme VIH (c'est-à-dire le nom de l'organisation communautaire)	
6	Cible	Personne ou type de personnel spécifique, espace physique (par exemple, le nom d'un point chaud spécifique), site web, base de données, etc. Ne nommez pas de personnes ici, sauf si vous avez leur permission.	
7	Où l'incident s'est produit	Adresse physique, en ligne, par téléphone, etc.	
8	Le motif présumé de l'agresseur (si connu)	Par exemple : intimidation, arrêt de la programmation, détournement de l'attention d'autres problèmes locaux.	
9	Description de l'incident de sécurité	Par exemple : Des messages Facebook sur la page du projet disaient " [collez un message spécifique ici] " ; ou des éducateurs pairs ont été arrêtés sans accusation alors qu'ils distribuaient des préservatifs à un groupe de HSH lors d'un événement mobile de dépistage au VIH.	
10	Conséquences programmatiques de l'incident de sécurité	Par exemple : Le partenaire d'exécution mènera uniquement des activités de sensibilisation en ligne jusqu'à ce que les activités de sensibilisation physiques soient considérées comme sûres.	

Journal des incidents de sécurité de l'exécutant			
	Question	**Comment répondre**	**Réponse**
11	Descriptions des actions prises pour répondre à l'incident de sécurité	Par exemple : Le JOUR-MOIS-ANNEE, le partenaire d'exécution ciblé dans le post Facebook a décidé qu'il n'était pas sûr de mener des activités de sensibilisation pendant une période de deux semaines et l'exécutant partenaire a déposé une plainte auprès de la police. Le JOUR-MOIS-ANNEE, les responsables du ministère de la Santé ont organisé une réunion avec les détenteurs du pouvoir et les forces de l'ordre locales ; ils ont discuté des menaces qui pèsent sur le partenaire d'exécution et ont créé un groupe WhatsApp qui peut être utilisé pour notifier et activer des alliés immédiatement en cas de besoin. Veuillez inclure les dates des actions entreprises (et continuez à mettre à jour cette ligne au fur et à mesure que des actions sont entreprises).	
12	Quel est l'incident de sécurité lié au test d'indexation ?	Sélectionnez une réponse : Oui, Non, ou Incertain	
13	Le test d'indexation était-il lié au Covid-19 ?	Sélectionnez une réponse : Oui, Non, ou Incertain	
14	A quels tests d'indexation ceci est lié ? (le cas échéant)	Notez si cet incident est lié à d'autres incidents de sécurité en indiquant ici les numéros des autres incidents de sécurité.	
15	Résolution de l'incident (le cas échéant)	Par exemple : le JOUR-MOIS-ANNEE, les pairs éducateurs ont été libérés de la détention, et ont reçu un soutien en matière de santé mentale.	

Annexe F : Exemple d'email post-session 1

Chère équipe,

Merci pour votre grande participation aujourd'hui. Vous trouverez ci-joint :

1. Les diapositives de la session d'aujourd'hui
2. L'aide-mémoire qui vous aidera à faire vos devoirs et à comprendre les concepts clés de la formation.
3. Le journal des incidents de sécurité à utiliser par votre organisation.

Vous pouvez trouver un enregistrement de la session d'aujourd'hui ici : FOURNIR L'URL

N'oubliez pas que vous avez été chargé d'examiner l'une des recommandations majeures et de partager les éléments suivants au début de la prochaine session : (1) un résumé de la recommandation, (2) comment vous utilisez actuellement la recommandation, et (3) comment vous pourriez utiliser la recommandation à l'avenir.

Nous nous réjouissons de vous voir à la session 2 le jour X à l'heure Z !

Noms des animateurs

Annexe G : Exemple d'email post-session 2

Merci pour votre grande participation aujourd'hui. Vous trouverez ci-joint :

1. Les diapositives de la session d'aujourd'hui

Vous pouvez trouver un enregistrement de la session d'aujourd'hui ici : FOURNIR L'URL

N'oubliez pas que chaque OSC a été chargée d'enseigner une compétence spécifique lors de notre prochaine session à l'heure X, à la date Y. Les missions sont décrites dans les diapositives (fournir les numéros de diapositives). Si vous souhaitez que je partage vos diapositives sur mon écran afin que vous n'ayez pas besoin de partager votre écran pendant notre session (cela pourrait être particulièrement important si vous avez des problèmes de connectivité), veuillez me les envoyer à l'avance.

