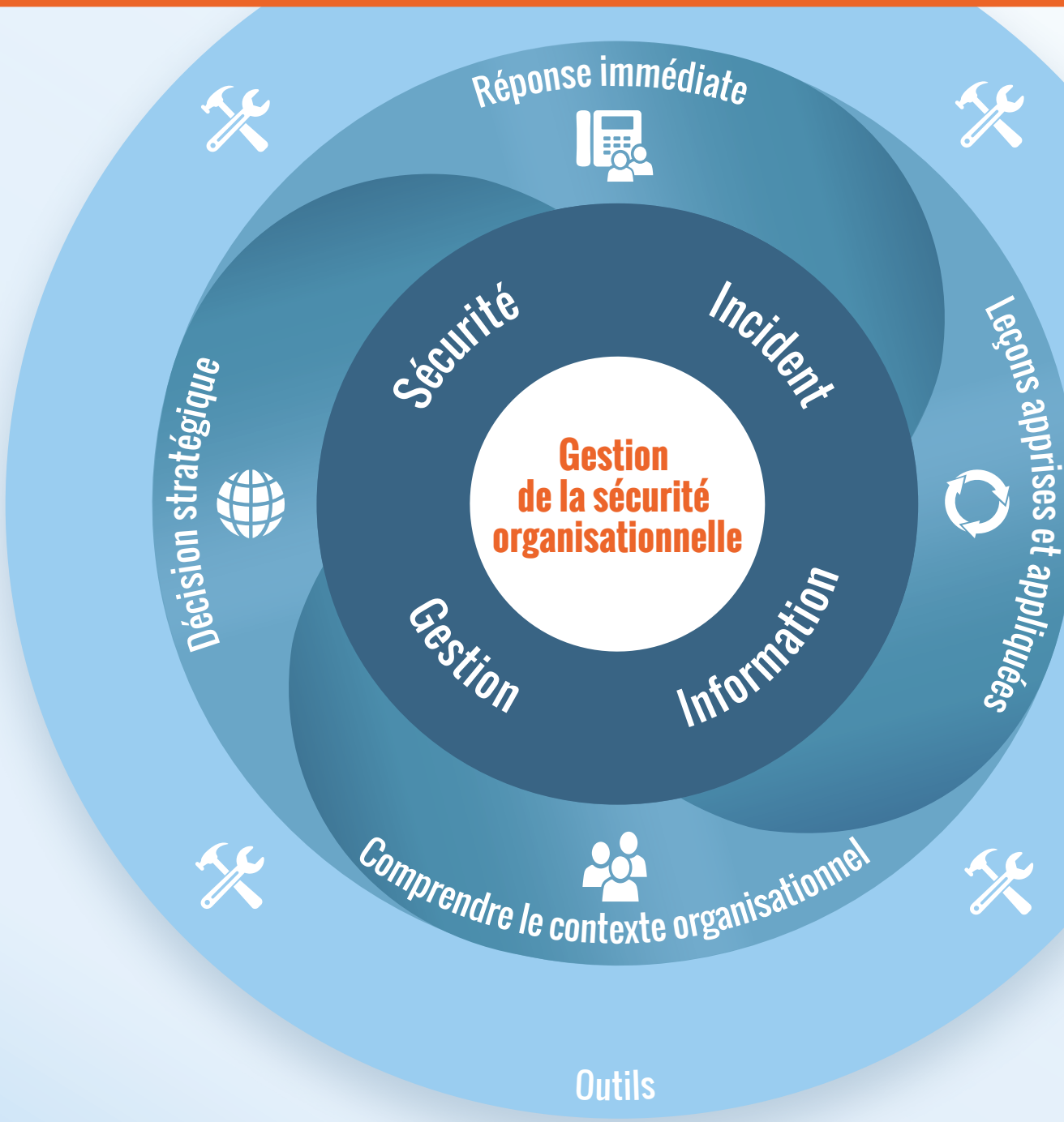
MANUEL DE GESTION DE L'INFORMATION ISSUE DES INCIDENTS DE SÉCURITÉ



Funded by European Union Humanitarian Aid

eisf

redr uk
people and skills for disaster relief

Aid in Danger

Insecurity Insight
Data on People in Danger

Publication date: Septembre 2017

« La gestion de l'information issue des incidents de sécurité implique la collecte, l'enregistrement, l'analyse et l'utilisation des informations afin de maintenir la sécurité du personnel et permettre l'accès aux bénéficiaires.Une bonne gestion de l'information issue des incidents de sécurité trouve le juste équilibre entre ses avantages et les coûts administratifs liés à son système de gestion. »

REMERCIEMENTS

Ce manuel a été élaboré en collaboration entre RedR UK, Insecurity Insight et EISF, dans le cadre du projet GIIS (Gestion de l'information issue des incidents de sécurité), financé par La Direction générale pour la protection civile et les opérations d'aide humanitaire européennes. Pour plus d'informations, veuillez consulter la page du projet sur le site de RedR.

Le coordinateur du projet Marine Meunier (RedR UK), Christina Wille (Insecurity Insight) et Lisa Reilly (EISF) ont largement contribué à ce manuel. L'éditeur est Adelicia Fairbanks (EISF). L'équipe du projet aimerait remercier les membres du Groupe Consultatif et d'autres contributeurs – trop nombreux pour les mentionner individuellement – pour avoir partagé avec nous leur expertise, leurs outils et leurs remarques très utiles. Le projet GIIS reconnaît l'ampleur des contributions apportées et la volonté et l'implication des organisations et des individus.

AVERTISSEMENT

Ce manuel est l'un des éléments d'un projet plus vaste visant à renforcer les capacités dans les secteurs humanitaires et de développement ; d'autres activités de renforcement des capacités complètent cet outil. Ce document reflète les pratiques actuelles dans le secteur, fournit des recommandations et des observations, y compris des points de vue ou des recommandations de tiers. Il n'est pas prescriptif, et c'est un travail en évolution.

RedR UK, Insecurity Insight et EISF ne seront pas tenus responsables au regard de la loi pour toute perte, dommage ou problèmes, car le projet GIIS s'est efforcé d'assurer l'exactitude et la qualité des informations présentées dans ce manuel découlant de l'utilisation ou de l'incapacité d'utiliser ou d'interpréter toute information venant de celui-ci. RedR UK, Insecurity Insight et EISF n'assumeront donc aucune responsabilité et ne seront pas responsables envers les utilisateurs, ou toute autre personne, pour d'éventuels dommages causés par les décisions ou actions prises en se basant sur les informations fournies dans ce manuel.

Les informations contenues dans ce document sont fournies « telles quelles », sans aucune condition, garantie ou autre modalité, et toute utilisation des informations contenues dans ce document est entièrement à vos risques et périls.

Conçu par Tutaev Design
Traduit par Abdoulaye Ndiaye et revisé par Emmanuelle Strub

ABRÉVIATIONS

AiD	Aid in Danger
AWSD	Aid Worker Security Database
EISF	European Interagency Security Forum
FAQ	Questions fréquemment posées
Siège	Siège Social
CICR	Comité International de la Croix-Rouge
OGI	Organisation Gouvernementale Internationale
DiH	Droit International Humanitaire
ONGI	Organisation Non Gouvernementale Internationale
ISO	Organisation Internationale de Normalisation
ONGL	Organisation Non Gouvernementale Locale
ONG	Organisation Non Gouvernementale
PSP	Premiers Secours Psychologiques
EAS	Exploitation et Abus Sexuels
PFS	Point Focal de Sécurité
GIIS	Gestion de l'Information issue des Incidents de Sécurité
SLT	Saving Lives Together
POS	Procédure Opérationnelle Standard
UNDSS	Département de la Sureté et de la Sécurité des Nations Unies
OMS	Organisation Mondiale de la Santé

TABLE DES MATIERES

INTRODUCTION

À PROPOS DE CE MANUEL

La gestion de l'information issue des incidents de sécurité (GIIS) est la collecte, la notification, l'enregistrement, l'analyse, le partage et l'utilisation des informations (y compris les données) liées à un incident de sécurité. La gestion de l'information issue des incidents de sécurité est un élément clé de la gestion globale des risques de sécurité d'une organisation, qui vise à renforcer sa sécurité organisationnelle afin d'améliorer son accès aux populations dans le besoin.

Le manuel GIIS vise à apporter une contribution importante à l'évolution des pratiques liées à la gestion de l'information issue des incidents de sécurité au sein des organisations non gouvernementales (ONG).

Le manuel vise à aider ses utilisateurs à établir et à développer une gestion efficace de l'information pour les systèmes de suivi et de surveillance des événements de sécurité, à l'interne et à l'externe, à travers l'organisation et également du secteur.

Ce document fait partie d'un projet plus large de GIIS qui vise à renforcer les réponses humanitaires aux crises en renforçant la capacité des ONGs à améliorer la gestion de l'information issue des incidents de sécurité et en améliorant leur capacité à partager les informations sur les incidents de manière sûre et appropriée et soutenir une bonne prise de décision à travers les différents niveaux d'une organisation.

Le manuel GIIS présente un large éventail d'outils et de conseils, allant des conseils sur la conception d'un rapport d'incident de sécurité efficace au partage efficace des informations sur les incidents de sécurité avec un large éventail de parties prenantes concernées. L'approche et le vocabulaire de gestion des risques de sécurité présentés dans ces lignes directrices suivent la norme mondiale publiée par l'Organisation internationale de normalisation (ISO), « Gestion des risques – Principes et lignes directrices » (désormais ISO 31000: 2009).

Ce manuel traite de la gestion de l'information issue des incidents de sécurité et non de la gestion des incidents de sécurité en tant que tels.

La plupart de ce manuel est applicable à tous les types d'incidents, y compris les incidents critiques, c'est-à-dire les événements qui perturbent les opérations normales de routine et qui nécessitent une réponse de gestion de crise de l'organisation. Tout au long, le terme 'incident' sera utilisé pour désigner tous les types d'incidents. Lorsqu'est fait référence à un incident critique, cela sera spécifié. Il peut parfois être fait référence à des « incidents non critiques », qui se rapportent à tous les incidents qui ne seraient pas considérés comme critiques et qui ne nécessitent donc pas de réponse de gestion de crise. Cependant, il est important de souligner que même si certains incidents peuvent être jugés critiques par une organisation, ils peuvent ne pas être jugés comme tels par une autre organisation qui a la capacité de gérer l'incident au moyen de procédures de gestion de routine.

Bien que souvent sous-évalué, la collecte et la gestion de l'information issue d'incidents jugés critiques, y compris les incidents évités de justesse, peuvent être tout aussi importantes pour l'analyse et la prise de décision en matière de sécurité que les informations sur les événements critiques. Ce manuel fournit donc des outils pour aider à élaborer des normes pour la déclaration et la gestion de l'information issue de tous les incidents, y compris ceux qui se produisent plus fréquemment et qui ne sont généralement pas jugés critiques.

Ce manuel reflète les pratiques actuelles dans le secteur et fournit des recommandations et des observations pour les ONG. Il s'appuie sur les ressources d'un large éventail d'experts, y compris l'European Interagency Security Forum (EISF), Insecurity Insight, RedR UK et de nombreuses organisations membres et de réseaux plus larges. Tout en utilisant les outils et les conseils existants, il vise à éviter la duplication en mettant en évidence et en tirant parti des éléments de la gestion de l'information issue des incidents de sécurité. Ce manuel n'est pas prescriptif, mais propose plutôt un large éventail d'options permettant aux organisations de renforcer leur gestion de l'information sur les incidents de sécurité.

Bien que ce manuel ait été rédigé en mettant l'accent sur les organisations et les opérations humanitaires, l'information est largement applicable à d'autres ONG, en particulier aux organisations axées sur le développement.

Cette version du manuel (publiée en septembre 2017) intègre les commentaires et les contributions des parties prenantes du secteur humanitaire et du développement.

Ceci est un document disponible gratuitement, et sera en ligne en anglais, français et arabe.

À qui ce manuel est destine ?

Le manuel GIIS s'adresse à toutes les personnes ayant un niveau de responsabilité quelconque en matière de gestion de l'information issue des incidents de sécurité au sein d'une organisation non gouvernementale, quel que soit leur poste ou leur lieu. Il est conçu comme un outil pour les conseillers, les gestionnaires, les points focaux et les analystes de sécurité, ainsi que pour les cadres supérieurs et les directeurs de projets / programmes ayant une responsabilité de sécurité au sein des ONG et comme s'adressant principalement aux praticiens.

Comment utiliser ce manuel ?

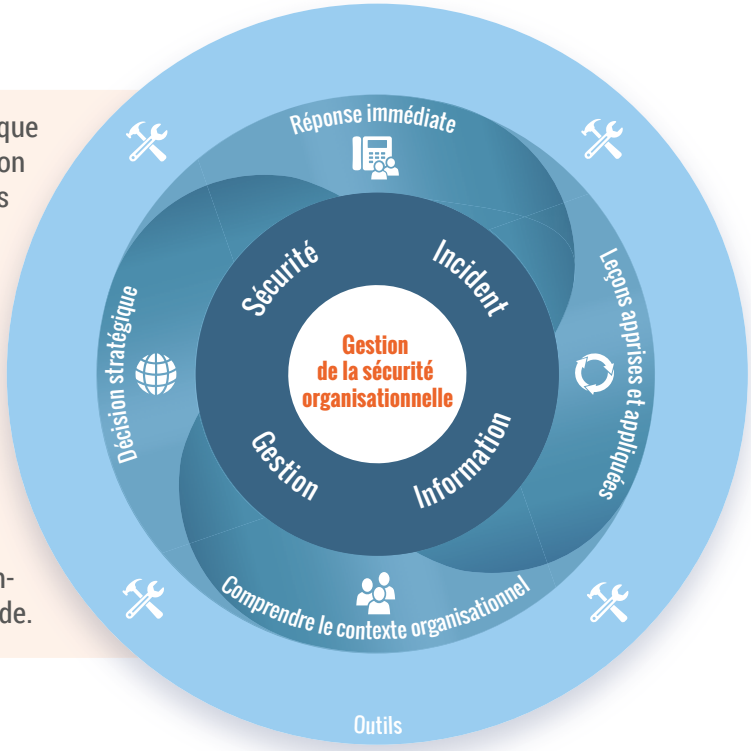
Le manuel GIIS est divisé en chapitres qui donnent un aperçu de la gestion de l'information issue des incidents de sécurité :

- Le manuel introduit d'abord le concept de GIIS et comment celui_ci s'intègre dans la gestion plus large des risques de sécurité d'une organisation.
- Il présente quatre objectifs clés de GIIS, en soulignant les étapes clés impliquées dans la gestion efficace de l'information issue des incidents de sécurité pour atteindre chaque objectif.
- Les outils sont référencés tout au long du texte et peuvent être trouvés à la fin de ce manuel.

Le diagramme suivant illustre les différentes composantes de la gestion de l'information issue des incidents de sécurité. La structure de ce manuel suit ce diagramme et chaque section du manuel indiquera quelle partie du cycle est en cours de discussion.

Le cycle GIIS : la sécurité organisationnelle afin d'obtenir un accès sans entrave à la livraison de l'aide

Le diagramme est cyclique pour montrer que la gestion de l'information issue des incidents de sécurité est un processus continu dans lequel tous les éléments s'alimentent les uns les autres pour atteindre quatre objectifs principaux. Au cœur de l'information issue des incidents de sécurité, il y a la sécurité organisationnelle avec comme objectif l'accès sans entraves de la livraison de l'aide.



Ce manuel fournit des points de discussion, des conseils et des modèles suggérés pour les quatre objectifs principaux de la gestion de l'information issue des incidents de sécurité qui se rapportent à quatre périodes distinctes et à différents niveaux d'orientation organisationnelle :

Objectif 1 : Informer la réaction immédiate et la réponse à un incident de sécurité. Le but est de s'assurer que l'information est recherchée et utilisée pour informer la réponse immédiate à l'incident. Cela se produit généralement au niveau du terrain et / ou du pays peu après que l'incident ait eu lieu.

Objectif 2 : Mettre en œuvre les leçons apprises après un incident de sécurité pour des actions de suivi et de prévention. L'objectif est de comprendre ce qui s'est passé en vue de planifier et de mettre en œuvre les changements et les procédures nécessaires pour traiter le risque d'événements futurs similaires, en mettant l'accent sur la prévention. Cela se produit généralement au niveau du pays / siège peu après l'événement de sécurité.

Objectif 3 : Comprendre le contexte de sécurité des ONG. Le but est d'améliorer les connaissances contextuelles en utilisant des données d'incidents internes et externes. Cela aidera à éclairer les décisions stratégiques, la communication globale et l'autoréflexion parmi les agences d'aide. Cela se produit généralement au niveau des pays et au niveau de la direction au sein du siège, et il est préférable de faire une révision régulièrement.

Objectif 4 : Informer la prise de décision stratégique dans une organisation. L'objectif est de faire le point sur la nature changeante des incidents, de comprendre les environnements de travail les plus difficiles, l'exposition globale de l'organisation au risque et d'identifier les meilleures réponses stratégiques. Cela se produit au niveau du pays, de la région et du siège dans un délai raisonnable après un événement de sécurité et pendant les phases de planification et de programmation.

Il est important de considérer les quatre objectifs comme faisant partie d'un ensemble, chacun d'entre eux alimentant l'objectif global de réduire les risques de sécurité pour l'organisation, améliorant ainsi l'accès à l'aide aux populations dans le besoin.

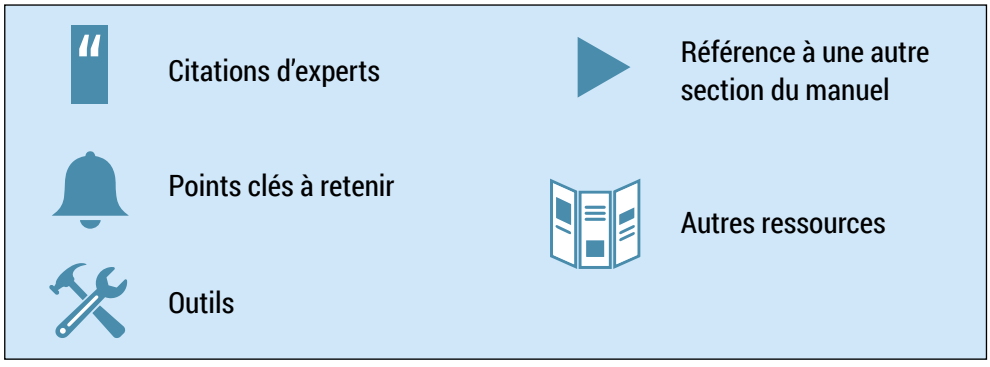
Chaque section fournit des conseils sur les étapes clés et sur la façon de créer des normes et des catégorisations bien définies qui permettent aux organisations d'analyser les données plus facilement. Lorsque les données sont partagées entre les organisations, les définitions standards et les procédures éthiques sont essentielles.

Les organisations et leur personnel sont invités à :

- Utiliser ce manuel pour mieux comprendre la gestion de l'information issue des incidents de sécurité et les étapes clés à suivre pour améliorer la gestion globale des risques de sécurité de leur organisation.
- Utiliser les outils fournis à la fin de ce manuel pour améliorer le système de gestion de l'information issue des incidents de sécurité de leur organisation. Trouvez une liste des outils ici.
- Utiliser la grille d'auto-évaluation 'Outil 1 : Grille d'auto-évaluation GIIS' pour évaluer les besoins de gestion de l'information issue des incidents de sécurité de leur organisation. Cet examen devrait être effectué à intervalles réguliers. Après une période définie, les organisations devraient revoir leurs progrès depuis leur auto-évaluation initiale.

Ce manuel peut être consulté dans son ensemble. Des chapitres seuls, ou des outils, peuvent être fournis à un personnel spécifique. Les quatre principaux objectifs décrits dans ce manuel sont distincts mais interdépendants : l'amélioration des pratiques pour atteindre un objectif aidera l'organisation à atteindre les autres objectifs et, dans l'ensemble, contribuera à la préparation opérationnelle et à la sécurité organisationnelle.

Pour plus de facilité, les icônes suivantes sont utilisées pour guider l'utilisateur dans l'identification des types de ressources fournies :



Pour faciliter la navigation, des outils et des références à des ressources externes, ainsi que des renvois à d'autres sections du manuel, sont en lien hypertextes.

Les boîtes sur le côté droit de chaque page sont en lien hypertextes au début du chapitre identifié.

Les références dans les notes de bas de page sont reliées aux « Références et Bibliographie » à la fin du manuel.

Définitions clés

Analyse : Le processus consistant à transformer des faits, des figures, des objets… non organisés en informations significatives qui peuvent être utilisées à différentes fins, telles que la prise de décision.

Compétences analytiques : La capacité de visualiser, articuler, conceptualiser ou résoudre des problèmes complexes ou simples, y compris la capacité d'appliquer une pensée logique pour décomposer des problèmes complexes en composants élémentaires.

Crise : Un événement nécessitant la meilleure réponse possible grâce à une gestion ou à des approches de routine. Cette réponse peut nécessiter soit une contribution supplémentaire par une gestion spécifique, soit être traitée au niveau supérieur (probablement au siège). Nombres d'organisations définiront comme 'critique' un incident qui doit être géré comme une situation de crise.

Données : Faits et statistiques recueillis ensemble pour référence ou analyse ; des informations brutes ou aléatoires qui se réfèrent ou sont définis par des conditions, des idées ou des objets.

Devoir de Protection : ou Duty of Care en anglais : « la responsabilité ou l'obligation légale d'une personne ou d'un organisme d'éviter les actes ou omissions, raisonnablement prévisibles, susceptibles de nuire à autrui[1] ». Les organisations devraient également considérer leur obligation morale[2].

Événement : Une occurrence ou un changement d'un ensemble particulier de circonstances. Dans ce manuel, les termes « événement » et « incident » sont utilisés indifféremment.

Flux d'information horizontal : Le partage d'informations entre les organisations ou entre les organisations et les parties prenantes.

Incident : Tout événement dans lequel la sécurité de manière globale ou la sécurité du personnel est compromise ; toute personne à charge ou toute autre tierce partie blessée dans le cadre des activités de l'organisation ; les biens personnels ou les biens de l'organisation sont volés, endommagés ou mis en péril ; lorsqu'il y a interférence dans la livraison de l'aide et/ou que le travail indépendant de l'organisme d'aide est compromis, y compris les atteintes à la réputation.

> **NOTE :** Les incidents peuvent être organisationnels, opérationnels (affectant directement l'organisation et sa capacité à fournir de l'aide) ou externes (affectant d'autres personnes extérieures à l'organisation). Signaler les deux peut être bénéfique pour la gestion de l'information issue des incidents de sécurité.

Les incidents peuvent en outre être classés comme suit :

Incident critique : Un incident qui perturbe les opérations normales et de routine. Un incident critique peut entraîner la mort, une blessure grave ou une maladie et

[1] Kemp, E. and Merkelbach, M. (2011). « Pouvez-vous être poursuivi » ? « Responsabilité juridique des organisations internationales d'aide humanitaire envers leur personnel », Initiative de gestion de la sécurité.

[2] Kemp, E. & Merkelbach, M. (2016). Devoir de protection: Examen de la décision Dennis / Norwegian Refugee Council et de ses implications. European Interagency Security Forum (EISF).

déclencher une réponse de gestion de crise d'une organisation. Ces incidents ont tendance à exiger une réponse urgente.

Les accidents évités de justesse : Evénements qui ont presque causés des dommages, des pertes à l'organisation, à son personnel ou à ses programmes, ou qui auraient pu causer des blessures graves, la mort ou des enlèvements mais qui n'ont causés que des dommages mineurs. Pouvant aussi être appelé un « quasi incident ».

NOTE : Les entraves administratives (par exemple, les barrières excessivement bureaucratiques en matière de douanes et barrières ponctuelles, l'octroi de visas ou de permis de voyage aux zones sinistrées, etc.) peuvent être considérées et signalées comme des incidents car elles peuvent également fournir des informations sur le contexte.

Accidents : Evénements aléatoires qui causent des dommages ou des pertes à une organisation, à son personnel ou à ses programmes. En revanche, les 'incidents' sont motivés par la volonté des individus de causer du tort à des personnes ou des entités, de saisir des biens ou de perturber la livraison de l'aide, soit en ciblant directement le personnel de cette agence ou de l'agence elle-même. Peu importe si un événement est un incident de sécurité ou un accident, les deux devraient être signalés. Cependant, lorsque ce manuel fait référence à des 'incidents' ou à des « incidents de sécurité », il se réfère principalement à des événements liés à la sécurité. Néanmoins, le lecteur est invité à garder à l'esprit que les modèles, les outils et les conseils contenus dans le présent document fournissent également des conseils utiles pour la gestion de l'information relative aux accidents, tels que les accidents de la route.

Enregistrement des incidents : Il s'agit de l'enregistrement formel des incidents dans un système de base de données qui permettra à l'organisation de suivre les événements, les actions de suivi potentielles, l'analyse de support et la tendance des données.

Rapport d'incident : Enregistrement formel ou informel des faits liés à un incident. Cette déclaration des faits peut être faite oralement ou à l'écrit, au moment de l'événement ou à la fin de l'incident. Un rapport d'incident est généralement fait en utilisant un document modèle. Il peut servir pour des actions de réponse immédiate ou une analyse plus approfondie ultérieurement. Ces rapports d'incidents impliquent la transmission d'informations selon un flux de notification d'incidents prédéfinis.

Information : Ce qui est véhiculé ou représenté par un processus particulier ou une séquence de données. C'est la communication ou la réception de la connaissance ou de l'intelligence. Les données brutes sont transformées en informations par analyse.

Gestion de l'information : Terme générique utilisé pour décrire les procédures et les lignes directrices visant à :

- Réglementer les types d'informations que les organisations collectent, stockent et communiquent ;
- Réduire les risques pour le personnel et les organisations inhérentes à ces processus ; et
- Veiller à ce que les personnes concernées puissent avoir accès à l'information en temps opportun[3].

[3] Ayre, R. (2010). *Le défi de la gestion de l'information: un exposé sur la sécurité de l'information pour les organisations humanitaires non gouvernementales sur le terrain.* EISF.

Détenteur de l'information : L'individu (ou groupe d'individus) ayant la capacité de créer, éditer, modifier, partager et restreindre l'accès aux données.

Sécurité de l'information : La « préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ... D'autres propriétés, comme l'authenticité, la responsabilité, la non répudiation et la fiabilité, peuvent également être incluses[4] ».

Personnel : Personnel, bénévoles et toute autre personne relevant de l'organisation, y compris les consultants, les partenaires, les visiteurs, etc.

Risque : « L'effet de l'incertitude sur les objectifs[5] ». Un risque peut également être la probabilité d'une menace affectant l'organisation et l'impact qu'elle aura si elle est effective.

Évaluation des risques : Processus visant à identifier les menaces à la sécurité et à la sûreté susceptibles d'affecter le personnel, les atouts et les programmes, également analyser leur probabilité et leur impact, afin de mesurer le degré de risque impliqué.

Sûreté (Security) : Absence de risque ou de préjudice résultant d'actes intentionnels de violence, d'agression et / ou d'actes criminels contre le personnel, les biens ou les propriétés de l'organisation.

Sécurité (Safety) : Absence de risque ou de préjudice résultant d'actes non intentionnels, accidentels ou fortuits.

Information issue des incidents de sécurité : Données et informations liées à un événement de sécurité spécifique ou à une séquence d'événements.

Gestion de l'information issue des incidents de sécurité : Collecte, rapport, enregistrement, analyse, partage et utilisation d'informations (y compris des données) liées à un incident de sécurité dans le but général d'obtenir un accès sans entraves à l'aide.

Sécurité de l'information : Les bonnes solutions techniques et de gestion qui s'appuient sur une formation efficace du personnel et des ressources suffisantes, constituant une forte culture de gestion de l'information dans laquelle le personnel applique des politiques de sécurité presque automatiquement.

- **Sécurité physique :** Protection du matériel informatique, des locaux servant de bureau et des biens de l'organisation contre les circonstances physiques et les événements qui pourraient causer de graves dommages ou pertes, y compris le vol, le feu et les catastrophes naturelles.

- **Sécurité numérique :** La protection des fichiers électroniques stockés sur les ordinateurs – depuis les téléphones portables et les assistants numériques personnels vers les clés USB et les ordinateurs - contre l'accès non autorisé, la corruption, la perte, l'utilisation abusive ou la destruction. Les mesures de sécurité numériques de base doivent toujours être respectées, telles que les mots de passe protégeant les comptes d'utilisateur, les réseaux Internet sans fil et les documents sensibles.

- **Accessibilité :** La catégorisation de l'information et du personnel afin que l'information ne soit accessible qu'au personnel pertinent ou ayant une ancienneté suffisante.

4 ISO/IEC 27000:2014
5 ISO 31000:2009

- **Sauvegardes :** Instructions sur la fréquence et la façon de sauvegarder les fichiers, en veillant à ce que l'interruption du programme soit réduite au minimum, car le risque de dommages matériels ou de perte ne peut jamais être complètement éliminé.

- **Destruction de l'information :** Des lignes directrices claires sur comment et quand l'information (dans sa forme matérielle ou numérique) doit être détruite, en sachant que cela doit être fait rapidement. Dans les environnements à haut risque, en particulier là où une surveillance sophistiquée est suspectée, certains types d'informations ne devraient peut-être pas être collectés ou enregistrés du tout. En outre, la gestion sensible de l'information devrait être clairement séparée de la gestion courante de l'information. Ainsi, si un contexte qui se détériore exige une destruction rapide des informations sensibles, il sera possible d'identifier rapidement ce qui doit être détruit.

- **Sécurité des communications :** Une politique de gestion de l'information doit identifier : comment et quoi communiquer dans des environnements particuliers. Les informations sont plus vulnérables lorsqu'elles sont communiquées : la radio n'est pas sécurisée, les appels téléphoniques peuvent être interceptés, les courriels interceptés, etc.

Gestion des risques de sécurité : La gestion des risques de sécurité est le processus d'identification, d'analyse, d'évaluation et d'atténuation des risques de sécurité pouvant affecter la capacité de l'organisation à fournir de l'aide.

Cadre de gestion des risques de sécurité : Ensemble de procédures, de protocoles, de plans, de mécanismes et de responsabilités qui appuient la réduction des risques de sécurité pour le personnel, les programmes et l'organisation.

Violence sexuelle : « Tout acte sexuel, tentative d'obtenir un acte sexuel, les remarques ou avances sexuelles non désirées, les actes visant à harceler la sexualité d'une personne, les recours à la coercition, les menaces verbales ou physiques par quelque personne que ce soit dans tout cadre, y compris mais non sans limites la maison ou le lieu de travail. La violence sexuelle prend de nombreuses formes, y compris le viol, l'esclavage sexuel et/ou la traite, la grossesse forcée, le harcèlement sexuel, l'exploitation et/ou les abus sexuels et l'avortement forcé[6] ».

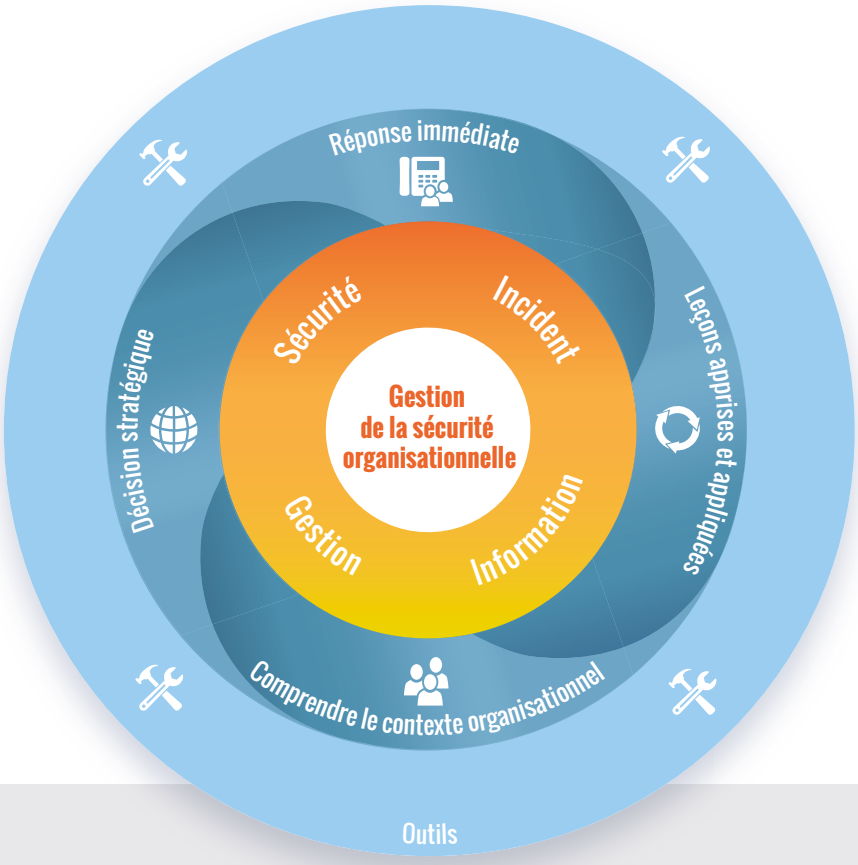
Typologie des incidents : La classification des incidents selon les types généraux.

Outil 2: Typologie des incidents propose une typologie utilisée par Insecurity Insight dans ses analyses et est basée sur les typologies utilisées par plusieurs organisations.

Flux d'informations vertical : Informations circulant de haut en bas dans la structure d'une organisation. Lorsqu'une partie prenante d'une région recueille des rapports d'incident et les envoie au siège pour une analyse plus détaillée, il s'agit d'un flux d'information ascendant. À mesure que les informations sont analysées et que les conclusions sont tirées, elles peuvent être diffusées dans le sens descendant vers le personnel de terrain.

[6] Inter-Agency Standing Committee (IASC). (2015). *Lignes directrices pour l'intégration des interventions de lutte contre la violence sexiste dans l'action humanitaire: Réduire les risques, promouvoir la résilience et favoriser le relèvement.*

CHAPITRE 1 : INTRODUCTION A LA GIIS



Cette section présente la gestion de l'information issue des incidents de sécurité et explique comment elle s'intègre dans une approche plus large de gestion des risques de sécurité, afin de renforcer la prévention et la préparation en cas d'incidents.

- Qu'est-ce que la gestion de l'information issue des incidents de sécurité ?
- Principaux défis dans la gestion de l'information issue des incidents de sécurité
- Gestion des risques de sécurité et GIIS
- Compétences en sécurité du personnel et GIIS
- Sécurité de l'information
- Gestion des incidents et GIIS: les avantages de la préparation organisationnelle
- Devoir de protection

Outils pertinents

- Outil 1: Grille d'auto-évaluation GIIS

Qu'est-ce que la gestion de l'information issue des incidents de sécurité ?

La gestion de l'information issue des incidents de sécurité concerne la collecte, la notification, l'enregistrement, l'analyse, le partage et l'utilisation des informations (y compris les données) liées à un événement ou une séquence d'évènements de sécurité.

Une gestion efficace de l'information issue des incidents de sécurité améliore les capacités d'une ONG à partager et à utiliser les informations sur les incidents en interne et en externe d'une manière sûre et appropriée afin de prendre de bonnes décisions aux différents niveaux de l'organisation.

La gestion de l'information issue des incidents de sécurité ne devrait pas être limitée aux cas graves de décès, de blessures ou d'enlèvements, ni aux pays les plus touchés par les incidents. Il est bénéfique que tous les incidents affectant la fourniture de l'aide soient signalés et analysés par les organisations. Cela permet aux organisations (entre autres) de :

- Adopter immédiatement des mesures de réduction des risques appropriées et efficaces, permettant aux responsables d'être informés rapidement afin qu'ils puissent offrir le soutien nécessaire au personnel affecté ou impliqué dans un incident ;
- Améliorer l'analyse du contexte en établissant des tendances et des modèles émergents sur la base desquels la hiérarchie peut prendre des décisions opérationnelles claires ;
- Informer les parties prenantes externes des menaces et des risques potentiels afin qu'ils puissent également mettre en place des réponses face à ces risques ;
- Avoir un enregistrement complet et institutionnalisé des incidents de sécurité.

Les étapes clés de la gestion de l'information issue des incidents de sécurité sont les suivantes :

- Signaler.
- Enregistrer.
- Analyser les données collectées lors d'un incident.
- Partager les informations (en interne et en externe).
- Prise de décision sur le terrain, généralement en réponse immédiate à un incident.
- Prise de décision au niveau national ou régional, en utilisant les informations sur les incidents signalés afin de mettre en œuvre les leçons apprises et ainsi améliorer les procédures de sécurité.
- L'analyse des données relatives aux incidents afin d'identifier les tendances et les modèles.
- Utiliser l'analyse des tendances afin de renseigner l'analyse contextuelle et l'évaluation des risques et de prendre des décisions éclairées sur les meilleures mesures à mettre en place afin d'améliorer la sécurité organisationnelle.
- La prise de décision stratégique au niveau du siège impliquant l'utilisation d'analyses de tendances établies à partir d'incidents signalés afin de prendre des décisions éclairées à tous les niveaux de l'organisation.

Ces étapes clés seront abordées plus en détail dans le « Chapitre 2 : Les quatre objectifs de la gestion de l'information issue des incidents de sécurité ».

Principaux défis dans la gestion de l'information issue des incidents de sécurité

Les défis de la gestion de l'information issue des incidents de sécurité peuvent être liés à des facteurs individuels et organisationnels.

Trop peu de rapports d'incidents
De nombreux incidents ne sont jamais signalés ou enregistrés. Les incidents non critiques sont plus souvent signalés que les incidents évités de justesse, même si les deux sont sous-déclarés. Cela ne signifie pas que ces types d'incidents ne se produisent pas, mais qu'ils attirent moins l'attention par rapport à d'autres incidents dans des environnements plus hostiles.

Les incidents non critiques dans des environnements hostiles peuvent indiquer une détérioration de la situation et une aggravation des tensions et doivent être signalés au responsable hiérarchique ou au point focal de sécurité approprié (PFS). Ils peuvent suggérer la nécessité de revoir l'analyse du contexte et des risques pour l'organisation.

Différences de définitions
Les perceptions quant à ce qui constitue un incident peuvent varier considérablement entre les organisations, ainsi qu'entre les individus d'une même organisation. Une ONG peut estimer qu'une courte rafale de coups de feu pendant la nuit vaut la peine d'être signalée, tandis qu'une autre ne le fera pas si les coups de feu sont fréquents dans l'environnement opérationnel. De même, le personnel international et national peut avoir des points de vue différents sur ce qui représente un incident nécessitant une notification.

Les personnes en charge de la sécurité doivent donner des directives claires sur ce qui constitue un incident nécessitant d'être rapporté dans des endroits donnés, afin d'assurer une approche cohérente dans toute l'organisation.

Tout le personnel devrait avoir une compréhension commune de la terminologie associée à la gestion de l'information issue des incidents de sécurité afin de pouvoir communiquer efficacement, tant en interne qu'en l'externe. Un manque de cohérence dans l'utilisation des termes est problématique pour l'analyse. Par exemple, les documents de sécurité peuvent mentionner des incidents connexes ou similaires tels que 'vol' et 'brigandage' sans expliciter la distinction. Afin de regrouper et de comparer les données de différentes organisations, ainsi que dans différents pays au sein d'une organisation, il est nécessaire avoir des définitions communes.

Risque réputationnel
Un incident de sécurité indique que quelque chose s'est mal passée quelque part. Même si les organisations humanitaires sont rarement responsables d'un incident de sécurité, elles peuvent souvent identifier des éléments liés à leurs procédures ou au comportement du personnel qui, sous une forme ou une autre, ont contribué à rendre l'événement possible ou les conséquences de l'incident. En raison de l'impact potentiel des informations relatives aux incidents sur la réputation d'une organisation, de nombreuses ONG peuvent préférer ne pas partager les détails de ce qui n'a pas fonctionné, en particulier avec des acteurs externes.

« Apprendre des quasi-accidents ainsi que des erreurs est une pratique courante dans d'autres industries. Dans le secteur de l'aviation, par exemple, toutes les entreprises sont obligées de signaler toute défaillance, qu'elle soit technique ou humaine, et cela a servi à élaborer des lignes directrices qui ont fait du transport aérien l'un des moyens de transport les plus sûrs aujourd'hui[7]. Par conséquent, partager l'apprentissage de ce qui a mal tourné au sein d'une ONG pourrait aider la communauté humanitaire et de développement dans son ensemble ».

