Note Méthodologique : Violence Agressions et Sûreté des Travailleurs

Synthèse structurée de la démarche et des étapes de réalisation de la mission.

Contexte & finalité de la méthodologie

- Tensions, incivilités et agressions possibles en accueil, terrain, milieu administratif.
- Relier prévention des risques, maîtrise opérationnelle et gouvernance dans la culture sécurité.
- Cadre adossé à ISO 45001 (planification, performance) et ISO 31000 (gouvernance des risques).
- Finalité: anticiper, réduire l'exposition, réagir vite, apprendre et améliorer en continu.

Objectifs de la mission

- Établir une politique claire, comprise et partagée.
- Fixer des objectifs de réduction du risque et des critères de succès.
- Mettre en place des procédures adaptées aux contextes d'activité.
- Former et entraîner les équipes à des gestes simples et efficaces.
- Assurer une réponse rapide et coordonnée aux événements.
- Suivre des indicateurs de pilotage et d'efficacité, avec revues périodiques.

> **Point clé :** Revue de direction au moins semestrielle et décision structurante documentée sous 15 jours après incident significatif.

Périmètre / livrables attendus

- Cartographie des menaces et hypothèses de risque (zones sensibles, flux visiteurs, incidents passés).
- Évaluation des risques: matrice de criticité, critères d'acceptabilité, priorisation.
- Dispositif de sûreté intégré: rôles, contrôle d'accès, modalités d'alerte, procédures de repli, seuils d'escalade.
- Référentiels/procédures opérationnelles (accueil, signalement, accompagnement post-événement).
- Plan de déploiement, parcours d'entraînement, supports pédagogiques et simulations.
- Système de pilotage: indicateurs, registre d'événements, comités, revue de direction, audits, mises à jour des consignes.

Démarche méthodologique (étapes)

Étape 1 – Analyse du contexte et cartographie des menaces

- Entretiens, analyse d'incidents, observation des postes, revue des aménagements et flux.
- Livrable: cartographie des menaces et hypothèses de risque partagées.
- Vigilance: sous-déclaration; instaurer un registre d'événements simple et bienveillant.

Étape 2 – Évaluation des risques et hiérarchisation

- Choix de la matrice, critères d'acceptabilité, ateliers pluridisciplinaires.
- Livrable: priorités opérationnelles et justification formalisée.
- Vigilance: ne pas surpondérer l'exceptionnel; révision formelle annuelle.

Étape 3 – Conception du dispositif de sûreté intégré

- Architecture O-H-T: rôles, contrôle d'accès, alertes, repli, conformité.
- Livrables: procédures, seuils d'escalade, plan d'assistance post-événement.
- Vigilance: éviter la sur-technologie; critères simples (délais alerte/intervention).

Étape 4 – Cadre social, coordination et procédures

- Articulation avec dialogue social et politiques existantes.
- Livrables: responsabilités clarifiées, consignes accueil, signalement, accompagnement.
- Vigilance: référentiels courts, visuels sur site, validations d'applicabilité.

Étape 5 – Déploiement, formation et entraînement

- Plan de déploiement, ingénierie pédagogique, exercices réalistes.
- Livrables: équipes entraînées, jalons de progression, évaluation in situ.
- Vigilance: hétérogénéité des pratiques; rappels réguliers et tuteurs internes.

Étape 6 – Pilotage, indicateurs et amélioration continue

- Indicateurs, comités de pilotage, revue de direction, audits internes.
- Livrables: tableau de bord, décisions tracées, retours d'expérience et mises à jour.
- Vigilance: prévenir l'essoufflement post-lancement; seuils d'alerte chiffrés.

Planning / durée / jalons

Jalon	Fréquence / délai	Repère
Comité de pilotage sécurité/sûreté	Trimestriel (minimum)	Repère de gouvernance (page)
Revue de direction	Semestrielle	ISO 45001 – performance/amélioration
Audit interne des procédures sensibles	Annuel	Repère opérationnel (page)
Entraînement des postes exposés	≥ 2 sessions/an; supports MAJ < 30 j après changement majeur	Section Formation (page)
Revue des droits d'accès (zones sensibles)	Trimestrielle	Contrôle d'accès (page)

Décisions post-incident significatif	Documentation < 15 jours	Objectifs/résultats attendus (page)

Rôles & responsabilités (client / consultant)

Client (organisation)

- Fournir les données: incidents, postes, aménagements, flux visiteurs.
- Impliquer l'encadrement, équipes terrain et représentants du personnel.
- Valider critères d'acceptabilité, priorités et procédures applicables.
- Déployer et maintenir les mesures (organisationnelles, humaines, techniques).
- Assurer le pilotage: comités, indicateurs, revues, traçabilité des décisions.

Consultant (accompagnement)

- Conduire entretiens, analyser incidents, observer postes et zones sensibles.
- Animer l'évaluation des risques: matrice, critères, ateliers pluridisciplinaires.
- Concevoir l'architecture de sûreté et rédiger les procédures/consignes clés.
- Concevoir l'ingénierie pédagogique et entraîner aux conduites à tenir.
- Outiller le pilotage: indicateurs, comités, préparation des audits et retours d'expérience.

Prérequis & données nécessaires (inputs)

- Historique d'événements/registre des faits, y compris incidents à faible gravité.
- Plans et aménagements des sites, zones sensibles, dispositifs d'alerte existants.
- Politiques et procédures actuelles (accueil, signalement, gestion de crise).
- Données d'activité: postes isolés, horaires étendus, interactions publiques sensibles.
- Critères/matrice de criticité et éléments de décision documentés.
- Référentiels de contrôle d'accès et registre des droits d'accès (si existants).
- Disponibilités des parties prenantes: encadrement, représentants du personnel, terrain.
- Contraintes réglementaires et RGPD (finalité, proportionnalité, durées de conservation).

Modalités de pilotage & qualité (comités, validations, risques)

- Comité de pilotage trimestriel; revue de direction semestrielle.
- Tableau de bord: exposition, activité, résultats; seuils d'alerte chiffrés.
- Traçabilité: registre d'événements; décisions post-incident documentées < 15 jours.
- Audits internes annuels; revues à froid et retours d'expérience formalisés.
- Révision périodique: cotations risques (au moins annuelle); droits d'accès (trimestrielle).
- Dialogue social et transparence pour la légitimité et l'acceptabilité.
- Risques à surveiller: sous-déclaration, dérive procédurale, essoufflement, sur-technologie.
- Conformité RGPD: finalité, proportionnalité, information, durée de conservation limitée.

Point clé : Prioriser l’utilité prouvée au poste et la lisibilité des consignes; mesurer sur le terrain (délais d’alerte/intervention) et ajuster rapidement.