Nous nous réjouissons de vous rencontrer pour notre session spéciale 3 le jour X à l'heure Z !

Noms des animateurs

Annexe H : Exemple d'email post-session 3

Merci pour votre grande participation aujourd'hui. Vous trouverez ci-joint :

1. Les diapositives présentées par tous les partenaires de mise en œuvre

Vous pouvez trouver un enregistrement de la session d'aujourd'hui ici : FOURNIR L'URL

Nous nous réjouissons de vous voir lors de notre session finale le jour X à l'heure Z !

Noms des facilitateurs

Annexe I : Exemple d'email post-session 4

Merci à tous d'avoir participé à cet important atelier ! Nous avons tous beaucoup appris ensemble. Vous trouverez en annexe de ce courriel

1. Le jeu de diapositives complet, y compris les diapositives partagées par les OSC lors de la session 3.
2. Un modèle de plan de sécurité
3. Un modèle de plan d'action
4. Une page sur les ressources d'urgence disponibles
5. Des conseils sur l'élaboration de procédures opérationnelles standard en matière de sécurité pour les responsables de la mise en œuvre de programmes VIH travaillant avec des populations clés.

Vous pouvez trouver un enregistrement de la session d'aujourd'hui ici : FOURNIR L'URL

N'oubliez pas que vous devez tous soumettre vos plans de sécurité pour examen à la personne X avant la date Y. Nous vous enverrons un retour d'information et vous aiderons également à réfléchir à la mobilisation des ressources pour les activités qui ne peuvent être réalisées à peu ou pas de frais.

Merci encore pour votre attention, votre participation et votre énergie. Nous nous réjouissons de pouvoir vous soutenir dans vos efforts pour assurer la sécurité des exécutants.

Noms des facilitateurs

Annexe J : Post-test

Ce test peut être saisi dans Google Forms pour recueillir les réponses par voie électronique. Pour obtenir des informations sur l'utilisation de Google Forms, cliquez ici : https://support.google.com/docs/answer/6281888?co=GENIE.Platform%3DDesktop&hl=fr.

Nous vous recommandons de rendre obligatoire chacune des questions ci-dessous. Pour ce faire, sélectionnez le bouton "obligatoire" dans Google Forms.

1. Laquelle de ces expressions décrit le mieux la "sécurité" ?
    a. L'absence de préjudice intentionnel
    b. Sécurité contre les erreurs médicales, telles que les piqûres d'aiguille
    c. Être prêt à faire face à des catastrophes naturelles, telles que des inondations.
    d. Toutes ces réponses

2. Pourquoi est-il important pour une organisation de suivre les incidents de sécurité (par exemple, les arrestations des pairs, les attaques contre la réputation de l'organisation sur les médias sociaux, les graffitis menaçants sur un centre d'accueil) ?
    a. L'organisation peut identifier des tendances, comme l'augmentation des attaques, et élaborer des plans qui tiennent compte de ces tendances. Par exemple, mettre en pause les actions de sensibilisation dans certaines zones.
    b. L'organisation dispose d'un dossier qu'elle peut partager avec le donateur pour expliquer les changements de performance.
    c. L'organisation sait quel cadre de ses travailleurs est le plus à risque et peut affecter des ressources supplémentaires pour les protéger.
    d. Toutes ces réponses

3. Sélectionnez vrai ou faux pour chaque affirmation ci-dessous.
    - Une entreprise est responsable de la création d'un environnement sécurisé pour ses employés.
    - Il suffit qu'une organisation dise à ses employés de "faire preuve de discernement" sans leur donner de directives précises.
    - Les travailleurs de proximité en ligne doivent toujours communiquer leur nom complet (prénom et nom).
    - Des mots de passe devraient être utilisés sur tous les ordinateurs de bureau et personnels.
    - L'épuisement du personnel peut être une conséquence des incidents de sécurité.
    - L'existence d'une politique en matière de harcèlement sexuel rend une organisation plus sûre.