Les organisations ont un avantage à définir clairement au niveau stratégique dans quelles situations partager les informations, en interne, en externe, comment assurer la confidentialité lorsque cela est nécessaire, et quelles étapes suivre afin de gérer l'information de façon pertinente.

Fardeau administratif
Documenter les incidents prend du temps et occupe des ressources humaines importantes. Toutefois, si les organisations réussissent à mettre en place un système efficace, le fardeau administratif peut être réduit, évitant ainsi que le personnel doive passer du temps à chercher les instructions sur la façon d'enregistrer et de signaler les incidents. Fournir des outils et des modèles permet non seulement de rendre l'enregistrement et les rapports plus cohérents au sein de l'organisation, mais aussi moins laborieux et donc plus susceptibles d'être fait.

La politique et les procédures de gestion de l'information issue des incidents doivent être expliquées au personnel et être aussi simples que possible.

La culture organisationnelle
Les cadres, à quelque niveau que ce soit, ont la responsabilité de partager l'information verticalement au sein de l'organisation, par ex. à leur supérieur hiérarchique ou à leur siège, mais les informations appropriées ne sont souvent pas partagées pour diverses raisons. Les cadres (nationaux et internationaux) peuvent ne pas partager l'information verticalement par crainte d'un contrecoup administratif, parce qu'ils ont commis une erreur ou pour « sauver la face ». Les membres du personnel national qui sont en première ligne sont les plus touchés par les morts et les blessés au niveau des ONG, mais ils peuvent penser que s'ils signalent un incident, leur réputation pourrait être affectée. Beaucoup craignent d'être pénalisés en ayant moins de possibilités de promotion ou, dans le pire des cas, de perdre leur emploi.

Toute mauvaise conduite ou violation des procédures de sécurité (ou code de conduite) peut être révélée par l'analyse des incidents. L'organisation peut décider si des mesures disciplinaires sont nécessaires. Cette question fait souvent l'objet de débats au sein des organisations, qui considèrent la question des sanctions comme un facteur supplémentaire de non-signalement. Les organisations auraient avantage à avoir une position claire à ce sujet et à équilibrer ces préoccupations. La réponse aux manquements, aux procédures de sécurité doit être cohérente. Les politiques de sécurité sont inefficaces si la direction ou le personnel de sécurité les enfreint sans conséquence.

Communication entre les organisations
Le partage d'information issue des incidents de sécurité, y compris les rapports d'incidents et de situations entre les organisations, peut s'avérer difficile. Surmonter les principaux défis de la collaboration, tels que la confidentialité, la confiance et la gestion de l'information, sont discutés plus en détail dans l'Objectif 3: Comprendre le contexte opérationnel.

[7] Wille, C. (2016). « Leçons tirées de l'industrie aéronautique: Que pouvons-nous apprendre pour la gestion des risques de sécurité humanitaire ? », *EISF*.

Gestion des risques de sécurité et GIIS

La gestion des risques de sécurité implique une organisation mettant en place des politiques, des protocoles, des plans, des mécanismes et délimitant les responsabilités du personnel pour permettre un meilleur accès humanitaire grâce à une meilleure sécurité organisationnelle. Le diagramme ci-dessous, qui illustre un cadre de gestion des risques de sécurité à l'échelle d'une organisation, présente les différents piliers qui permettent une gestion efficace des risques de sécurité[8].

Gestion des risques de sécurité
Cadre

Alors que le suivi des incidents est mis en évidence comme un pilier essentiel du cadre de gestion de la sécurité (CGS), une bonne gestion de l'information issue des incidents de sécurité peut alimenter et renforcer tous les éléments clés de la gestion des risques de sécurité.

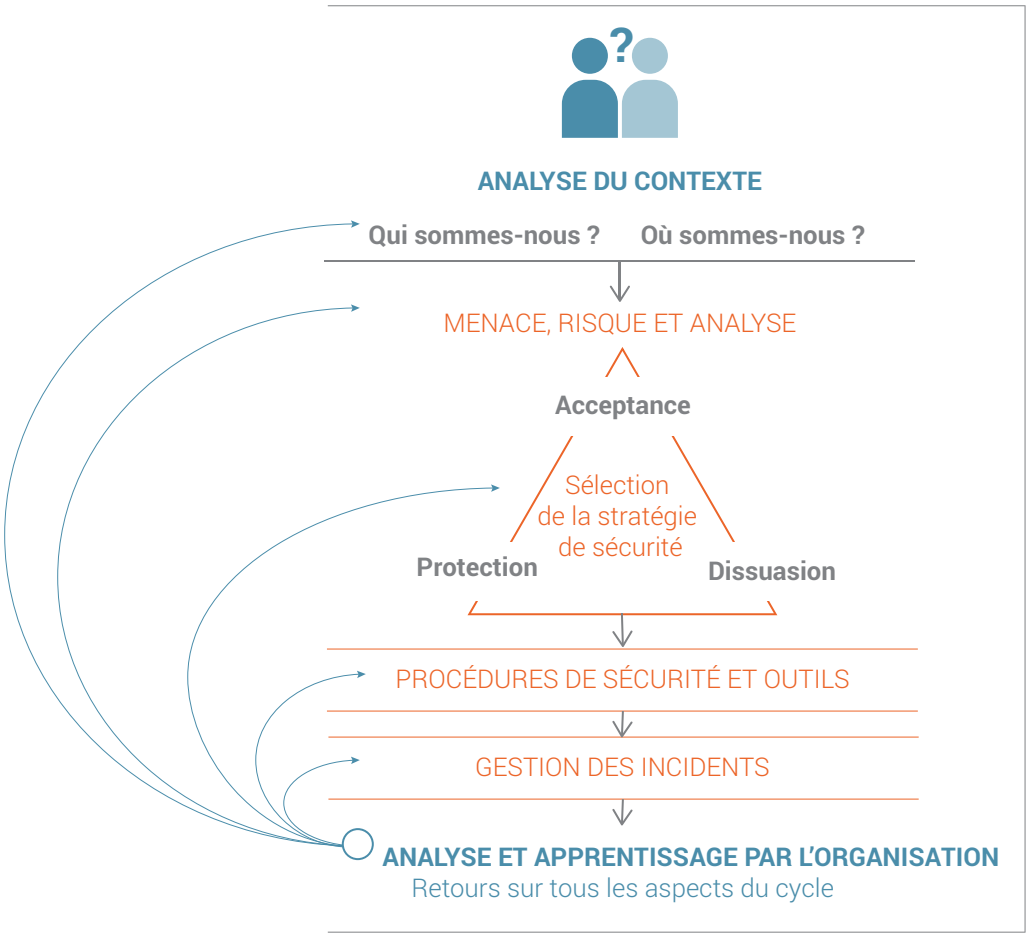
De la mise en place des structures de gestion de crise en temps opportun après un incident critique à l'utilisation des informations non critiques pour informer le personnel des risques liés aux déplacements, la gestion des incidents de sécurité est un élément crucial de la bonne gestion des risques de sécurité.

« Un incident est l'occasion parfaite d'apprendre et de s'améliorer. Son analyse devrait alimenter tout le cadre de gestion de la sécurité ».

Les points focaux de sécurité et les analystes peuvent utiliser les informations provenant d'incidents internes ainsi que d'autres sources pour comprendre le contexte dans différents endroits. Les informations extraites et analysées après un incident devraient nourrir l'analyse des risques en mettant en évidence les menaces et les vulnérabilités dans le contexte donné. Il peut éclairer l'examen des procédures opérationnelles standard (POS) et des plans d'urgence, et peut également être utilisé comme un bon argument à l'appui de l'adoption de changements de politique.

[8] Bickley, S. (2017). *Gestion des risques de sécurité: un guide de base pour les petites ONG.* EISF.

Le diagramme suivant[9] illustre les étapes clés de la gestion des risques de sécurité. Une bonne gestion de l'information issue des incidents permettra aux organisations d'utiliser ces informations pour informer chaque étape de ce processus.



Compétences en sécurité du personnel et GIIS

L'organisme pour les professionnels de la sécurité des ONG, INSSA (International NGO Safety and Security Association), inclut la gestion de l'information comme l'une des compétences clés pour les responsables de la sécurité au niveau national, régional, global et stratégique.

Le personnel à chaque niveau renforcera les systèmes et procédures de gestion des risques de sécurité de l'organisation, et il est extrêmement important de :

- Définir clairement les responsabilités relatives à la sécurité du personnel à chaque niveau ; et
- Veiller à ce que le personnel bénéficie du soutien et de la formation nécessaires pour assumer ses responsabilités en fonction du niveau auquel il se trouve.

Pour plus d'informations sur l'interconnexion entre la gestion des personnes et la sécurité organisationnelle, reportez-vous au « module de gestion des personnes » du guide EISF « Security to Go ».

[9] Ce diagramme provient des cours d'introduction sur la sécurité de RedR UK.

Sécurité de l'information

Dans le contexte de la gestion de l'information issue des incidents, il est important qu'une organisation s'assure que les moyens de communication utilisés pour la communication, la collecte, l'analyse, le partage, le stockage et l'utilisation de l'information sont sécurisés.

Les organisations doivent souvent équilibrer la nécessité d'avoir une gestion de l'information sécurisée avec les contraintes budgétaires. Il est néanmoins crucial d'aborder la sécurité des données, quelles que soient les ressources financières disponibles. Pour une analyse des radios, téléphones mobiles, satellites, courriels et autres aspects techniques de la gestion de l'information, veuillez consulter le guide GPR8 de l'ODI et son chapitre sur les télécommunications et le guide « Security to Go » de l'EISF.

Le devoir légal et éthique des ONG d'assurer la confidentialité des informations est primordial, en particulier s'il s'agit de « données personnelles » – c'est-à-dire toute information relative à une personne identifiée ou identifiable. Les échecs dans la création ou la mise en œuvre de politiques de gestion de l'information peuvent avoir des répercussions négatives sur le personnel et les organisations et entraîner des poursuites et des réparations.

« Une bonne gestion de l'information issue des incidents de sécurité est en partie liée à bien équilibrer les avantages que procurent la collecte, l'enregistrement et la communication de certaines informations et les risques que comportent ces actions ».

Les ONG devraient renforcer leur culture de gestion de l'information en veillant à ce que la sécurité de l'information soit intégrée dans des politiques et des procédures plus larges de gestion des risques, et intégrée de manière transparente dans la réflexion organisationnelle et programmatique. La plupart des risques peuvent être atténués par la sensibilisation à ceux-ci, le bon sens et une bonne discipline : on parle ici de 'bonne gestion interne'. Une bonne gestion comprend le travail administratif, et les copies papier ainsi que la sécurité informatique – la meilleure sécurité informatique au monde ne protège pas du personnel laissant des documents sur son bureau la nuit ou mettant des documents sensibles dans les bacs sans les déchiqueter.

La sécurité de l'information n'est pas un défi à relever uniquement par les départements informatiques. La 'bonne gestion' et les solutions techniques reposent sur une formation efficace du personnel et des ressources suffisantes, et ainsi constitue une culture de gestion de l'information solide dans laquelle le personnel met en œuvre les politiques de sécurité presque automatiquement.

Pour garantir une bonne sécurité de l'information dans la gestion des incidents, les organisations doivent aborder les principaux problèmes suivants à tous les niveaux et toutes les étapes de la collecte, de la notification, de l'enregistrement, de l'analyse, de l'utilisation et du partage des informations :

- **Sécurité physique :** Protection du matériel informatique, des installations de bureau et des biens de l'organisation contre les éléments et les événements pouvant causer des dommages ou des pertes graves, y compris le vol, l'incendie et les catastrophes naturelles.
- **Sécurité numérique :** Protection des fichiers électroniques stockés sur des périphériques informatiques – depuis les téléphones portables et les tablettes ou

ordinateurs portables jusqu'aux ports USB et ordinateurs – contre l'accès non autorisé, la corruption, la perte, l'utilisation abusive ou la destruction. Les mesures de sécurité numériques de base doivent toujours être respectées, telles que la protection avec des mots de passe, des réseaux Internet sans fil et les documents sensibles.

- **Accessibilité :** La classification des informations et du personnel afin que certaines informations ne soient accessibles qu'au personnel ayant des rôles appropriés ou ayant une ancienneté adéquate (voir « Catégories d'informations » dans « Objectif 3 »).
- **Sauvegardes :** Directives sur la façon de sauvegarder les fichiers, et à quelle fréquence, en veillant à ce que l'interruption du programme soit réduite au minimum, car le risque de dommage ou de perte de matériel ne peut jamais être complètement éliminé.
- **Destruction de l'information :** Des directives claires sur la manière et le moment où l'information doit être détruite (sous sa forme papier et électronique), en sachant que cela doit être fait rapidement. Dans les environnements à forte menace, en particulier ceux dans lesquels une surveillance sophistiquée est suspectée, certains types d'informations ne devraient peut-être pas être collectés et enregistrés. De plus, la gestion de l'information sensible devrait être clairement séparée de la gestion courante de l'information. Ainsi, si un contexte qui se détériore exige une destruction rapide d'informations sensibles, il sera possible d'identifier rapidement ce qui doit être détruit.
- **Sécurité des communications :** Une politique de gestion de l'information devrait identifier comment et quoi communiquer dans des environnements particuliers. L'information est peut-être la plus vulnérable lorsqu'elle est communiquée: la radio n'est pas sécurisée, les appels téléphoniques peuvent être écoutés, les courriels interceptés, etc. ...

Voir le guide GPR8 de l'ODI pour un chapitre sur la sécurité des communications.

« Security in a Box »

Un élément clé de la sécurité de l'information est d'avoir de solides outils et stratégies de sécurité numérique. « Security in a Box » est une initiative développée conjointement par Front Line Defenders et Tactical Technology Collective, qui a abouti à la création de guides communautaires fournissant des conseils personnalisés sur les outils et les tactiques adaptés aux besoins de groupes particuliers. Ceux-ci couvrent les principes de base des plates-formes de réseaux sociaux et des téléphones mobiles, y compris des conseils sur la façon de les utiliser de manière plus sécurisée. Les outils et les guides tactiques de Security in a Box offrent des instructions étape par étape sur la façon d'installer et d'utiliser les logiciels et services de sécurité numérique les plus essentiels (ces ressources peuvent être téléchargées depuis leur site Web).

Gestion des incidents et GIIS : les avantages de la préparation organisationnelle

Bien que la gestion des incidents ne soit pas au centre de ce manuel, nous suggérons que la gestion de l'information issue des incidents est un élément clé de leur gestion et du travail de préparation organisationnelle.

La préparation organisationnelle implique la mise en place de procédures et d'une formation claires sur la gestion des incidents et la gestion de l'information issue de ces incidents, ce qui assurera les meilleures réactions et réponses possibles aux événements.

Les incidents, en particulier les incidents critiques, ont généralement les caractéristiques suivantes :

- Un effet de surprise ;
- Information insuffisante ;
- L'escalade des événements pouvant dépasser la capacité de réponse ;
- Une attention et un regard extérieur importants ;
- Perte de contrôle (réelle ou perçue) ;
- Perturbation des processus normaux de prise de décision ; et
- Les personnes directement touchées ont tendance à se concentrer sur le court terme.

À moins que les incidents ne soient critiques, ils sont habituellement traités dans le cadre de procédures préétablies. Même les incidents non critiques peuvent créer de la confusion et de la panique chez ceux qui ne sont pas prêts à y répondre.

Le but de la préparation et de la gestion des incidents de sécurité est de réduire l'impact des incidents, d'améliorer la capacité de l'organisation à faire face au présent et à apprendre pour continuer à s'améliorer à l'avenir.

Suite à un incident, une organisation visera à :

- Prévenir d'autres préjudices et assurer la santé et/ou la sécurité des victimes et du personnel ;
- Assurer le personnel et les familles des victimes qu'une réponse responsable et efficace est en cours ;
- Garantir une gestion organisationnelle continue tout au long de l'incident, en particulier s'il s'agit d'un événement continu, tel qu'un enlèvement ;
- Garantir la continuité du programme ;
- Réduire la perte d'actifs (tels que téléphones, ordinateurs, véhicules, etc.) ;
- Remplacer les biens perdus à la suite d'un vol qualifié, etc.
- S'acquitter des responsabilités organisationnelles et réduire le risque de réclamations en justice ;
- Déposer des plaintes (par exemple, informer les autorités locales compétentes de toute menace contre le personnel) ;
- Sauvegarder l'image et la réputation de l'organisation ;
- Partager les informations critiques avec d'autres ONG et partenaires qui peuvent également être à risque pendant ou après un incident ;
- Préparer des communiqués de presse et/ou informer les médias et les organes d'information humanitaires / de développement d'informations spécialisées qui informent le public tout en protégeant les personnes concernées.

La sensibilisation à la sécurité, la menace, la vulnérabilité et l'analyse des risques, les procédures efficaces, la tenue d'exercices de sécurité et de sûreté, le réseautage étendu avec les partenaires et les organismes externes et une bonne planification d'urgence sont autant de moyens proactifs de gérer les incidents.

La préparation organisationnelle est essentielle à la gestion efficace des incidents et à la gestion de l'information issue des incidents de sécurité.

Bien que les politiques de sécurité ne puissent pas couvrir toutes les éventualités, disposer de plans d'urgence et de plans de gestion des incidents, les mettre à jour régulièrement et les mettre en œuvre, tout en mettant en place des procédures de gestion de crise efficaces, contribueront à maîtriser la situation et maintenir des opérations sécurisées.

> *« Dans le cas d'un événement sensible, par ex. la violence sexuelle contre un membre du personnel, répondre préalablement à la question « et si l'auteur d'un incident de violence sexuelle est un membre du personnel ? » aidera l'organisation et son personnel à se préparer à cette éventualité ».*

Il est extrêmement utile de traiter des incidents survenant plus fréquemment afin de réfléchir à des questions telles que :

- Avons-nous répondu de manière appropriée et du mieux que nous pouvions au(x) dernier événement(s) ?
- Qu'avons-nous appris des incidents évités de justesse et avons-nous apporté des changements à notre façon de travailler en fonction de ce que nous avons appris ?

Avant qu'un incident ne se produise, et comme bonne pratique de gestion, il est conseillé à une organisation de s'assurer qu'une gestion solide de l'information issue des incidents fait partie des politiques et procédures globales de gestion des incidents de l'organisation. Une organisation peut le faire en :

- Développant, mettant en œuvre et revoyant régulièrement les politiques et les procédures organisationnelles. Par exemple, sur la gestion et la notification des incidents, y compris les incidents évités de justesse, sur les cas de violence sexuelle ou d'autres événements particulièrement sensibles, sur la sécurité des données, les ressources humaines (RH), etc.
- Choisissant un système d'enregistrement et de signalement qui permet une gestion sûre des informations sur les incidents de sécurité à l'intérieur et à l'extérieur de l'organisation (voir « Objectif 4 – Enregistrement systématique des incidents » pour plus de détails sur les systèmes d'enregistrement).
- Définissant une structure et en identifiant les rôles et les responsabilités dans la gestion des incidents et la gestion de l'information issue des incidents pour tout le personnel et les responsables désignés et les points focaux, à chaque niveau de l'organisation du terrain au siège.
- Évaluant et identifiant les ressources (internes et externes) pour permettre à l'organisation de répondre efficacement et effectivement à tout incident.
- Orientant et formant le personnel clé sur la gestion des incidents et la gestion de l'information relatives à ces incidents.

Les organisations sont mieux armées si elles incluent des procédures claires et une formation à la gestion de l'information dans le cadre de la réponse globale à la gestion des incidents. Cela garantira que les données sont collectées, analysées et rapportées de manière appropriée, en soutenant la réponse immédiate à l'incident mais aussi en fournissant des avantages à long terme pour l'organisation.

Voir l'Outil 1 : Grille d'auto-évaluation GIIS pour un formulaire d'auto-évaluation qui aide les organisations à évaluer leurs forces et leurs faiblesses dans la gestion de l'information issue des incidents de sécurité.

Devoir de protection

La GIIS a quatre objectifs principaux, décrits plus en détail dans le chapitre 2 : les quatre objectifs de la gestion des incidents de sécurité, mais l'argument principal en faveur d'une gestion efficace de l'information de sécurité est de maintenir le personnel, les programmes et l'organisation en sécurité. Une gestion rigoureuse des risques de sécurité organisationnelle favorise un meilleur accès aux populations dans le besoin, mais permet également aux organisations, en tant qu'employeurs, d'assumer leurs responsabilités en matière de devoir de protection envers le personnel.

Les ONG ont un devoir de protection légal (et sans doute moral) : « Le devoir de protection est une obligation légale imposée à un individu ou à une organisation exigeant qu'il respecte une norme de protection raisonnable tout en accomplissant des actes (ou des omissions) raisonnablement prévisibles au risque de nuire aux autres[10] ».

Ce devoir de protection vis-à-vis du personnel et des non-salariés sur lesquels l'organisation exerce un certain contrôle[11] impose aux ONG de mettre en place de solides systèmes et processus de gestion des risques de sécurité[12]. Cette obligation comprend la mise en œuvre d'une gestion solide de l'information issue des incidents de sécurité.

Un système efficace de gestion de l'information issue des incidents de sécurité appuiera :

- Une meilleure compréhension de l'environnement de la menace et le développement de mesures pertinentes de prévention ou de mitigation du risque
- La documentation des connaissances organisationnelles ; et
- Une meilleure connaissance et compréhension des tendances du secteur et des pratiques communautaires, notamment en matière de sécurité.

En cas de détérioration significative du niveau de sécurité, en particulier dans les environnements de conflit et de post-conflit, il est impératif que les organisations disposent de procédures leur permettant de démontrer leur devoir de protection pour l'ensemble de leur personnel et de leurs responsables.

> *« Si la gestion des incidents peut être considérée comme un outil d'apprentissage crucial en matière de gestion des risques de sécurité, la gestion de l'information devient le meilleur moyen de démontrer la maturité de l'organisation dans l'analyse des événements et la prise de décision. Une collecte de données, une analyse, un rapport et un enregistrement approfondis des incidents auxquels une organisation fait face et la façon dont elle les aborde pourraient être une partie vitale de la défense d'une organisation, si un incident se produisait et qu'une procédure judiciaire était ouverte ».*

10 Kemp, E. and Merkelbach, M. (2011). « Pouvez-vous être poursuivi ? Responsabilité juridique des organisations internationales d'aide humanitaire envers leur personnel », Initiative de gestion de la sécurité.
11 Inclus les consultants, les visiteurs, les volontaires.
12 Kemp, E. and Merkelbach, M. (2016). « Devoir de protection : un examen de la décision Dennis / Norwegian Refugee Council et de ses implications », *EISF*.

Étude de cas : Dennis vs Norwegian Refugee Council (NRC) 2015

Dans ce qui a été considéré comme le premier cas d'étude du devoir de protection dans le secteur de l'aide, Dennis vs Norwegian Refugee Council (NRC) met en évidence quelques leçons importantes sur la gestion de l'information des incidents de sécurité.

Résumé des faits :

Le 29 juin 2012, Steven Dennis, un employé de NRC, a été blessé et kidnappé, ainsi que trois autres collègues, à la suite d'une attaque lors d'une visite officielle dans l'un des camps de réfugiés à Dadaab, au Kenya. Quatre jours plus tard, les otages ont été libérés lors d'une opération de sauvetage armée menée par les autorités kényanes et des milices locales. Trois ans plus tard, Dennis a déposé une plainte auprès du tribunal de district d'Oslo contre son ancien employeur, NRC, pour obtenir une indemnisation et obtenir des dommages et intérêts suite à l'enlèvement. Après un examen minutieux des faits entourant l'affaire, le tribunal a statué que le NRC avait été grossièrement négligent et a ordonné à l'organisation d'indemniser Dennis[13].

Leçons apprises :

Le plan de sécurité de NRC, qui reposait sur des informations provenant de sources et d'incidents internes et externes, indiquait que le risque d'enlèvement était élevé. Son analyse a également indiqué que le personnel international courait un risque plus élevé d'enlèvement que le personnel national. Cette information a été utilisée pour mettre en place des mesures efficaces de traitement des risques, y compris l'utilisation d'escortes armées et la restriction des visites officielles dans la région. Cependant, NRC a modifié les procédures de sécurité avant la visite officielle en se fondant sur une réévaluation des risques. Sur la base des éléments de preuve fournis, le tribunal a jugé cette réévaluation peu claire et injustifiée. Essentiellement, les informations sur lesquelles reposait la décision de sécurité ont été jugées faibles et en contradiction avec les informations de sécurité robustes précédemment enregistrées.

NRC a soutenu que le risque d'enlèvement avait diminué en raison de l'absence d'enlèvements dans la région au cours des neuf mois précédents. Le tribunal a toutefois estimé que l'absence d'incidents ne signifiait pas nécessairement que le risque avait disparu, mais pouvait également être attribué à de fortes mesures de traitement des risques, notamment l'absence de visites officielles et le recours à des escortes armées pour toutes les ONG opérant à Dadaab à l'époque. Une meilleure analyse des non-incidents aurait pu aider NRC à déterminer le niveau de risque réel plutôt que le niveau perçu.

Une fois l'incident survenu, NRC a restreint la quantité d'informations à partager à propos de l'incident avec le personnel affecté et impliqué. On a fait valoir que ce manque de transparence de la part de l'organisation avait joué un rôle important dans la décision de Dennis de poursuivre NRC.

Dans ce cas, une gestion plus stricte de l'information de sécurité aurait pu amener NRC à prendre différentes décisions en matière de sécurité en lien avec la visite officielle, ce qui aurait pu empêcher l'incident de se produire.

[13] Kemp, E. and Merkelbach, M. (2016). « Devoir de protection : un examen de la décision Dennis / Norwegian Refugee Council et de ses implications », *EISF*.

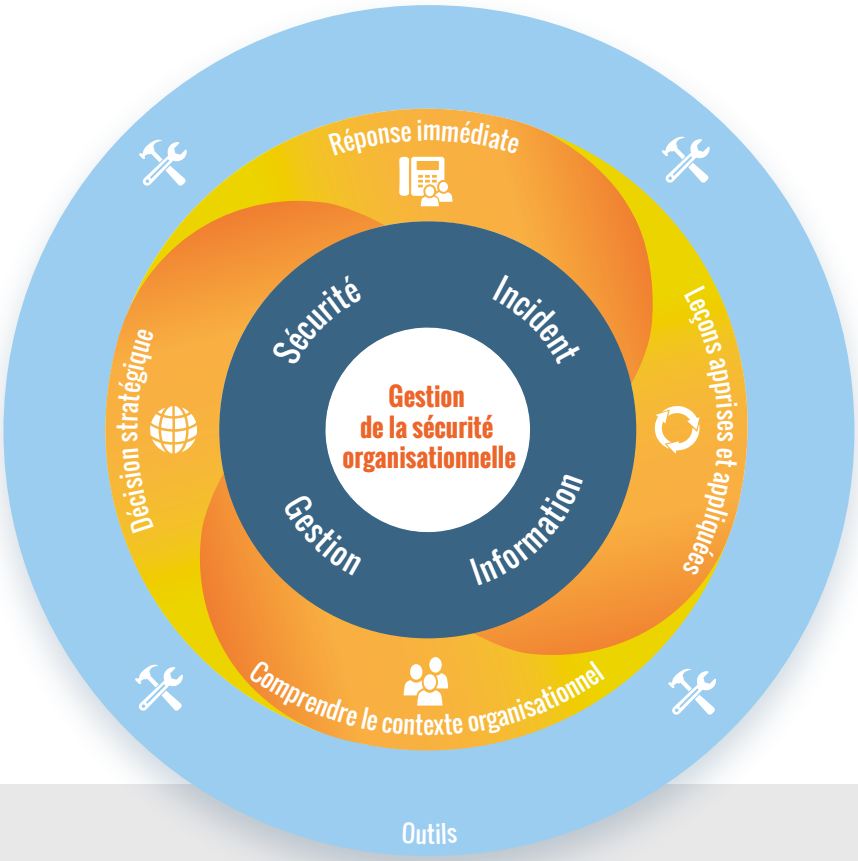
Cependant, si l'incident s'était produit, la documentation des informations de sécurité fiables utilisées pour prendre des décisions de sécurité aurait pu aider NRC à défendre ces décisions.

Une approche différente du partage de l'information après l'incident pourrait également avoir abouti à une discussion moins litigieuse et plus ouverte sur les échecs et les leçons apprises entre l'organisation et le personnel affecté.

Irish Aid a élaboré des lignes directrices pour aider les organisations à mieux démontrer leur engagement à respecter leurs obligations en matière de devoir de protection. Ces lignes directrices ont pour but de fournir aux organisations des conseils sur la façon d'atteindre un haut niveau de professionnalisme dans l'accomplissement de leurs objectifs opérationnels. Chaque sujet est accompagné d'actions clés, d'indicateurs et de notes d'orientation. Le respect de ces lignes directrices devrait aider l'organisation à se conformer à ses responsabilités en matière de devoir de protection et démontrer que les procédures de signalement des incidents de sécurité incluent les bonnes personnes, de la bonne manière et au bon moment[14]. Le Département fédéral des affaires étrangères (DFAE), la Stabilisation Unit (SU) et le Center for International Peace Operations (ZIF) ont également publié récemment des lignes directrices sur le devoir de protection. Ceux-ci peuvent être trouvés ici.

[14] Irish Aid. (2013). *Lignes directrices de l'aide irlandaise pour la gestion des risques professionnels en matière de sécurité et de sûreté des ONG*. ALNAP.

CHAPITRE 2 : LES QUATRE OBJECTIFS DE LA GIIS

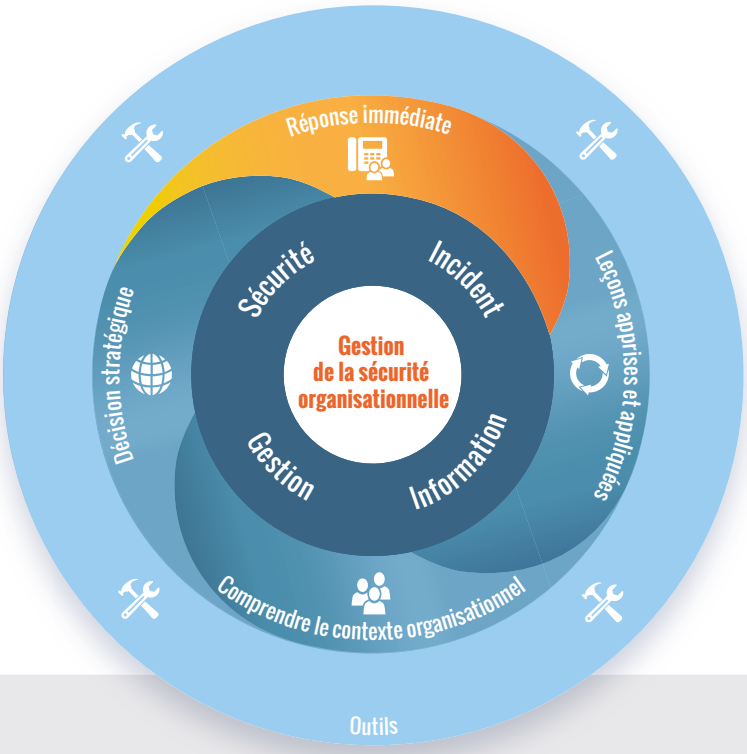


Ce chapitre donne un aperçu des quatre principaux objectifs de la gestion de l'information issue des incidents de sécurité et les principales étapes à suivre pour les atteindre. Il couvre :

- Objectif 1 : Réponse immédiate
- Objectif 2 : Leçons apprises et appliquées
- Objectif 3 : Comprendre le contexte opérationnel
- Objectif 4 : Prise de décision stratégique

- Tous les outils sont pertinents pour ce chapitre.

1. OBJECTIF 1 : RÉPONSE IMMÉDIATE



Cette section traite de la gestion de l'information issue des incidents de sécurité dans le but d'informer sur la réaction immédiate suite à un incident et la réponse à apporter. Elle couvre :

- 1.1 Conseils sur la manière de signaler un incident : quoi, quand, comment et à qui
- 1.2 Faire face au stress
- 1.3 Processus de suivi des incidents de sécurité
- 1.4 Communication
- 1.5 Traitement des cas sensibles: les violences sexuelles contre le personnel

Outils pertinents :

- Outil 2 : Typologie des incidents
- Outil 3 : Incident organisationnel ou externe
- Outil 4 : Modèle de rapport d'incident
- Outil 5 : Grilles d'analyse des incidents
- Outil 6 : Comment effectuer un débriefing factuel
- Outil 7 : Bonnes pratiques en matière de signalement des incidents liés au genre et mécanismes de plainte pour signaler l'exploitation et les abus sexuels (EAS)

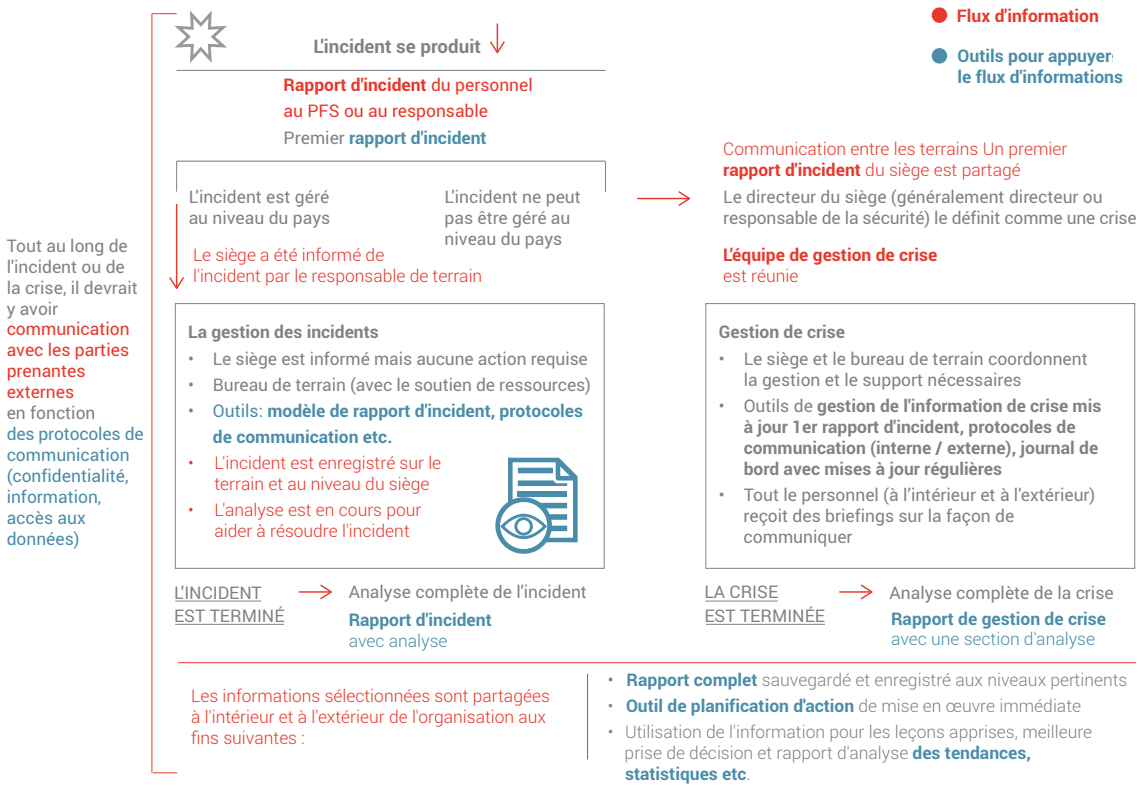
> *« Habituellement, le personnel impliqué dans un incident donne un premier appel d'urgence au point focal de sécurité. Sur la base des informations partagées verbalement, le point focal de sécurité fournit des conseils et cherche des informations de base, telles que qui a fait quoi à qui, où et quand. Ensuite, lorsque le personnel est en sécurité, le rapport d'incident est rempli de manière plus approfondie par le point focal de sécurité, en utilisant les informations recueillies lors d'un débriefing approprié avec le personnel impliqué dans l'incident ».*

L'un des principaux objectifs de la gestion de l'information issue des incidents de sécurité est d'informer sur la réaction et la réponse immédiate à apporter. Le but est de s'assurer que l'information est recherchée et utilisée par les décideurs et le personnel concerné pour apporter une réponse immédiate à l'incident. Cela se produit généralement au niveau du terrain et/ou du pays, pendant ou peu après l'événement.

Les informations enregistrées et rapportées devraient aider à identifier le soutien requis pour le personnel concerné et à déterminer si l'organisation doit mettre en œuvre des changements immédiats dans ses opérations, tels que la restriction des mouvements ou la suspension temporaire des opérations. Par ailleurs, il existe un lien direct entre les informations requises et les options de réponse à prendre en compte.

Lorsqu'un incident survient, le personnel doit hiérarchiser les rapports, les réponses et les enregistrements.

Les organisations ont besoin d'un flux d'informations efficace garantissant que tous les personnels concernés au siège, dans les bureaux régionaux, dans les bureaux de pays et sur le terrain disposent des informations nécessaires et que l'information déclenche des mécanismes de réponses appropriées. Le diagramme suivant[15] montre le flux possible d'informations à travers une organisation suite à un incident de sécurité.



[15] Ce diagramme provient des cours d'introduction sur la sécurité de RedR UK.

Les informations concernant un incident peuvent être partagées avec d'autres organisations travaillant dans la même zone ou dans le même pays pour leur permettre de prendre éventuellement des mesures de précaution et d'éviter que l'incident ne se reproduise.

Un bon signalement et un enregistrement immédiat de l'incident sont essentiels pour une bonne gestion de l'information.

Rappelez-vous que le but de la notification immédiate est de fournir un soutien immédiat au personnel.

1.1 Conseils sur la maniere de signaler un incident : quoi, quand, comment, et a qui ?

Les organisations devraient donner des instructions au personnel sur la gestion de l'information issue des incidents de sécurité, et cela devrait commencer par fournir des directives claires sur la façon de signaler les incidents.

> *« Souvent, les procédures de signalement d'incident sont traitées dans la section POS d'un plan de sécurité. Certaines organisations ont décidé d'élaborer un document à part pour couvrir la politique de signalement des incidents de l'organisation et fournir des conseils au personnel à tous les niveaux de l'organisation (du siège au terrain) en le liant à d'autres documents internes (RH, code de conduite, politique de sécurité, etc.) ».*

L'établissement d'un protocole de rapport d'incident efficace permet à la direction de :

- Soutenir les personnes touchées ;
- Discerner les tendances et les types d'incidents ;
- Améliorer la formation, les procédures et les structures physiques ; et
- Allouer les ressources de manière adéquate.

Il est important que le personnel sache à qui il doit s'adresser, et que les procédures de signalement décrivent la manière de rapporter un incident ainsi que les étapes suivantes. Le tableau suivant délimite les principales étapes pour signaler et analyser un incident ainsi que les différents moments pour le faire.

Quand	Étape	Mesures
Juste après l'incident	Brève description chronologique des faits.	Le rapport d'incident est terminé, des mesures de réponse immédiate ont été prises.
	Analyse préliminaire des risques.	
Suite à la réponse immédiate à l'événement	Débriefing factuel après l'incident : Quels sont les faits / analyses à réviser / à ajouter au rapport d'incident de sécurité après l'introduction de nouveaux éléments / informations ?	Modifications à apporter au (x) rapport (s) d'incident de sécurité déjà soumis intégrant de nouvelles informations. Le plan d'action est conçu. Les POS sont réévaluées. Commentaires fournis à la personne signalant un incident et au personnel concerné sur les mesures prises.
	Nouvelle analyse des risques, par exemple, humains, financiers et matériels, opérationnels, juridiques, réputationnels, etc. et des actions entreprises ou à entreprendre afin de réduire ces risques.	
Dans les semaines suivant l'incident	Le point focal sécurité ou le responsable s'assure que des mesures sont prises et détermine si l'analyse précédente était exacte.	Les rapports d'incident sont mis à jour si nécessaire. Le plan d'action est examiné, considéré comme atteint, ou un nouveau est développé. Toutes les POS mises à jour restent en place ou reviennent aux conditions précédentes. Commentaires fournis au personnel concerné.
	Décider si l'incident est 'fermé' aux fins de la gestion des incidents. Sinon, un autre plan d'action devrait être élaboré.	

Quoi signaler ?

La plupart des organisations utilisent une définition large des incidents de sécurité devant faire l'objet d'un rapport. Il est important que cette définition soit standard dans toute l'organisation pour assurer la cohérence, et il est important d'inclure tous les incidents: critiques, non critiques et quasi-incidents. Voir « Introduction – Définitions clés » pour les définitions relatives à la gestion de l'information issue des incidents de sécurité.

Une organisation peut être affectée par différents types d'incidents qui ne sont pas directement liés à des problèmes de sécurité (par exemple, la santé et les accidents domestiques). L'organisation doit décider si ces cas doivent être signalés et enregistrés par les mêmes mécanismes. Si ce n'est pas le cas, il convient de préciser au personnel quel est le processus alternatif pour signaler les incidents de santé et d'accidents domestiques. Si ils sont combinés dans le même système d'enregistrement, une indication claire sous la forme d'un étiquetage indiquant la catégorie de chaque événement doit être incluse pour permettre à l'analyse de se concentrer sur toutes les catégories de sécurité ou de santé et d'accidents domestiques.

« En cas de doute, l'incident doit être signalé au responsable de la sécurité, au point focal de sécurité ou au siège. Ils décideront de la suite à donner à l'incident ».

Il n'est pas possible de définir l'ensemble des situations pouvant constituer un incident de sécurité. Le terme est, par conséquent, défini très largement et inclut, mais n'est pas limité à :

- Tous les crimes impliquant le personnel et les biens de l'organisation (par exemple, vol, cambriolage, braquage de véhicule, enlèvement, etc.) ;
- Tous les cas où le personnel de l'organisation est menacé par une arme ou par des actes de violence ;
- Tous les cas de harcèlement ou de comportement menaçant de quelque nature que ce soit ;
- Les actes de guerre et les conflits armés tels que les bombardements, les mines, les tirs ou l'agression militaire ;
- Le pillage, les attaques contre les biens et le vandalisme ;
- Tous les cas dans lesquels du personnel de l'organisation peut être impliqué dans des activités illégales ;
- Toutes les violations des règles de sécurité de l'organisation ;
- Tous les cas de tentatives de corruption pour l'accès à des emplacements, des routes ou des populations affectées, qu'elles soient abouties ou non ;
- Toutes menaces internes et les cas de fraude au sein d'une oganisation.

Il devrait également être précisé quand il convient de signaler les incidents survenant en dehors des heures de bureau pour le personnel national ou aux heures privées du personnel international. Une bonne pratique impliquerait la déclaration de tous les incidents, même en dehors des heures normales de service, car cela améliore l'analyse du contexte. Dans ces circonstances, toutefois, les procédures de déclaration peuvent être différentes.

« Donnez des exemples d'incidents de sécurité qui devraient être signalés, qui aideront le personnel à identifier ce qui constitue un incident. La catégorisation n'est pas nécessaire au début du processus, mais elle aidera le personnel à comprendre s'il doit le rapporter. Les gens ont besoin d'exemples pertinents pour leur zone d'opérations. Vous pouvez également décider de discuter régulièrement d'une catégorie d'incident qui n'est pas bien connue des membres de l'équipe. Les études de cas sont nombreuses ».

Pour une liste complète des types d'incidents, voir l'Outil 2 : Typologie des incidents.

Les organisations doivent indiquer clairement au personnel si les incidents signalés doivent également inclure ceux qui sont externes à l'ONG, c'est-à-dire qui ont un impact sur d'autres organisations. Les organisations se concentrent souvent sur le signalement et l'enregistrement des incidents organisationnels (incidents ayant un impact direct sur l'organisation, son personnel, ses propriétés et sa réputation) et n'incluent pas les incidents externes dans son système de rapport et d'enregistrement. Les événements externes sont généralement surveillés au niveau du terrain afin de ne pas manquer d'informations contextuelles importantes, mais l'organisation doit définir ce qui constitue un incident affectant l'organisation et la procédure à suivre pour signaler officiellement les événements externes. Cela prend du temps mais les organisations peuvent compter sur des organismes externes travaillant pour la communauté des ONG pour enregistrer et rendre compte des événements externes.

« La mission sur le terrain a souvent la responsabilité de suivre et d'enregistrer ces types d'incidents, dans le cadre de leurs indicateurs d'évaluation des risques, et ces incidents ne sont pas enregistrés dans les statistiques générales de l'organisation ».

Voir Outil 3: Incident organisationnel ou externe.

Lors de la déclaration d'un incident, un modèle aide à assurer la cohérence des rapports. Ce modèle peut être dans un document Word, une feuille de calcul, une plateforme en ligne, etc., et devrait comprendre :

- Le (s) auteur (s) du rapport (y compris les coordonnées, poste (s) et date) ;
- Ce qui s'est passé (description et type d'incident) ;
- Le(s) victime (s) (nationale, internationale, genre, âge, etc.) ;
- Le type de réponse apportée ;
- Quand l'incident s'est produit ;
- Où l'incident s'est produit ;
- Si l'incident était accidentel ou délibéré, les détails, en particulier dans le cas où l'incident est délibéré ;
- Les décisions prises, les actions de suivi (mises en œuvre ou recommandées) et l'analyse.

Si un incident nécessite une réponse urgente, des conseils peuvent être donnés au personnel pour s'assurer qu'il priorise les '6Q' :

- Qui est impliqué ?
- Qu'est-il arrivé ?
- Où l'incident s'est-il produit ?
- Quand l'incident s'est-il produit ?
- Qu'avez-vous fait à ce sujet ?
- De quel soutien avez-vous besoin ?

Voir Outil 4 : Modèle de rapport d'incident, comprenant les informations demandées immédiatement pour la gestion de l'information issue des incidents et l'analyse préliminaire.

Voir Outil 5 : Grilles d'analyse des incidents incluant des questions additionnelles et d'autres éléments pouvant être ajoutés ultérieurement pour une analyse approfondie.

La cohérence dans la rédaction des rapports d'incident de sécurité peut être améliorée par la formation du personnel. Les directives ci-après sur la façon de décrire un incident peuvent être mises à la disposition du personnel avec un modèle de rapport d'incident.

Langage	Utilisez des termes spécifiques et décrivez clairement ce qu'il s'est passé. Soyez précis sur les détails et ne supposez pas que les autres comprendront les généralités. Par exemple, évitez d'utiliser des mots tels que « agressif », « contrarié » ou « agité ». A la place, énoncez le comportement que vous avez observé qui vous a fait penser que la personne était agressive, bouleversée ou agitée. Rappelez-vous que la description de l'incident est ce sur quoi les autres se baseront pour obtenir des informations concernant les individus impliqués et l'incident. Il est important de veiller à ce que le rapport ne transmette pas d'images négatives des personnes impliquées. Le rapport a la capacité d'influencer les autres, il faut donc prendre soin de s'assurer qu'il est correctement préparé et qu'il donne un débriefing factuel de l'incident. Examinez votre rapport avant de le soumettre pour vous assurer que vous n'avez pas utilisé de terminologie subjective ou laissé des questions sans réponse.
Fiabilité de l'observation	Les autres personnes qui ont entendu ou vu l'incident sont-elles d'accord avec le débriefing que vous avez écrit ? Si une autre personne a été impliquée dans l'incident ou en a été témoin, il est conseillé de consulter cette personne pour s'assurer que le rapport concorde avec les observations de cette personne. Différentes personnes auront des perceptions différentes d'un incident et si les opinions de certaines personnes sont ignorées, cela peut être contradictoire. En outre, il est important de noter que les souvenirs des individus changent avec le temps.
Objectivité	Lors de la rédaction d'un rapport d'incident de sécurité sur un événement actuel, tout doit être fait pour être aussi objectif que possible et éviter d'être influencé par une situation antérieure. En tant qu'auteur du rapport d'incident, vous l'écrivez en tant que greffier et non en tant que juge. Par conséquent, assurez-vous que le rapport est exempt de jugement, de sarcasmes ou de commentaires condescendants.
Cause de l'incident	Si vous estimez que vous n'avez pas d'informations factuelles, vous pouvez exprimer votre opinion à condition que vous fassiez clairement la distinction entre votre opinion et les faits. Même si la cause réelle d'un incident reste inconnue après que vous ayez essayé de la déterminer, vous devez fournir autant d'informations que vous avez sur ce qui s'est passé avant ou pendant l'événement, car cela peut donner une idée au lecteur. Si vous n'avez pas été témoin de l'incident ou de l'événement, vous pouvez toujours rédiger un rapport d'incident. Cependant, assurez-vous d'indiquer que l'information est basée sur ce qui vous a été rapporté et par qui.

Quand signaler
Le niveau de détail des rapports et les moments où ils sont faits dépendent de la catégorie de l'incident :

- **Les incidents nécessitant une action immédiate** doivent être signalés immédiatement dans le but de demander un soutien et des instructions supplémentaires. Les incidents critiques qui constituent une menace importante et/ou permanente pour le personnel, les biens ou les programmes de l'organisation nécessitent généralement une communication immédiate et une réponse urgente.
- **Incidents pour lesquels aucune action immédiate n'est requise :** Les incidents ou quasi-incidents qui reflètent l'insécurité ou un changement du contexte, mais qui ne présentent pas de risque immédiat pour le personnel, les biens ou les programmes de l'organisation, ne sont pas urgents et peuvent donc faire partie d'un rapport quotidien ou hebdomadaire destiné à un supérieur hiérarchique direct ou à un Point Focal Sécurité.

Les rapports d'incident peuvent être complétés en différentes étapes au fur et à mesure que de plus amples informations sont disponibles.

Immédiatement : les rapports d'incidents immédiats sont faits dès qu'il est possible de le faire, souvent par radio ou par téléphone. Une situation peut être déroutante dans un premier temps, il faut donc prendre le temps d'évaluer ce qui vient de se passer, quel est le niveau de sécurité du personnel et des autres personnes impliquées, et quelle aide est nécessaire. Lorsque vous signalez un incident au téléphone ou à la radio, le personnel doit parler clairement, avec précision et concision. S'il n'est pas possible de fournir tous les détails (en raison d'un manque de temps ou parce qu'il est dangereux de le faire pendant un incident en cours), fournir toutes les informations possibles afin de déclencher la réponse appropriée. Même le partage d'informations le plus bref peut sauver des vies.

Le personnel susceptible de recevoir des rapports d'incidents immédiats (tels que les opérateurs radio, les supérieurs hiérarchiques et les PFS) doit être formé à la manière de réagir. Savoir quelles questions poser et être empathique envers la personne qui signale l'incident peut avoir un impact important sur l'efficacité de la réponse et le bon rétablissement de la ou des personnes touchées.

Dans les heures et jours suivants : Certains incidents peuvent nécessiter un ou plusieurs rapports de suivi. Ceux-ci peuvent être réalisés aussi souvent que nécessaire, avec une fréquence et un niveau de détail pré-déterminés et révisés régulièrement. Dans une situation active, le PFS ou l'autorité désignée doit tenir un registre des événements et des actions prises. Cela permettra non seulement de tenir un registre des décisions et des activités pour améliorer la gestion de la situation, mais également de fournir les élements nécessaires aux points d'information ou de situation et, en dernier lieu, de soutenir l'apprentissage organisationnel. Les informations doivent être partagées par écrit lorsque cela est possible, afin de réduire le risque de mauvaise communication et d'incompréhension. Cela aide également les personnes stressées à mieux cadrer leurs pensées. Voir la section ci-dessous sur 'Gérer le stress'.

Une fois l'incident stabilisé ou « terminé » : Certains incidents peuvent nécessiter un rapport d'incident de sécurité complet / final, généralement sous forme écrite. Dès qu'il sera approprié de le faire, les participants seront tenus de fournir un compte rendu écrit de l'événement et des mesures prises. Lorsque le terrain doit prendre des mesures spécifiques pour traiter les risques, notamment en apportant des modifications aux procédures existantes, à la formation, à l'allocation des ressources, etc., des mesures de suivi doivent être clairement indiquées, les personnes responsables de leur mise en œuvre identifiées et un calendrier spécifié. Les rapports de suivi subséquents doivent

enregistrer la progression des actions recommandées jusqu'à leur achèvement. Le rapport d'incident complet devrait constituer la base de la réévaluation ou de la mise à jour des POS pertinentes de l'organisation. Voir l'Objectif 2 pour plus de détails.

Le personnel doit être informé et savoir à quoi s'attendre et ce qu'il doit demander lorsqu'il signale un incident. Les éléments déclencheurs doivent être clairement identifiés et les protocoles de réponses clairement expliquées à l'avance. Pour réduire le nombre d'incidents ne faisant pas l'objet d'un rapport, la procédure doit être claire mais flexible : les rapports peuvent être simples ou plus approfondis si nécessaire.

Dans la mesure du possible, il est préférable de préparer un rapport immédiatement après l'incident lorsque les faits sont encore clairs. Cependant, et en fonction de la gravité de l'événement, le personnel peut être émotionnellement impliqué à ce moment-là ; il peut donc être utile de demander à une tierce personne de relire le rapport avant de le soumettre.

Comment signaler

La procédure concernant les rapports d'incidents doit identifier les moyens de communication les plus sûrs, en tenant compte des trois différents moments de la notification.

Elle devrait préciser si des radios, des téléphones satellites ou des courriels doivent être utilisés et s'assurer que le personnel est formé pour utiliser les dispositifs de manière sûre et sécurisée (en utilisant l'encodage si nécessaire). Le personnel devrait être sensibilisé à la nécessité d'assurer la confidentialité du signalement des incidents.

La procédure devrait également clarifier les différences entre les les canaux de communication en fontion des différents types d'incidents. Par exemple, un cambriolage et un incident de violence sexuelle nécessiteront des mécanismes de signalement différents. Les incidents nécessitant une réponse administrative, par ex. les déclarations d'assurance, le remplacement des biens, etc., peuvent également nécessiter une procédure spécifique. Pour plus d'informations sur le signalement des cas sensibles, voir « Traitement des cas sensibles : violence sexuelle contre le personnel » dans la section ci-dessous.

Il est possible de développer différentes procédures de déclaration d'incidents en fonction de la nature de l'incident, c'est-à-dire du niveau de confidentialité et de sensibilité requis. Néanmoins, il est important de souligner que le canal utilisé ne devrait généralement pas être l'élément le plus important (à moins qu'il y ait de graves problèmes d'interception ou de confidentialité). En particulier pour les incidents nécessitant une intervention urgente, ce qui compte le plus, c'est que l'information soit transmise le plus rapidement possible aux destinataires prévus afin que les personnes touchées obtiennent le soutien dont elles ont besoin.

Il est également crucial que le personnel respecte la confidentialité de l'information à l'interne, pour s'assurer qu'il n'y ait pas d'interférence dans la gestion de l'événement. Les points focaux peuvent utiliser le tableau « Catégories d'informations' dans l'Objectif 3 ».

A qui signaler

Tout le personnel devrait être en mesure de signaler un incident et la procédure de signalement de l'organisation devrait indiquer clairement à qui le personnel doit signaler les incidents. Par exemple, cela peut se faire par courrier électronique à une personne en particulier ou par le biais d'un système de signalement en ligne qui envoie automatiquement des rapports aux membres du personnel concernés au sein de l'organisation.

Le tableau suivant fournit des exemples de catégories de personnes, leurs tâches et responsabilités correspondantes en cas d'incident.

Qui	Tâches et / ou responsabilités
Tout le personnel	Devrait signaler l'incident à son responsable ou au point focal de sécurité désigné.
Point focal de sécurité (au niveau du terrain ou du bureau national) Responsable (au niveau du terrain ou du bureau national)	Après avoir reçu le rapport d'incident initial, assurez-vous que le personnel concerné bénéficie d'un soutien, informez le bureau national/régional du soutien nécessaire, suivez l'incident et organisez un débriefing et une analyse de l'incident. Devrait suggérer des mesures opérationnelles immédiates au responsable régional. Assurer la communication avec le personnel de terrain si nécessaire.
Point focal national ou régional pour la sécurité Responsable (pays ou région)	Après avoir reçu des informations du bureau local ou du bureau national, assurer le soutien aux personnes affectées, transmettre l'information au Siège, assurer le suivi et les retours éventuels si le personnel est évacué. Discuter et convenir de mesures opérationnelles immédiates potentielles au niveau national ou le responsable de terrain.
Responsable de la sécurité ou conseiller (au niveau du siège)	Après avoir reçu des informations du bureau régional ou du bureau national, vous devez vous assurer que l'assistance du siège est fournie si nécessaire. Assurer la liaison avec les décideurs au niveau du siège afin de valider le niveau de gestion approprié.
Responsable et directeur exécutif / DG (au niveau du siège)	Recevront l'information issue de l'incident de la part du responsable de la sécurité / du conseiller au niveau du siège et/ou des responsables au niveau régional ou national. Devraient assurer le suivi des actions spécifiques au niveau du siège, si celles-ci sont nécessaires. Assurer la communication de l'incident au personnel du siège si cela s'avère nécessaire.

Le flux d'informations issues d'un incident doit être adapté par chaque organisation pour refléter les positions du personnel, la hiérarchie et la présence opérationnelle.

Les responsabilités du personnel en matière de signalement et de gestion de l'information issue des incidents de sécurité doivent être clairement identifiées dans les documents de référence (politique de gestion des risques de sécurité, politique de signalement des incidents, code de conduite, etc.) et les procédures. Les rôles devraient être mis en évidence pendant le processus d'intégration et régulièrement pendant toute la mission.

1.2 Faire face au stress

Le personnel qui signale un événement pendant qu'il se produit ou immédiatement après est susceptible d'être soumis à un stress important. Il est recommandé que le personnel qui reçoit le premier rapport verbal s'efforce :

- De rester calme ;
- D'identifier la personne qui fait le rapport ;
- D'assurer la sécurité des personnes impliquées dans l'incident ;
- De hiérarchiser les informations requises, par ex. le statut, ce qui a été fait, ce qui doit être fait immédiatement ;
- De collecter les informations en fonction du modèle de rapport d'incident ;

- De rassurer la personne signalant l'incident et convenir d'une communication ultérieure.

Le but de ce premier rapport est d'obtenir les faits nécessaires pour guider une réponse immédiate. Ce n'est pas un débriefing émotionnel (souvent appelé désamorçage). Un soutien psychologique ainsi qu'un débriefing émotionnel pour les personnes à la suite d'un événement traumatique doivent être effectués par des professionnels si besoin. Ce débriefing émotionnel (ou désamorçage) est surtout pertinent pour les incidents critiques, mais certains incidents non critiques auront également des effets traumatisants sur la personne impliquée. L'organisation devrait s'assurer que le personnel est soutenu dans les deux situations.

1.3 Processus de suivi des incidents de sécurité

Tous les incidents de sécurité doivent faire l'objet d'un suivi pour s'assurer que toutes les informations issues de l'incident sont prises en compte afin d'alimenter les leçons apprises, les mises à jour contextuelles et la prise de décision.

Le processus de suivi des incidents fournit des rapports mis à jour en fonction de faits nouveaux ou émergents. C'est également un processus très utile à suivre lorsqu'il y a des changements de personnel dans des postes clés pertinents, comme par exemple, le point focal de la sécurité. Dans certains cas, cela peut nécessiter l'élaboration d'une nouvelle version du rapport d'incident.

Ce processus devrait prendre en compte chaque nouvel événement ou nouvelle action réalisée pendant la gestion de l'incident, jusqu'à la conclusion et la clôture de l'incident.

Les incidents critiques, tels que l'enlèvement du personnel, peuvent s'inscrire dans la durée, et les nouvelles informations disponibles de façon sporadiques. Il est important que l'organisation traite correctement cette nouvelle information afin qu'elle puisse être analysée et prise en compte dans le processus de prise de décision. Cela devrait faire partie du plan de gestion de crise.

Des processus de suivi doivent être définis pour tous les incidents, afin de garantir que les informations et les leçons apprises ne soient pas perdues ou ne soient pas dépriorisées dans des environnements changeants.

Débriefing factuel
Un débriefing factuel devrait avoir lieu après que le personnel concerné ait reçu le soutien approprié à la suite d'un incident. Il est recommandé que ce débriefing ait lieu dans les 48 heures suivant un incident de sécurité. L'étendue du débriefing variera en fonction de la nature et de la complexité de l'incident.

Lors de l'organisation d'un débriefing factuel à des fins de collecte d'informations, il est important de garder les principes de base des premiers secours psychologiques (PSP)[16] en mémoire:

- Ne procéder à un débriefing qu'après avoir assuré la sécurité physique et psychologique de base de l'individu ;
- Le débriefing doit avoir lieu dans un espace sûr ;
- Viser à responsabiliser l'individu affecté ;
- Etre clair sur le processus, les attentes et les actions de suivi.

[16] Pour plus d'informations sur le PSP, voir les directives de l'Organisation mondiale de la santé (OMS) cliquez ici.

Il est important de garder en tête que l'impact sur certains personnels des incidents évités de justesse et des petits incidents peut être beaucoup plus important que l'impact sur l'organisation. Par exemple, une expérience de harcèlement par des membres de la communauté ou une agression ratée peut affecter profondément un individu.

Voir l'Outil 6 : Comment effectuer un débriefing factuel pour plus d'indication sur la façon d'organiser un débriefing à des fins de collecte et d'analyse de l'information. Veuillez noter que ceci n'est pas une tentative de former les lecteurs sur les Premiers Secours Psychologiques ni comment devenir des professionnels de l'investigation. Il s'agit d'une liste de conseils pour mener des entrevues afin d'établir des faits vérifiés et utiles à la déclaration d'incidents.

Sources d'information

Les informations recueillies doivent être vérifiées de façon précise en discutant avec les parties prenantes internes et externes pour avoir les différentes perspectives, c'est-à-dire de recouper les informations recueillies.

Un élément critique dans l'analyse des informations de sécurité est la crédibilité de l'information et la validité de la source.

La grille de fiabilité et de validité suivante est un outil simple qui peut vous aider dans ce processus de vérification[17].

Fiabilité de la source

	Classement	Description
A	Complètement fiable	Aucun doute sur l'authenticité, la fiabilité ou la compétence de la source. Source d'une fiabilité complète.
B	Habituellement fiable	Doutes mineurs. Source de l'information la plupart du temps est valide.
C	Assez fiable	Doutes. A fourni des informations valides dans le passé.
D	Pas habituellement fiable	Doutes importants. A fourni des informations valides dans le passé.
E	Non fiable	Manque d'authenticité, de fiabilité et de compétence. Sources des informations invalides
F	La fiabilité ne peut pas être jugée	Information insuffisante pour évaluer la fiabilité. Peut ou peut ne pas être fiable.

Validité de l'information

	Classement	Description
1	Confirmé	Logique, cohérente avec d'autres informations pertinentes, confirmée par des sources indépendantes.
2	Probablement vrai	Logique, compatible avec d'autres informations pertinentes, non confirmée.
3	Peut-être vrai	Raisonnablement logique, accepte certaines informations pertinentes, non confirmées.
4	Douteuse	Pas logique mais possible, pas d'autre information sur le sujet, non confirmée.
5	Improbable	Pas logique, contredite par d'autres informations pertinentes.
6	L'information ne peut pas être vérifiée	La validité de l'information ne peut être déterminée.

[17] Armée des États-Unis. (2006). *Manuel de terrain No. 2-22.3*. Opérations de collecte d'intelligence humaine.

Par exemple : une note d'information classée A3 provient d'une source très fiable, mais l'information est seulement possiblement vraie. Alors qu'une notation D1 est une source d'information généralement non fiable mais qui a fourni des informations confirmées (vérifiées par d'autres sources).

Cette matrice est plus facile à utiliser si l'organisation dispose d'une cartographie des parties prenantes mise à jour. La fiabilité de la source ne s'observe que sur le long terme; le PFS devrait vérifier régulièrement toutes les informations opérationnelles fournies, afin d'évaluer la fiabilité des sources et la validité des informations reçues.

Les organisations peuvent recevoir des informations de sécurité de la part d'autres ONG ou individus de manière indirecte, par l'intermédiaire d'une tierce partie ou en contournant les interlocuteurs habituels. Ceci est parfois appelé flux d'information diagonal. Par exemple, des témoins du braquage d'un véhicule d'ONG n'ayant aucun moyen de contacter directement l'organisation ont appelé le consortium à la place. Le consortium a relayé le message au directeur de la sécurité de l'ONG, qui a, à son tour, relayé le message au bureau national sur le terrain.

1.4 Communication

Une politique devrait être élaborée au niveau organisationnel afin de définir quelles informations de sécurité devraient être partagées et avec qui, de façon interne et externe, en particulier immédiatement après un incident, et identifier la personne responsable du partage de l'information entre les différents niveaux d'une organisation (du terrain au Siège) et en externe. Cette politique doit couvrir les questions de confidentialité afin de protéger l'identité des personnes touchées et des autres parties prenantes si nécessaire. Il est recommandé qu'un point focal à chaque niveau pertinent au sein de l'organisation (du terrain au Siège) soit identifié comme étant responsable des communications externes, afin de s'assurer qu'elle est bien faite et en temps opportun.

« L'éthique de l'utilisation de l'information privilégiée dans les zones de conflit tout en gérant les incidents de sécurité doit être abordée. Un point focal de sécurité devrait être capable de filtrer des informations spécifiques à des fins d'adhésion éthique, tout en diffusant efficacement les informations pertinentes pour assurer la sûreté et la sécurité du personnel et la mission de l'organisation ».

Les mécanismes de coordination peuvent être utilisés par les organisations pour collecter des informations et les intégrer dans leurs analyses contextuelles et la gestion des incidents ; à la fois avec des procédures formalisées et également en améliorant les relations professionnelles informelles avec les acteurs clés.

Le chef d'équipe ou le PFS doit déterminer le niveau d'information à partager à l'intérieur comme à l'extérieur de l'organisation, conformément à la politique de sécurité.

Communiquer avec les autorités
Concernant de nombreux incidents, il peut être approprié de partager ce que l'on sait avec la police ou d'autres autorités locales, particulièrement lors d'un incident critique comme un bombardement, une attaque, un enlèvement ou une agression, afin de réduire l'impact et /ou pour réduire la probabilité que des événements similaires affectent d'autres personnes.

L'accord et la collaboration avec le gouvernement hôte sont souvent une composante clé des opérations efficaces des ONG. Par conséquent, dans certains contextes, il est fortement recommandé aux organisations de signaler les incidents aux autorités locales et à la police. Néanmoins, informer les autorités doit se faire sur une base contextuelle, en tenant compte de divers facteurs, et cette décision doit être considérée en amont d'un incident et incluse dans les procédures ou les plans d'urgence de l'organisation.

Communiquer avec les médias

Les incidents de sécurité importants ou critiques peuvent attirer l'attention et la pression de sources externes, en particulier des médias. D'autres incidents peuvent également intéresser les médias, en fonction de leur agenda.

La principale préoccupation devrait toujours être la sécurité des personnes directement touchées par l'incident et le bien-être de leurs collègues et de leurs familles. Le partage de certaines informations peut mettre en danger des vies. Cependant, la rapidité avec laquelle la bonne information circule peut sauver des vies. La manière dont une organisation réagit, non seulement à l'incident, mais aussi à l'information et aux opinions à son sujet, est importante pour la sécurité du personnel et de l'organisation.

Rappelez-vous : une fois que l'information est dans le domaine public, elle ne peut plus être rétractée, alors que des détails supplémentaires peuvent toujours être publiés plus tard.

Les tâches organisationnelles clés doivent être adaptées à l'ampleur de l'incident traité et la responsabilité de celles-ci doit être assignée pendant la phase de planification. Consultez le tableau suivant pour guider le personnel responsable de la préparation de la stratégie de sécurité des communications externes d'une organisation, notamment en ce qui concerne les relations avec les médias.

	Assurez-vous de contrôler vos informations.
	Continuez à suivre les informations disponibles sur l'événement de toutes les sources.
	Prioriser la surveillance des réseaux sociaux pour rester au courant des informations disponibles sur l'incident dans le domaine public. Surveiller les sources en langues locales ainsi que dans la langue de travail du siège et d'autres le cas échéant.
	Identifier ou pré-identifier un porte-parole.
	Chercher à empêcher la publication. Si cela n'est pas possible, corrigez et/ou supprimez les histoires, les messages, les images et les films problématiques de n'importe quelle source. Expliquez que c'est parce que l'attention des médias peut mettre en danger le personnel.
	Assurez-vous que les appels téléphoniques entrants des medias sont consignés avec la date et l'heure et renvoyés au porte-parole principal.
	Préparez des messages clés et des réponses aux FAQ pour les porte-parole principaux et/ou supplémentaires.
	Briefer et préparer le principal porte-parole et porte-paroles supplémentaires.
	Rédiger une déclaration écrite à lire par le porte-parole si nécessaire ; cela aide à s'assurer que les personnes retiennent le message.
	Tenez-vous-en aux faits et n'offrez pas d'informations « hors sujets ».
	Aligner la communication interne et externe.
	Enregistrer les décisions prises et les facteurs qui ont influencé la prise de décision.

	Assurez-vous que l'ONG est considérée comme une source d'information crédible, fiable et sûre.
	Dites la vérité, évitez d'utiliser « aucun commentaire ». Ne spéculez pas. Si une réponse est requise mais que l'information est limitée, émettez une déclaration d'attente.
	Respectez les journalistes et leurs délais et rappelez-les. Inviter les medias à consulter le site Web de l'ONG ou les comptes des réseaux sociaux pour obtenir des mises à jour, Ex. Twitter.
	Proposer d'inclure les médias dans la liste des adresses e-mail de l'agence, en s'assurant qu'ils reçoivent des nouvelles et des communiqués de presse mis en ligne sur Internet.
	Utilisez des outils tels que Twitter pour publier des informations en bref, avec des liens vers le site Web où les déclarations et les communiqués de presse peuvent être lus.
	S'assurer que tous les membres du personnel qui ont des rôles externes (tels que les gardiens et les chauffeurs) connaissent la réponse appropriée à toute

	Gardez toujours à l'esprit que l'objectif principal est la sécurité et la protection du personnel directement concerné.
	Ne divulguez pas les données personnelles des personnes affectées ou impliquées dans l'incident.

Voir le guide de EISF « Gérer le message » pour obtenir des conseils et des outils supplémentaires, y compris un modèle de déclaration d'attente.

Collaborer avec d'autres organisations

Une grande partie du dispositif global de sécurité pour toute organisation humanitaire devrait être une coopération étroite et un partage d'informations avec d'autres organisations et ONGs opérant dans la même zone ou des zones estimées pertinentes sur le plan opérationnel.

La coordination dans la communication est particulièrement pertinente lorsqu'un incident de sécurité concerne un groupe d'individus de différentes organisations. Anticiper cette coordination sera la clé de la réponse immédiate, et une gestion cohérente et coordonnée des incidents et des rapports d'incidents devrait être discutée et convenue à l'avance. Cela peut être traité dans des procédures spécifiques.

Lorsque l'information issue des incidents de sécurité n'est pas collectée, gérée et diffusée horizontalement, il sera difficile d'avoir une image claire de la menace d'une région. Les mécanismes de collaboration en matière de sécurité se développent lorsque la communication verticale et horizontale circule 'en boucle fermée' (c'est-à-dire fournit un retour d'information) et lorsque tous les acteurs travaillent de manière coordonnée.

Un débriefing avec d'autres organisations pertinentes doit rapidement avoir lieu à la suite d'un incident de sécurité, si le partage d'informations est jugé approprié

Le formulaire de rapport d'incident pourrait être utilisé comme document d'orientation pour conduire le débriefing. Le PFS et/ou les responsables concernés devraient identifier à l'avance les données / informations les plus pertinentes pouvant être partagées avec d'autres organisations. Ces décisions devraient toutefois prendre en considération la catégorie d'information dans laquelle se trouvent les différentes parties des données sur les incidents (voir « Objectif 3 »).

Les éléments clés du débriefing de l'incident doivent être axés sur la clarification : qui a fait quoi, où et quand. Afin de protéger les personnes touchées, les organisations ne devraient pas révéler qui était impliqué. Cependant, si l'ethnicité, la nationalité ou d'autres facteurs personnels sont considérés comme fondamentaux, réfléchissez à la façon dont cette information peut être partagée tout en préservant la confidentialité. L'établissement de relations de confiance avant qu'un incident ne se produise est essentiel pour le partage d'informations nuancées.

Un débriefing peut également être vu comme une opportunité de solliciter l'appui d'autres organisations, qu'il s'agisse de soutien logistique, d'assistance, de coordination et de partage d'informations ou, dans des circonstances plus extrêmes, de position politique commune sur une question particulière (voir « Objectif 4 »).

Comme toujours, la décision de partager l'information devrait prendre en compte tout type d'impact possible sur la sécurité du personnel de l'organisation et des autres personnes concernées.

Lorsqu'une organisation reçoit des informations sur un incident de sécurité touchant une autre organisation, en particulier si il s'agit d'un incident critique, il est conseillé de :

- Évitez de contacter l'ONG qui dirige la gestion de l'incident (si l'incident est en cours), à moins qu'il y ait des informations pertinentes à partager qui peuvent les aider à répondre à l'incident.
- Évitez tout type d'interférence sauf si demandé.
- Ne partagez pas davantage l'information (l'ONG concernée décide qui doit être mis au courant).
- Évaluer l'opportunité de mettre en œuvre des mesures spécifiques pour réduire l'exposition de votre organisation à un événement similaire, communiquer ce besoin aux principales parties prenantes internes et mettre en œuvre les mesures de traitement des risques identifiés.
- Définir les informations nécessaires pour expliquer les mesures ci-dessus (si nécessaire) sans divulguer d'informations confidentielles.
- Essayez de réduire les rumeurs possibles au sein de l'organisation en répondant aux questions et en demandant au personnel de maintenir la confidentialité.
- Évaluer la nécessité de revoir et de mettre à jour les mesures de sécurité pour l'organisation.

Les organisations travaillant dans une région similaire devraient utiliser des mécanismes de collaboration pour partager des informations utiles à d'autres organisations dans l'évaluation du contexte sécuritaire. La structuration spécifique de ce type de partage d'information entre différentes organisations est discutée plus en détail dans « l'Objectif 3 ».

1.5 Traitement des cas sensibles : violence sexuelle contre le personnel

Certains incidents doivent être abordés avec attention et un soin particulier, notamment en ce qui concerne la gestion de l'information. L'impact de ces incidents peut avoir des effets d'entraînements particuliers pour les personnes concernées, l'organisation et les organisations humanitaires et de développement en général.

Dans cette section, nous faisons référence aux incidents de sécurité qui sont souvent considérés comme particulièrement traumatisants pour les individus impliqués. Par souci de clarté, nous utiliserons l'exemple spécifique de la violence sexuelle contre le personnel humanitaire, bien que les principes et l'approche de gestion décrits dans

cette section puissent s'appliquer à d'autres types de situations, y compris les enlèvements ou le meurtre de personnel. Les lignes directrices de cette section devraient être utilisées en conjonction avec le reste du manuel, et les utilisateurs devraient réfléchir à l'approche centrée sur les survivants.

Les éléments recueillis par le rapport « Report the Abuse[18] » suggèrent que la violence sexuelle, qui va du harcèlement sexuel au viol, se produit dans les lieux de travail des ONG et que la majorité des auteurs sont des collègues de la victime. Les travailleuses humanitaires sont particulièrement à risque, bien que les hommes puissent également subir des violences sexuelles.

Un rapport publié en 2016 sur ce sujet a montré que seulement 16% des ONG humanitaires évaluées avaient une seule mention de la violence sexuelle comme étant un risque pour le personnel dans leurs politiques et procédures, sans parler des mécanismes de réponse complets, sensibles ou centrés sur les victimes[19].

L'élaboration d'un système approprié de gestion de l'information issue des incidents de sécurité qui inclut l'information sur la violence sexuelle contre le personnel constituera un grand pas en avant vers l'élaboration de meilleures stratégies de prévention et de réponse.

La violence sexuelle contre les travailleurs humanitaires est une menace sérieuse qui non seulement nuit à la sûreté et à la sécurité des membres du personnel, mais peut aussi dégrader considérablement l'efficacité et l'efficience des opérations des ONG. Il est important de considérer la violence sexuelle comme une violation des droits, ce qui signifie qu'une dimension de protection est directement applicable à la gestion de tels cas.

Sous-déclaration : Raisons et obstacles

La déclaration de la violence sexuelle est taboue dans de nombreux contextes, pays et cultures. Il y a plusieurs raisons pour lesquelles les incidents de violence sexuelle pourraient être sous-déclarés dans le contexte humanitaire :

- Manque de connaissance ou absence de canaux ou de procédures pour signaler de tel incident.
- Manque d'investissement organisationnel dans la formation et les connaissances nécessaires pour recevoir des rapports de violence sexuelle.
- Des preuves ou des recours légaux limités, ou des préoccupations selon lesquelles le signalement de l'incident n'entraînera ni justice ni rétribution.
- Préoccupations concernant l'étiquetage discriminatoire, le blâme de la victime ou les réponses taboues sur le viol au sein de l'organisation et de ses employés.
- La honte, la culpabilité ou l'humiliation socialement enracinée au sujet de la violence sexuelle.
- Crainte de représailles, conséquences professionnelles ou personnelles.
- Manque de confiance dans le système de réponse.

Tous ces points sont des raisons pour lesquelles un individu pourrait ne pas signaler un tel incident, et la structure organisationnelle et la culture de l'organisation étayent la plupart d'entre eux. Chaque ONG devrait réfléchir à la culture qu'elle crée et savoir si elle est accessible, communicative, ouverte à une rétroaction constructive, fiable, sensible et centrée sur les survivants. Engager le personnel à tous les niveaux dans des discussions productives et sûres autour de cette question peut considérablement changer certaines des préoccupations qui font que ces incidents sont peu ou pas signalés.

[18] Voir le site Web « Report the Abuse » pour plus d'informations : http://reporttheabuse.org/about/

[19] Nobert, M. (2016). *Liste de contrôle pour la prévention, les politiques et les procedures: Répondre à la violence sexuelle dans les contextes humanitaires et de développement.* Signaler l'abus.

« Pour le moment, il n'existe pas de bonnes pratiques que les ONG pourraient suivre pour prévenir la violence sexuelle sur leur lieu de travail et respecter le devoir de protection qu'elles doivent à leur personnel. Des directives détaillées sur la façon de réagir en cas d'incident sont également indisponibles. Un rapport de bonnes pratiques sur l'abus est en train d'être développé avec le premier outil prévu pour publication au printemps / été 2017[20] ».

Considérations importantes concernant la violence sexuelle et la GIIS :

- **Consentement :** À toutes les étapes de la collecte et de l'utilisation des informations fournies par une victime à propos d'un incident, son consentement doit être obtenu.
- **Formation sur la gestion des incidents de violence sexuelle et l'écriture de rapports :** Les connaissances sur la façon de recevoir des informations sur un incident de violence sexuelle et la façon de réagir de manière appropriée peuvent réduire significativement le traumatisme et créer la confiance dans les structures hiérarchiques d'une organisation.
- **Fournir des définitions claires sur la violence sexuelle :** Informer le personnel de la signification, par exemple, du harcèlement sexuel ou de l'agression sexuelle aidera à établir une politique plus claire.

Voir Outil 2 : Typologie des incidents pour les définitions relatives à la violence sexuelle.

Réponse immédiate

Lorsqu'un incident de violence sexuelle a été signalé ou porté à l'attention de l'organisation par un tiers, le premier plan d'action doit toujours être de s'assurer que la victime se trouve dans un endroit où elle se sent en sécurité et que son état physique, émotionnel et ses besoins sont pris en compte. Une fois que cela a été établi, il y a un certain nombre de mesures recommandées qui devraient être prises pour s'assurer que l'information sur l'incident ne devienne pas une rumeur, ne dégénère pas une situation ou ne mette pas en danger la victime.

Les points focaux désignés sont invités à prendre les mesures immédiates suivantes :

- **Clarifiez les prochaines étapes :** Clarifiez avec la victime quelle est la ligne de conduite qu'elle aimerait que l'organisation prenne. Cette position devrait être vérifiée régulièrement pour voir si la victime est toujours consentante.

- **Confidentialité :** Assurez-vous que les autres membres du personnel qui connaissent l'incident n'en parlent pas à ceux qui ne sont pas au courant. Il est conseillé de leur donner une réponse standard si des questions sont posées, par ex. 'Je ne peux pas répondre à cette question, veuillez contacter le responsable'.

- **Communications :** Établir une ligne de communication directe avec un point focal désigné au siège. Les communications entre le terrain et le siège devraient être gérées et contrôlées uniquement par les personnes désignées sur le terrain. Cette communication ne devrait pas impliquer une série d'intermédiaires. La situation ne devrait pas être discutée là où la discussion peut être écoutée ou entendue.

[20] De plus amples informations sur le contenu de cet outil, et sur la manière dont Reporter un abus aide les organisations humanitaires à lutter contre la violence sexuelle sur leur lieu de travail, peuvent être trouvées en visitant their website ou reaching out directly.