- Toutes les organisations qui desservent des membres de la population clé devraient collaborer avec la police.
- Partager une photo de soi en ligne peut donner à un agresseur des informations à utiliser contre vous.
- Travailler avec des chefs religieux peut aider à protéger une organisation.
- Le fait d'avoir un porte-parole dans les médias peut protéger une organisation.

4. Une menace est un signe que quelqu'un veut faire du mal à une autre personne ou la punir. Laquelle des questions suivantes vous aide à comprendre la gravité d'une menace pour votre programme/organisation ?
    a. Qui profère cette menace ?
    b. S'agit-il d'une série de menaces qui est devenue plus fréquente ou systématique au fil du temps ?
    c. Quelle est la gravité de la menace selon vous ?
    d. Quel est l'objectif de cette menace ?
    e. Toutes ces questions

5. Laquelle des propositions suivantes est correcte ?
    a. Nous devons supprimer toutes les vulnérabilités pour limiter les risques pour nos programmes.
    b. Certaines vulnérabilités ne peuvent pas être supprimées ; la chose la plus importante à faire est d'être conscient des vulnérabilités.
    c. La vulnérabilité est la même chose que la faiblesse.

6. De quoi avez-vous besoin avant de pouvoir élaborer un plan de sécurité ?
    a. Une compréhension des menaces les plus graves pour votre organisation.
    b. Une compréhension de vos capacités de sécurité existantes.
    c. Une compréhension de vos vulnérabilités actuelles.
    d. Le financement pour mettre en œuvre le plan.
    e. Tout ce qui précède.
    f. A, B, et C

Annexe K : Clé de réponse Post-test

1. A
2. D
3. Vrai ou faux (voir chaque déclaration)
    - Une organisation est responsable de la création d'un environnement sécurisé pour ses travailleurs. (VRAI)
    - Il suffit à une organisation de dire à ses employés de "faire preuve de discernement" sans leur donner de directives précises. (FAUX)
    - Les travailleurs de proximité en ligne doivent toujours communiquer leur nom complet (prénom et nom). (FAUX)
    - Des mots de passe devraient être utilisés sur tous les ordinateurs de bureau et personnels. (VRAI)
    - L'épuisement du personnel peut être une conséquence des incidents de sécurité. (VRAI)
    - Le fait d'avoir une politique sur le harcèlement sexuel rend une organisation plus sûre. (VRAI)
    - Toutes les organisations qui desservent les membres de la population clé devraient collaborer avec la police. (FAUX)
    - Partager une photo de soi en ligne peut donner à un agresseur des informations à utiliser contre vous. (VRAI)
    - Travailler avec des chefs religieux peut aider à protéger une organisation. (VRAI)
    - Avoir un porte-parole dans les médias peut aider à protéger une organisation. (VRAI)
4. E
5. B
6. F

Annexe L : Exemple d'évaluation

1. **Le contenu de cette formation est intéressant**

   Pas du tout d'accord — tout à fait d'accord
   1 2 3 4 5

2. **Le contenu de cette formation m'aidera à faire mon travail.**

   Pas du tout d'accord — tout à fait d'accord
   1 2 3 4 5

3. **Je peux partager avec d'autres ce que j'ai appris aujourd'hui**

   Pas du tout d'accord — tout à fait d'accord
   1 2 3 4 5

4. **Je recommanderais cette formation à d'autres personnes.**

   Pas du tout d'accord — tout à fait d'accord
   1 2 3 4 5

5. **La vitesse de l'animateur est**

   a. Très lente b. Correcte c. Trop rapide

6. **Veuillez nous faire part de vos préoccupations concernant le partage de cette formation avec d'autres personnes.**

7. **Je pourrais utiliser avec succès la technologie (par exemple, Zoom, Teams, Mentimeter, Google Forms) employée dans cette formation.**

   Pas du tout d'accord — tout à fait d'accord
   1 2 3 4 5

8. **Veuillez partager toute autre information que vous jugez importante pour les animateurs.**

Annexe M : Plan de sécurité

Risque de quelque chose :			
Menace	**Vulnérabilités**	**Capacité existante**	**Capacité requise**

Annexe N : Plan d'action

#	Top 10 des capacités à renforcer	Nécessite des ressources financières supplémentaires ? (O/N)	Quand la capacité sera-t-elle pleinement renforcée ?	Les principales personnes responsables
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				