- **Gestion des médias :** Prendre des mesures proactives envers les médias s'il semble que l'incident sera couvert par la presse, persuadant les rédacteurs et les journalistes d'utiliser au maximum les initiales du survivant, et non leur nom complet. Il est conseillé de convenir d'un nom de code, d'un mot de code ou d'un numéro de dossier pour désigner la victime. Toutes les mesures prises concernant la presse doivent être discutées en profondeur avec la victime dans le cas où elles seraient identifiables.

- **Gestion des rapports :** Les lignes hiérarchiques doivent être clairement identifiées avant qu'un incident ne se produise, puis suivies lorsqu'un rapport est produit. Cela doit inclure des lignes alternatives de signalement sur le terrain, en veillant à ce qu'il y ait plusieurs personnes à qui des rapports puissent être faits, de genres, d'orientations sexuelles (si possible), et de milieux culturels différents. Ces personnes doivent avoir une formation appropriée pour recevoir des rapports de violence sexuelle. Il devrait également y avoir des lignes de signalement qui contourneraient le niveau de terrain, pour les situations où la haute direction sur le terrain peut être impliquée ou ne pas faire confiance pour traiter adéquatement un incident de violence sexuelle.

- **Prise de décision en matière de gestion :** en raison de la sensibilité de l'information, des mesures spécifiques doivent être mises en place pour garantir que les statistiques sur les incidents de violence sexuelle ne soient pas perdues.

Les informations sur comment et à qui rendre compte devraient être largement diffusées dans un langage simple et clair à divers endroits d'activités de l'organisation. Cela peut inclure la mise en place de copies papier du processus dans chaque bureau de terrain, en veillant à ce qu'il soit accessible à ceux qui n'ont pas accès aux ordinateurs. En outre, les informations sur le processus de déclaration devraient être disponibles dans toutes les langues pertinentes pour l'environnement opérationnel. Si l'alphabétisation est une préoccupation, des moyens créatifs devraient être employés pour s'assurer que tout le monde comprend ses droits et comment réagir en cas de violence sexuelle. Lors de l'élaboration de systèmes de rapports, ceux-ci doivent prendre en compte les normes culturelles locales et peuvent être différents pour différents membres du personnel, par ex. national et international.

La collecte d'informations

Après un rapport initial, des informations supplémentaires relatives à l'incident doivent être collectées. La collecte des informations de sécurité nécessaires dans ces circonstances exigera probablement une formation et des compétences spéciales pour que l'incident soit traité avec sensibilité, professionnalisme et exhaustivité, d'une manière qui ne nuise pas aux personnes impliquées.

Les conseils suivants guident le personnel qui collecte des informations sur un incident de violence sexuelle :

- Lorsque vous demandez de l'information à la victime au sujet de l'incident, allez-y lentement et laissez-lui du temps pour des pauses et regrouper ses pensées. Commencez avec questions générales et ouvertes jusqu'à ce qu'un résumé complet des événements ait été énoncé. Des questions pour des détails spécifiques peuvent suivre une fois qu'une explication générale a été fournie.

- Être conscient du fait que demander cette information peut être traumatisant pour la victime. Vous pouvez rendre ce processus plus facile en fournissant le temps et l'espace nécessaires pour que la victime parle de son expérience dans un endroit et une atmosphère sécurisés et encourageants, et en étant un auditeur actif et empathique.

- Les questions doivent être posées dans un environnement où la victime se sent en sécurité et à l'aise. L'option d'être accompagné par un collègue, un ami ou un point focal de confiance devrait être respectée et encouragée. Bien que cela puisse sembler un petit geste, s'assurer que des objets tels que de l'eau et des mouchoirs sont présents aidera à créer un climat où le survivant se sentira soutenu.

- Ne posez pas de questions qui perpétuent les tabous du viol ou les attitudes blâmant la victime, telles que : « Êtes-vous sûr que c'est ce qui s'est passé ? », « Que portiez-vous ? » ou « Qu'avez-vous fait pour provoquer cet événement ? ».

- Dans la mesure du possible, recueillez les vêtements de la victime ou tout autre objet pouvant aider à prouver devant un tribunal que des violences sexuelles ont eu lieu. Ces articles doivent être rangés aussi proprement et méticuleusement que les circonstances le permettent.

- Si le survivant ne s'est pas douché ou nettoyé lui-même, encouragez-le à consulter un médecin si cela est possible, y compris la possibilité de prendre une pilule du lendemain ou une prophylaxie post-exposition (PPE). S'assurer que l'accès et l'utilisation de la pilule du lendemain et de la PPE est inclue dans les procédures.

- Après avoir posé des questions à la victime, assurez-vous qu'elle sera dans un endroit sûr avec un soutien adéquat. Bien que votre rôle consiste principalement à poser des questions, vous devez néanmoins confirmer qu'elles ont accès à un soutien psychosocial nécessaire ou à des moyens d'accéder à ces structures de soutien et, si nécessaire, prendre des mesures pour s'assurer que cela est fourni.

- Assurer la victime à tous les stades de l'entretien qu'on la croit, qu'elle sera informée de toutes les étapes suivantes, et qu'elle n'a pas mérité ou causé ce qui lui est arrivé.

- Après avoir recueilli les détails pertinents de l'événement, assurez-vous que ces informations sont stockées de manière sécurisée dans un endroit où elles ne seront pas accessibles ou ne seront pas divulguées. Dans la mesure du possible, utilisez des noms de code, des mots de code ou un numéro de dossier pour désigner la victime, même dans les communications internes.

Nous avons tendance à supposer qu'une personne pourrait être plus à l'aise de communiquer avec quelqu'un du même sexe, mais ce n'est pas toujours le cas et des options devraient être offertes. Ces options devraient inclure, si possible, la diversité des orientations sexuelles, des nationalités, des origines raciales, des religions et d'autres profils divers.

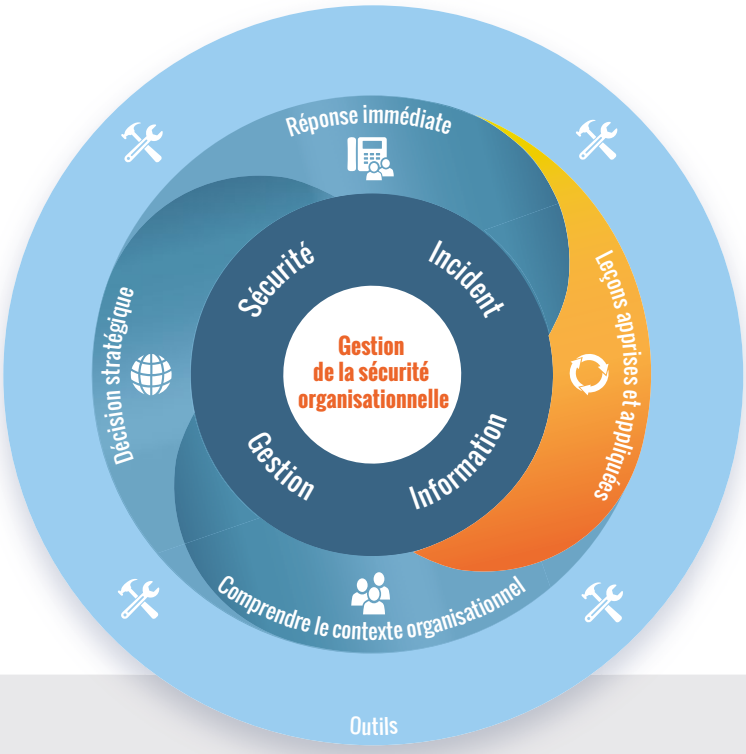
Il convient de noter dès le départ que la collecte d'informations sur les situations sensibles, ainsi que le signalement de tels incidents, doivent protéger l'identité des personnes concernées, sans compromettre le partage d'informations et la sécurité de la communauté humanitaire. En ce qui concerne les signalements, il y a également une ligne de démarcation entre le maintien de la confidentialité de l'incident, l'identité de la victime et l'envoi du message que les victimes devraient avoir honte de leurs expériences. En utilisant une approche sensible axée sur la victime, il est possible de réduire les risques de franchir cette ligne.

Il convient également de noter que le fait d'entendre parler d'incidents sensibles peut être un élément déclencheur pour la personne qui recueille l'information, comme pour celui qui a survécu à l'incident. Un traumatisme vicariant peut survenir et un soutien psychosocial doit être fourni si nécessaire.

Voir Outil 7 : Bonnes pratiques en matière de signalement des incidents liés au genre et mécanismes de plainte pour signaler l'exploitation et les abus sexuels (EAS)

Lorsqu'il existe une possibilité que la sûreté et la sécurité du personnel d'autres ONG sur le terrain soient ou seront compromises, les informations sur l'incident doivent être partagées de manière appropriée avec d'autres organisations ou par des réseaux tels que le Département de la sûreté et de la sécurité des Nations Unies (UNDSS) ou des forums de sécurité d'ONG. La victime doit donner son consentement à ce partage de l'information, et son rôle pour s'assurer que cet événement n'arrive pas à d'autres personnes doit être souligné.

2. OBJECTIF 2 : LEÇONS APPRISES ET APPLIQUÉES



Cette section traite de la gestion de l'information issue des incidents de sécurité dans le but de recueillir des données, de les traiter et de les analyser, de les transformer en informations utiles, de tirer les leçons de l'incident et de mettre en œuvre des actions de suivi. Elle couvre :

- 2.1 Analyse post-incident
- 2.2 Mise en œuvre des leçons apprises
- 2.3 Analyse et suivi des cas sensibles

Outils pertinents :

- Outil 5 : Grilles d'analyse des incidents
- Outil 8 : Plan d'action pour le suivi des incidents

Le deuxième objectif principal de la gestion de l'information issue des incidents de sécurité est de mettre en œuvre les leçons apprises après un incident pour des mesures de suivi et de prévention.

Le but est de comprendre ce qui s'est passé en vue de planifier et de mettre en œuvre les changements et les procédures nécessaires pour prévenir, traiter le risque ou atténuer l'impact d'événements similaires. Cela se produit généralement au niveau du pays / siège peu après l'évènement de sécurité.

Un examen des incidents doit être effectué au sein de l'organisation une fois que l'incident est considéré comme « clos ». Un incident est généralement considéré comme clos par une organisation lorsque les rapports requis ont été produits, les leçons apprises, les protocoles mis à jour, et que l'incident a cessé d'évoluer. Définir le statut d'un incident aide à l'analyse.

Statut de l'incident vs statut de gestion des incidents

Les organisations ont avantage à définir une liste d'états d'incidents qui seront applicables aux événements et à leur gestion. Cela aide le processus de suivi des informations sur les incidents et en particulier l'analyse post-incident :

- Statut d'incident :
  - En cours : toujours en cours.
  - Terminé : l'événement principal est considéré « terminé » par l'organisation.

- Statut de gestion des incidents :
  - Ouvert : l'incident principal est terminé mais la gestion de l'impact et son analyse sont toujours en cours. L'enquête est en cours.
  - Clos : lorsque toutes les leçons apprises et les actions prises sont mises en œuvre.

Pour les incidents de longue durée, tels que l'enlèvement, il est utile d'effectuer un examen intermédiaire en temps réel des actions entreprises après l'événement initial afin que ces apprentissages ne soient pas perdus.

Une analyse à posteriori peut être réalisée avec le personnel directement affecté par ou impliqué dans les réponses et les décisions organisationnelles qui ont pu influencer la manière dont l'incident s'est produit.

Cela nécessite une analyse de l'information qualitative pour une évaluation franche des facteurs qui ont contribués à accroitre la vulnérabilité et influencer les réactions spécifiques qui se sont produites au cours de l'événement. Le processus de collecte d'informations devrait être mené dans une atmosphère de confidentialité et de confiance. Il est important d'éviter de blâmer le personnel affecté à la suite d'un incident.

2.1 Analyse post-incident

L'analyse post-incident considère comment le personnel et l'organisation ont été directement affectés par l'incident et s'ils ont été pris en charge de manière adéquate. Elle examine comment les politiques organisationnelles ou le comportement individuel peuvent avoir contribué à rendre l'incident possible et interroge si de meilleurs conseils peuvent être nécessaires. Elle examine en outre comment les réponses organisationnelles ont contribuées (ou entravées) à atténuer ou résoudre les problèmes qui ont découlé de l'incident.

L'analyse cherche à comprendre les différents «pourquoi» des incidents de sécurité : pourquoi les incidents se produisent-ils et quelles sont les raisons derrière un incident de sécurité ? Cependant, cela n'a d'intérêt que si des mesures appropriées sont prises par l'ensemble de l'organisation pour s'assurer que ces incidents soient moins susceptibles de se reproduire.

Il est conseillé de documenter l'impact réel de l'incident ainsi que les mesures à prendre pour réduire la probabilité qu'il ne se reproduise, ainsi que son impact si c'était le cas. Concernant les incidents critiques, l'analyse doit également inclure une évaluation du processus de gestion, à savoir quelles décisions ont été prises, quand et pourquoi. Le processus écrit est impératif si l'organisation doit systématiquement documenter les leçons apprises de l'incident et refléter cet apprentissage dans les opérations et les politiques futures, ainsi que fournir des preuves de l'apprentissage organisationnel pour renforcer les responsabilités liées au devoir de protection de l'organisation.

Certains points importants à garder à l'esprit lors de la planification d'une analyse d'incident de sécurité peuvent être catégorisés en trois groupes, comme ci-dessous.

Les raisons de mener une analyse d'incident de sécurité :

- Cela aide à comprendre les causes profondes des incidents de sécurité.
- Faire une analyse détaillée est la clé pour identifier de nouvelles ou meilleures mesures d'atténuation, pour renforcer les procédures et le niveau global de sécurité de l'organisation et ainsi permettre un meilleur accès aux populations vulnérables.
- Cela aide à identifier les motifs de l'incident, par exemple, si une attaque est délibérée ou non. La distinction est importante pour comprendre le contexte opérationnel. Si les preuves indiquent qu'un incident a été délibéré, cela aide également à déterminer si, et pourquoi, l'organisation a été délibérément ciblée.
- En incluant des éléments d'analyse dans chaque rapport d'incident de sécurité, une organisation peut ainsi constituer une base d'informations qui permettra l'analyse des tendances.

Une analyse de l'incident devrait se concentrer sur les points suivants :

- Avant l'incident, les procédures ont-elles été suivies et des changements sont-ils nécessaires ?
- Est-ce que l'organisation ou l'individu a été ciblé ? Est-ce parce que quelque chose a provoqué une attaque ? Le membre du personnel affecté était-il perçu comme étant riche ou comme une cible facile ?
- L'organisation n'est-elle plus acceptée dans la région ?
- Quel a été l'impact de l'incident sur les activités du programme ?
- Les procédures de traitement de l'incident étaient-elles appropriées ?

Parmi les facteurs contribuant fréquemment aux incidents de sécurité, nous pouvons citer :

- Gestion inefficace des risques de sécurité et/ou ignorance des procédures.
- Manque de sensibilisation et de formation de base en matière de sécurité.
- Profil de l'organisation dans le pays et comment celle-ci est perçue par la population locale (par exemple, comportement, insensibilité culturelle, etc.).
- Relations interpersonnelles et problèmes personnels (y compris les problèmes internes de ressources humaines).
- Criminalité due à la richesse visible ou perçue.
- Manque d'information entraînant une mauvaise prise de décision en matière de sécurité.

- Prise de risque inutile.
- Incidents de sécurité liés au stress.
- Le personnel repousse les limites où se sent trop à l'aise dans un environnement à risque.

Les organisations devraient considérer le fait de partager avec d'autres organisations leurs conclusions (ou une partie de celles-ci) sur les causes d'un incident et sur la façon de mieux gérer des situations particulières.

Pour plus d'informations, consultez les différents tableaux de l'Outil 5 : Grilles d'analyse des incidents.

Il est important d'analyser un incident dans son contexte global de sécurité (voir « Objectif 3 ») mais aussi à la lumière d'autres incidents, soit dans la zone, soit en suivant des schémas similaires. Cette analyse de tendance est rendue possible grâce à l'enregistrement systématique des incidents au sein de l'organisation. Ceci est discuté plus en détail dans « l'Objectif 4 ».

2.2 Mise en œuvre des leçons apprises

L'avantage le plus évident de la collecte d'informations à partir d'un incident de sécurité est de l'utiliser immédiatement pour adapter les programmes, par exemple modifier les plans de voyage et les visites sur le terrain et ainsi améliorer la sécurité organisationnelle. Le contenu de l'analyse contribuera à déterminer le niveau d'accès, les paramètres du projet et sa mise en œuvre, avec des liens vers les ressources humaines, la budgétisation, le suivi et l'évaluation au niveau opérationnel.

D'autres exemples de leçons apprises à partir de l'information sur les incidents comprennent :

- Des changements immédiats dans les opérations et la mise à jour des POS et des plans de contingence ; analyser ensemble des incidents différents peut entrainer des décisions au niveau du pays.
- Développement de nouveaux indicateurs pour le suivi du contexte de sécurité et l'évaluation des risques.
- Le partage de leçons apprises entre les bureaux à travers le monde permettra d'intégrer ces informations dans l'examen périodique des procédures, des politiques et des plans de sécurité nationaux.

Un bon document d'analyse des incidents de sécurité inclura une section pour les actions recommandées, liées aux causes identifiées. Les bonnes pratiques suggèrent de joindre un plan d'action de suivi au rapport d'analyse des incidents, afin de s'assurer que les recommandations sont effectivement mises en œuvre.

En utilisant le système informatique de l'organisation, il est possible de lier le plan d'action aux outils de planification et d'envoyer des rappels automatiques et des notifications au personnel responsable.

Voir Outil 5 : Grilles d'analyse d'incidents pour des exemples d'actions qui peuvent être mises en œuvre après une analyse par rapport aux causes des incidents.

Voir Outil 8 : Plan d'actions pour le suivi des incidents.

2.3 Analyse et suivi des cas sensibles

L'analyse d'un événement doit respecter les principes suivants : confidentialité, neutralité et professionnalisme.

En cas de violence sexuelle au sein d'une organisation, la principale fonction de la phase d'analyse, aux fins du présent manuel, est de déterminer quelles mesures doivent être prises, administrativement ou juridiquement. Cela différera grandement entre les organisations et les contextes d'opérations.

S'il est possible de le faire sans exposer les détails sensibles de l'événement ou de la victime, consultez ceux qui jouent des rôles similaires sur le terrain pour recueillir des informations sur la situation sécuritaire générale et d'autres incidents de violence sexuelle sur le terrain.

Utilisez cet outil et tout autre outil pour effectuer une analyse de sécurité afin de déterminer si d'autres membres du personnel, l'organisation ou la communauté plus large des ONG sont également à risque de subir des violences sexuelles ou d'autres formes de violence.

L'analyse de ces types d'événements devrait également inclure l'analyse d'impact, y compris le traumatisme primaire et le traumatisme vicariant, ainsi que la formation et d'autres actions réactives qui pourraient être nécessaires pour la prévention de tels incidents à l'avenir.

Consulter les points focaux - sur le terrain et au siège - pour identifier les actions de suivi nécessaires et s'assurer qu'elles sont mises en œuvre. Des consultations supplémentaires peuvent être nécessaires avec les départements des ressources humaines, juridique, éthique, le bien-être du personnel ou les services médicaux, selon les besoins de l'organisation. L'information partagée devrait être fondée sur le besoin de savoir et des mesures visant à faciliter les poursuites doivent être prises à la demande de la victime et avec son consentement. Une action en justice prise dans un contexte particulier peut varier considérablement en fonction du profil de la personne et de l'environnement opérationnel légal. Les besoins et les désirs de la victime de poursuivre l'affaire devraient régir toute action en justice. Consulter le personnel national et les autres acteurs pour déterminer si la justice légale est possible dans le contexte et les risques auxquels la victime pourrait être confrontée en empruntant cette voie. Dans certains endroits, il se peut que ce ne soit pas du tout une option réaliste et, dans de tels cas, il faudra peut-être gérer les attentes.

Même si l'on sait qu'un membre de l'organisation a été victime de violence sexuelle, ou si une victime a pris les mesures nécessaires pour signaler un cas, plusieurs éléments doivent être pris en compte. Tout d'abord, présenter un rapport ne signifie pas automatiquement qu'une victime voudra que les détails soient largement partagés et discutés. À toutes les étapes du processus d'établissement du rapport, la victime devrait être informée et consentir à savoir qui a été informé de son expérience. Il incombe au personnel concerné, au responsable et à l'organisation de protéger l'identité de la victime et la confidentialité des détails de l'affaire[21].

[21] Van Brabant, K. (2010). « Chapitre 12: agression sexuelle » dans *GPR8 – Gestion de la sécurité opérationnelle dans les environnements violents, édition révisée.* Humanitarian Practice Network/ Overseas Development Institute (ODI).

Si une victime souhaite que son identité soit signalée ou partagée, ou que d'autres détails d'identification soient partagés, cela devrait également être respecté. L'approche centrée sur les victimes face aux incidents de violence sexuelle prévoit que les décisions et les désirs de la victime dictent le déroulement du processus de signalement et leurs soins.

L'information sur la confidentialité devrait être communiquée à la victime d'une manière qui indique clairement que tout désir de garder ses caractéristiques d'identification contenues sera respecté. Elle ne devrait pas ressentir le besoin de le faire car elle ne devrait y avoir aucune honte à avoir été soumis à la violence sexuelle. Veillez également à ce que la victime sache qu'elle pourra faire connaître son identité à une date ultérieure, si tel est son choix.

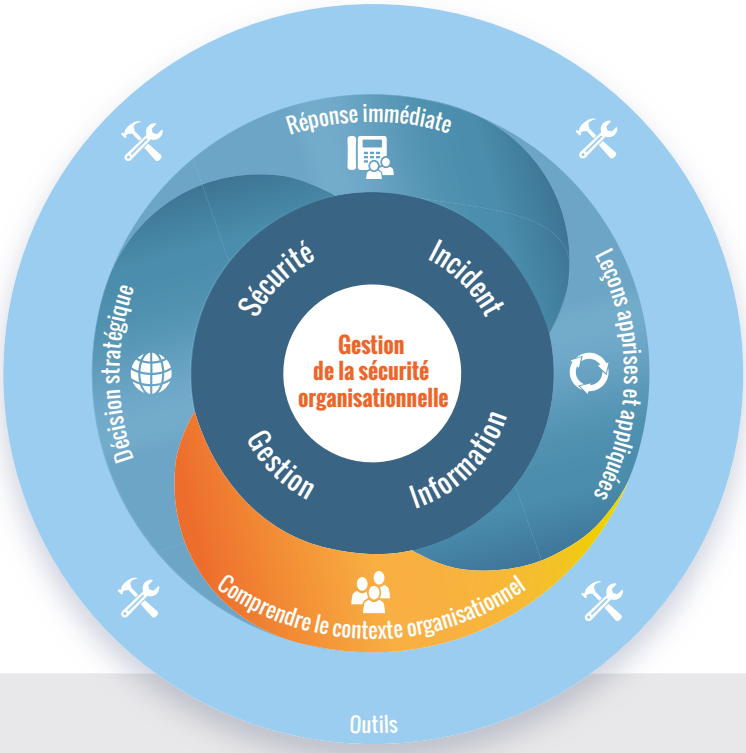
Quelles informations seront communiquées, et à qui, devraient d'abord être discutées avec la victime et obtenir son consentement. Dans certains cas, il n'y a pas d'autre choix que de fournir des détails sur l'incident à d'autres, mais en permettant aux victimes de participer au processus, nous pouvons nous assurer qu'elles reprennent le pouvoir qu'elles ont perdu pendant l'incident de violence sexuelle.

Seuls les détails pertinents doivent être communiqués aux personnes jugées nécessaires, afin de réduire les risques de dommages supplémentaires.

Si nécessaire, pour assurer la sécurité des autres membres de l'organisation, les informations sur l'événement peuvent être partagées avec d'autres employés. Cela devrait être fait d'une manière sensible, en protégeant la victime dans la mesure du possible. Si l'écoute des incidents de violence sexuelle devrait être soulevée, alors assurez-vous que les autres membres du personnel ne subissent pas de traumatisme vicariant et assurez-vous que tous les membres de l'organisation ont accès à un soutien psychosocial.

Tout en maintenant l'approche centrée sur les victimes, l'organisation doit également trouver un moyen de s'assurer que le fait de ces types d'incidents est reconnu au niveau du pays et du siège. Le harcèlement sexuel et la violence sexuelle apparaissent très rarement dans les plans de sécurité nationaux ou dans les registres des risques organisationnels, même lorsqu'ils sont reconnus anecdotiquement comme un problème.

3. OBJECTIF 3 : COMPRENDRE LE CONTEXTE OPÉRATIONNEL



Cette section traite des avantages de comprendre le contexte opérationnel et les moyens de le faire. Elle souligne en particulier comment collaborer avec d'autres organisations afin de partager les informations sur les incidents ainsi que des ressources pour obtenir des informations contextuelles. Elle couvre :

- 3.1 Aspects pratiques du partage d'informations de sécurité
- 3.2 Partage externe d'informations sur les incidents
- 3.3 Forums pour le partage d'informations sur les incidents de sécurité
- 3.4 Ressources externes d'analyse des tendances contextuelles

Outil pertinent :

- Outil 2 : Typologie des incidents

Le troisième objectif principal de la gestion de l'information issue des incidents de sécurité est de comprendre le contexte de sécurité opérationnelle d'une organisation. De bonnes connaissances contextuelles permettent aux organisations de prendre des décisions saines en matière de sécurité et d'opération au niveau national, régional et du siège. L'analyse des modèles d'incidents signalés par les organisations constitue la source d'information la plus efficace sur un contexte de sécurité spécifique.

Toutefois, pour avoir la compréhension la plus complète d'un contexte et obtenir la meilleure utilisation stratégique des informations sur les incidents de sécurité, les analyses de sécurité doivent inclure des informations sur les incidents provenant de plusieurs organisations et de sources multiples.

> *« Les informations sur le contexte général de la sécurité peuvent être obtenues auprès de diverses sources, parmi lesquelles d'autres organisations, les médias (y compris les médias humanitaires et axés sur le développement) et des informations fournies par des fournisseurs de services spécialisés souvent sur une base d'abonnement ».*

Les ONG trouvent souvent utile d'évaluer leurs incidents par rapport à des organisations comparables, que ce soit en termes programmatiques (humanitaires, de développement ou droits de l'homme, etc.) ou de taille (par exemple en termes de présence ou de personnel). Pour les plus petites organisations, il peut être vital d'avoir accès à des informations supplémentaires sur les incidents provenant du même pays avant que des tendances puissent être identifiées.

L'analyse des modèles d'incidents signalés par plusieurs organisations est l'une des sources d'information les plus efficaces du contexte de sécurité spécifique. Les conclusions analytiques tirées d'un aperçu global des incidents de sécurité peuvent être utilisées par les organisations pour évaluer leurs propres tendances et informer les stratégies et la communication au sein des organisations et du secteur humanitaire et de développement dans son ensemble.

L'analyse des tendances peut également être un outil utile pour informer les médias et influencer l'opinion publique et les bailleurs de fonds.

3.1 Aspects pratiques de partage de l'information de sécurité

Les catégories d'information – de confidentiel à public

Le partage de certaines informations peut être considéré comme une obligation pour les organisations et une question stratégique. Dans le cadre de la préparation opérationnelle, les ONG devraient décider quelles informations sur les incidents elles souhaitent partager à l'extérieur et dans quel but. Le tableau ci-dessous fournit un exemple sur la façon dont la sensibilité de l'information peut affecter l'accès à toutes les étapes de la gestion de l'information de sécurité, ainsi que la gestion de l'incident à un niveau plus stratégique au sein d'une organisation.

Classification	Accès
Confidentiel : Les informations confidentielles ont une valeur significative pour l'organisation, et la divulgation ou la diffusion non autorisée de celles-ci pourrait entraîner des dommages sérieux à la réputation ou avoir un impact négatif sur les opérations de l'organisation.	Seuls ceux qui ont vraiment besoin d'un accès explicite devraient l'obtenir, et seulement au moindre degré nécessaire avec (les principes « besoin de savoir » et « privilège minimum »). Lorsqu'elles sont présentes hors des bureaux de l'organisation par exemple dans des ordinateurs portables, des tablettes ou des téléphones, les informations confidentielles doivent être protégées par des ouvertures de session dédiées et éventuellement des dispositifs de cryptage et/ou des plates-formes cryptées.
Limité : La divulgation ou la diffusion de cette information n'est pas prévue, car elle peut avoir un impact sur la vie des gens, entraîner une certaine publicité négative, des dommages à la réputation ou des pertes financières potentielles pour l'organisation.	Particulièrement pour les cas sensibles, telle que la violence sexuelle. Dans de telles circonstances, tout partage d'informations nécessite le consentement explicite de la personne concernée.
Usage interne : La diffusion de l'information aux parties prenantes concernées garantit un bon fonctionnement organisationnel et des réponses internes au sein de l'organisation. Sa sortie ne causera aucun dommage à l'organisation ou à son personnel, mais est néanmoins considérée comme indésirable.	Les informations restreintes sont soumises à des contrôles d'accès pour un petit groupe du personnel. Elles doivent être conservées de manière à empêcher tout accès non autorisé, c'est-à-dire sur un système qui nécessite un utilisateur validé et approprié pour se connecter avant que l'accès ne soit accordé.
Publique : La diffusion de l'information à travers les journaux, des médias et d'autres canaux ne présenterait aucun risque pour l'organisation ou son personnel, et sa publication serait considérée comme souhaitable ou au moins non-répréhensible.	Les informations à utilisation interne peuvent être divulguées ou diffusées aux membres appropriés de l'organisation, aux partenaires et à d'autres personnes, selon ce que les propriétaires de l'information jugent approprié, sans aucune restriction sur le contenu ou l'heure de publication. Les informations publiques peuvent être divulguées ou diffusées sans aucune restriction sur le contenu. La divulgation ou la diffusion de l'information ne doit pas enfreindre les lois ou règlements applicables, tels que les règles de confidentialité.

Lorsque l'on décide de la catégorie d'information à prendre en compte, il faut également tenir compte de l'impact que le 'ne pas savoir' aura sur les autres parties prenantes.

Par exemple, un incident d'enlèvement se produit le long d'une route fréquemment utilisée par de nombreuses ONG opérant dans la région. Cela peut être considéré comme une information confidentielle, car la diffusion de détails sur cet incident pourrait avoir un impact sérieux sur le bien-être du personnel, la capacité à mettre en œuvre des programmes et la réputation de l'organisation. Cependant, ne pas diffuser l'information en temps opportun pourrait entraîner l'enlèvement d'autres personnes. Par conséquent, il est important de savoir comment les informations peuvent être partagées en toute sécurité entre les acteurs horizontalement afin de permettre la restriction de certaines parties de l'information sur l'incident plutôt que sa confidentialité.

Certaines informations ne devraient jamais être divulguées publiquement ou partagées par le biais d'un mécanisme de partage d'informations, telles que des données personnelles de personnes affectées par un incident, y compris des contacts familiaux, etc.

Le partage d'informations sur les incidents et les réseaux sociaux
Ces dernières années, les réseaux sociaux sont devenus une ressource pertinente et importante lorsqu'il s'agit d'obtenir ou de partager des informations liées à la sécurité. Grâce aux moteurs de recherche de Twitter ou Facebook, une énorme quantité d'informations contextuelles et de sécurité peut être trouvée.

Les réseaux sociaux, notamment Twitter et Facebook, peuvent également être utilisés pour alerter, de manière privée, les autres, y compris des groupes de personnes, sur les incidents ou les situations dangereuses. Ces sources d'information doivent cependant être comprises et gérées pour assurer une gestion sécurisée de l'information. Les recommandations ci-dessous peuvent être partagées avec tout le personnel de l'organisation et s'appliquer à chaque étape du cycle GIIS.

Recommandations autour des réseaux sociaux et des rapports d'incidents :

- **Personnaliser les paramètres de confidentialité :** Ajustez les paramètres de confidentialité sur le site et sélectionnez les options qui limitent les personnes autorisées à voir les informations.
- **Séparer personnel et professionnel :** Utiliser différents noms d'utilisateur et photos sur différents sites, car ils peuvent être utilisés pour rechercher des connexions entre des informations professionnelles et personnelles.
- **Attendre avant de poster :** Une fois que quelque chose est mis en ligne, il toujours est présent. Même le contenu qui est supprimé peut parfois être consulté par le site Web ou par des captures d'écran de la publication originale. Le texte qui contient des informations personnelles, un comportement ou des informations sur la localisation peut présenter un risque de sécurité.
- **Désactivez la géolocalisation :** De nombreux sites ou applications de réseaux sociaux demandent l'accès à l'emplacement de l'appareil, mais dans la plupart des cas, cela n'est pas nécessaire. En plus d'accéder à l'emplacement de l'appareil, certains sites rendent cette information publique. Lorsque des personnes se connectent sur des sites comme Facebook, elles peuvent partager leur position exacte avec d'autres.

En raison de la nature des plateformes et de la vitesse à laquelle l'information est partagée sur les réseaux sociaux, l'information n'est pas vérifiée et peut ne pas être fiable. Les organisations doivent prendre en compte la source et la fiabilité des informations relatives à la sécurité et à la confidentialité de celles-ci, avant toute prise de décision ou partage.

« Un groupe WhatsApp créé dans le but d'informer chaque PFS d'une région d'incidents se produisant dans sa zone de responsabilité doit être géré avec soin. Seul l'administrateur devrait pouvoir ajouter des membres au groupe. Tout ajout devrait être validé et au moins communiqué à tous les membres. Les règles et les codes de communication doivent être convenus et les participants doivent s'assurer que l'accès à cette conversation WhatsApp est protégé, en cas de perte ou de vol de leur téléphone ».

3.2 Partage externe d'informations sur les incidents

Le partage avec d'autres organisations

Le partage d'informations sur la sécurité, les rapports d'incidents et de situations, et l'analyse des vulnérabilités entre les organisations ne se font pas naturellement[22]. Cependant, il est de plus en plus reconnu que le partage d'informations de sécurité dans un contexte opérationnel spécifique et la notification rapide des incidents à d'autres ONG de la zone relèvent de la responsabilité collective[23].

Les organisations peuvent partager des informations directement les unes avec les autres, via des forums ou via des services de partage d'informations sur la sécurité des ONG (voir « Forums de partage d'informations sur les incidents de sécurité » et « Ressources externes d'analyse des tendances contextuelles » ci-dessous).

Il existe malheureusement de nombreux obstacles potentiels au partage d'informations sur la sécurité entre les organisations :

- La mise en commun des données pour mieux comprendre les caractéristiques uniques des incidents de sécurité des ONG nécessite que les organisations soient disposées à partager leurs données globales d'incidents de sécurité sur la base d'accords de confidentialité.
- La structure organisationnelle, la mission, la culture, le clan et les différentes conceptions régionales, religieuses, historiques et ethniques peuvent entraver la collaboration et le partage d'informations pertinentes sur la sécurité.
- Certaines organisations (ou individus au sein d'une organisation) peuvent percevoir la sécurité comme un obstacle aux opérations alors que d'autres peuvent mettre trop l'accent sur leur autonomie, ne pas s'associer ou collaborer avec d'autres parties prenantes dans la région.
- Un conflit de personnalités entre des acteurs clés en matière de sécurité peut sérieusement entraver la coopération et la collaboration. Bien que l'importance des relations interpersonnelles pour établir la confiance ne puisse être surestimée, les réseaux formels fournissent une base pour construire des structures plus formel les de partage de l'information qui ne dépendent pas uniquement de la personnalité de chacun et ainsi se poursuivre malgré les changements du personnel.

[22] Schafer, J. and Murphy, P. (2010). *Collaboration en matière de sécurité: Guide des meilleures pratiques*. InterAction Unité de Sécurité – InterAction.

[23] Van Brabant, K. (2010). *GPR8 – Gestion de la sécurité opérationnelle dans les environnements violents, édition révisée.* Humanitarian Practice Network/Overseas Development Institute (ODI).

- Le manque général de ressources humaines et financières disponibles pour la sécurité empêche souvent les organismes de contribuer ou de participer pleinement aux efforts de collaboration.
- L'approche de la sécurité peut être considérablement différente entre les organisations. Ces différences peuvent rendre difficile la collaboration sur les services de sécurité communs, mais la coordination et le partage d'informations et d'approches aideront toutes les parties à mieux comprendre le contexte et à mettre en œuvre des mesures de gestion des risques de sécurité mieux éclairées et efficaces.
- Les préoccupations concernant l'utilisation indiscrète d'informations sensibles partagées dans les mécanismes de coordination peuvent souvent constituer un obstacle important au partage d'informations. Il y a des exemples d'informations partagées dans des forums qui apparaissent dans la presse, bien que ce soit une exception. Il est important d'être pleinement informé de la nature exacte de tout mécanisme de coordination, de la manière dont l'information est traitée, des attentes et des responsabilités en matière de traitement de l'information et des conséquences de toute violation des termes de l'accord.
- La sécurité n'est qu'une des nombreuses priorités des organisations lors de la mise en œuvre des programmes. Cependant, il a été démontré à maintes reprises que les mauvaises pratiques de sécurité et le manque de coordination de la part d'une organisation peuvent avoir un impact sur la capacité de la communauté dans son ensemble à obtenir et conserver l'accès pour les opérations humanitaires et de développement.

Une fois que les obstacles au partage de l'information sont identifiés, les collaborateurs devraient s'appuyer sur leur professionnalisme et leurs acquis pour trouver un terrain d'entente et travailler vers une solution mutuellement convenue

Il est important de se rappeler que le comportement d'une organisation peut avoir un impact sur la sécurité de tous. Si une organisation ne transmet pas les informations importantes sur les incidents, y compris les quasi-incidents, une autre organisation peut subir un événement avec des conséquences importantes, plutôt que d'être capable de l'éviter ou d'en limiter l'impact. La collaboration est la clé de la connaissance contextuelle et de la sécurité organisationnelle globale.

Le partage avec les bailleurs de fonds
Certaines organisations envoient des rapports d'analyse post-incident aux bailleurs de fonds pour accompagner les rapports trimestriels ou à mi-parcours s'il y a eu une interruption dans la programmation en raison de l'insécurité croissante ou d'un plus grand nombre d'incidents. Les rapports aident à informer les bailleurs de fond de la situation sur le terrain et appuient les décisions sur l'extension du programme. L'organisation devrait décider stratégiquement si elle souhaite partager ses rapports d'incident avec les bailleurs, tout en s'assurant qu'ils respectent toutes les exigences contractuelles.

3.3 Forums pour le partage d'informations sur les incidents de sécurité

Vous trouverez ci-dessous des informations sur certains forums et groupes dédiés à la coordination et à la collaboration en matière de sécurité, spécialisés dans la collecte, l'analyse et le partage d'informations sur les incidents de sécurité.

Chacun a un mandat différent et donc différents mécanismes de collecte et de partage de l'information. Cependant, tous sont d'excellentes sources d'information et peuvent aider à améliorer la gestion des risques de sécurité.

- **Plateformes globales de base de données d'incident**
  - AWSD : Aid Worker Security Database (Base de données sur la sécurité des travailleurs humanitaires)
  - SiND : Security in Numbers Database (Base de données de sécurité en chiffres)
- **Niveau du siège**
  - EISF European Interagency Security Forum (Europe)
  - InterAction (États-Unis)
  - Dutch Security Network (Pays Bas)
  - UK NGO Security Focal Point Group (Royaume Uni)
  - CINFO – Communauté de pratique de sécurité (Suisse)
  - Coordinadora Security Working Group (Espagne)
  - Canadian Interagency Security Forum (Canada)
- **Niveau Régional**
  - Forum sur la sécurité et la sûreté humanitaires dans la région Moyen Orient et Afrique du Nord
  - Forum régional de la sécurité en Afrique de l'Ouest
- **Niveau Pays**
  - International NGO Safety Organisation (INSO) et ses bureaux régionaux
  - Pakistan Humanitarian Forum
  - NGO Forum – Soudan du Sud
- **Autres**
  - Réunions sécurité avec des agences des Nations Unies, dans le cadre « Saving Lives Together » (SLT) Framework

Certaines des informations fournies par ces forums seront publiques (sources ouvertes) alors que d'autres peuvent nécessiter une adhésion. Les organisations devraient contacter les forums globaux, régionaux, locaux et/ou sur le terrain pour la coordination et le partage de l'information en matière de sécurité, selon les besoins et si ils sont disponibles.

3.4 Ressources externes d'analyse des tendances contextuelles

> *« Les ONG pourraient trouver utile de comparer leurs tendances en matière d'incidents à celles d'organisations similaires. Une telle approche nécessite le partage de données sur les tendances clés entre les organisations dans un format anonymisé qui ne permet plus l'identification d'une seule organisation ».*

Les responsables de la sécurité et les analystes doivent envisager l'analyse des informations internes sur les incidents ainsi que des informations de sécurité collectées à l'extérieur, notamment par le biais de réseaux de partage d'informations.

Les informations sur les incidents externes permettent une meilleure connaissance contextuelle de l'environnement opérationnel de l'ONG.

L'utilisation de classification standardisée facilite la comparaison des informations entre les organisations. Les classifications standard sont fournies par le projet Aid In Danger.

Outil 2 : Typologie des incidents

Le tableau ci-dessous donne une vue instantanée de quatre ressources clés qui fournissent des données d'incidents de sécurité et/ou des tendances basées sur des informations d'incidents de sécurité provenant de sources multiples. Il est suivi par des informations plus détaillées sur chacune de ces ressources.

Nom	Principales caractéristiques
AWSD	Fournit une description des incidents dans lesquels le personnel a été tué, blessé ou enlevé. Un rapport annuel offre un aperçu et une analyse des tendances mondiales.
ASWD et AiD	Fournit un bulletin mensuel d'événements en sources ouvertes ; des aperçus des tendances couvrant un large éventail d'incidents (au-delà de ceux dans lesquels des membres du personnel ont été tués, blessés ou kidnappés) ; et une analyse des incidents de sécurité partagés et mis en commun par les organisations. Fournit également un accès aux données via Humanitarian Data Exchange.
INSO	Fournit des informations sur les incidents à ses organisations membres dans les pays où il est présent. INSO fournit également un tableau de bord montrant les données d'incidents clés.
Saving Lives Together	Le cadre « Saving Lives Together » (SLT est une initiative conjointe des Nations Unies, d'organisations internationales et d'ONG. Les organisations partenaires de l'initiative SLT reçoivent divers rapports d'incidents du Département de la sûreté et de la sécurité des Nations Unies (UNDSS).

AWSD La base de données sur la sécurité des travailleurs humanitaires
Aid Worker Security Database (AWSD), un projet de Humanitarian Outcomes, enregistre les principaux incidents de violence contre les travailleurs humanitaires, avec des rapports d'incidents de 1997 à nos jours. Initié en 2005, ASWD est la seule ressource globale complète pour les statistiques sur les attaques majeures contre les opérations d'aide aux civils, et fournit la base de preuves pour l'analyse de l'environnement de sécurité changeant pour une réponse humanitaire.

Les données sur les incidents sont collectées à partir de sources publiques, via un filtrage systématique des médias / réseaux sociaux, et à partir des informations fournies directement par les organisations humanitaires et les entités de sécurité opérationnelle. Le projet maintient également des accords avec un certain nombre de consortiums de sécurité régionaux et sur le terrain pour le partage direct d'informations et la vérification des incidents. Les rapports d'incidents sont recoupés et vérifiés chaque année avec toutes les organisations humanitaires pertinentes. Cela inclut les Nations Unies, les ONG locales et les ONG internationales en plus des consortiums de sécurité dans le pays.

Actuellement dans sa cinquième année de mise en ligne, ASWD est la seule base de données interactive accessible au public en son genre. ASWD permet aux organisations de télécharger l'intégralité de des données et offre une interface de programmation pour le développement externe d'applications utilisant des données d'ASWD.

Le rapport annuel sur la sécurité des travailleurs humanitaires est basé sur des preuves empiriques provenant des données, offre des éclairages et des analyses sur les tendances globales ainsi que des recommandations sur des questions cruciales de sécurité opérationnelle.

Pour plus d'informations ou pour apporter des informations et des modifications à ASWD, veuillez envoyer un courriel à info@humanitarianoutcomes.org.

Le projet d'Aid id in Danger

Le projet « Aid in Danger » d'Insecurity Insight surveille systématiquement les rapports de sources ouvertes pour les incidents qui affectent négativement la distribution de l'aide et collabore avec les partenaires des organisations d'aide pour collecter et combiner leurs rapports d'incidents de sécurité. Toutes les données sont stockées dans la base de données SiND (Security in Numbers Database) pour l'analyse. Le projet a débuté en 2008 en tant que sous-produit de l'initiative Soins de santé en danger du CICR. Aid in Danger vise à surveiller l'impact de la violence et les actes délibérés qui interfèrent avec la fourniture de l'aide. Le projet 'Aid in Danger' suit une série d'incidents qui affectent la fourniture de l'aide : des menaces de violence aux décisions administratives, refus de permis ou de visas, à la destruction des infrastructures et de l'impact de la criminalité. Le projet surveille également les enlèvements, les décès et les blessures du personnel.

Pour respecter les préoccupations de confidentialité des organismes participants, la base de données SiND n'est pas accessible au public. Les ensembles de données contenant des sous-ensembles sélectionnés à partir desquels des informations personnelles identifiables ont été supprimées, sont disponibles sur la page Insecurity Insight du Humanitarian Data Exchange.

Le projet « Aid in Danger » publie un rapport mensuel sur les événements déclarés en source ouverte, des mises à jour régulières, des analyses de tendances et un aperçu des données confidentielles des organisations en coopération avec EISF.

Pour plus d'informations ou pour devenir une organisation participante, veuillez envoyer un courriel à info@insecurityinsight.org.

INSO International NGO Safety Organisation

L'International NGO Safety Organisation INSO est le principal mécanisme de coordination de la sécurité pour les ONG opérant dans des contextes à haut risque, avec plus de 850 membres dans le monde.

Fondée en 2011, l'organisation humanitaire britannique travaille sur le terrain pour fournir aux ONG enregistrées une gamme de services gratuits incluant le suivi des incidents en temps réel, les rapports analytiques, la cartographie, le support aux incidents critiques, la gestion des crises, l'orientation du personnel, la formation sur la sécurité personnelle, la gestion de la sécurité et la gestion de crise. Les plateformes INSO sont actuellement actives en Afghanistan, en Irak, en Syrie, en Palestine (Gaza), en Somalie, au Kenya, en RDC, en RCA, au Cameroun, au Nigeria, au Mali et en Ukraine, avec de nouvelles ouvertures chaque année.

L'inscription à INSO est strictement limitée aux ONG locales et internationales et doit être demandée dans le pays d'opération. Les plateformes INSO appliquent un code de conduite strict dans lequel les membres partagent les informations entre eux de manière confidentielle.

Au niveau mondial, l'INSO fournit des données d'incidents de sécurité d'ONG via son tableau de bord de données clés (Key Data DashBoard) et lancera en 2018 le Centre de données sur les conflits et les affaires humanitaires, CHDC (Conflict and Humanitarian Data Center) qui est une base de données centralisée contenant tous les incidents collectés sur son réseau de plateformes.

Avec plus d'un million d'entrées initiales, le CHDC sera l'un des plus grands référentiels mondiaux de ce type et soutiendra la recherche contextuelle à long terme ainsi que l'analyse tactique plus immédiate.

Les ONG éligibles qui ne sont pas déjà enregistrées sont invitées à contacter l'INSO via leur page d'inscription ou via info@ngosafety.org.

« Dans certains pays, les incidents de sécurité peuvent être considérés en relation avec les événements signalés par l'INSO. Au niveau mondial, les organisations peuvent consulter la base de données sur la sécurité des travailleurs humanitaires pour les cas critiques d'enlèvements de personnel, de blessures ou de décès. Pour un plus grand nombre d'incidents, les organisations peuvent rejoindre la base de données Aid in danger – SiND ».

Le cadre de Saving Lives Together

Le cadre « Saving Lives Together » (SLT) est une initiative conjointe des Nations Unies, des organisations internationales (OI) et des ONG. Initié en 2006 et révisé en 2015, le cadre SLT reconnaît que les Nations Unies et leurs organisations partenaires– OI et ONG – font l'objet de menaces sécuritaires collectives et souligne l'importance de la collaboration « pour assurer la sécurité de l'aide humanitaire et au développement ». L'objectif de SLT est « d'améliorer la capacité des organisations partenaires à prendre des décisions éclairées et à mettre en œuvre des dispositions de sécurité efficaces pour améliorer la sûreté et la sécurité du personnel et des opérations[24] ». Les organisations partenaires du cadre SLT reçoivent des rapports d'incidents quotidiens de UNDSS.

Les recommandations de SLT, tout en se concentrant principalement sur la collaboration entre l'ONU et les ONG internationales, fournissent des indications intéressantes aux organisations pour renforcer la collaboration dans la gestion de l'information sur les incidents[25].

Le cadre SLT et les notes d'orientation peuvent être téléchargés ici.

Pour plus d'informations contacter UNDSS dans le pays ou au via :

M. Lloyd Cederstrand, OCHA (Liaison opérationnelle et coordination) : cederstrand@un.org

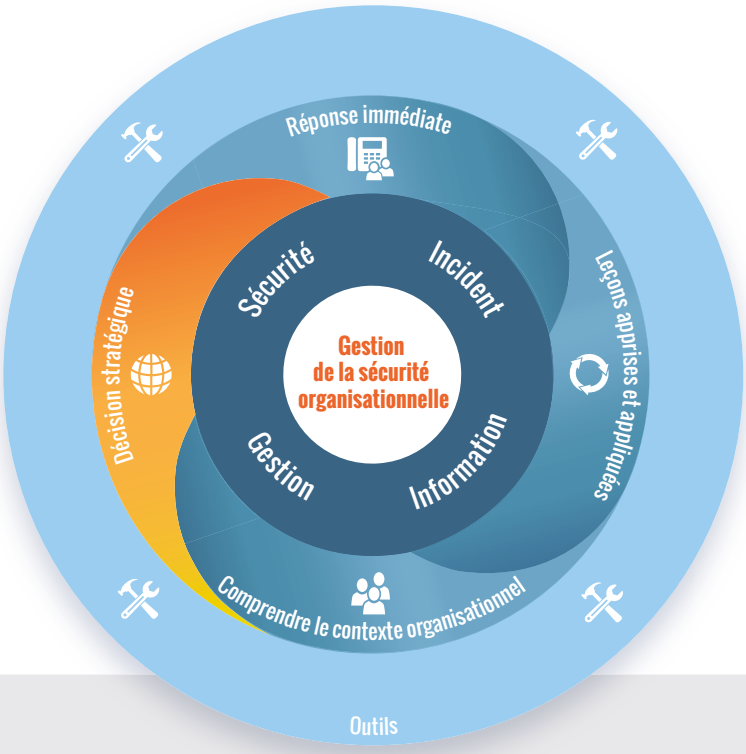
Centre de communications de l'UNDSS (Assistance aux communications d'urgence 24/7) : undsscomscen@un.org, Tel : +1 917 367 9438/9

Directeur exécutif d'EISF : eisf-director@eisf.eu.

[24] Comité permanent interorganisations (CPI). (2015). « Saving Lives Together – Un cadre pour améliorer les accords de sécurité entre les organisations intergouvernementales, les ONG et les Nations Unies sur le terrain (Octobre 2015) », CPI.

[25] L'initiative SLT ne signifie pas que l'ONU assume la responsabilité de la sécurité de l'ensemble de la communauté humanitaire. L'ONU peut disposer de ressources telles que des avions pour les évacuations et des équipements de communication qu'elle utilisera, quand ils le pourront, pour soutenir la communauté des ONG, mais ce n'est pas une obligation, et tous les coûts encourus seront probablement transférés à l'ONG. Les ONG doivent assumer la responsabilité de leur propre sûreté et sécurité et les utiliser comme il se doit. La même chose s'applique à la gestion de l'information sur les incidents.

4. OBJECTIF 4 : PRISE DE DÉCISION STRATÉGIQUE



Cette section traite de la gestion de l'information issue des incidents de sécurité dans le contexte de la prise de décisions stratégiques, principalement au niveau régional ou au siège. L'objectif est d'aider les points focaux de sécurité et les analystes à enregistrer l'information issue des incidents de sécurité de manière systématique, à utiliser l'informations issue des analyses de tendances et à communiquer les résultats aux principales parties concernées à l'intérieur comme à l'extérieur de l'organisation. Le but est d'informer les décideurs stratégiques afin de s'assurer que l'information sur l'incident est prise en compte à tous les niveaux de la planification, des procédures et des projets organisationnels. Elle couvre :

- 4.1 Enregistrement systématique des incidents : quel système utiliser?
- 4.2 Analyse des tendances pour éclairer la prise de décision stratégique
- 4.3 Structures organisationnelles pour discuter des questions stratégiques de sécurité
- 4.4 Comment utiliser l'information issue des incidents de violence sexuelle à un niveau stratégique
- 4.5 Utilisation de l'information issue des incidents de sécurité pour le plaidoyer stratégique

Outils pertinents :

- Outil 2 : Typologie des incidents
- Outil 9 : Systèmes GIIS
- Outil 10 : Conservation de l'information issue des incidents
- Outil 11 : Technologie pour signaler et enregistrer les incidents
- Outil 12 : Analyse et comparaison des tendances des données
- Outil 13 : Questions de niveau stratégique pour les décisions relatives à la gestion des incidents

Le quatrième objectif principal de la gestion de l'information issue des incidents de sécurité est d'éclairer la prise de décision stratégique au sein d'une organisation.

Une analyse régulière au niveau du siège doit être effectuée pour identifier les tendances et les modèles afin d'éclairer la prise de décision stratégique à long terme pour l'ensemble de l'organisation. L'objectif est de faire le point sur la nature changeante des incidents de sécurité, de comprendre les environnements de travail les plus difficiles, l'exposition globale de l'organisation au risque et d'identifier les meilleures réponses stratégiques.

La vision est devenue plus globale avec l'amélioration des technologies de communication et la disponibilité de l'information dans le monde entier. Les incidents ne peuvent plus être considérés comme un problème purement national. Par exemple, une campagne de l'organisation dans une région déterminée peut avoir un effet papillon.

L'analyse de l'information issue des incidents a des implications pour une bonne gestion à plus grande échelle, ce qui peut inclure des décisions concernant :

- Où opérer ?
- Comment communiquer sur les programmes ;
- Quelles polices d'assurance sont nécessaires ;
- Dans quelle mesure la gestion des risques de sécurité doit-elle être budgétisée pour les opérations nationales ?

L'analyse de la sécurité peut également être utilisée pour mettre en évidence des préoccupations plus générales concernant le mandat principal d'une organisation et les difficultés d'accès aux populations bénéficiaires.

Certaines organisations réalisent ce type d'analyse sur une base annuelle, d'autres plus fréquemment. Outre les revues pré-planifiées, des révisions ponctuelles doivent être effectuées chaque fois qu'il y a un changement significatif dans la mission, le profil ou les contextes opérationnels de l'organisation. Chaque ONG profite régulièrement de la revue de son profil d'incident de sécurité. Cette analyse est rendue possible grâce à un flux d'informations effectif entre les bureaux extérieurs et le siège et à un système efficace qui enregistre les incidents signalés de manière systématique et standardisée afin de faciliter l'analyse comparative et la prise de décision stratégique.

La prise de décision stratégique en matière d'information issue des incidents de sécurité devrait prendre en compte l'analyse des informations internes sur les incidents ainsi que les informations de sécurité collectées à l'extérieur, notamment par le biais de réseaux de partage d'informations. La comparaison des tendances internes avec les tendances externes peut signaler des vulnérabilités internes clés et des éléments de gestion des risques de sécurité qui nécessitent un traitement au sein de l'organisation.

4.1 Enregistrement systématique des incidents : quel systéme utiliser ?

Un bon système d'enregistrement, de stockage, de classification et de récupération des données relatives aux incidents de sécurité est un élément essentiel de l'analyse des incidents de sécurité et de la prise de décision stratégique. Les organisations ont mis en place différents mécanismes pour signaler, collecter et enregistrer les incidents au niveau national dans un lieu déterminé. En ce qui concerne les systèmes en ligne, il existe de nombreuses solutions qui vont des modèles libres, en source ouverte, facilement personnalisables aux systèmes sur mesure préparés par des sociétés privées.

Quel que soit le système utilisé par une organisation, il est important que le système d'enregistrement et de cartographie des incidents soit conçu pour répondre aux besoins de tous les utilisateurs, du débriefing à l'analyse des tendances. Les nouvelles technologies sont d'apport important dans ce domaine.

Il existe deux approches qu'une ONG peut utiliser en utilisant la technologie pour développer un système d'enregistrement et de cartographie des incidents :

- Soit une solution autonome intégrée dans les serveurs et les systèmes de l'organisation ; ou
- Soit un 'logiciel en tant que service' lorsque le système est hébergé par un fournisseur de services externe.

La décision sur l'approche à adopter dépendra de facteurs tels que la stratégie technologique de l'organisation, sa taille, du nombre probable d'incidents, des ressources et des capacités à gérer le système ainsi que la protection des données. Le tableau suivant récapitule certains des systèmes disponibles pour signaler, stocker et analyser les incidents de sécurité affectant une organisation au niveau central.

	Rapport d'incident et système d'enregistrement	Méthode
Système conçu et géré à l'intérieur	Récit écrit de l'incident ; associé à une feuille de calcul pour enregistrer les incidents à l'aide d'un codage systématique.	Cela peut se faire via des courriels électroniques, des documents ou des feuilles de calcul Google, une plateforme Google partagée, une plateforme de partage. Un tableur peut être utilisé pour classer les informations soumises dans un format écrit en utilisant des champs de données spécifiques qui doivent être complétés.
	Système en ligne utilisant des plateformes de source ouvertes existantes.	Le système de signalement d'incidents peut être construit en tant qu'extension de plateformes existantes utilisées pour le courriel électronique, telles qu'une plateforme de partage. Les plates-formes en ligne comme Ushahidi peuvent être personnalisées pour créer un système global de rapport d'incident et de gestion de l'information.
Systemes externes	Abonnement à une plateforme en ligne pour la gestion des données	Certaines entreprises privées et organisations à but non lucratif proposent des plateformes en ligne pour la gestion de l'information sur les incidents de sécurité.
	Système en ligne personnalisé	Certaines organisations ont commandé le développement de systèmes en ligne spécifiques à l'organisation.

Voir l'Outil 9 : Systèmes GIIS pour un tableau plus détaillé illustrant les systèmes disponibles pour la gestion de l'information issue des incidents et un résumé des inconvénients et des avantages de ces différents systèmes.

Les organisations de petites tailles ou les ONG disposant de ressources limitées peuvent opter pour les deux premières méthodes d'enregistrement et de compte rendu des incidents, étant donné la simplicité de la mise en place et de la maintenance de ces systèmes, ainsi que leur coût relativement faible. Les systèmes les plus avancés peuvent convenir à des organisations plus importantes, confrontées à un nombre élevé d'incidents et nécessitant un système flexible correspondant aux besoins spécifiques de l'organisation[26].

Les outils de stockage d'incidents

Un modèle de base de stockage des incidents doit contenir les informations suivantes :

- **Pays, région et lieu** – Soyez précis.
- **Date et heure de la journée** – Quand l'incident s'est produit, combien de temps il a duré et quand l'incident s'est-il terminé.
- **Qu'est-il arrivé** – Un résumé succinct et concis de l'incident
- **Catégorie d'incident** – Catégories analytiques pour l'analyse des tendances de données - voir les outils 2 et 10 pour les options suggérées
- **Qui a été impliqué** – A la fois interne et externe, à la fois les victimes et le soutien de la direction.
- **Actions et décisions prises** – Résumé des actions / décisions clés prises et par qui.
- **Changements opérationnels** – Aperçu des changements immédiats apportés en réaction à l'incident.
- **Analyse et commentaires** – Résumé du document d'analyse suite à l'incident.
- **Statut** – L'incident de sécurité est-il toujours en cours ? Est-ce que toutes les informations ont été documentées ?

Ce manuel fournit des exemples d'outils de stockage d'incidents dans Excel. Ces documents peuvent être trouvés sous Outil 2 : Typologie de l'incident et Outil 10 : Conservation de l'information issue des incidents.

Les besoins d'analyse et de statistiques futurs doivent être identifiés avant la conception de l'outil de stockage des incidents. Des colonnes doivent être créées pour permettre l'analyse des tendances et le développement de statistiques à l'aide des paramètres Excel.

Les systèmes en ligne

Les fonctions clés qu'une organisation peut rechercher dans un système en ligne :

- Un référentiel unique d'incidents sur le Web ;
- L'accès à des rapports électroniques à partir d'un PC connecté à Internet ou d'un appareil mobile ;
- La notification de différents groupes en fonction des détails du rapport d'incident soumis ;
- L'assurance de la sécurité des données – les informations soumises ne sont accessibles que sur une base contrôlée, sur la base du « besoin de savoir » ;
- L'assurance que les données sont protégées pendant la transmission ;
- L'assurance que les données sont sauvegardées.

[26] De Palacios, G. (2017, à paraître). « Gérer les informations liées à la sécurité: un examen plus approfondi des systèmes de signalement des incidents », *EISF*.

Les éléments clés à décider :

- Comment les utilisateurs finaux vont alimenter le référentiel ;
- Comment s'assurer que l'accès au référentiel est sécurisé sur la base du « besoin de savoir » ;
- Comment notifier différents groupes de personnes en fonction des détails de la soumission d'incident ;
- Comment s'assurer que l'information est capturée entièrement et précisément à partir de la source de l'incident ;
- Comment valider électroniquement les informations capturées ;
- Dans quelle mesure le système serait-il utilisé pour le suivi des cas (serait-ce seulement un dépôt ou y aurait-il aussi des étapes de suivi ?) ;
- Sur quel type de fonction d'analyse s'appuie-t-on pour élaborer, construire pardessus.

Les éléments clés à mettre en place avant de se lancer dans le développement d'un système en ligne :

- Définir les catégories d'incidents ;
- Donner des instructions claires pour les utilisateurs sur les catégories.

Quels que soient les outils et les systèmes, il est important de définir, techniquement, qui accède aux données stockées sur le terrain, au niveau national, régional et au siège. Les mots de passe, les cryptages, les groupes fermés, les processus de validation par les pairs pour l'accès, etc. sont des exemples de méthodes qui peuvent être utilisées pour s'assurer que l'information est partagée avec les parties prenantes appropriées. Voir « Introduction – Sécurité de l'information » pour plus de détails sur la sécurité de l'information.

Voir l'Outil 11 : Technologie pour signaler et enregistrer les incidents afin d'obtenir des exemples et des descriptions de systèmes en ligne pour l'enregistrement et la déclaration les incidents.

4.2 Analyse des tendances pour éclairer la prise de décision stratégique

Une fois les informations issues des incidents consolidées dans un système central y compris les catégories analytiques, il est possible d'analyser de manière plus stratégique les informations de sécurité pour guider les décisions.

Les responsables de la sécurité, les points focaux et les analystes doivent transformer les données en informations utiles. Cette information sera partagée sous forme de tendances et de statistiques avec les cadres supérieurs identifiés pour soutenir les processus décisionnels.

La plupart des organisations classent les incidents de sécurité et de sûreté. La catégorisation facilite l'analyse et l'extraction de statistiques.

Les données peuvent être ventilées par catégories clés (Outil 2: Typologie des incidents) et présentées sous forme de rapports de synthèse d'analyse des tendances (Outil 12 : Analyse et comparaison des tendances des données).

La nature de cette analyse au niveau stratégique dépend du nombre d'incidents de sécurité signalés dans une organisation. S'il n'y en a qu'une poignée, une note écrite qui résume les principaux événements peut être la meilleure méthode pour présenter les tendances. Si le nombre d'événements signalés augmente, il sera important de développer un suivi plus systématique des tendances basées sur des statistiques.

La liste de questions suivante peut aider les points focaux de sécurité à élaborer des conclusions stratégiques et des recommandations d'action supplémentaires à la suite d'une bonne analyse des incidents de sécurité sur des événements passés.

- Quels types d'incidents de sécurité le personnel et l'organisation ont-ils rencontrés ?
- Dans quels pays sont-ils apparus ?
- À quel point êtes-vous satisfait de la façon dont les bureaux nationaux semblent avoir utilisé les incidents de sécurité, y compris les incidents évités de justesse, pour apprendre et améliorer leurs pratiques ?
- Quels incidents de sécurité subissent d'autres organisations dans le même pays et comment cela se compare-t-il aux incidents signalés au sein de votre organisation ?
- Comment les incidents de sécurité ont-ils affecté la livraison de l'aide ?
- Peut-on évaluer l'impact des incidents de sécurité sur la livraison de l'aide ?
- Quelles étaient les causes principales des incidents de sécurité ?
- Les causes des incidents peuvent-elles être classées selon la stratégie de réponse qui peut être nécessaire ?
- Pouvons-nous utiliser les données pour identifier un seuil de risque que notre organisation est prête à accepter ?

Voir Outil 13 : Questions de niveau stratégique pour les décisions relatives à la gestion de l'information issue des incidents, pour une liste complète de questions et d'actions possibles recommandées.

Outil de visualisation Google Earth Pro

La cartographie géographique des événements peut être un outil utile pour visualiser les incidents afin de soutenir l'analyse et les rapports à la direction de l'organisation. Plusieurs options existent pour afficher des informations visuellement. Si c'est l'option préférée, les détails nécessaires pour la géolocalisation et le type d'incident doivent être inclus dans le rapport initial car il n'est pas efficace ni précis de le faire rétrospectivement.

Si les bonnes informations sont disponibles (coordonnées GPS, codes couleur, types d'incidents, etc.), une simple option permettant de montrer l'emplacement des incidents peut être de convertir un document Excel en document KML, puis de lier celui-ci à Google Earth Pro. Si le document Excel-KML contient les informations correctes, les événements seront automatiquement sélectionnés sur une carte Google[27].

Assurez-vous que vos paramètres garantissent la confidentialité en réduisant l'accès à l'information.

[27] Pour obtenir des conseils étape par étape sur le processus de conversion d'un document Excel en KML, voir : https://www.earthpoint.us/ExcelToKml.aspx

4.3 Structures organisationnelles pour discuter des questions stratégiques de sécurité

Les organisations peuvent discuter des problèmes de sécurité d'un point de vue stratégique dans plusieurs contextes.

Un comité de gestion des risques de sécurité, par exemple, peut se réunir à intervalles réguliers (par exemple une fois par an ou plus fréquemment) dans le but de réunir les membres nommés du conseil d'administration, de la direction, le responsable de la sécurité ou l'équipe de sécurité.

Le personnel de sécurité est souvent chargé de préparer la réunion, à laquelle ils présentent ensuite les tendances en matière de sécurité et élaborent l'ordre du jour pour la discussion.

Dans ce type de réunion, il peut être avantageux de couvrir :

- Les tendances des incidents de sécurité au cours des dernières années, présentées comme :
  - Un tableau des incidents de sécurité par pays ;
  - Un tableau des incidents de sécurité par catégorie ;
  - Un tableau sur la gravité des incidents (impact) ;
  - Un tableau sur les causes des incidents.

- Une analyse des conséquences des incidents de sécurité signalés, par exemple :
  - Les incidents humains ayant un impact psychologique et/ou physique,
  - Les conséquences opérationnelles,
  - Les conséquences organisationnelles telles que celles qui affectent la réputation de l'ONG,
  - Les conséquences pour la gestion des risques de sécurité.

- Des recommandations sur la façon de garantir que le travail continue dans ces environnements.
- Les notations de contexte et niveaux de sécurité opérationnels.
- Les obstacles aux rapports d'incidents dans l'organisation.
- Une étude de cas qui illustre un thème important à discuter avec tout le monde et qui conduit à l'élaboration d'un plan d'action pour des cas similaires (par exemple plan de communication en cas d'incidents, établissement de relations avec les autorités locales, etc.).
- L'espace pour répondre aux questions des décideurs présents au personnel de sécurité.

Pour plus d'exemples sur la préparation de l'analyse de sécurité sur les réunions d'examen, voir l'Outil 12 : Analyse et comparaison des tendances des données.

L'examen des documents de sécurité, tels que le niveau de risque acceptable, le cadre de gestion des risques de sécurité, la stratégie de sécurité, la politique de sécurité, le plan de gestion de crise, etc., devrait figurer à l'ordre du jour même s'il n'est pas considéré comme une « action requise ». Il est important de documenter la procédure régulièrement pour justifier du devoir de protection.

4.4 Comment utiliser l'information issue des incidents de violence sexuelle à un niveau stratégique

La meilleure façon pour les organisations d'aborder les incidents de violence sexuelle contre leur personnel est de tirer des leçons apprises de l'expérience pour s'assurer que l'organisation réussit mieux à protéger son personnel et à réagir à ces types d'incidents à l'avenir. Cela continue à être un sujet délicat pour le personnel, alors l'organisation devrait s'efforcer activement de créer la confiance et l'ouverture pour discuter en interne de ce type d'incidents.

Il faudrait analyser si il est stratégique et bénéfique d'être ouvert sur les incidents de violence sexuelle avec les médias ou dans des forums mondiaux avec d'autres membres de la communauté des ONG.

> *« Être ouvert sur une plateforme plus large peut également créer l'espace pour que d'autres ONG entreprennent des changements similaires au sein de leurs propres organisations, contribuant à une augmentation globale de la sécurité et de la sûreté du personnel des ONG ».*

Si des détails sur un événement spécifique doivent être utilisés pour mettre en évidence le problème et les leçons apprises au niveau global, la victime doit donner son consentement. Dans la mesure du possible, elle devrait être impliqué dans ce processus et donner une voix directrice à la création d'un récit autour de l'incident et des leçons apprises.

Lorsque la victime a donné son consentement pour partager son expérience – sur le terrain ou à l'échelle globale – il faut veiller à ce qu'elle reçoive un soutien supplémentaire au moment où l'information est rendue publique, y compris un congé spécifique, un soutien psychosocial, etc.

Il est possible de partager des informations sur les tendances et des apprentissages organisationnels sans compromettre les droits de l'individu et cela devrait être encouragé.

4.5 Utilisation de l'information issue des incidents de sécurité pour le plaidoyer stratégique

Une organisation devrait décider, sur le plan stratégique, si il convient d'utiliser l'information issue des incidents obtenues en interne, et éventuellement aussi à l'extérieur, à des fins de plaidoyer.

De nombreuses organisations signalent qu'il est de plus en plus difficile d'assurer un accès sécurisé et une livraison de l'aide aux civils dans le besoin. Toutefois, en l'absence de données consolidées à l'échelle du secteur sur ces incidents et en l'absence d'une stratégie collective efficace sur la manière de traiter les obstacles délibérés ou l'impunité des auteurs, la plupart des organismes ne peuvent aborder que des cas individuels.

Les ONG ont fait de grands progrès dans le développement de stratégies de gestion des risques de sécurité pour répondre aux contextes de sécurité en constante évolution. Cependant, cela n'a pas été accompagné d'un plaidoyer humanitaire commun pour répondre aux préoccupations qui vont au-delà de la stratégie de gestion des risques de

sécurité d'une organisation individuelle. L'ampleur de l'insécurité pour l'action humanitaire reste ainsi cachée, chaque cas étant traité en silence et, dans la plupart des cas, avec les auteurs rarement traduits en justice. Il existe des possibilités de développer une stratégie de plaidoyer sectorielle pour répondre à des préoccupations complexes.

Certains incidents de sécurité sont au-delà de ce qu'une organisation peut contrôler et peuvent nécessiter une campagne de plaidoyer conjointe avec d'autres organisations. Par exemple, l'utilisation croissante d'armes explosives dans les zones peuplées affecte la sécurité du personnel et entrave la fourniture de l'aide. Lorsque les autorités nationales ne prennent pas les mesures requises contre les auteurs, les organisations peuvent avoir besoin de rechercher un soutien international dans le cadre d'enquêtes ou de faire pression pour que des poursuites soient engagées.

À un niveau plus global, il est important que le secteur de l'aide veille à ce que les informations sur les défis créés par des contextes de sécurité volatiles soient régulièrement mises à la disposition des principales parties prenantes telles que les donateurs, les décideurs, les médias et le grand public. Des preuves documentées de la violence contre les travailleurs humanitaires ou des incidents qui affectent la fourniture de l'aide sont nécessaires pour soutenir les efforts plus larges visant à améliorer la protection des travailleurs humanitaires et de leurs opérations pour soutenir un accès sans entraves aux populations vulnérables. Collectivement, le secteur de l'humanitaire et du développement pourrait faire davantage pour rappeler au public et aux décideurs politiques les difficultés et les dangers auxquels les travailleurs sont confrontés lorsqu'ils fournissent de l'aide dans des environnements précaires.

Cependant, lorsque les organisations envisagent de mener une campagne de plaidoyer, elles doivent envisager les conséquences possibles pour la sûreté et la sécurité du personnel ainsi que la mise en œuvre du programme.

Quel type de données est nécessaire pour le plaidoyer ?
Les médias et les autres parties prenantes ont tendance à demander d'abord des chiffres qui illustrent l'ampleur du problème. Par conséquent, beaucoup d'efforts ont été déployés pour essayer de quantifier le nombre de personnes touchées. Cependant, cela n'est pas forcément nécessaire pour une stratégie. Les campagnes précédentes ont montré que la description de la nature d'un problème peut être assez puissante pour encourager le changement. La campagne contre les mines terrestres antipersonnel, par exemple, a commencé par se concentrer sur la présentation de contextes individuels avec des détails tirés des programmes du Comité International de la Croix-Rouge (CICR) au Cambodge et en Angola plutôt qu'un problème quantifié. Comme la description frappante de l'impact des mines terrestres sur l'individu a attiré l'attention de l'opinion publique, la campagne a été en mesure d'obtenir des résultats impressionnants[28].

Les incidents affectant la sécurité des ONG peuvent être utilisés pour décrire la nature et l'impact d'un problème, même si on ne sait pas à quel point il est fréquent. Il existe des opportunités pour la communauté humanitaire de toucher un public plus large et les décideurs clés avec des récits solides sur la façon dont leur travail et leur personnel sont affectés par les contextes dans lesquels ils travaillent.

[28] Pour une description générale des sur la campagne efficace « interdire les mines terrestres » voir l'article suivant ici. L'un des premiers articles très influent du CICR a reconnu que le chiffre total n'était pas connu mais décrivait l'impact et l'effet des mines terrestres en termes généraux sur les civils. Voir l'article ici.

L'une des sources les plus convaincantes démontrant l'impact de l'insécurité sur la fourniture de l'aide sont les rapports d'incidents que les organisations produisent pour leur propre gestion des risques de sécurité. La simple existence des données démontre le problème mieux que toutes les données spécifiquement collectées à des fins de plaidoyer. Ce peut être une occasion manquée de ne pas exploiter cette ressource pour plaider en faveur d'une meilleure protection ou, au moins, d'un meilleur financement pour les politiques liées à la sécurité et d'une meilleure formation en matière de sécurité pour le personnel.

Générer collectivement ces données en tant que secteur de l'aide peut contribuer à renforcer le plaidoyer en faveur de la protection des travailleurs humanitaires et des programmes, et permettre aux bailleurs de fond de mieux accepter que la gestion des risques de sécurité soit un coût direct qui devrait être inclus dans les demandes de financement.

Il est important de ne pas exposer des individus ou des cas spécifiques dans le but d'en faire un sujet politique. Les données collectives réduisent ce risque.

Les hauts responsables au sein des organisations peuvent faire avancer ce programme en contribuant au partage de données avec d'autres organisations et en renforçant les liens entre le personnel de sécurité et le personnel chargé des politiques et du plaidoyer au sein de leur propre organisation. Cela permet de s'assurer que les analyses des incidents de sécurité multi-organisationnelles sont utilisées de manière stratégique par le personnel chargé des politiques et du plaidoyer.

Étude de cas : Healthcare in Danger (Soins de Santé en Danger), CICR

En 2008, le CICR a commandé une étude dans 16 pays pour documenter la manière dont la violence affectait la prestation des soins de santé, en utilisant des données sur les incidents dans des contextes choisis[29]. Cette étude est devenue la première base de données pour commencer à aborder la violence contre les travailleurs de la santé, ce qui a été illustré depuis par de nombreuses études de cas supplémentaires[30]. Depuis lors, le CICR a géré le projet Health Care in Danger, qui combine des activités de sensibilisation et des conseils pratiques sur la manière d'améliorer la sécurité des agents de santé[31].

D'autres organisations ont également commencé à aborder ce problème. Depuis 2014, dix membres de la *Coalition Protéger la Santé dans les Conflits* ont publié conjointement des rapports annuels sur les attaques contre les soins de santé, qui combinent des données et des informations provenant de différentes organisations pour maintenir la question à l'ordre du jour mondial[32]. Plus de 20 membres de la coalition, y compris plusieurs organisations humanitaires, aident à diffuser l'information afin d'encourager une meilleure protection des soins de santé[33].

En 2016, l'Organisation mondiale de la santé (OMS) a publié des données sur les attaques contre les soins de santé sur son site Web[34].

29 ICRC. (2011). *Une étude sur seize pays: les soins de santé en danger.* ICRC.
30 Pour plus d'informations, voir : http://healthcareindanger.org/resource-centre/
31 Pour plus d'informations, voir : http://healthcareindanger.org/hcid-project/
32 Pour plus d'informations, voir : https://www.safeguardinghealth.org/
33 Pour une liste des organisations humanitaires soutenant la Coalition Protéger la santé dans les conflits, voir page 2 ici.
34 Voir: http://www.who.int/emergencies/attacks-on-health-care/en/. Veuillez noter que ce site sera bientôt mis à jour. Voir aussi Lieberman, A. (2017). « L'OMS se prépare à lancer une base de données en ligne pour suivre les attaques des agents de santé », *Devex*.

En mai 2016, le Conseil de sécurité des Nations unies a adopté la résolution 2286 qui établit une feuille de route pour la protection des soins de santé dans les conflits[35].

En mai 2016, le Conseil de sécurité des Nations unies a adopté la résolution 2286 qui établit une feuille de route pour la protection des soins de santé dans les conflits. Ces exemples montrent comment l'utilisation efficace des données peut contribuer à mettre et garder cette question importante à l'ordre du jour.

Le Groupe de travail sur la protection de l'action humanitaire

Le Groupe de travail sur la protection de l'action humanitaire étudie des options pour une action mondiale collective visant à protéger les travailleurs humanitaires[36]. Le groupe de travail réunit des praticiens d'organisations humanitaires opérationnelles, des experts en sécurité, des experts politiques et des universitaires, et est dirigé conjointement par le Programme de formation avancée en action humanitaire du Harvard Humanitarian Initiative et Action Contre la Faim. L'objectif est de surmonter la tendance des organisations humanitaires à travailler de façon isolée face à cet environnement de plus en plus difficile à travers une réflexion collective, un plaidoyer plus fort et plus cohérent dans le secteur humanitaire et des actions conjointes pour réaffirmer le respect du droit international humanitaire (DIH) et la protection de l'action humanitaire. Le DIH étant la responsabilité des États, ce n'est qu'à l'échelle mondiale que la communauté humanitaire peut faire pression pour un changement dans un contexte qui, pour le moment, devient moins propice à l'aide humanitaire pour atteindre les civils dans le besoin.

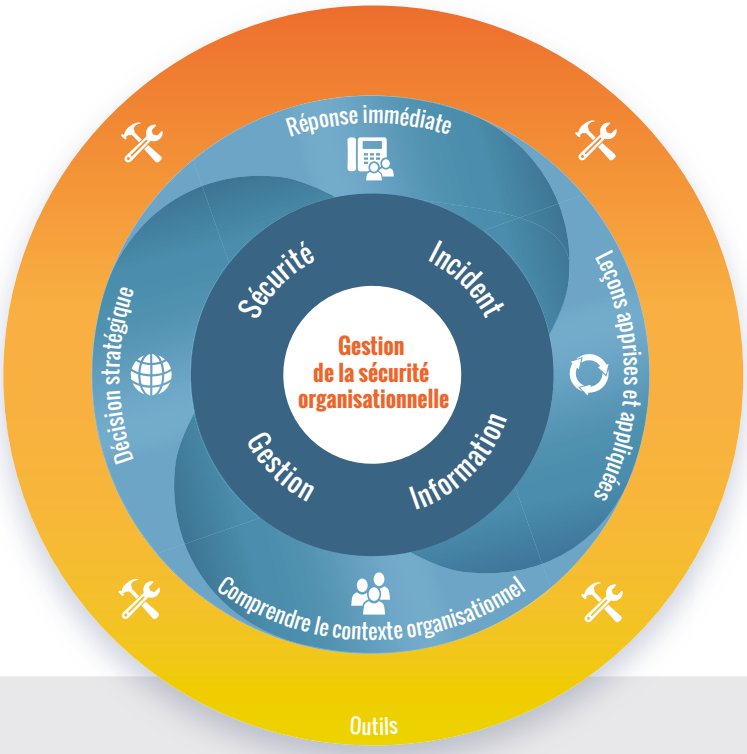
L'une des premières constatations du groupe de travail a été qu'un meilleur partage systématique de l'information sur les incidents de sécurité est nécessaire pour aider à identifier les principales tendances et priorités. Le groupe de travail a également identifié un manque de coopération directe et de communication entre les responsables de la gestion des risques de sécurité et les départements de plaidoyer dans de nombreuses organisations comme un obstacle à un travail plus efficace. Le groupe de travail cherche à collaborer avec les points focaux de sécurité et le personnel au sein des organisations pour identifier les cas où un plaidoyer commun peut soutenir la réponse aux problèmes de sécurité.

Pour plus d'informations sur le groupe de travail, veuillez contacter:
Lise Fouquat: lfouquat@actioncontrelafaim.org
Pauline Chetcuti: pchetcuti@actioncontrelafaim.org
Julia Brooks: jbrooks@hsph.harvard.edu

[35] United Nations. (2016). « Le Conseil de sécurité a adopté la résolution 2286 (2016), condamnant fermement les attaques contre les installations médicales et le personnel dans les situations de conflit », *Nations Unies*.

[36] ATHA. (2016). « Projet de politique: protection de l'action humanitaire », *ATHA*.

CHAPITRE 3 : OUTILS



Cette section contient des outils d'aide à la gestion de l'information issue des incidents de sécurité. Ils doivent être lus et utilisés conjointement avec le contenu écrit de ce manuel. Les outils sont organisés comme suit (cliquez sur l'élément pour accéder à l'outil) :

- Outil 1 : Grille d'auto-évaluation GIIS
- Outil 2 : Typologie des incidents
- Outil 3 : Incident organisationnel ou externe
- Outil 4 : Modèle de rapport d'incident
- Outil 5 : Grilles d'analyse des incidents
- Outil 6 : Comment effectuer un débriefing factuel
- Outil 7 : Bonnes pratiques en matière de signalement des incidents liés au genre et mécanismes de plainte pour signaler l'exploitation et les abus sexuels (EAS)
- Outil 8 : Plan d'action pour le suivi des incidents
- Outil 9 : Systèmes GIIS
- Outil 10 : Conservation de l'information issue des incidents
- Outil 11 : Technologie pour signaler et enregistrer les incidents
- Outil 12 : Analyse et comparaison des tendances des données
- Outil 13 : Questions de niveau stratégique pour les décisions relatives à la gestion de l'information issue des incidents de sécurité

OUTIL 1 : GRILLES D'AUTO-ÉVALUATION

Veuillez utiliser ce tableau comme guide pour les éléments typiques d'un système de gestion de l'information issue des incidents.

QUESTIONS GÉNÉRALES	
Combien de bureaux de terrains / nationaux / régionaux sont actuellement opérationnels dans votre organisation ?	
Nombre d'employés (personnel international, personnel national, bénévoles, etc.)	
Combien de points focaux de sécurité travaillent actuellement avec vous ?	
Au niveau du siège, partagez-vous la responsabilité de la mise en œuvre du cadre de gestion des risques de sécurité ? Si oui, avec qui (fonction) ?	
CADRE DE GESTION DES RISQUES DE SÉCURITÉ	En place dans l'organisation (oui / non / en partie)
Les responsabilités décisionnelles en matière de gestion des risques de sécurité sont-elles clairement établies à tous les niveaux ?	
Votre organisation utilise-t-elle des informations sur le contexte de sécurité à d'autres fins telles que le plaidoyer, la communication avec les donateurs et/ou la programmation ?	
GESTION DES INCIDENTS ET DES CRISES	
L'organisation a-t-elle une politique de gestion des incidents / crises ?	
Existe-t-il un cadre de gestion des incidents au niveau du terrain / pays (procédures) ?	
Existe-t-il un cadre de gestion des incidents au niveau du siège (procédures) ?	
Le cadre de gestion des incidents inclut-t-il un arbre de communication ?	
Le cadre de gestion des incidents traite-t-il les incidents évités de justesse ?	
Formez-vous votre personnel à la gestion des incidents et/ou des crises et effectuez-vous des simulations ?	
L'organisation utilise-t-elle un système de gestion des incidents en ligne ?	

L'organisation utilise-t-elle un logiciel de traitement de texte ou un tableur comme base de son système de gestion des incidents ?	
Existe-t-il une procédure de communication sur les incidents convenue avec la compagnie d'assurance de l'organisation ?	
Existe-t-il un lien entre la politique de gestion des risques de sécurité et la politique RH de votre organisation ?	
COLLECTE D'INFORMATIONS SUR L'INCIDENT	
Avez-vous une définition organisationnelle du terme 'incident' ?	
Votre organisation utilise-t-elle des catégories définies pour décrire différents types d'incidents ? Si oui, sont-elles standardisées avec les catégories utilisées par les autres ONG avec lesquelles vous êtes partenaire ?	
Existe-t-il un modèle de rapport d'incident au niveau du terrain / national ? Si oui, a-t-il été standardisé avec d'autres ONG avec lesquelles vous êtes partenaire ?	
Existe-t-il une procédure de débriefing émotionnel (désamorçage) sur le terrain ?	
Existe-t-il une procédure de débriefing factuel sur le terrain ?	
Existe-t-il un système de stockage sécurisé pour les informations collectées sur le terrain ?	
Existe-t-il un système de stockage sécurisé pour les informations collectées au niveau national / régional ?	
Existe-t-il un système de stockage sécurisé pour les informations collectées au niveau du siège ?	
Votre organisation collecte-t-elle des informations sur les incidents externes (c'est-à-dire ceux qui n'ont pas d'impact sur votre organisation) ?	
RAPPORT ET ENREGISTREMENT DE L'INFORMATION SUR L'INCIDENT	
Existe-t-il une procédure pour signaler les incidents ?	
Existe-t-il des lignes directrices pour le modèle de rapport d'incident ?	
Existe-t-il un arbre de communication clair pour chaque bureau terrain ?	
Y a-t-il une liste de contacts disponibles au niveau du terrain / pays ?	
Existe-t-il un système d'enregistrement des incidents au niveau du terrain / pays ?	
Existe-t-il un système d'enregistrement des incidents au niveau régional ?	
Existe-t-il un système d'enregistrement des incidents au niveau du siège ?	
Consignez-vous les pertes et les dommages sur l'infrastructure ou les équipements ?	

Enregistrez-vous les menaces orales, écrites et cybernétiques dans votre organisation ?	
Enregistrez-vous les obstacles administratifs ?	
Consignez-vous la violence sexuelle (y compris le harcèlement) ?	
Les incidents associés à la violence sexuelle sont-ils signalés à l'aide du cadre de gestion régulière des incidents ?	
Est-ce que vous enregistrez les incidents évités de justesse ?	
Le système est-il sûr à tous les niveaux ? Les données sont-elles sécurisées ?	
ANALYSE DE L'INFORMATION ISSUE DE L'INCIDENT	
Existe-t-il un deuxième modèle de rapport d'incident fournissant des indications sur les informations à collecter à des fins d'analyse (par exemple, 72 heures après l'événement) ?	
Est-ce que quelqu'un au niveau du terrain / pays est responsable de l'analyse d'un incident ?	
Est-ce que quelqu'un au niveau régional est en charge de l'analyse d'un incident ?	
Est-ce que quelqu'un au niveau du siège fournit une analyse / vérification des résultats de l'analyse régionale et de terrain / pays ?	
Formez-vous votre personnel pour améliorer ses compétences analytiques ? (pas nécessairement et uniquement sur des sujets liés à la sécurité)	
Existe-t-il un système en place au niveau des pays pour cartographier (par exemple via une feuille de calcul) et analyser les incidents ?	
Existe-t-il une consultation des ressources externes (parties prenantes ou informations) pendant l'analyse, au niveau du terrain / pays ?	
Existe-t-il une consultation des ressources externes (parties prenantes ou informations) pendant l'analyse, au niveau régional ?	
Existe-t-il une consultation des ressources externes (parties prenantes ou informations) pendant l'analyse, au niveau du siège ?	
PARTAGE DE L'INFORMATION ISSUE DE L'INCIDENT	
Existe-t-il une ligne directrice ou une politique générale de « classification de l'information » dans l'organisation ?	
Existe-t-il une politique de communication interne au niveau du terrain / pays ?	
Existe-t-il une politique de communication interne au niveau régional ?	
Existe-t-il une politique de communication interne au niveau du siège ?	
L'organisation fait-elle partie d'un groupe de sécurité d'ONG sur le terrain / pays ? (exemples)	

L'organisation fait-elle partie d'un groupe de sécurité d'ONG au niveau régional ? (exemples)	
L'organisation fait-elle partie d'un groupe de sécurité d'ONG au niveau du siège ? (exemples)	
Existe-t-il une politique de communication externe au niveau du terrain / pays ?	
Existe-t-il une politique de communication externe au niveau régional ?	
Existe-t-il une politique de communication externe au niveau du siège ?	
L'organisation utilise-t-elle les réseaux sociaux pour la communication générale ?	
L'organisation a-t-elle établi des liens avec les medias ?	
L'organisation dispose-t-elle d'un système de cartographie des acteurs au niveau du terrain / pays ?	
L'organisation dispose-t-elle d'un système de cartographie des acteurs au niveau régional ?	
L'organisation dispose-t-elle d'un système de cartographie des acteurs au niveau du siège ?	
La tradition de la communication interne est-elle orale / écrite ?	
La tradition de la communication externe est-elle orale / écrite ?	
Existe-t-il un document de passation pour les points focaux de sécurité sur le terrain contenant des informations sur les incidents ?	
Le personnel est-il formé au partage d'informations sur les incidents et sur les politiques organisationnelles ?	
Les dirigeants et les membres du conseil d'administration bénéficient-ils de ce partage d'information ?	
UTILISATION DE L'INFORMATION ISSUE DE L'INCIDENT	
Y a-t-il une personne identifiée au niveau du terrain / pays en charge des actions de suivi (à mi-parcours) ?	
Existe-t-il une communication de suivi 1 mois après l'incident (les niveaux peuvent varier) ?	
Existe-t-il une communication de suivi 3 mois après l'incident (les niveaux peuvent varier) ?	
Existe-t-il un suivi de la mise en œuvre par le siège des leçons apprises ?	
Votre organisation effectue-t-elle une analyse quantitative ?	
Votre organisation effectue-t-elle une analyse qualitative ?	
Existe-t-il un système au niveau national pour effectuer une analyse quantitative des données sur les incidents ?	

Existe-t-il un système au niveau du siège pour effectuer une analyse quantitative des incidents ?	
Y a-t-il des réunions sur le terrain pour présenter les tendances en matière de données au personnel ?	
Y a-t-il des réunions au niveau national pour présenter les tendances en matière de données au personnel ?	
Y a-t-il des réunions au niveau régional pour présenter les tendances en matière de données au personnel ?	
Y a-t-il des réunions au niveau du siège pour présenter les tendances en matière de données au personnel?	
Les PFS de terrain / pays sont-ils consultés par les personnels du programme ?	
Le conseiller / responsable de la sécurité du siège est-il consulté par les personnels du programme ?	
Les membres de l'exécutif et du conseil d'administration sont-ils inclus dans l'analyse (par exemple l'analyse des tendances) ?	
Les informations sur les tendances en matière de données sont-elles partagées avec les parties prenantes externes ?	
Les tendances en matière de données de votre propre organisation sont-elles utilisées dans le plaidoyer ?	

OUTIL 2 : TYPOLOGIE DES INCIDENTS

Les définitions suivantes des différents types d'incidents sont données à titre indicatif. Les organisations n'ont pas besoin d'utiliser toutes les catégories dans leur gestion de l'information issue des incidents de sécurité. Cependant, elles sont encouragées à utiliser les définitions standards proposées pour faciliter l'échange de données et les comparaisons inter-organisations.

Les incidents sont définis en catégories (accident, action de l'autorité, crime, etc.) et sous-catégories associées. Les organisations peuvent choisir d'utiliser uniquement les catégories, les sous-catégories sélectionnées ou combinées.

Les catégories générales remplissent des fonctions différentes. Certaines regroupent les impacts sur l'événement (par exemple, décès ou dommages), d'autres la nature de l'événement (par exemple, la violence sexuelle), tandis que d'autres incluent des informations sur l'auteur de l'acte, en plus de décrire la nature de l'événement (par exemple, action criminelle ou d'autorité). D'autres incluent le contexte dans lequel l'événement s'est produit (par exemple l'insécurité générale) alors que d'autres catégories décrivent les moyens (par exemple l'utilisation d'armes). D'autres classifient la réponse de l'organisation.

C'est en fonction de l'analyse voulue que l'on utilise la catégorie la plus appropriée. Un seul événement peut être considéré à partir d'une variété de perspectives.

Pour la plupart des événements, plus d'une des catégories générales sont pertinentes. Les sous-catégories peuvent être traitées comme mutuellement exclusives, ce qui signifie qu'une seule des sous-catégories s'applique.

Voir aussi la définition des catégories d'événements utilisées dans l'analyse des tendances de Insecurity Insight et les données sur Humanitarian Data Exchange.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Accident Maladie Catastrophe naturelle Tout accident de la route impliquant des membres du personnel ou des véhicules de l'organisation et d'autres incidents non Intentionnels, les accidents, catastrophes ou maladies soudaines.	**Accident : Décès**	Tout décès involontaire qui ne peut être attribué à des causes naturelles. Les causes de décès accidentel peuvent inclure des accidents de véhicules, des blessures graves, etc.
	Accident : Autre	Un incident aléatoire qui entraîne des dommages au personnel et/ou des dommages sur les biens de l'organisation.
	Accident : Véhicule	Un accident impliquant le véhicule d'une organisation. Véhicule désigne toute forme de transport, y compris, mais sans s'y limiter, les voitures, les camions, les autobus, les mobylettes, etc.
	Accident : Incendie	Tout incendie involontaire ou de cause naturelle endommageant la propriété ou mettant en danger le personnel. Cela peut inclure les incendies de forêt ou les incendies accidentels (tels que les incendies électriques ou les fuites de gaz), etc.
	Maladie	Toute maladie grave d'un employé.
	Catastrophe Naturelle	Catastrophe naturelle qui survient ou est prévue dans une ville ou un pays où l'organisation a un bureau. Les catastrophes naturelles peuvent inclure les tremblements de terre, les éruptions volcaniques, les ouragans, les tornades, les dégâts provoqués des tempêtes (grêle, inondations soudaines, etc.), les inondations, les tsunamis, etc.
Action de l'autorité (AA) Actions directes ou indirectes prises par un acteur étatique ou non étatique qui entrave la livraison de l'aide.	**AA : Abus de pouvoir**	L'utilisation de pouvoirs législatifs, exécutifs ou autres autorisés par des représentants du gouvernement pour des gains privés illégitimes. L'acte illégal d'un fonctionnaire ne constitue un abus de pouvoir que si l'acte est directement lié à ses fonctions officielles.
	AA : Accès refusé	Actes qui : a) empêchent une organisation d'atteindre les bénéficiaires ou les bénéficiaires potentiels pour l'évaluation des besoins ou la fourniture directe de services b) empêchent les bénéficiaires d'accéder aux services fournis par une organisation.
	AA : Accusations	Une accusation de la part des autorités du pays d'accueil d'actes répréhensibles.
	AA : Application des lois	Application de lois, de décrets, ou de règlements existants ou nouveaux qui, lorsqu'ils sont appliqués, ont un effet réel sur la livraison de l'aide. Cela peut inclure la confiscation de matériel, mettre des personnes / organisations sur des listes de surveillance, etc.
	AA : Arrestation (Voir aussi Accusations, détentions et emprisonnements)	Arrestations de personnel. Ceux qui procèdent à l'arrestation doivent exercer des fonctions gouvernementales (comme la police) afin de différencier cet incident d'un incident de prise d'otages. Les arrestations suivent généralement des accusations formelles.
	AA : Poursuites judiciaires	Accusation légale formelle faite par une autorité gouvernementale affirmant qu'un membre du personnel ou l'organisation a commis un crime.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Authority action (AA) Actions directes ou indirectes prises par un acteur étatique ou non étatique qui entrave la livraison de l'aide.	**AA : Checkpoint**	Un poste de contrôle non frontalier ou frontalier érigé dans des zones contrôlées par des militaires, des paramilitaires ou des groupes armés afin de surveiller ou de contrôler les mouvements de personnes et de matériel ayant une incidence sur la fourniture de l'aide.
	AA : Refus de visa	Retarder ou refuser un timbre officiel, un visa ou tout autre permis autorisant l'entrée dans un pays ou un territoire d'un pays requis pour livrer une aide.
	AA : Détention	Garder un membre du personnel en détention avant les accusations officielles ou sans aucune charge officielle; comprend la détention temporaire pendant des heures ou des jours.
	AA : Expulsion	Acte de forcer un membre du personnel ou une organisation à quitter un pays ou un territoire.
	AA : Amende	Somme d'argent qui doit être payée par l'organisation parce qu'elle n'a pas respecté une règle ou une loi.
	AA : Fermeture forcée	Ordre du gouvernement ou d'autres autorités d'arrêter les opérations dans un pays ou un territoire ; inclut la fermeture affectant seulement un ou plusieurs programmes.
	AA : Action gouvernementale	Action du gouvernement hôte ou donateur qui a un impact direct ou indirect sur la capacité financière d'une organisation à fournir de l'aide ; comprend le gel des fonds, l'introduction de taxes ou la suppression des subventions.
	AA : Emprisonnement	Détention d'un membre du personnel dans un lieu officiel connu ou inconnu, comme une prison, souvent suite à des accusations formelles.
	AA : Introduction de lois	Fait référence à la rédaction ou au vote des lois, décrets ou règlements qui, lorsqu'ils sont appliqués, auront un effet potentiel ou réel sur la livraison de l'aide. Cela peut inclure, mais sans s'y limiter, des procédures d'enregistrement restrictives, des règles d'importation, ou la divulgation régulière de sources financières.
	AA : Enquête	Le processus ou l'acte d'examiner les faits liés aux allégations contre les membres du personnel ou de l'organisation.
	AA : Perquisition	Perquisition des locaux de l'organisation par les autorités.
Crime Incidents criminels ayant une incidence sur les biens d'une organisation ou sur un membre du personnel.	**Crime : Vol à main armée**	Un vol à main armée ou dans lequel les auteurs du vol portent des armes à feu qui ont affecté des employés ou des biens
	Crime : Incendie criminel	Tout incendie volontaire mettant en danger la vie des employés ou endommageant des biens. Les incendies criminels comprennent, mais sans s'y limiter, l'utilisation de dispositifs incendiaires, le sabotage intentionnel de systèmes électriques ou de conduites / réservoirs de gaz, et l'utilisation d'un accélérateur pour détruire les biens.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Crime Incidents criminels ayant une incidence sur les biens d'une organisation ou sur un membre du personnel.	**Crime : Chantage**	Les menaces, l'extorsion ou la manipulation d'une personne pour l'obliger à faire quelque chose ; y compris à donner quelque chose, en particulier de l'argent, par la force ou la menace.
	Crime : Cambriolage	L'acte de pénétrer illégalement dans les locaux ou les véhicules de l'organisation, avec l'intention de voler.
	Crime : Vol avec infraction	S'introduire dans une résidence, généralement avec l'intention de voler. Utiliser uniquement si les personnes dormaient ou ne se sont pas rendu compte du cambriolage.
	Crime : Braquage / Détournement de véhicule	Tout incident dans lequel un véhicule contenant un employé (s) ou appartenant à l'organisation est saisi de force.
	Crime : Cyber attaque	Exploitation délibérée de systèmes informatiques, et de réseaux tributaires de la technologie perturbant et pouvant compromettre les données et mener à la cybercriminalité.
	Crime : Fraude	Acte trompeur ou criminel en vue d'obtenir un gain financier ou personnel.
	Crime : Intrusion	Fait de s'introduire dans les locaux d'une organisation, ses véhicules ou ses résidences sans y être invité, par des criminels ou des civils (mais pas par les autorités de l'État).
	Crime : Pillage	Vol pendant les troubles, la violence, les émeutes ou d'autres bouleversements.
	Crime : Piraterie	Attaquer et voler des navires en mer ou des bateaux sur les rivières.
	Crime : Vol qualifié	Événements dans lesquels a) l'agresseur n'était pas armé, b) le membre du personnel était présent pendant l'incident et est parfaitement conscient d'avoir été volé, et c) des biens ont été pris.
	Crime : Vol de biens	Toute situation dans laquelle des biens personnels sont volés à un employé ou dans un lieu sans que la victime ne s'en aperçoive.
	Crime : Vol de biens de l'organisation	Toute situation dans laquelle un bien de l'organisation (au-delà d'une valeur prédéfinie) est volé sans qu'un membre du personnel ne s'en aperçoive.
	Crime : Vandalisme	Destruction ou endommagement délibéré des biens de l'organisation ou de son personnel. Dégâts matériels.
Dégradation Toute dégradation des biens de l'organisation.	**Dégâts matériels**	Toute dégradation ou détérioration matériels, au-delà d'un montant prédéfini, involontaire (par exemple, catastrophes naturelles, accidents, etc.) ou intentionnelle (par exemple, les émeutes qui causent des dommages matériels, etc.) sur les biens de l'organisation.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Mort Tout décès de membres du personnel pour une cause quelconque	**Décès : Accident**	(Voir Accident)
	Décès : Intentionnel (homicide)	(Voir TBK)
	Décès : Naturel	Tout décès pouvant être attribué à une cause naturelle, telle qu'une crise cardiaque, une maladie ou un accident vasculaire cérébral.
	Décès : Suicide	La mort volontaire et intentionnelle d'un employé. Le suicide est défini comme la prise volontaire et intentionnelle de sa propre vie.
Insécurité générale (IG) Les incidents liés au contexte qui créent de l'insécurité et affectent directement ou indirectement la livraison de l'aide. Affecte ou non directement l'agence, son personnel ou son infrastructure.	**IG : Activité armée**	Actions armées d'un État, une entité non étatique ou une entité armée organisée.
	IG : Attaque sur une autre organisation	Attaque sur une autre organisation qui n'a pas directement affecté l'agence.
	IG : Coup d'Etat	Coups d'Etat, mutinerie et autres rébellions de la part de toute force armée. Un coup d'Etat est défini comme une tentative (généralement armée), réussie ou non, violente ou non, de remplacer un gouvernement. Une tentative de coup d'Etat peut être politiquement déstabilisante.
	IG : Tirs croisés / combats actifs	Toute situation dans laquelle un employé ou un bien de l'organisation est pris dans une attaque ou un échange de tirs entre deux ou plusieurs groupes armés. Dans cette situation, les employés impliqués et les biens ne sont pas la cible de l'attaque.
	IG : Manifestation	Toute manifestation (y compris les contestations, marches, sit-in, piquets de grève, etc.) qui est non-violente. Rassemblement de masse de personnes à des fins politiques ou sociales.
	IG : Fusillade	Tirs délibérés sur des personnes autres que le personnel de l'organisation (voir aussi TBK : homicide et UA : armes à feu).
	IG : La grève / non présentation	Décision délibérée du personnel de ne pas venir travailler pour des raisons autres que médicale.
	IG : Troubles	Agitation civile ou politique, ainsi que les comportements assimilés à ceux d'une foule ou présentés comme tumultueux. Ces comportements incluent le pillage, les soulèvements en prison, mise à feu par la foule de différents biens, les combats avec la police (et généralement les manifestants).
Tué, blessé ou kidnappé (TBK) : Tout incident entraînant la mort, les blessures ou l'enlèvement d'un membre du personnel. Généralement les événements critiques.	**TBK : Rapt / détournement / prise d'otage / enlèvement**	Tout incident dans lequel le personnel est saisi de force. Cet incident peut ou non impliquer une demande de rançon.
	TBK : Battu	Incident dans lequel un membre du personnel a été agressé, à coups de poings ou pieds ou avec des objets (bâtons ou objets contondants).
	TBK : Décès : Intentionnel (homicide) / assassiné	Tout décès intentionnellement causé, par exemple, par balle, attaque physique, empoisonnement, etc. Les morts intentionnelles n'incluent pas les suicides.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Tué, blessé ou kidnappé (TBK) : Tout incident entraînant la mort, les blessures ou l'enlèvement d'un membre du personnel. Généralement les événements critiques.	**TBK : Disparu**	Incident dans lequel un membre du personnel a disparu ou est porté disparu. Distinction entre la disparition et les enlèvements : a) par acteur : les acteurs non étatiques ont tendance à enlever les personnes alors que les acteurs étatiques ont tendance à les faire « disparaître ». Elles deviennent alors des personnes « disparues » ; b) par la communication des auteurs de l'enlèvement du personnel : les ravisseurs ont tendance à faire des demandes (par exemple, une rançon) alors que l'on n'a plus de nouvelles personnes enlevées et des personnes disparues. c) par motif : les enlèvements tendent à répondre à une demande spécifique tandis que les disparitions tendent à être effectuées pour faire taire un membre du personnel, souvent pour des raisons politiques.
	TBK : Torture	Mutilation physique intentionnelle / blessure qui est explicitement qualifiée de torture du personnel.
	TBK : Blessés	Incident dans lequel un membre du personnel a été blessé. La plupart des blessures dans cette catégorie sont causées par des armes, en opposition à la sous-catégorie « battu ».
Motif Classification du motif de(s) l'auteur (s).	**Motif : Attaque**	Attaques ciblant directement l'organisation.
	Motif : Mauvais endroit, mauvais moment	Attaques non dirigées contre l'organisation ou son personnel mais dans lesquelles les membres du personnel ou des biens de l'organisation ont été affectés parce qu'ils se trouvaient près d'une attaque générale ou d'une attaque ciblée contre une autre entité ou individu.
Evité de Justesse (EJ) Les incidents qui auraient pu causer un préjudice ou affecter la livraison de l'aide. Comprend toute situation dans laquelle un incident de sécurité est survenu mais ne s'est pas produit, a eu lieu près d'un travailleur humanitaire / d'une organisation / d'un programme, ou lorsque les personnes impliquées ont pu éviter tout dommage grave. (S'il y a des dommages, l'événement est inclus dans la sous-catégorie sous TBK).	**EJ : Crime**	L'incident évité de justesse s'est produit dans le contexte d'un événement criminel.
	EJ : Armes explosives	L'incident évité de justesse s'est produit dans le cadre de la détonation d'une arme explosive (par exemple, un bombardement d'un bâtiment voisin ou un attentat à la bombe dans un restaurant fréquenté par des membres du personnel de l'organisation). Il s'agit des événements spécifiques par opposition ceux d'utilisation générale d'armes explosives dans un environnement non sécurisé.
	EJ : TBK	L'incident a évité de justesse qu'un membre du personnel ne soit tué, blessé ou kidnappé.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Mesures de sécurité (MS) Actions entreprises par les organisations en réponse à l'insécurité généralisée ou à un incident de sécurité.	**MS : Evacuation : médicale**	Evacuation d'un employé pour des raisons médicales, généralement à cause des blessures ou d'une maladie qui ne peuvent pas être traitées de manière adéquate à l'hôpital local, au cabinet du médecin ou au centre de traitement.
	MS : Evacuation : non-médicale	Evacuation d'un employé pour des raisons de sécurité. Notez que l'évacuation fait référence au retrait du personnel du pays d'opération. Le déplacement du personnel vers un autre endroit du pays pour des raisons de sécurité est appelé relocalisation.
	MS : Hibernation	Fait de rester à l'abri jusqu'à ce que le danger soit passé ou qu'une aide supplémentaire soit fournie.
	MS : Couvre-feu imposé	Imposition d'un couvre-feu dans une ville ou un pays où l'organisation a un bureau.
	MS : Fermeture de bureau	Décision de fermer un bureau en réponse au contexte général de sécurité ou à un événement spécifique.
	MS : Surveillance constante	Suivi actif d'une situation de sécurité en vue de potentiellement changer les mesures de sécurité.
	MS : Suspension du programme	Modification importante du programme en arrêtant une activité ou un projet spécifique.
	MS : Déménagement	Déplacement du personnel vers une autre ville ou bureau dans le pays d'opération pour des raisons de sécurité.
	MS : Déplacement restreint, pas de couvre-feu	Toute restriction de déplacement affectant le personnel. Ce type d'événement est semblable à une alerte et peut être le résultat d'une agitation politique ou sociale, d'une épidémie ou d'une catastrophe naturelle.
Violence sexuelle Tout incident dans lequel un membre du personnel a subi une forme quelconque de violence sexuelle.	**Violence sexuelle : comportement sexuel agressif**	Comportement potentiellement violent axé sur des pulsions sexuelles gratifiantes.
	Violence sexuelle : tentative d'agression sexuelle	Tentative de contact sexuel sur le corps d'une autre personne sans son consentement.
	Violence sexuelle : viol	Rapports sexuels (pénétration orale, vaginale ou anale) contre la volonté et sans le consentement de la personne.
	Violence sexuelle : agression sexuelle	Acte de contact sexuel sur le corps d'une autre personne sans son consentement.
	Violence sexuelle : commentaires sexuels non désirés	Avances verbales qui comprennent siffler, crier, et/ou dire des phrases sexuelles, façon explicites ou implicite ou qui ne sont pas souhaitées.
	Violence sexuelle : attouchements sexuels non désirés	Toucher, d'une nature sexuelle non désirée indépendamment de l'intensité du toucher, d'une façon sexuelle non souhaitée. Cela peut inclure masser, tâter, s'accaparer toute partie du corps d'une autre personne.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Violence sexuelle Tout incident dans lequel un membre du personnel a subi une forme quelconque de violence sexuelle.	**Violence sexuelle : harcèlement sexuel**	Toucher, d'une nature sexuelle non désirée indépendamment de l'intensité du toucher, d'une façon sexuelle non souhaitée. Cela peut inclure masser, tâter, s'accaparer toute partie du corps d'une autre personne. Avances sexuelles importunes, demandes de faveurs sexuelles et autres comportements verbaux ou physiques à caractère sexuel qui ont un impact sur l'emploi de la personne ciblée. Par exemple: a) la soumission à un tel comportement est explicitement ou implicitement la condition pour qu'une personne garde son emploi, ou b) la soumission ou le rejet d'un tel comportement est utilisé contre la personne, ou c) un tel comportement a pour objet ou pour effet d'interférer déraisonnablement avec la performance au travail d'une personne ou de créer un environnement de travail intimidant, hostile ou offensant.
Menace Menace(s) directe(s) ou indirecte(s) faite(s) par un acteur étatique ou non étatique qui entravent la livraison de l'aide.	**Menace : harcèlement en personne**	Événements dans lesquels un membre du personnel est directement harcelé par une personne ou un groupe de personnes (par exemple, le harcèlement sur les activités ou du programme de l'organisation).
	Menace : intimidation en personne	Evénements dans lesquels un membre du personnel est directement intimidé par une personne ou un groupe de personnes (par exemple, un membre du personnel s'est senti intimidé par des acteurs armés patrouillant près d'une distribution de nourriture).
	Menace : menaces en personne	Evénements dans lesquels un membre du personnel est directement menacé par une personne ou un groupe de personnes; devrait inclure une certaine forme de conséquence en cas de non-conformité (par exemple, une menace de représailles pour ne pas inclure une personne dans une activité de l'organisation).
	Menace : menaces à distance contre l'organisation	Événements dans lesquels l'organisation ou un membre du personnel est menacé pas en personne mais par un mécanisme distant (par exemple, courrier électronique, SMS, téléphone ou via des menaces générales diffusées sur un site Web ou sur les réseaux sociaux (Twitter, Facebook). Inclure les menaces directes lancées par les civils lors des manifestations.
	Menace : risque de réputation	Événements impliquant un risque perçu, réel ou potentiel pour le logo / l'emblème, l'image ou la réputation de l'organisation.
	Menace : menace de fermeture	Événements impliquant la menace d'une fermeture forcée d'une activité, d'un programme ou d'une organisation.
	Menace : Témoin	Événements dans lesquels un membre du personnel est témoin d'une attaque ou d'un crime contre un autre membre du personnel, des membres de la famille ou des bénéficiaires.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Utilisation d'armes (UA) Actes incluant le type d'arme qui a été utilisé dans l'incident, ce qui a affecté le personnel, l'infrastructure ou la livraison de l'aide.	**UA : Explosifs : Bombes aériennes**	Armes explosives larguées par voie aérienne, y compris les armes incendiaires, à l'exclusion des bombes à sous-munitions et des missiles sol-sol.
	UA : Explosifs : Bombes à fragmentation	Armes explosives larguées ou lancées au sol éjectant des sous-munitions plus petites.
	UA : Explosifs : Grenades à main	Petit engin explosif lancé à la main, conçu pour exploser après un impact ou après un certain temps.
	UA : Explosifs : Mines	Toute explosion de mine impliquant du personnel.
	UA : Explosifs : Autres	Toute autre arme explosive non répertoriée ou une combinaison des éléments ci-dessus.
	UA : Explosifs : RCIED	Un engin explosif improvisé télécommandé, tel qu'une bombe, aurait été laissé sur le bord de la route et aurait explosé lorsque la cible serait proche.
	UA : Explosifs : Sol-sol	Comprend des missiles, des mortiers ou des obus lancés à partir d'un système de lancement mobile ou stationnaire, y compris des grenades propulsées par fusée.
	UA : Explosifs : SVIED	Explosif improvisé par une ou des personne(s), par ceinture explosive ou explosive dans un sac à dos.
	UA : Explosifs : VBIED	Dispositif explosif improvisé transporté par un véhicule, par voiture piégée, ou une voiture contenant un engin explosif.
	UA : Biologique	Toute utilisation d'armes biologiques dans une ville ou un pays dans lequel l'organisation a un bureau.
	UA : Chimique	Toute utilisation d'armes chimiques dans une ville ou un pays dans lequel l'organisation a un bureau.
	UA : Nucléaire	Toute utilisation d'armes nucléaires, explosives ou non, dans une ville ou un pays où l'organisation a un bureau.
	UA : Radiologique	Toute utilisation d'armes radiologiques, communément appelées « bombes sales », dans une ville ou un pays où l'organisation a un bureau. Les incidents possibles impliquant des armes radiologiques vont des attaques contre des centrales nucléaires aux attaques de dispositifs nucléaires improvisés qui pourraient être construits à partir de matériaux radiologiques volés.
	UA : Armes à feu légères	Toute utilisation d'armes à feu ou d'armes de poing impliquant des employés ou des biens de l'organisation.

CATÉGORIES	SOUS CATÉGORIES	DÉFINITION
Occupation	**Occupation des bureaux de l'organisation**	La saisie et l'occupation de tout bâtiment, entrepôt ou complexe immobilier d'organisations par des agents civils ou gouvernementaux.
Autres	**Autre incident**	Un incident qui ne peut pas être décrit correctement par l'une des catégories d'incidents prédéfinies dans cette liste. Notez que si cette catégorie est sélectionnée, le rapporteur doit fournir une description complète de l'incident dans le champ 'Description de l'incident'.

OUTIL 3 : INCIDENT ORGANISATIONNEL OU EXTERNE

Les organisations se concentrent souvent sur le signalement et l'enregistrement des incidents organisationnels (incidents ayant un impact sur l'organisation, son personnel, ses biens et sa réputation) et non sur les incidents externes (incidents ayant un impact sur d'autres organisations). L'organisation doit définir ce qui constitue un incident affectant l'organisation et décider si les incidents externes doivent également être signalés et enregistrés.

Voici un exemple de grille élaborée par une organisation pour aider à évaluer ce qui serait considéré comme un incident organisationnel et ce qui ne le serait pas. Ce qui suit peut faire l'objet d'adaptations et de modifications, en fonction de la politique et des procédures de sécurité d'une organisation. Veuillez trouver une version vierge ci-dessous.

PERSONNE IMPLIQUÉE	HEURES DE TRAVAIL		IMPACT SUR LES BIENS DE L'ORGANISATION		QUALIFICATION
	Oui	Non	Oui	Non	
Le personnel n'est pas originaire du pays d'origine (affectation internationale)	X		X		Incident organisationnel
	X			X	Incident organisationnel
		X	X		Incident organisationnel
		X		X	Si pas de violence : Non Si avec violence : Oui
Le personnel est originaire du pays	X		X		Incident organisationnel
	X			X	Incident organisationnel
		X	X		Incident organisationnel
		X		X	Incident non organisationnel
Partie prenante externe contractée par l'organisation	X		X		Incident organisationnel
	X			X	Incident non organisationnel
		X	X		Dépend du type d'incident ou de biens et de l'impact de l'incident : oui ou non
		X		X	Incident non organisationnel

Pour votre organisation, utilisez :

PERSONNE IMPLIQUÉE	HEURES DE TRAVAIL		IMPACT SUR LES BIENS DE L'ORGANISATION		QUALIFICATION
	Oui	Non	Oui	Non	
Le personnel n'est pas originaire du pays d'origine (affectation internationale)					
Le personnel est originaire du pays					
Partie prenante externe contractée par l'organisation					

OUTIL 4 : MODÈLE DE RAPPORT D'INCIDENT

Ce modèle examine les informations les plus immédiates nécessaires à la gestion des incidents de sécurité et à l'analyse préliminaire.

COORDONNÉES DE L'AUTEUR :	
Fiabilité de la source et estimation de la validité de l'information[37] (selon la grille d'analyse approuvée) :	

1. COORDONNÉES DE L'AUTEUR DU RAPPORT	
Auteur du rapport :	Nom complet, poste (relation avec l'organisation si externe).
L'auteur du rapport est-il impliqué dans l'incident ?	Oui / Non
Date du rapport :	Date de soumission (et version du rapport si ce n'est pas la première version).
2. INFORMATION GÉNÉRALE SUR L'INCIDENT	
Localisation :	Détails exacts sur l'endroit de l'incident (y compris les coordonnées GPS si possible)
Date de l'incident :	Date de l'incident (si unique) ou séquence détaillée des incidents si plusieurs événements.
Heure de l'incident :	Moment exact de l'incident (si unique) ou séquence détaillée / calendrier des incidents si plusieurs événements (heure du jour / nuit).
Programme pays :	Détails exacts sur le(s) programme(s) d'ONG concerné(s).
3. CATÉGORISATION DE L'INCIDENT	
Type d'incident :	Intentionnel ou accidentel ; Interne à l'organisation ou externe ; Piratage ; vol ; extorsion ; accident de la circulation ; etc.

[37] Ce qui peut être indiqué au début de chaque rapport ou dans le rapport lui-même.

4. INDIQUER LA GRAVITÉ DE L'INCIDENT	
Evité de justesse :	Toute situation dans laquelle un incident de sécurité a failli survenir ou s'est produit à proximité d'un travailleur humanitaire / d'une organisation / d'un programme, ou lorsque les personnes concernées ont pu éviter tout dommage grave.
Non critique :	Les personnes n'ont pas été menacées physiquement et/ou psychologiquement. Aucune blessure.
Modéré :	Les personnes ont été menacées physiquement et/ou psychologiquement. Blessures mineures qui ne nécessitent pas de suivi médical prolongé.
Sérieux :	Blessures graves nécessitant un suivi médical prolongé. Menace grave pour l'intégrité physique et/ou psychologique.
Mortel :	Un membre du personnel de l'organisation est mort en conséquence directe de l'incident.
Encore inconnu :	

5. DESCRIPTION DE L'INCIDENT
Présentez brièvement mais précisément une description de l'événement.

6. VICTIME(S)	
Nom(s) complet(s) : Personnel national / international :	Veuillez indiquer si la victime est un membre du personnel national ou international. Quelle est leur nationalité ?
Genre :	Homme(s) ou Femme(s) ou Autre
Age :	Quel âge a la (les) victime(s) ?
Autres détails pertinents pour l'affaire :	La personne souffrait-elle d'un handicap ou d'une maladie qui aurait pu avoir un impact sur l'événement ?
Ancienneté et poste dans l'organisation :	Depuis combien de temps la personne travaille-t-elle sur ce programme ? Position / responsabilité de la victime au sein de l'organisation.
Etat actuel de la victime :	Indemne, blessé (préciser la gravité, physique ou psychologique) ou décédé.

7. TÉMOINS
Indiquez le(s) nom(s) complet(s) et les coordonnées personnelles des personnes présentes lorsque l'incident s'est produit et qui peuvent aider à clarifier les faits.

8. MESURES IMMÉDIATES PRISES À LA SUITE DE L'ACCIDENT	
Contacts internes :	Qui a été informé en interne de l'incident (programme / mission) ?
Contacts externes : *Bailleurs* *Autres organisations humanitaires / de développement :* *Médias :* *Autre :*	Quelles autorités externes (locales ou nationales, administratives et/ou judiciaires, militaires) ont été contactées suite à l'incident ?
Actions prises concernant les programmes :	L'incident a des conséquences pour le programme telles que la réduction du personnel ou la cessation des activités ou du programme dans son ensemble.
Mesures prises affectant le personnel impliqué :	Le suivi / débriefing / appui psychologique est / était nécessaire pour le personnel impliqué dans l'incident.
9. ANALYSE PRÉLIMINAIRE – RISQUE(S) POUR LE PROGRAMME	
Opérationnel :	Quelles mesures d'atténuation ont été prises ? Si l'incident implique de nouveaux risques ou augmente un risque préexistant pour les opérations de l'organisation, veuillez préciser.
Ressources humaines :	Quelles mesures d'atténuation ont été prises ? Si l'incident implique de nouveaux risques ou augmente un risque préexistant pour le personnel de l'organisation, veuillez préciser.
Financier / Matériel :	Quelles mesures d'atténuation ont été prises ? Si l'incident implique de nouveaux risques ou augmente un risque préexistant au niveau financier ou pour les propriétés de l'organisation, veuillez le préciser.
Légal / Réputation :	Quelles mesures d'atténuation ont été prises ? Si l'incident implique de nouveaux risques ou augmente un risque préexistant au niveau légal ou pour l'image de l'organisation, veuillez préciser.
Autres :	
10. SUPPORT DU SIÈGE	
Indiquez si un support du siège est nécessaire et si oui, de quel support s'agit-il ?	

OUTIL 5 : GRILLES D'ANALYSE DES INCIDENTS

Ces grilles vont guider l'analyse des impacts et des causes d'un incident, et la façon dont la gestion et le suivi ont été mis en œuvre pendant et après cette première analyse.

1. IDENTIFICATION DE L'IMPACT DE L'INCIDENT

Durée de l'incident	Combien de temps a duré l'incident ?
Type de contexte	Selon les catégorisations utilisées dans l'organisation du contexte et du type et niveau de violence.
Phase de sécurité	Tel que défini dans les documents de sécurité de l'organisation.
Estimation de la perte	
Organisation	
Argent	Indiquez quels ont été les coûts directs pour l'organisation à la suite de l'incident (chiffres).
Equipement	Indiquer si l'équipement / les biens ont été endommagés et leur valeur.
Documentation	Indiquer si des documents sensibles (par exemple, une liste de personnel) ou quelque chose utilisée pour authentifier des documents (par exemple, des tampons) sont manquants.
Autres	
Personnel	
Argent	Indiquez le montant d'argent perdu par le personnel pendant l'incident.
Equipement	Indiquer si des biens appartenant au personnel ont été endommagés pendant l'incident et leur valeur.
Documentation	Indiquer si des documents personnels appartenant au personnel sont manquants.
Autres	
Débriefing émotionnel	Indiquez si un débriefing émotionnel a été fait ou non. Spécifiez la date.

2. IDENTIFICATION DES CAUSES DE L'INCIDENT

FACTEURS CONTRIBUTIFS POTENTIELS (RÉPONSES MULTIPLES POSSIBLES)		
Type d'activités	L'incident est lié au type de travail de l'organisation.	Spécifier
Manque d'acceptance de notre programme	L'incident est le résultat du manque d'acceptance du programme.	Spécifier
Mesures de protection insuffisantes	L'incident est le résultat de l'absence de mesures de protection.	Spécifier
Non-respect des règles de sécurité et/ou des POS ?	L'incident est le résultat d'une non-conformité aux règles de sécurité et/ou aux procédures.	Spécifier
Insouciance / manque de vigilance	L'incident est le résultat de l'imprudence ou du manque de vigilance de l'équipe.	Spécifier
Manque d'équipement de communication	L'incident est le résultat du manque (absence ou dysfonctionnement) d'équipement de communication nécessaire à la sécurité et à la sûreté de l'équipe.	Spécifier
Conflit (s) au sein de l'équipe	L'incident est le résultat d'un conflit entre deux ou plusieurs membres de l'équipe.	Spécifier
Incompétence / conduite du véhicule non contrôlée	L'incident est le résultat du manque de capacité du conducteur à gérer le moyen de transport impliqué dans l'incident.	Spécifier
Comportement inapproprié	L'incident est le résultat du comportement inapproprié d'un ou plusieurs membres de l'équipe (violation du code de conduite, vêtements inappropriés, etc.).	Spécifier
Changement de contexte	L'incident est le résultat du changement de la situation globale (c'est-à-dire le contexte).	Spécifier
Conflit culturel externe	L'incident est le résultat de conflits préexistants au sein de la communauté tels que des confrontations ethniques ou religieuses.	Spécifier
Autre	Décrire le(s) facteur(s) non répertorié(s) pouvant avoir contribué à l'incident.	

3. IDENTIFICATION DU MOTIF ET ACTIONS POTENTIELLES

QUESTION/ PROCESSUS	RÉPONSE	IMPLICATION POTENTIELLE (BASÉE SUR L'ÉVALUATION)	ACTIONS POSSIBLES DE L'ORGANISATION
1. Est-ce que cet incident s'est déjà produit avant et à quel point était-ce similaire ?	Oui	Menace précise (attestée par des pièces justificatives)	Communiquer les évaluations de la menace, continuer à les utiliser comme base pour les décisions de sécurité
	Non	Menace non précise (attestée par des pièces justificatives)	Revoir l'évaluation de la menace et les mesures de sécurité basées sur celle-ci
	Non	Menace ancienne (mise en évidence par des pièces justificatives)	Revoir l'évaluation de la menace et les mesures de sécurité basées sur celle-ci
2. Si les procédures appropriées ont été suivies, quel a été le résultat ?	Positif	Les procédures appropriées ont été suivies	Renforcer les procédures
		Le personnel a eu de la chance	Reconsidérer les procédures
	Négatif	Pratiques de sécurité imparfaites	Reconsidérer les pratiques de sécurité
		Tendance à prendre des risques élevés	Communiquer au personnel Former / reformer le personnel
3. Si les procédures appropriées n'ont pas été suivies, quel a été le résultat ?	Positif	Procédures inappropriées	Reconsidérer les procédures ou leur applicabilité à toutes les situations
		Le personnel a eu de la chance	Reconsidérer les procédures
	Négatif	Manque de connaissance des procédures, éventuellement pour les raisons suivantes : • Pas de briefing de sécurité pour le nouveau personnel ; • Absence d'un plan de sécurité (POS et plans d'urgence) ; • Une attention insuffisante à fournir au personnel des séances d'information sur la sécurité et l'accès au plan de sécurité ; • Manque de temps et d'encouragement pour le personnel à lire le plan de sécurité.	Considérer une façon de mieux communiquer avec le personnel
		Échec des tentatives de suivi des procédures, éventuellement pour les raisons suivantes : • Les procédures sont trop compliquées à retenir et à suivre ; • Nécessite une formation qui n'a pas été fournie ; • Nécessite un équipement qui n'est pas toujours disponible ou qui fonctionne.	Reconsidérer les procédures, la formation, la disponibilité de l'équipement

QUESTION/ PROCESSUS	RÉPONSE	IMPLICATION POTENTIELLE (BASÉE SUR L'ÉVALUATION)	ACTIONS POSSIBLES DE L'ORGANISATION
3. Si les procédures appropriées n'ont pas été suivies, quel a été le résultat ?	Négatif	Le personnel n'est pas d'accord avec les procédures, peut-être pour les raisons suivantes : • Des procédures inappropriées ; • Nécessité d'une formation plus poussée pour convaincre le personnel de l'importance des procédures ; • Pratiques d'embauche inappropriées ; • Un manque de mise en œuvre des procédures au sein de l'organisation.	Reconsidérer les pratiques appropriées en matière de sécurité

4. ANALYSE DE LA GESTION DE L'INCIDENT

Rendre compte aux responsables de programme	Avec quel succès l'information a-t-elle été transmise ? Les délais de l'organisation ont-ils été respectés ?
Arbre de communication	Dans quelle mesure la transmission de l'information dans l'ensemble du site a-t-elle été efficace ? L'arborescence des communications a-t-elle fonctionné correctement ?
Rôles et responsabilités	Les responsables savaient-ils quoi faire en fonction de leurs responsabilités et de leurs tâches ?
Pré-identification des personnes-ressources clés avant l'incident	Avons-nous clairement identifié des personnes clés (externes et internes) qui nous ont aidés dans la gestion de l'incident ? Avons-nous essayé de contacter une institution / autorité pour nous aider ? Avons-nous identifié la ou les personnes-ressources clés ? Indiquez cette personne de contact.
Communication Siège – Terrain – Siège	Comment était la communication entre le siège et le terrain ? De quoi avons-nous besoin pour nous améliorer ?
Autre	

OUTIL 6 : COMMENT EFFECTUER UN DEBRIEFING FACTUEL

Le processus de débriefing factuel devrait commencer après l'organisation des premiers soins ou des traitements médicaux (physiques et psychologiques) pour la (les) personne(s) concernée(s). Lors de l'organisation d'un débriefing factuel à des fins de collecte d'informations, il est néanmoins important de garder à l'esprit les principes de base des premiers secours psychologiques : débriefing lorsque la sécurité physique et psychologique de base est assurée, création d'un espace sûr, responsabilisation de la victime, le processus, les attentes et les actions de suivi, etc[38].

Un débriefing factuel ne doit pas être confondu avec un débriefing émotionnel (également appelé désamorçage). Un événement traumatisant devrait être traité par des professionnels ou du personnel qualifié fournissant des PSP.

Les informations ci-dessous ne sont pas une tentative de former les lecteurs sur les Premiers Soins Psychologiques (PSP), ou de devenir des enquêteurs professionnels. Il s'agit d'une liste de conseils pour mener des entrevues sûres et utiles aux fins d'établissement des faits, dans le cadre de la déclaration des incidents.

Au début d'un débriefing factuel, rappelez à tous les participants que le but du débriefing est d'apprendre et de prévenir, et non de trouver la faute.

Préparation à un débriefing :

- Identifiez qui effectue le débriefing.
- Identifier qui est présent ; les procédures organisationnelles doivent définir si le personnel impliqué dans l'incident doit être présent ensemble ou séparément. La procédure peut indiquer que c'est un choix qui doit être fait au cas par cas, en fonction de la nature de l'événement et des contraintes logistiques. Bien que l'organisation d'un débriefing collectif présente clairement des avantages (logistiques, mais aussi pour la saisie du récit), elle peut aussi entraîner une réécriture de l'incident et une modification des faits (les témoins et les victimes s'influencent, leurs perceptions varient, le personnel peut craindre de donner des opinions sur les causes et les responsabilités devant les autres, etc.).

[38] Pour plus d'informations sur le PFA, voir les directives de l'Organisation mondiale de la santé cliquez ici.

- Informez les personnes faisant l'objet d'un débriefing de qui sera présent pendant celui-ci.
- Identifiez un espace sûr pour que le débriefing ait lieu. Choisissez un endroit sûr et pratique pour la personne, comme une salle de conférence ou un bureau privé.
- Permettre à la personne chargé du débriefing de suggérer le meilleur moment (en tenant compte des autres contraintes), en accord avec les procédures de débriefing de votre organisation.
- Préparez vos questions ; les questions peuvent suivre le modèle de rapport d'incident et couvrir les mêmes éléments. Vous pourriez ne pas avoir besoin de leur demander pendant l'entrevue mais ils vous guideront si nécessaire. Elles doivent être des questions ouvertes.
- Pratiquez la conscience de soi en identifiant vos propres biais potentiels et en les mettant de côté pendant le débriefing. L'analyse viendra plus tard.

Étapes du débriefing :

1. Conduisez l'interview dans un endroit calme et privé. Mettez l'individu à l'aise quand il arrive et offrez un verre d'eau, du thé ou du café. Assurez-vous qu'ils ne sont pas fatigués et qu'ils ont été débriefés émotionnellement.
2. Indiquer que le but du débriefing est l'établissement des faits et non la recherche des fautes.
3. Ne promettez pas la confidentialité, mais dites à la personne que vous partagerez l'information avec seulement ceux qui ont besoin de savoir.
4. Fournissez à la personne une estimation approximative du temps que prendra le débriefing.
5. Demandez à l'individu de raconter sa version de ce qui s'est passé sans l'interrompre. Prenez des notes ou enregistrez leurs réponses.
6. Posez des questions de clarification pour remplir les informations manquantes. Utilisez des questions ouvertes.
7. Raconter l'information obtenue à la personne interrogée. Corrigez les incohérences.
8. Demandez à l'individu ce qui, selon lui, aurait pu prévenir l'incident, en se concentrant sur les conditions et les événements qui ont précédé l'événement. Cela peut compléter l'analyse.
9. Évitez d'exprimer vos pensées, vos opinions ou vos conclusions au sujet de l'incident ou de ce que dit l'individu.
10. Informez la personne interrogée des prochaines étapes.
11. Remerciez l'individu.
12. Terminez la documentation du débriefing en remplissant le modèle de rapport d'incident.

Exemples de questions ouvertes :

- Où étiez-vous au moment de l'incident ?
- Que faisiez-vous à ce moment-là ?
- Qu'avez-vous observé qui aurait pu être inhabituel ?
- Qu'avez-vous vu ou entendu ?
- Quelles étaient les conditions environnementales (temps, lumière, bruit, etc.) à ce moment-là ?

- Que faisaient les travailleurs blessés à ce moment-là ?
- Selon vous, qu'est-ce qui a causé l'incident ?
- Comment, selon vous, des incidents similaires pourraient-ils être évités à l'avenir ?
- Y a-t-il d'autres témoins? Connaissez-vous les noms d'autres témoins ?
- Comment êtes-vous connecté avec les autres personnes impliquées dans l'incident ?
- Quels autres détails aimeriez-vous partager ?

Ce qu'il faut éviter :

- Intimider, interrompre ou juger l'individu.
- Aider l'individu à répondre aux questions.
- Poser des questions suggestives.
- Poser plusieurs questions en même temps.
- Devenir émotionnellement impliqué.
- Sauter aux conclusions.
- Révéler les découvertes de l'enquête.
- Faire des promesses qui ne peuvent être tenues.

Analyse :

Afin de responsabiliser l'individu et lui donner l'opportunité de partager des commentaires perspicaces, il est suggéré que vous lui demandiez son analyse de l'incident lors du débriefing. Néanmoins, rappelez-vous que leur jugement peut être affecté par l'événement traumatique. Les causes de l'incident devront être analysées par la personne qui remplit le rapport d'incident. Le but du débriefing d'établissement des faits est de déterminer tous les facteurs qui ont contribué à la survenue de l'incident.

Les questions suivantes peuvent vous aider dans votre analyse des facteurs :

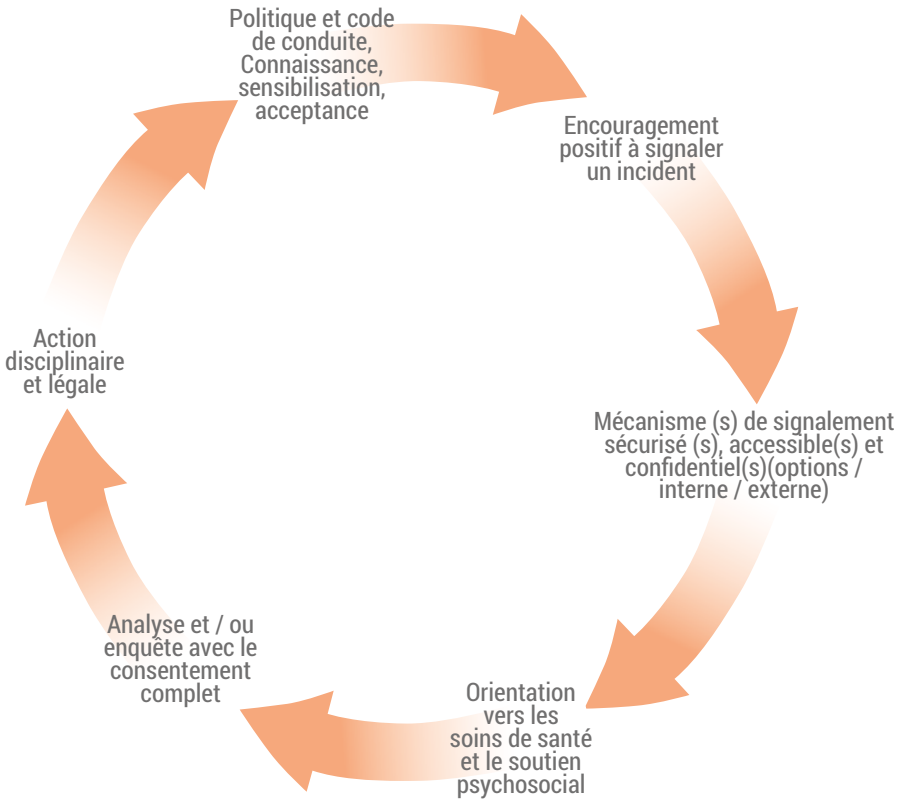
- Une situation dangereuse était-elle un facteur contributif ?
- L'emplacement était-il un facteur contributif ?
- La procédure a-t-elle été un facteur contributif ?
- Le manque d'équipement de protection individuelle ou d'équipement d'urgence a-t-il joué un rôle ?
- Les POS étaient-elles un facteur contributif, et devraient-elles être mises à jour pour refléter une nouvelle réalité sur le terrain?
- La dynamique de l'équipe a-t-elle été un facteur contributif et comment pensez-vous que nous pourrions l'améliorer ?

Des déclarations telles que « le personnel était négligent » ou « l'employé n'a pas suivi les procédures de sécurité », « mauvais moment, mauvais endroit » ne sont pas à la source d'un incident. Pour éviter ces conclusions trompeuses, concentrez-vous sur les raisons de l'incident, par ex. « Pourquoi l'employé n'a-t-il pas suivi les procédures de sécurité ? »

OUTIL 7 : BONNES PRATIQUES EN MATIÈRE DE SIGNALEMENT DES INCIDENTS LIES AU GENRE ET MÉCANISMES DE PLAINTES POUR SIGNALER L'EXPLOITATION ET LES ABUS SEXUELS (EAS)

Cet outil propose un résumé des bonnes pratiques en matière de signalement et de suivi des incidents liés au genre et les EAS. Il doit aider les organisations à développer et adapter leurs propres systèmes.

Cycle de signalement des incidents sensibles[39]



[39] Cet outil est extrait de Persaud, C. (2012). Genre et sécurité: Lignes directrices pour l'intégration du genre dans la gestion des risques de sécurité. EISF.

Politique :
La politique est à la base de la bonne déclaration des incidents et peut inclure une clause de dénonciation. Un accent particulier devrait être mis sur le suivi des rapports d'incidents. Il devrait y avoir des rapports obligatoires pour des incidents spécifiques, sauf dans les situations où il s'agit d'une option pour un individu, comme les cas de harcèlement et de violence liée au genre. L'exploitation et les abus sexuels relèvent d'un code de conduite et d'une politique différente. Les membres du personnel ont le devoir de signaler les cas d'exploitation et d'abus sexuels ou sinon de faire l'objet de possibles mesures disciplinaires (voir ci-dessous pour plus d'informations).

Conscience :
Le personnel doit être conscient de ce qui constitue un incident, en mettant particulièrement l'accent sur les situations moins discutées telles que le harcèlement, la violence liée au genre, les accidents évités de justesse ou les incidents mineurs. La sensibilisation peut être augmentée tout en créant du réconfort et de la confiance en encourageant les rapports d'incidents pendant l'induction, les orientations, les formations, les réunions, etc. Le personnel doit connaître ses droits et ses options.

Options / procédures de signalement d'incident :
Plusieurs canaux devraient être établis pour le signalement des incidents. Cela offre des options supplémentaires pour le personnel en fonction de leur niveau de confort ou de leur besoin de confidentialité. Les options comprennent (mais ne sont pas limitées à) : rapports en ligne via l'intranet, la hot line téléphonique (en PCV ou sans frais), points focaux, canaux qui contournent certains niveaux hiérarchiques (dans les cas où ils sont signalés) etc.

Utilisation des points focaux :
Les points focaux doivent être soigneusement sélectionnés et formés en fonction de leur profil personnel, de leurs capacités, de leur habilité à maintenir la confidentialité et de leur objectivité. Avoir un nombre varié de points focaux aux profils divers (internationaux et nationaux, hommes et femmes) peut augmenter l'aisance et l'accès aux procédures de signalement.

Analyse / enquêtes :
Le suivi des incidents éclairera par la suite l'analyse des risques, les mesures de réduction des risques ou les niveaux de sensibilisation du personnel. Un certain niveau d'enquête interne, mené par des personnes extrêmement bien formées, peut être nécessaire en cas de violation des politiques internes. Cela justifiera de notifier les autorités locales / police pour enquête externe en cas de violation confirmée des lois locales.

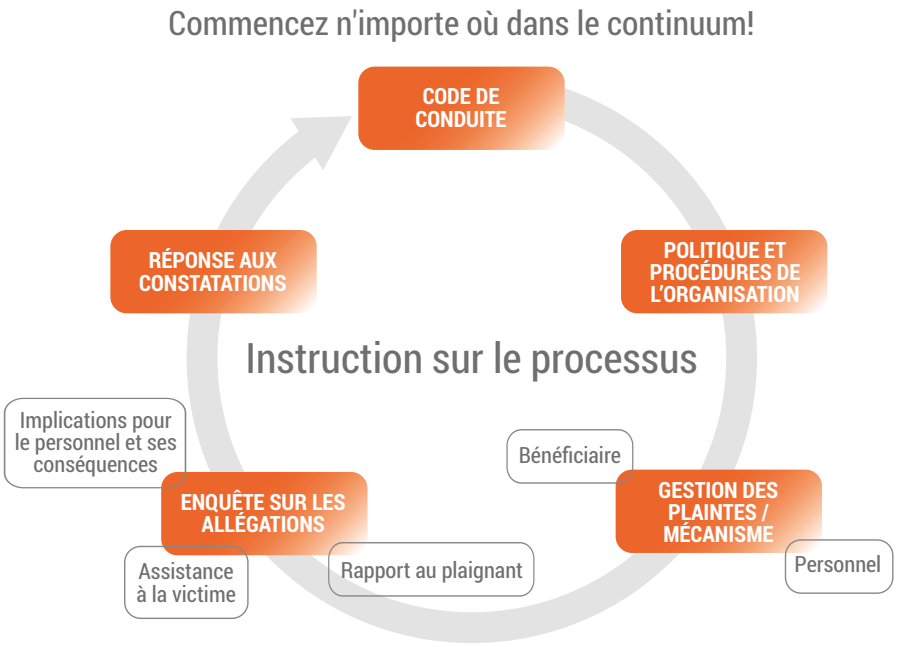
Procédures disciplinaires :
En cas de faute de la part d'un membre du personnel (en fonction de la gravité de l'incident et des lois locales, notamment du droit du travail), des mesures disciplinaires doivent être prises et appliquées de la même façon au personnel qu'il soit local / national / international / masculin ou féminin.

Mémoire institutionnelle :
Évitez d'engager toute personne ayant des antécédents de perpétration de tout type d'incident grave, y compris la corruption, le harcèlement sexuel ou la violence sexuelle, y compris l'exploitation sexuelle, les abus sexuels et la violence domestique. Cela peut sembler évident, mais il y a une longue histoire, à travers des exemples anecdotiques, d'auteurs réembauchés dans un pays différent parfois même par la même organisation. Si les lois pertinentes régissant les employeurs et les employés le permettent, coordonner avec d'autres organismes pour établir un système d'échange de renseignements sur les employés dont les contrats ont été résiliés pour harcèlement, violence sexuelle ou EAS. Des pratiques d'embauche prudentes qui comprennent la vérification des références et un contrôle sont impératives.

Cadre d'exploitation et d'abus sexuels (EAS) :
Principes d'EAS définis par l'Inter Agency Standing Committee (IASC)

- L'exploitation et les abus sexuels commis par des travailleurs humanitaires constituent des fautes graves et sont donc des motifs de licenciement ;
- Les relations sexuelles avec des enfants (personnes de moins de 18 ans) sont interdites quel que soit l'âge de la majorité ou l'âge du consentement localement. La croyance erronée dans l'âge d'un enfant n'est pas une défense ;
- L'échange d'argent, d'emploi, de biens ou de services à des fins sexuelles, y compris les faveurs sexuelles ou d'autres formes de comportement humiliant, dégradant ou d'exploitation, est interdit. Cela comprend l'échange d'assistance due aux bénéficiaires ;
- Les relations sexuelles entre les travailleurs humanitaires et les bénéficiaires sont fortement découragées car elles sont basées sur des dynamiques de pouvoir intrinsèquement inégales. De telles relations compromettent la crédibilité et l'intégrité du travail d'aide humanitaire ;
- Lorsqu'un travailleur humanitaire a des préoccupations ou des soupçons concernant des abus sexuels ou d'exploitation par un collègue, que ce soit dans la même organisation ou non, il / elle doit signaler ces préoccupations par le biais des mécanismes de signalement établis des organisations ;
- Les travailleurs humanitaires sont tenus de créer et de maintenir un environnement qui prévient l'exploitation et les abus sexuels et promeut la mise en œuvre de leur code de conduite. Les responsables à tous les niveaux hiérarchiques ont des responsabilités particulières pour soutenir et développer des systèmes qui maintiennent cet environnement.

Cycle de rapport EAS[40]



Source : Guide InterAction et ses modules d'apprentissage sur la lutte contre l'EAS.

40 InterAction. (2010). *Guide étape par étape d'InterAction sur la lutte contre l'exploitation et les abus sexuels.* InterAction.

OUTIL 8 : PLAN D'ACTION POUR LE SUIVI DES INCIDENTS

Cet outil répertorie les questions à inclure dans le plan d'action, qui devrait être mis en œuvre après chaque incident, quel que soit sa gravité.

Numéro de référence de l'incident : #

Action à prendre (une ligne par action)	Description de l'action à prendre en termes précis
Par qui	À quel niveau, nom ou position ?
Par qui	Qui va être impliqué, en interne ou externe à l'organisation ?
Logistique requise et budget	Coûts et besoins estimés, procédures d'achats l'organisation
Quand ?	Quand est-ce que l'action doit être mise en œuvre? Date fixe ou revue périodique ?
Qui est responsable de l'action mise en œuvre	Le responsable hiérarchique est-il responsable de cela ? Le SFP ? Quelqu'un d'autre ?
Revue et validation	Par qui et quelle date ?
Signature	Signature du personnel impliqué dans la mise en œuvre et dans le contrôle

Statut de l'incident :
Statut de gestion de l'incident :

OUTIL 9 : SYSTÈMES GIIS

Systèmes accessibles pour signaler, enregistrer, stocker et analyser les incidents de sécurité affectant l'organisation au niveau central.

ENREGISTREMENT D'INCIDENT ET MÉTHODE DE RAPPORT	SYSTÈME	AVANTAGES	DÉSAVANTAGES	ÉLÉMENTS DE COÛT DE MISE EN ŒUVRE ET DE FONCTIONNEMENT
Récit écrit de l'incident	• Courriels • Feuille Google • Plate-forme Google partagée • SharePoint	Coût d'installation très faible	Ne fonctionne bien que s'il est utilisé systématiquement. Risques : • Savoir-faire et parfois même accès perdu à l'occasion du départ du personnel. • Rapports très inégaux ; avec des implications pour la comparabilité de l'information. Nécessite beaucoup de temps au cours du processus d'analyse. process.	Coût lié au temps passé par le personnel pour la mise en place du système. Coût lié au temps passé par le personnel pour rédiger les rapports narratifs. Coût lié au temps passé par le personnel pour transformer l'information en un format systématique. Coût lié au temps de travail du personnel pour effectuer l'analyse. Cette partie peut prendre beaucoup de temps car le système lui-même ne prend pas en charge l'analyse.

ENREGISTREMENT D'INCIDENT ET MÉTHODE DE RAPPORT	SYSTÈME	AVANTAGES	DÉSAVANTAGES	ÉLÉMENTS DE COÛT DE MISE EN ŒUVRE ET DE FONCTIONNEMENT
Feuille de calcul Excel pour enregistrer les incidents à l'aide d'un codage systématique	Feuille de calcul Excel configurée pour les champs à enregistrer. La feuille de calcul Excel peut être utilisée pour classer systématiquement les informations soumises dans un format écrit.	Faibles coûts d'installation. Aucun coût de consultant requis car le travail peut facilement être fait en interne. Peut très bien fonctionner pour les organisations qui commencent à enregistrer des incidents et qui ont un nombre limité d'incidents à enregistrer et à gérer.	Peut devenir difficile à gérer lorsque trop de catégories et de types d'événements sont suivis. Nécessite une analyse de tendance très manuelle qui peut prendre beaucoup de temps. Seule la personne ayant accès à la feuille de calcul a tendance à connaître et à comprendre le système. Moins d'incitation pour le personnel à signaler car ils peuvent ne pas être conscients du système d'enregistrement.	Coût lié au temps passé pour développer un système Excel approprié. Le cout du personnel traduisant l'information écrite en catégories codées. Le coût du personnel pour effectuer l'analyse.
Abonnement à une plateforme en ligne pour la gestion des données	Certaines entreprises privées et certains organismes à but non lucratif offrent des plateformes en ligne pour la gestion de l'information issue des incidents de sécurité.	Systèmes efficaces dans les fonctions d'analyse intégrées. La plupart des systèmes permettent différents niveaux d'accès permettant un accès sur mesure pour le personnel de terrain ainsi que pour la direction. Les problèmes techniques sont externalisés. L'accès direct pour le personnel de terrain augmente l'incitation à signaler. Assure une fourniture de l'information plus élevée et systématique puisque tout le monde utilise le même système avec les mêmes instructions. Réduit la charge de travail du personnel d'analyse du Siège, car l'analyse peut être une fonction intégrée.	Coûts de fonctionnement mensuels Il peut être difficile ou coûteux de demander des modifications pour adapter le système aux exigences spécifiques à l'organisation	Frais d'inscription

ENREGISTREMENT D'INCIDENT ET MÉTHODE DE RAPPORT	SYSTÈME	AVANTAGES	DÉSAVANTAGES	ÉLÉMENTS DE COÛT DE MISE EN ŒUVRE ET DE FONCTIONNEMENT
Système en ligne personnalisé	Certaines organisations ont commandé le développement de systèmes en ligne spécifiques à l'organisation. Certaines organisations ont pu utiliser les systèmes existants et créer des rapports en tant qu'extension des plates-formes existantes utilisées pour le courrier électronique, telles que SharePoint.	Le système correspond aux besoins organisationnels et aux définitions internes. S'il est connecté à des systèmes existants, le personnel peut apprendre à l'utiliser beaucoup plus rapidement.	Coûts de développement élevés si des spécialistes informatiques externes sont nécessaires. Si les organisations peuvent utiliser leur département informatique, les coûts sont moins élevés. Les coûts de maintenance peuvent être élevés si il est nécessaire d'utiliser des consultants informatiques externes, mais moins si elle est assurée par le service informatique interne.	Coûts de développement et de maintenance

OUTIL 10 : CONSERVATION DE L'INFORMATION ISSUE DES INCIDENTS

Structures de base à utiliser sur les feuilles Excel pour enregistrer les incidents
Concevoir la structure idéale pour stocker de l'information issue des incidents de sécurité sur une feuille de calcul Excel est une tâche très difficile. Le large éventail d'événements différents qui devraient être pris en compte pour la prise de décision stratégique dans le contexte de la sécurité et les informations détaillées requises sur certains aspects rendent impossible l'existence d'une structure simple adaptée à toutes les situations. Le défi consiste à trouver le juste équilibre entre le maintien de la simplicité et de la praticabilité tout en conservant les informations clés requises, avec suffisamment de détails pour que l'information soit significative pour émettre des recommandations.

Ce guide fournit deux exemples de format différents sur la façon dont l'information issue des incidents peut être stockée dans une feuille de calcul Excel. Les organisations qui conçoivent leur propre feuille de calcul sont encouragées à regarder les exemples fournis et à mélanger et assortir les éléments les plus adaptés à leurs propres priorités. Veuillez consulter d'autres outils pour les définitions suggérées des différents domaines.

Les deux exemples de feuilles de calcul Excel pour l'enregistrement des incidents peuvent être consultés et téléchargés à partir de la page du projet RedR. Voir les éléments ci-dessous :

- Feuille de calcul des catégories d'événements SiND
- Modèle de journal d'incident

Vous trouverez ci-dessous les principes clés à prendre en compte lors de la conception d'une feuille de calcul Excel pour les informations sur les incidents de sécurité.

Unités d'analyse
Chaque ligne d'une feuille de calcul Excel stocke une unité clé d'information. Dans la plupart des cas, ce sera l'événement. Chaque ligne est un événement unique. Les colonnes sont utilisées pour fournir des détails sur l'événement.

Pour enregistrer d'autres unités d'information, comme traiter les membres du personnel comme des unités individuelles (plutôt qu'un numéro associé à un événement), ou enregistrer des détails sur le matériel perdu ou suivre une réponse, on peut procéder de la manière suivante :

- Créez une deuxième / troisième / quatrième feuille sur le classeur Excel pour 'personnel', 'matériel' ou 'réponse'. Sur ces nouvelles feuilles de calcul, chaque rangée stocke les informations individuelles sur chaque personne, chaque élément endommagé ou perdu, ou chaque réponse, etc. Chaque feuille de calcul compte donc une unité différente. Si quatre membres du personnel sont affectés en une seule fois, la feuille de calcul de l'événement comporte une rangée (une unité) pour l'événement mais quatre rangées (quatre unités) pour le personnel (voir les exemples ci-dessous). Si deux voitures sont endommagées, la «feuille de matériel» comporte deux rangées, une pour chaque voiture. Chaque membre du personnel et chaque voiture deviennent ainsi une unité à part entière. Ces feuilles peuvent être utilisées pour stocker des détails utiles à l'analyse globale.

  - L'avantage d'un tel système est qu'il devient plus facile de fournir une analyse détaillée au-delà de la description de l'événement. Il est également possible d'utiliser des listes déroulantes de plusieurs catégories exclusives choisies pour chaque individu. La feuille contient plus d'informations sous une forme plus condensée. L'inconvénient est que les données deviennent plus complexes.
  - Si des feuilles de calcul supplémentaires sont ouvertes, il est essentiel d'utiliser des numéros d'identité d'événement uniques dans la première colonne pour s'assurer qu'il est possible de relier les informations à l'événement.

- Intégrez une unité différente (telle que le personnel, le matériel) dans la feuille où l'unité d'analyse est l'événement. Cela peut être fait en créant une série de colonnes supplémentaires chaque fois que l'unité de comptage est changée d'événement en personnel, matériel ou réponse. Différentes couleurs peuvent être utilisées pour l'indiquer.

  - Par exemple, les colonnes pourraient inclure le nombre de personnes affectées par l'événement par autant de colonnes supplémentaires que nécessaire pour classer tout le personnel par des informations supplémentaires, qui doivent ensuite être divisées en plusieurs colonnes d'options (voir la base de données Aid Worker Security Database comme un exemple de comment les informations détaillées sur le personnel peuvent être enregistrées les unes à côté des autres).

Quelques différences d'informations sur les feuilles Excel simples ou multiples
Les exemples ci-dessous montrent les mêmes informations sur quatre personnes affectées dans un même événement, stockées par unité d'analyse « événement » et unité d'analyse « personnel ». Stocker les informations sur le personnel sur une feuille de calcul où l'unité d'analyse est l'événement nécessite plus de colonnes pour stocker moins de détails. Il n'est pas non plus possible de stocker des détails sur les individus (il serait très difficile d'ajouter les informations supplémentaires sur le travail ou si l'assurance prenait en charge le soutien psychologique post incident). Si le personnel constitue l'unité d'analyse, il est facile d'enregistrer des informations plus détaillées. Ce détail supplémentaire pourrait aider à repérer les tendances ou à identifier des recommandations d'action spécifiques, par exemple en matière de prise en charge par l'assurance.

Feuille unique pour les unités d'événement :

UNITÉ D'ANALYSE	NOMBRE DE MEMBRES DU PERSONNEL AFFECTÉS	FEMME	HOMME	MEMBRE DU PERSONNEL INTERNATIONAL	MEMBRE DU PERSONNEL NATIONAL	AUTRE	MORTS	BLESSÉS
Event 1	4	1	3	1	2	1	1	3

Plusieurs feuilles pour différentes unités (par exemple personnel, matériel ou réponse) :

UNITÉ D'ANALYSE	IDENTITÉ D'ÉVÉNEMENT UNIQUE	SEXE	STATUT	EMPLOI	IMPACT	PRISE EN CHARGE PAR L'ASSURANCE DU SOUTIEN PSYCHOLOGIQUE
Personnel 1	Évènement 1	Femme	Membre du personnel international	Personnel professionnel	Blessé	Couvert
Personnel 2	Évènement 1	Homme	Membre du personnel national	Chauffeur	Mort	Non applicable
Personnel 3	Évènement 1	Homme	Membre du personnel national	Personnel professionnel	Blessé	Pas couvert
Personnel 4	Évènement 1	Homme	Volontaires	Volunteer	Blessé	Pas couvert

Options multiples ou mutuellement exclusives
Les informations peuvent être enregistrées en tant qu'options multiples (plus d'une description s'applique) ou en tant qu'options mutuellement exclusives (une seule option peut s'appliquer).

- **Plusieurs options** sont présentées dans des colonnes l'une à côté de l'autre. Chaque colonne représente une caractéristique particulière et la feuille de calcul est utilisée pour indiquer que l'option spécifique s'applique à l'événement. Cela peut être fait en choisissant « oui », un nombre (par exemple « 1 ») ou une option dans une liste déroulante. Les options qui ne s'appliquent pas sont soit laissées vides (moins de travail dans le codage) soit identifiées comme ne s'appliquant pas en choisissant « non applicable » ou « 0 » (cela permet de vérifier que les nombres totaux sont corrects et de repérer les erreurs).
- **Les options mutuellement exclusives** sont présentées sous la forme d'options de liste déroulante qui peuvent être choisies lors du remplissage d'informations dans une colonne particulière. Les listes déroulantes vous permettent d'enregistrer des informations supplémentaires et d'assurer la cohérence de l'orthographe. Cependant, elles ne devraient être utilisées que si une seule option peut s'appliquer. Voir la feuille de calcul des catégories d'événements SiND pour des exemples de menus déroulants.
- **Des options multiples et mutuellement exclusives** peuvent être combinées dans la gestion des données. Une feuille de calcul bien conçue peut contenir une série de colonnes présentant plusieurs options (par exemple, toutes ou certaines des options peuvent s'appliquer à chaque événement et les colonnes sont remplies si nécessaire). Ces options ont une liste associée d'options de listes déroulantes mutuellement exclusives (par exemple, chaque fois qu'une des options est choisie, le système indique non seulement « oui » ou un nombre mais spécifie la sous-catégorie sous l'option). Pour un exemple d'un tel système, voir la feuille de calcul des catégories d'événements SiND.

OUTIL 11 : TECHNOLOGIE POUR SIGNALER ET ENREGISTRER LES INCIDENTS

Chaque système pour signaler et enregistrer les incidents est différent et a ses propres avantages et inconvénients. Le modèle le plus approprié à une organisation dépendra de son niveau de capacité technologique, de l'échelle de ses opérations, de sa taille et de ses ressources financières, etc.

Voir le tableau ci-dessous pour une comparaison de certains systèmes de rapports d'incidents en ligne[41].

	GRATUIT	SOURCE OUVERTE (GRATUIT)	AUTORISÉ	AUTONOME	LOGICIEL EN TANT QUE SERVICE	STANDARD	FAIT SUR MESURE	GRAPHIQUES INTÉGRÉS	NIVEAU DE PROTECTION DES DONNÉES
Ushahidi		●		●		●			●●
SIMSON	●		●		●	●		●	●●
Open DataKit		●		●		●		●	●●
SharePoint	●		●	●	●	●		●	●●
NAVEX Global™	●		●		●		●	●●	●●
IRIS	●		●				●	●	●●
RIMS			●				●	●	●●

●● Non analysé

La section suivante présente les avantages et les inconvénients des systèmes actuellement utilisés par les organisations qui ont contribué à ce manuel. Pour en savoir plus sur un système, veuillez suivre les liens fournis.

41 Certaines des informations partagées dans cet outil ont été extraites d'un article non publié de l'EISF: De Palacios, G. (2017). « Gérer les informations liées à la sécurité: un examen plus approfondi des systèmes de signalement des incidents », *EISF*.

SharePoint

Ceci est une application Web qui s'intègre à Microsoft Office. Il est principalement vendu comme système de gestion et de stockage de documents. Cependant, le produit est hautement configurable et l'utilisation varie considérablement entre les organisations. Bien qu'il nécessite l'achat d'une licence pour son utilisation, certains des produits Microsoft Office 365 sont gratuits pour les organisations à but non lucratif. SharePoint est un système qui peut être utilisé pour partager des informations sous différentes formes; il est possible de créer des formulaires en ligne auxquels seuls les utilisateurs autorisés peuvent accéder.

AVANTAGES	LIMITES
En tant que produit Microsoft, il est compatible avec les logiciels de traitement de données tels que Word, Excel, PowerPoint, etc. Cela permet à une organisation d'exporter facilement les données du système vers ces applications et de partager et analyser les informations à l'aide d'un logiciel familier. Elles pourraient ne pas avoir besoin d'une nouvelle installation de logiciel ou de formation du personnel sur l'utilisation de la nouvelle plate-forme. Le développement du système peut être géré en interne par l'équipe informatique déjà en charge du développement et de la maintenance de SharePoint.	Bien qu'il soit possible d'exécuter des enquêtes à l'aide de SharePoint, il ne s'agit pas d'un logiciel spécialement conçu pour signaler ou collecter des données. La représentation des données dans une carte n'est pas intégrée par défaut dans le système et il faudrait le faire en installant un module supplémentaire.

Ushahidi

Ushahidi a été développé pour cartographier la violence au Kenya pendant et après les violences post-électorales en 2008. Les rapports peuvent être envoyés via un certain nombre de plateformes, y compris un formulaire en ligne, un e-mail, un message texte ou des réseaux sociaux tels que Twitter. Une fois ces rapports reçus, ils peuvent être revus par un administrateur afin de valider et d'approuver le contenu, afin qu'ils puissent apparaître sur la carte de sa page principale.

Ushahidi est un logiciel libre et gratuit pour la collecte d'informations, la visualisation et la cartographie interactive. Le formulaire de rapport peut être personnalisé afin qu'une organisation puisse collecter les informations qui sont importantes pour elle, et une fois les rapports validés, il est possible de les voir reflétés dans une carte regroupée selon la catégorie d'incident prédéfinie. La plate-forme peut être programmée pour alerter les responsables de la sécurité lorsqu'un nouvel incident a été signalé, afin qu'ils puissent apporter un soutien aux victimes et valider le rapport. Ushahidi peut également alerter les autres utilisateurs une fois le rapport validé.

AVANTAGES	LIMITES
Le principal avantage d'Ushahidi est qu'il peut être téléchargé gratuitement sur Internet. L'installation du système n'est pas compliquée et puisque l'organisation décide où installer le logiciel, les données restent sous le contrôle de l'organisation.	Le principal inconvénient d'Ushahidi est que la représentation statistique des informations contenues dans la base de données n'est pas intégrée dans le système, et que des solutions externes doivent être combinées à cette fin. C'est une excellente solution pour la collecte de données, mais d'autres ressources sont nécessaires pour l'analyse des données. La plate-forme Ushahidi n'est plus en cours de développement, ce qui pourrait causer des problèmes au fur et à mesure que d'autres technologies connexes évoluent. Ces problèmes potentiels peuvent éventuellement être résolus par le personnel informatique.

SIMSON

Le système SIMSON a été spécialement conçu pour les ONG par le Center for Safety and Development (CSD). SIMSON est un système de signalement des incidents de sécurité en ligne où les utilisateurs peuvent voir les incidents signalés représentés sur une carte. Les ONG qui utilisent SIMSON ne doivent pas installer, programmer ou écrire le code d'un logiciel. Le Center for Safety and Development (CSD) fournit également un support pour l'exécution de la plateforme et la gestion des sauvegardes. Les incidents peuvent être filtrés par catégories, organisation, lieu, calendrier et autres informations et indicateurs liés à la sécurité. Les utilisateurs reçoivent des alertes par e-mail des nouveaux rapports d'incidents en fonction de leur place dans l'organisation et de leurs droits d'accès dérivés. Les incidents peuvent être analysés dans SIMSON à l'aide de graphiques et de tableaux. Les données d'incident peuvent également être téléchargées sous forme de fichier Excel. Les documents et les rapports d'incidents peuvent être téléchargés et, à la discrétion de l'organisation, partagés avec d'autres parties prenantes, par exemple, des compagnies d'assurance ou d'autres ONG. Il existe une procédure spéciale « incident sensible » qui n'informe que les agents désignés de votre organisation. Ceci est pertinent lorsqu'il s'agit par exemple d'incidents d'agression sexuelle.

Pour en savoir plus, un aperçu de SIMSON peut être téléchargé à partir de la page Web du CSD en suivant ce lien.

AVANTAGES	LIMITES
Le système est prêt à l'emploi, à destination des ONG et soutenu par le CSD. Les organisations n'ont donc pas besoin d'investir des ressources dans son développement, sa maintenance, ses sauvegardes. Les données d'incident peuvent être analysées dans SIMSON ou en exportant les données dans un fichier Excel.	Bien que le CSD garantisse aux organisations utilisant le système que, si elles le souhaitent, elles sont les seules à pouvoir consulter leurs rapports d'incident, les ONG peuvent souhaiter contrôler leurs données relatives à la sécurité et aux incidents et hésiter à déléguer cette responsabilité à des tiers. La personnalisation du formulaire de rapport pour les besoins spécifiques de l'organisation peut ne pas être facile.

World Vision International and NAVEX Global

World Vision International (WVI), en partenariat avec le fournisseur international de rapports sur les risques NAVEX Global, a créé un système de signalement des incidents en ligne pour la communication d'incidents, de plaintes, de harcèlement et d'autres événements. Ce système va au-delà de la stricte communication des incidents de sûreté et de sécurité et englobe d'autres éléments d'une approche de gestion des risques tels que la corruption, les poursuites judiciaires, la réputation, etc., en plusieurs langues. NAVEX Global adapte son système de débriefing aux besoins et aux caractéristiques de l'organisation qui l'utilise. Le système de signalement des incidents permet la contribution de diverses sources et tout le personnel de WVI est en mesure de faire rapport sur la plate-forme, car il sert également de système de lanceurs d'alerte.

Pour en savoir plus sur le système de signalement des incidents World Vision International, consultez le document suivant.

AVANTAGES	LIMITES
La combinaison du formulaire de signalement d'incident avec le canal de lanceur d'alerte, le mécanisme de plainte des bénéficiaires, etc. réduit la diversité possible des systèmes utilisés à des fins similaires. Avoir le soutien d'une entreprise dédiée à la gestion de l'éthique et de la conformité derrière le système peut aider à mettre en perspective les données des rapports d'incidents avec d'autres domaines de gestion des risques.	Le formulaire peut être relativement détaillé, ce qui, malgré ses avantages, peut décourager les rapports en raison de son long processus. C'est probablement aussi une solution que seules les grandes organisations peuvent se permettre.

IRIS

Basé sur Ushahidi, IRIS est une plateforme qui peut être utilisée pour signaler des incidents via une interface en ligne, et visualiser où ces incidents ont eu lieu sur une carte. Il est possible de personnaliser le modèle de rapport d'incident pour répondre aux besoins de débriefing de l'organisation utilisant le système.

La plate-forme peut être utilisée en tant que « logiciel en tant que service », ainsi qu'en l'installant sur les serveurs d'une organisation, ce qui permet un contrôle total des données rapportées. Seuls les utilisateurs enregistrés peuvent accéder à l'interface et différents privilèges peuvent être définis en fonction du profil de l'utilisateur. Les rapports peuvent être soumis via l'interface en ligne ou via une connexion à faible bande passante.

La plate-forme est multilingue et les rapports peuvent être filtrés par défaut ou par des champs personnalisés. Les responsables et les autres utilisateurs peuvent être avertis lorsque de nouveaux incidents ont été signalés afin qu'un soutien immédiat puisse être fourni aux victimes pendant que le reste de l'équipe est informé pour prendre les mesures appropriées.

Les données peuvent être extraites de la plate-forme et transmises au logiciel de visualisation de données afin que les statistiques sur les incidents puissent être utilisées pour tirer les leçons apprises, donner des recommandations, fournir des briefings, utiliser comme information de base pour l'analyse des risques, etc.

AVANTAGES	LIMITES
Facile à installer et à utiliser, hautement personnalisable dans son apparence et dans la façon dont les informations sont collectées. IRIS est basé sur Ushahidi version 2, qui est une plate-forme open source, peut être développé pour répondre aux besoins de débriefing des organisations qui l'utilisent, pour l'adapter aux nouveaux développements et technologies et pour le rendre compatible avec d'autres systèmes existants. Les utilisateurs sont illimités et fonctionnent sans licence. Les organisations ne paient donc que pour l'installation et la personnalisation. Les données existantes sur les incidents peuvent être importées dans le système lors de l'installation.	La connexion de la liste des utilisateurs avec le répertoire actif de l'organisation devrait être développée, mais les utilisateurs peuvent être créés un par un et accéder aux informations accordées au cours du processus. Le logiciel original a été conçu pour partager largement les informations rapportées. Bien qu'il soit possible d'avoir un profil utilisateur 'reporter uniquement', la limitation de l'accès à l'information doit être soigneusement planifiée.

RIMS

Le service de gestion des incidents de la Risk Management Society (RIMS) offre un système simple et facile à utiliser qui utilise principalement des descriptions d'incidents basées sur des tests. Il permet aux catégories personnalisées de coder les aspects des événements. Il est possible de créer des graphiques. La plate-forme existe uniquement en anglais.

Dans l'exemple considéré, le système était principalement utilisé par le département RH autour des assurances. L'utilisation du système pour l'analyse des incidents de sécurité était limitée. Il n'a donc pas été possible de déterminer si ce système aurait pu fonctionner correctement s'il avait été entièrement configuré pour répondre aux besoins de gestion de l'information issue des incidents de sécurité, au-delà des descriptions d'incidents basées sur les tests et en particulier des analyses.

AVANTAGES	LIMITES
Facile à utiliser. Le personnel peut utiliser le système pour signaler des incidents sans beaucoup de formation. Il est facile de configurer des champs personnalisés et de naviguer sur le site. C'est un système facile et très accessible pour stocker les descriptions d'incidents de sécurité.	L'exemple examiné utilisait principalement des descriptions d'événements basées sur du texte. Le système n'envoie pas de rappels.

OUTIL 12 : ANALYSE ET COMPARAISON DES TENDANCES DES DONNEES

Conseils lors de la comparaison des données de tendances d'organisation avec des données d'incident de sécurité plus larges.

Questions clés et considérations

- Quelles sont les similitudes et les différences dans les tendances entre votre organisation et celles qui apparaissent dans les données regroupées ?
- Pourquoi y a-t-il des similitudes et des différences ? Réfléchissez à chaque aspect observé séparément et demandez :
  - Pourquoi vois-je des similitudes ou des différences dans cette sous--catégorie de types d'incidents ?
  - Est-ce dû à l'environnement externe général ?
  - Comment ces tendances sont-elles affectées par les pays dans lesquels votre organisation travaille ou les programmes mis en œuvre par votre organisation ?
  - Est-ce que l'une ou l'autre des différences pourrait être le résultat de pratiques de signalement (les vôtres ou celles d'autres organisations) ?
  - Où votre organisation a-t-elle plus d'incidents d'un type particulier ?
  - Où votre organisation a-t-elle moins d'incidents d'un type particulier ?
- Rechercher des similitudes dans les tendances et essayer de donner une explication des similitudes.
- Regardez les différences. Essayez de suggérer une explication pour les différences.
- Assurez-vous d'être précis. Si vous êtes sûr qu'un élément est un fait, dites-le. Si vous le pensez mais n'avez pas de preuve, utilisez des termes comme « les données suggèrent », ou «il apparaît à partir des informations disponibles ».
- Identifier les tendances clés :
  - Quelles tendances clés peuvent être repérées ?
  - Les données suggèrent-elles des tendances émergentes dont les organisations doivent tenir compte ?
- Décrivez les tendances aussi spécifiques que possible.
  - Ces tendances sont-elles mondiales ?
  - Y a-t-il des tendances dans un pays spécifique ?
  - À quelle catégorie d'événements de sécurité se réfèrent-ils ?
  - Soyez aussi précis que possible en nommant les types d'incidents que vous voyez augmenter et où cela peut se produire. Si vous le pouvez, fournissez des détails sur qui ou quoi peut être particulièrement affecté.

- Réfléchissez aux tendances générales du contexte global de l'aide telles qu'elles apparaissent dans l'analyse des tendances ou qu'elles soient visibles dans les données au niveau mondial ou national. Essayez de décrire le contexte général de la distribution de l'aide, les changements récents, les menaces ou tendances émergentes.
- Pensez aux différences de tendances entre les données de votre organisation et celles des autres organisations (à l'exclusion de celles qui résultent des différences de signalement). Tenez compte des pays dans lesquels votre organisation travaille, des programmes offerts par votre organisation et des faiblesses ou points forts du cadre de gestion des risques de sécurité de votre organisation.
- Si vous le faites une seconde ou une troisième fois, pensez aux différences entre les données les plus récentes et les analyses précédentes. Décrivez les changements et suggérez des explications.
- Identifier les mesures à prendre :
  - Y a-t-il des questions émergentes de l'examen des données que vous pourriez suivre ?
  - Qui peut vous aider à en savoir plus ?
- Contactez le pays / bureau régional / fournisseur de services d'information avec des questions afin d'obtenir un aperçu de la réalité derrière les tendances de données.
- Pensez à ce que vous mettrez en œuvre dans votre plan d'action au cours des prochaines semaines / mois.

Développer un plan d'action

- Les données suggèrent-elles que le point focal de sécurité devrait prendre des mesures spécifiques ?
- Les données suggèrent-elles que de nouveaux risques émergents ou des situations d'escalade devraient être ajoutés aux formulaires de consentement éclairé à discuter avec le personnel ?
- Les données suggèrent-elles qu'un type d'événement particulier devrait être mis en évidence lors de la formation pour un contexte spécifique ?
- Les données mettent-elles en évidence les risques spécifiques qui devraient être discutés plus en détail avec les PFS nationaux et régionaux pour voir si des changements de politique sont nécessaires ?
- Les données mettent-elles en évidence les problèmes qui doivent être portés à l'attention de la hiérarchie dans l'organisation ?
- Votre analyse des données suggère-t-elle que votre organisation a besoin d'améliorations dans la gestion de l'information issue des incidents de sécurité à un certain niveau au sein de l'organisation ?

Problèmes éventuels à signaler aux collègues, que ce soit sur le terrain ou au niveau de la direction ou du conseil d'administration

- Nommez des tendances spécifiques qui devraient être surveillées de près. Suggérez-leur de les mettre régulièrement à l'ordre du jour.
- Mettre en évidence un risque particulier et spécifique et suggérer une discussion interne sur le seuil de risque acceptable pour un type particulier d'événement dans un contexte particulier pour aider à formuler une politique claire.

- Suggérer des activités spécifiques pour améliorer la gestion de l'information issue des incidents de sécurité afin d'améliorer la capacité de l'organisation à repérer les tendances et à demander la mise en œuvre d'éléments spécifiques (voir la grille d'évaluation pour un élément spécifique pouvant être amélioré).

Communiquez vos conclusions finales et votre plan d'action

Rédigez un document concis et clair qui :

- Mentionne les sources et les méthodes utilisées.
- Indique que vous avez pris en compte les données et que vous avez confiance dans vos résultats (vous pouvez inclure le fait que vous avez ignoré d'approfondir un aspect spécifique parce que vous pensez que c'est le résultat d'un biais de compte rendu).
- Dressez une liste claire des tendances qui vous préoccupent. Choisissez un maximum de trois. Si c'est un exercice régulier, incluez les tendances clés de l'analyse passée.
- Répertoriez l'action que vous recommandez :
  - Pour vous-même en précisant ce que vous avez fait, vous êtes en train de le faire ou que vous allez faire.
  - Au cours des prochains mois pour répondre aux besoins identifiés :
  - Pour d'autres collègues (sur le terrain ou la hiérarchie). Gardez ceux pour les autres à une seule tâche en suggérant comment vous allez faciliter le processus et ce que vous aurez besoin d'eux comme leur apport, de soutien.

Comparez vos données avec les données regroupées par Insecurity Insight via la base de données SiND d'Aid in Danger en utilisant l'analyse des tendances publiée ou en vous rendant à Humanitarian Data Exchange, en plus de vos données d'incidents de sécurité passés.

Voir un exemple de rapport d'analyse de données de tendance multi-organisations ici.

OUTIL 13 : QUESTIONS DE NIVEAU STRATÉGIQUE POUR LES DÉCISIONS RELATIVES À LA GESTION DE L'INFORMATION ISSUE DES INCIDENTS

Après une bonne vue d'ensemble du type d'incident de sécurité survenu, examinez les données et déterminez si elles indiquent une action de suivi requise. Recherchez des informations supplémentaires et mettez fin au rapport d'incident de sécurité avec des recommandations spécifiques.

La liste de questions suivante peut aider les points focaux de sécurité à élaborer des conclusions stratégiques et des recommandations d'action supplémentaires à la suite d'une bonne analyse des événements de sécurité.

QUESTIONS À PRENDRE EN COMPTE LORS DE L'ANALYSE DES DONNÉES D'INCIDENT DE SÉCURITÉ ANALYSÉES	ACTION DE SUIVI POSSIBLE	POSSIBLE RECOMMANDATION D'ACTION À RAJOUTER À LA FIN DU RAPPORT D'ANALYSE
1. Quels types d'incidents de sécurité le personnel et l'organisation ont-ils rencontrés? 2. Dans quels pays sont-ils apparus ?		
Notre organisation prépare-t-elle adéquatement le personnel au type d'événements possibles qu'il peut rencontrer ?	Identifiez dans quelle mesure les personnes ont été bien préparées pour les types d'événements qui se produisent. Identifiez le coût des formations pertinentes et ajoutez une estimation budgétaire.	Suggérer le besoin de formations spécifiques ou de sensibilisation pour le personnel travaillant dans des contextes affectés par des types d'incidents particuliers.
L'assurance couvre-t-elle les réponses requises pour le personnel ou pour faire face aux dommages matériels ?	Renseignez-vous auprès des employés concernés, qu'ils aient reçus ou qu'ils auraient aimé recevoir un soutien psychologique après un incident. Vérifiez si un tel soutien est couvert par l'assurance. Vérifiez à quel point il est facile ou au contraire coûteux de remplacer des objets perdus (assurance ou autre).	Suggérez des lacunes dans la couverture d'assurance. Proposer une stratégie pour faire face à la perte matérielle dans les contextes nationaux où cela semble être un risque accru.

QUESTIONS À PRENDRE EN COMPTE LORS DE L'ANALYSE DES DONNÉES D'INCIDENT DE SÉCURITÉ ANALYSÉES	ACTION DE SUIVI POSSIBLE	POSSIBLE RECOMMANDATION D'ACTION À RAJOUTER À LA FIN DU RAPPORT D'ANALYSE
3. En tant que point focal sécurité du siège, dans quelle mesure êtes-vous satisfait de la façon dont les bureaux de pays semblent avoir utilisé les incidents de sécurité et les incidents évités de justesse pour apprendre et améliorer leurs pratiques ? **4. Quels sont les incidents de sécurité rencontrés par d'autres organisations dans le même pays et comment cela se compare-t-il aux incidents signalés au sein de votre organisation ?**		
Y a-t-il des bureaux pays qui ne déclarent systématiquement pas leur incident au siège ?	Entamer un dialogue avec le personnel clé pour savoir pourquoi aucun ou seulement quelques incidents ont été signalés.	Recommander de revoir les instructions sur comment et quand signaler. Recommander de modifier le système de signalement de manière à encourager les rapports systématiques. Recommander un meilleur support de la part de la direction pour démontrer les avantages d'un débriefing systématique.
Y a-t-il des bureaux pays qui connaissent des types particuliers d'incidents ? Comment ces incidents se comparent-ils à ceux vécus par d'autres organisations ?	Entamer un dialogue avec le personnel clé pour savoir pourquoi des incidents particuliers se produisent fréquemment ou jamais.	
5. Comment les incidents de sécurité ont-ils affecté la fourniture de l'aide ? **6. Peut-on évaluer l'impact des incidents de sécurité sur la fourniture de l'aide ?**		
Vos collègues ont-ils signalé dans quelle mesure les incidents ont perturbé votre travail ?	Entamer un dialogue avec des collègues sur la meilleure façon de décrire l'impact des incidents de sécurité sur la livraison de l'aide.	Rajoutez des déclarations sur la manière dont les incidents de sécurité ont affecté la distribution de l'aide.
Vos collègues ont-ils chiffré la perte de temps et de perte matérielle du personnel ?	Entamer un dialogue avec le personnel sur la meilleure façon de faire perdre du temps au personnel et des biens matériels.	Rajoutez des déclarations sur coûts des incidents de sécurité pour les opérations.
Vos collègues ont-ils signalé dans quelle mesure l'incident de sécurité a affecté l'accès humanitaire?	Entamer un dialogue avec le personnel pour décrire comment la sécurité affecte l'accès aux populations bénéficiaires et combien de personnes pourraient ne pas être atteintes en raison de problèmes de sécurité.	Rajoutez des déclarations sur la façon dont les incidents de sécurité affectent l'accès aux populations bénéficiaires.

QUESTIONS À PRENDRE EN COMPTE LORS DE L'ANALYSE DES DONNÉES D'INCIDENT DE SÉCURITÉ ANALYSÉES	ACTION DE SUIVI POSSIBLE	POSSIBLE RECOMMANDATION D'ACTION À RAJOUTER À LA FIN DU RAPPORT D'ANALYSE
7. Quels étaient les principaux contextes d'incidents de sécurité ? **8. Le contexte des incidents peut-il être classé et quelle stratégie de réponse peut-être nécessaire ?**		
Combien d'incidents ont pu se produire en raison d'échecs dans une bonne stratégie d'acceptance ? Dans quels domaines y a-t-il eu un échec d'acceptance ? Acteurs non étatiques, autorités, bénéficiaires, personnel, entrepreneurs ou autres ?	Entamer un dialogue au sein de l'organisation sur la meilleure stratégie d'acceptance et comment la mettre en œuvre efficacement.	Nommer la zone ou la population cible pour laquelle une meilleure stratégie d'acceptance doit être développée. Suggérer une meilleure formation à la stratégie d'acceptance pour le personnel se rendant dans un pays spécifique pour traiter avec un acteur spécifique.
Combien d'incidents ont pu se produire parce que le personnel n'a pas respecté les règles ou les règlements ou s'est comporté de manière irresponsable ?	Entamer un dialogue au sein de l'organisation sur la meilleure façon de promouvoir le code de conduite éthique pour le personnel et assurer le respect des procédures de sécurité.	Énumérer les aspects de comportement qui pourraient être inclus dans un code de conduite personnel est tenu d'adhérer. Énumérer les domaines de comportement où le personnel ne respecte pas les règles et suggère un mécanisme pour mieux les appliquer.
Combien d'incidents ont pu se produire en raison de facteurs personnels liés à l'origine, aux antécédents ou aux liens familiaux du membre du personnel ?	Rechercher des conversations au sein de l'organisation sur la façon de traiter les facteurs de risque liés à la vie domestique, l'origine ethnique ou d'autres facteurs privés.	Dressez la liste des contextes et des pays où des politiques et procédures spécifiques peuvent être nécessaires, notamment : • Comment répondre si un membre du personnel est affecté par la violence domestique • Comment réagir lorsqu'il y a un risque de discrimination ethnique ou de violence • Quel code de conduite éthique à attendre du personnel local lorsque les intérêts commerciaux ou politiques de la famille élargie pourraient affecter le personnel.

QUESTIONS À PRENDRE EN COMPTE LORS DE L'ANALYSE DES DONNÉES D'INCIDENT DE SÉCURITÉ ANALYSÉES	ACTION DE SUIVI POSSIBLE	POSSIBLE RECOMMANDATION D'ACTION À RAJOUTER À LA FIN DU RAPPORT D'ANALYSE
7. Quels étaient les principaux contextes d'incidents de sécurité ? **8. Le contexte des incidents peut-il être classé et quelle stratégie de réponse peut-être nécessaire ?**		
Combien d'incidents sont survenus parce que le personnel ou l'organisation se trouvait au mauvais endroit au mauvais moment ?	Entamer un dialogue au sein de l'organisation dans quelle mesure est-elle prête à accepter les risques généraux liés au terrorisme, à la criminalité ou à d'autres incidents qui ne ciblent pas spécifiquement l'organisation.	Dresser la liste des pays présentant un risque accru d'incidents échappant au contrôle des meilleures politiques de sécurité.
Combien d'incidents sont survenus en raison de l'action des acteurs étatiques ?	Identifier les acteurs étatiques responsables dans les documents internes et essayer d'identifier des pistes pour rechercher un dialogue avec ces acteurs étatiques. Parlez à vos collègues de plaidoyer et envisagez de développer une campagne conjointe avec d'autres ONG pour sensibiliser le public.	Suggérer des voies possibles pour les conversations à suivre par les représentants des pays ou la direction en utilisant les canaux diplomatiques ou le soutien d'autres organisations (par exemple le CICR). Identifier les domaines dans lesquels une organisation pourrait envisager une campagne de plaidoyer avec d'autres, comme le bombardement d'infrastructures ou l'impunité des poursuites.
9. Pouvons-nous utiliser les données pour identifier un seuil de risque que notre organisation est prête à accepter ?		
Quels types de décisions ont été prises pendant la période analysée pour donner une indication du seuil de risque que l'organisation est prête à prendre ?	Pensez de façon critique à votre propre prise de décision concernant les risques de sécurité. Quels sont les principes et les seuils sur lesquels vous vous basez ? Entamez un dialogue avec d'autres membres du personnel de l'organisation et déterminez si vous utilisez les mêmes principes et seuils.	Recommander l'élaboration d'un seuil de risque clairement défini à communiquer au personnel.
Dans quelle mesure cette prise de décision était-elle cohérente entre différents contextes ?		
Y a-t-il une relation entre les incidents de sécurité signalés et les décisions spécifiques prises ?		

Références et Bibliographies

ATHA. (2016). « Projet : Protection de l'action humanitaire », *ATHA*. Disponible sur : http://www.atha.se/policy-project-protection-of-aid-workers

Ayre, R. (2010). *Le défi de la gestion de l'information : un exposé sur la sécurité de l'information pour les organisations humanitaires non gouvernementales sur le terrain*. EISF. Disponible sur : https://www.eisf.eu/wp-content/uploads/2014/09/0119-Ayre-EISF-2010-The-Information-Management-Challenge-A-Briefing-on-Information-Security-for-Humanitarian-Non-Governmental-Organisations-in-the-Field.pdf

Bickley, S. (2017). *Gestion des risques de sécurité : un guide de base pour les petites ONG*. EISF. Disponible sur : https://www.eisf.eu/library/security-risk-management-a-basic-guide-for-smaller-ngos/

Buth, P. (2010). *Gestion de crise des incidents critiques*. EISF. Disponible sur : https://www.eisf.eu/wp-content/uploads/2014/09/0121-Buth-2010-Crisis-Management-of-Critical-incident-2010.pdf

Davidson, S. (2013). *Gérer le message: Gestion de la communication et des médias en cas de crise de sécurité*. EISF. Disponible sur : https://www.eisf.eu/library/gerer-le-message/

Davis, J. et al. (2017). *Sécurité : Boîte de gestion des risques pour les organisations d'aide humanitaire. 2e édition*. EISF. Disponible sur : https://www.eisf.eu/wp-content/uploads/2017/03/2124-EISF-2017-Security-to-go_a-risk-management-toolkit-for-humanitarian-aid-agencies-2nd-edition.pdf

De Palacios, G. (2017). 'Gestion de l'information liée à la sécurité: un examen plus approfondi des systèmes de signalement des incidents', *EISF*.

Dick, A. (2010). *Création d'une terminologie commune de sécurité pour les ONG* : une étude comparative. Initiative de gestion de la sécurité. Disponible sur : https://www.eisf.eu/wp-content/uploads/2014/09/0647-Dick-2010-Creating-Common-NGO-Security-Terminology-A-Comparative-Study.pdf

Earth Point. (inconnu). « Excel vers KML - Afficher les fichiers Excel sur Google Earth », *Earth Point*. Disponible sur : https://www.earthpoint.us/ExcelToKml.aspx

Hoelscher, K., Miklian, J. and H. M. Nygård. (2015). *Comprendre les attaques contre les travailleurs humanitaires*. Peace Research Institute Oslo (PRIO) Conflict Trends. Disponible sur : http://file.prio.no/publication_files/prio/Hoelscher,%20Miklian,%20Nyg%C3%A5rd%20-%20Understanding%20Attacks%20on%20Humanitarian%20Aid%20Workers,%20Conflict%20Trends%206-2015.pdf

ICRC. (2011). *Une étude sur seize pays : les soins de santé en danger*. ICRC. Disponible sur : https://www.icrc.org/eng/assets/files/reports/report-hcid-16-country-study-2011-08-10.pdf?__hstc=163349155.76b9edd98545ef10cf2630f8704dd68b.1500037719517.1500037719517.1500838137193.2&__hssc=163349155.2.1500838137193&__hsfp=520750989

InterAction. (2010). *Guide étape par étape d'InterAction sur la lutte contre l'exploitation et les abus sexuels. Interaction*. InterAction. Disponible sur : https://www.interaction.org/sites/default/files/2010.6%20-%20Step%20by%20Step%20Guide%20-%20Comments%20Version.pdf

Inter-Agency Standing Committee (IASC). (2008). *Orientations opérationnelles sur les responsabilités des chefs de groupe / secteur et OCHA dans la gestion de l'information*. WHO. Disponible sur : http://www.who.int/hac/network/global_health_cluster/iasc_operational_guidance_on_information_management_v3.pdf

Inter-Agency Standing Committee (IASC). (2015). *«Saving Lives Together – Un cadre pour améliorer les accords de sécurité entre les organisations intergouvernementales, les ONG et les Nations Unies sur le terrain, (octobre 2015)»*, *IASC*. Disponible sur : https://interagencystandingcommittee.org/collaborative-approaches-field-security/content/saving-lives-together-framework-improving-security-0

Inter-Agency Standing Committee (IASC). (2015). *Lignes directrices pour l'intégration des interventions de lutte contre la violence sexiste dans l'action humanitaire: Réduire les risques, promouvoir la résilience et favoriser le relèvement*. Disponible sur : http://www.europarl.europa.eu/meetdocs/2014_2019/documents/femm/dv/gbv_toolkit_book_01_20_2015_/gbv_toolkit_book_01_20_2015_en.pdf

Inter-Agency Standing Committee (IASC). (2016). *Protection contre l'exploitation et l'abus sexuels (PEAS) Coopération inter-agences dans les mécanismes de plainte basés sur la communauté: Procédures mondiales d'exploitation normalisées*. IASC. Disponible sur : http://reliefweb.int/report/world/protection-sexual-exploitation-and-abuse-psea-inter-agency-cooperation-community-based

International Organization for Standardization (ISO). (2009). ISO 31000:2009 : Gestion des risques – Principes et lignes directrices.

International Organization for Standardization (ISO). (2014). ISO/IEC 27000:2014 : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Vue d'ensemble et vocabulaire.

Irish Aid. (2013). *Lignes directrices de l'aide irlandaise pour la gestion des risques professionnels en matière de sécurité et de sûreté des ONG*. ALNAP. Disponible sur : http://www.alnap.org/resource/11229

Kemp, E. and Merkelbach, M. (2011). «Pouvez-vous être poursuivi? Responsabilité juridique des organisations internationales d'aide humanitaire envers leur personnel », *Initiative de gestion de la sécurité*. Disoinible sur : https://www.eisf.eu/library/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/

Kemp, E. and Merkelbach, M. (2016). « Devoir de protection : un examen de la décision Dennis / Norwegian Refugee Council et de ses implications », *EISF*. Disponible sur : https://www.eisf.eu/ library/duty-of-care-a-review-of-the-dennis-v-norwegian-refugee-council-ruling-and-its-implications/

Lieberman, A. (2017). « L'OMS se prépare à lancer une base de données en ligne pour suivre les attaques des agents de santé », *Devex*. Disponible sur : https://www.devex.com/news/who-readies-to-launch-online-database-tracking-health-worker-attacks-90331#.WWYjVPrtmqh.twitter

Martinsson, J. (2010). « Leçons importantes sur la campagne contre les mines », *The World Bank*. Disponible sur : https://blogs.worldbank.org/publicsphere/important-lessons-landmine-s-campaign%20

Merkelbach, M. (2017). *Directives volontaires sur le devoir de protection envers le personnel civil détaché*. Département fédéral des affaires étrangères (DFAE), Unité de stabilisation (US) et Centre des opérations internationales de paix (ZIF). Disponible sur : http://www.zif-berlin.org/fileadmin/uploads/experten-einsaetze/Voluntary_Guidelines_on_the_Duty_of_Care_to_Seconded_Civilian_Personnel_Final_170420.pdf

Nobert, M. (2016). *Liste de contrôle pour la prévention, les politiques et les procédures: Répondre à la violence sexuelle dans les contextes humanitaires et de développement*. Signaler l'abus. Disponible sur : http://www.reporttheabuse.org/take-action/preventing-sexual-violence/

Nobert, M. (2017). « Pourquoi devrions-nous nous attaquer à la violence sexuelle dans les lieux de travail humanitaires? », *EISF*. Disponible sur : https://www.eisf.eu/news/why-should-we-address-sexual-violence-in-humanitarian-workplaces/

OMS. (2017). *Attaques sur les sites Web de soins de santé*. Disponible sur : http://www.who.int/emergencies/attacks-on-health-care/en/

Parlov, A. (1995). « Vers une interdiction mondiale des mines terrestres », *Revue internationale de la Croix-Rouge. Disponible sur* : https://www.icrc.org/eng/resources/documents/article/other/57jmmj.htm

Persaud, C. (2012). *Genre et sécurité: Lignes directrices pour l'intégration du genre dans la gestion des risques de sécurité*. EISF. Disponible sur : https://www.eisf.eu/wp-content/uploads/2014/09/1137-Persaud-2012-Gender-and-Security-Guidelines-for-Mainstreaming-Gender-in-Security-Risk-Management.pdf

RedR UK and EISF. (2016). *Rapport: Inclusion et sécurité des travailleurs humanitaires LGBTI*. RedR Royaume-Uni. Disponible sur : https://www.eisf.eu/wp-content/uploads/2016/08/2091-RedR-and-EISF-2016-REPORT-INCLUSION-AND-SECURITY-OF-LGBTI-AID-WORKERS-WORKSHOP-22-01-2016.pdf

Safeguarding Health in Conflict Coalition. (2017). *Arrêt de l'impunité : les attaques dans le secteur de la santé dans 23 pays en conflit en 2016*. Disponible sur : https://www.safeguardinghealth.org/sites/shcc/files/SHCC2017final.pdf

Saving Lives Together. (2016). « Lignes directrices pour la mise en œuvre du cadre « Saving Lives Together », *Saving Lives Together*. July 2016. Disponible sur : https://www.eisf.eu/library/guidelines-for-the-implementation-of-the-saving-lives-together-framework/

Schafer, J. and Murphy, P. (2010). *Collaboration en matière de sécurité: Guide des meilleures pratiques*. InterAction Security Unité de Sécurité – InterAction. Disponible sur : https://acceptanceresearch.files.wordpress.com/2010/10/interaction_security-collaboration-best-practices-guide-201111.pdf

Nations Unies. (2016). « Le Conseil de sécurité adopte la résolution 2286 (2016), condamnant fermement les attaques contre les installations médicales et le personnel dans les situations de conflit », *Nations Unies*. Disponible sur : https://www.un.org/press/en/2016/sc12347.doc.htm

Armée des États-Unis. (2006). *Manuel de terrain No. 2-22.3. Opérations de collecte d'intelligence humaine*. Disponible sur : https://fas.org/irp/doddir/army/fm2-22-3.pdf

Van Brabant, K. (2001). *HPG Report 9 : Intégrer la gestion organisationnelle de la sûreté et de la sécurité*. Humanitarian Policy Group/ODI. Disponible sur : https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/297.pdf

Van Brabant, K. (2010). *GPR8 – Gestion de la sécurité opérationnelle dans les environnements violents, édition révisée*. Réseau de pratique humanitaire / Overseas Development Institute (ODI). Disponible sur : http://odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf

Wansbrough-Jones, A. and Dixon, M. (2014). « *Saving Lives Together* » *: Un examen des pratiques existantes de coordination de la sécurité des ONG et des Nations Unies sur le terrain*. Boîte à outils de coordination. Disponible sur : http://www.coordinationtoolkit.org/wp-content/uploads/Saving-Lives-Together-Review-of-NGO-and-UN-Security-Coordination-Practices.pdf

WHO, War Trauma Foundation and World Vision International. (2011). *Premiers secours psychologiques: Guide pour les travailleurs de terrain*. OMS. Disponible sur : http://www.who.int/mental_health/publications/guide_field_workers/en/

Wille, C. (2016). « Leçons tirées sur l'industrie aéronautique: Que pouvons-nous apprendre pour la gestion des risques de sécurité humanitaire »?, *EISF*. Disponible sur : https://www.eisf.eu/news/lessons- from-the-aviation-industry-what-can-we-learn-for-humanitarian-security-risk-management/

Williamson, C. (2017). La gestion des personnes dans la sécurité: une boîte à outils de gestion des risques pour les organisations d'aide humanitaire. *EISF*. Disponible sur : https://www.eisf.eu/news/people-management-and-security-risk-management/

INFORMATIONS ADDITIONNELLES

Organisations

RedR UK est une ONG humanitaire internationale qui soutient les acteurs humanitaires à travers le monde par la formation et le soutien technique. Fondée en 1980 en tant que service, RedR est devenue une agence de premier plan dans le renforcement des capacités du secteur, atteignant des dizaines de milliers de professionnels de l'aide humanitaire et des centaines d'organisations. Nous avons une présence internationale avec des bureaux au Royaume-Uni, au Soudan, au Kenya et en Jordanie et offrons une formation aux humanitaires à l'échelle mondiale à partir de ces centres régionaux.

RedR UK est un fournisseur de premier plan de formation et de renforcement des capacités dans le secteur humanitaire, formant plus de 7.000 humanitaires dans plus de 55 pays chaque année. Ayant travaillé au renforcement des capacités humanitaires pendant plus de 35 ans et soutenu des dizaines de milliers d'humanitaires, RedR a développé une expertise qui fait de nous un leader dans l'apprentissage des adultes dans le secteur. Nous possédons de l'expérience dans la prestation de programmes de renforcement des capacités comprenant des formations en face à face, du coaching et du mentorat, des simulations au niveau du bureau et sur le terrain, des déploiements, des consultations à court terme et l'apprentissage en ligne. En plus de nos programmes d'apprentissage de haute qualité, nous avons contribué de manière significative à l'efficacité de l'offre d'apprentissage dans le secteur. L'expérience de RedR UK en matière de livraison et de gestion de programmes innovants de renforcement des capacités humanitaires lui permet d'être bien placée pour gérer le projet de gestion de l'information issue des incidents de sécurité.

Insecurity Insight est un groupe leader d'experts dédiés à la production et à l'analyse de « données sur les personnes en danger », avec une expérience dans le développement de systèmes de surveillance des incidents à la pointe de la technologie pour la communauté humanitaire. Depuis 2009, Insecurity Insight travaille en partenariat avec des organisations humanitaires pour développer un mécanisme de partage et d'analyse d'incidents confidentiels.

European Interagency Security Forum est un réseau indépendant de points focaux de sécurité qui représentent actuellement 85 ONG humanitaires européennes opérant à l'international. L'EISF s'est engagé à améliorer la sécurité des opérations de secours et du personnel. Il vise à accroître l'accès sécurisé des organisations humanitaires aux personnes touchées par des situations d'urgence. La clé de son travail est le développement de la recherche et des outils qui favorisent la sensibilisation, la préparation et les bonnes pratiques. L'EISF facilite les échanges entre les organisations membres et d'autres organismes tels que l'ONU, les donateurs institutionnels, les institutions universitaires et de recherche, le secteur privé et un large éventail d'ONG internationales. La vision de l'EISF est de devenir un point de référence mondial pour la pratique appliquée et la connaissance collective, et la clé de son travail est le développement de la recherche pratique pour la gestion des risques de sécurité dans le secteur humanitaire.

CONTACTS
Pour partager des ressources et en savoir plus sur le projet, veuillez contacter:

RedR UK	Marine Menier: marine.menier@redr.org.uk
Insecurity Insight	Christina Wille: christina.wille@insecurityinsight.org
EISF	Lisa Reilly: eisf-director@eisf.eu