# Cours : Risques, management et concepts de la SIE

## Introduction

Les attentats du 11 septembre, les menaces de pandémie, les catastrophes majeures, les troubles géopolitiques dans le monde et face au contexte d'accroissement de la menace malveillante et plus spécifiquement de la menace terroriste, font peu à peu prendre conscience à l'entreprise qu'elle doit se soucier de sa sûreté, car elle porte désormais également de lourdes responsabilités en la matière. Ainsi, il est nécessaire que les sites à risques (industriels, tertiaires…etc.) identifient leurs vulnérabilités face à des actes de malveillance.

La sûreté interne d'établissement (SIE) est un nouveau concept dans la pratique du management sécuritaire en Algérie, qui a été mis en place dans les années 1990 par les pouvoirs publics. L'objectif assigné est de préserver les infrastructures, les équipements et le déroulement normal des activités professionnelles sur les lieux de travail contre toute action à portée illégale ou criminelle, faire échec à toute tentative d'injustice, de sabotage, d'agression ou de perturbation destructrice visant les infrastructures. De ce fait, et à la faveur des lois et décrets promulgués et assurant la fonction de sûreté interne des établissements, bon nombre d'entreprises ont choisi de confier la sécurité de leur patrimoine à des sociétés de gardiennage. Cependant, les missions essentielles de la sûreté interne visent surtout les aspects de la prévention, la protection, la défense et, d'une manière générale, la mise en sûreté du patrimoine public, des biens et des personnes qui lui sont liés. Il doit certainement y avoir une grande confusion entre les deux concepts, celui de faire «garder» une entreprise et celui de la «protéger». Il serait alors plus logique de mettre en place des dispositifs adéquats de protection et de défense contre toute tentative ou acte de malveillance qu'il soit d'origine accidentelle ou criminelle. Dans ce cas précis, ce n'est plus le travail d'une équipe de «gardiens» mais plutôt d'agents de protection et de surveillance bien formés, habilités et dotés de «moyens appropriés» et conséquents. On est en sûreté lorsque l'on est à l'abri de toute menace, de tout risque. La sécurité et la sûreté des biens et des personnes est une obligation légale imposée à tout chef d'entreprise.

## 1. Notions de sûreté interne d'établissement

### 1.1. La sûreté interne d'établissement, c'est quoi ?

La sûreté concerne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux actes intentionnels, spontanés ou réfléchis ayant pour but de nuire, ou de porter atteinte dans un but de profit psychique ou/et financier.

Elle correspond à la démarche ainsi qu'aux méthodes et dispositions associées visant à limiter les risques de nature malveillante. Cette volonté de nuire peut donc porter atteinte aux personnes (Pressions, harcèlement, agression, escroquerie, détournement entrainant des pertes de savoir-faire, actes terroristes…), aux biens matériels (Vol, vandalisme, incendie, destruction d'outil de production) ou immatériels (Vol d'informations confidentielles, espionnage économique et industriel, atteintes à l'image).

Selon le décret exécutif n° 96-158 du 16 Dhou El Hidja 1416 correspondant au 4 mai 1996 fixant les conditions d'application des dispositions de sûreté interne d'établissement prévues par l'ordonnance n° 95-24 du 30 Rabie Ethani 1416 correspondant au 25 septembre 1995 relative à la protection du patrimoine public et à la sûreté qui lui sont liées ;

Article 2 : La sureté interne d'établissement est une fonction organique et permanente assurée par des dispositifs et des mesures graduels et adaptés, à visée essentiellement dissuasive et préventive et le cas échéant coercitive.

## 1.2. La malveillance

La malveillance est souvent la manifestation d'une violence « gratuite » par pure volonté de nuire. Elle se manifeste de plusieurs manières au sein d'une installation industrielle. L'acte malveillant peut être réalisé dans l'entreprise par du personnel interne ou externe à celle-ci.

- Une menace interne peut survenir lorsqu'un employé proche d'une entreprise disposant d'un accès autorisé abuse de son accès et qui a un impact négatif sur les informations ou les systèmes critiques de l'organisation. Il n'est pas nécessaire que cette personne soit un employé: des tiers vendeurs, entrepreneurs et partenaires peuvent également constituer une menace. Les risques potentiels de menaces internes sont nombreux, notamment l'installation de logiciels malveillants, la fraude financière, la corruption de données ou le vol d'informations précieuses.

Pour contrer tous ces scénarios possibles, les entreprises doivent mettre en œuvre une solution de protection des intrus avec les actions suivantes:

- ***Détecter les menaces internes :*** *d*écouvrez l'activité des utilisateurs à risque en identifiant les comportements anormaux.
- ***Enquêter sur les incidents :*** *e*nquêter sur les activités des utilisateurs suspects en quelques minutes et non en quelques jours.
- ***Prévenir les incidents :*** réduisez les risques grâce aux notifications et au blocage des utilisateurs en temps réel.
- ***Protéger la confidentialité des utilisateurs*** : anonymiser les données utilisateur pour protéger la confidentialité des employés et des sous-traitants et respecter les réglementations.
- ***Satisfaire à la conformité*** : répondez aux principales exigences de conformité relatives aux menaces internes de manière simplifiée.
- **Menaces externes** : incidents résultant d'activités humaines intentionnelles ou accidentelles externes. Par exemple, les troubles civils, le terrorisme, les activités criminelles, les vols externes, les appareils explosifs improvisés, les attaques armées, les incendies criminels, les entrées non autorisées…etc.

## 1.3 Sûreté en entreprise : que dit la réglementation ?

Le règlement de la sûreté interne comprend l'ensemble des règles, des consignes, des limitations, des indications sur les conduites à tenir face à des circonstances déterminées dont l'application et l'observance sont obligatoires pour les personnels, les visiteurs et les usagers.

Les principaux textes législatifs relatifs à la SIE en Algérie sont :

- Ordonnance n° **95** – **24** du 30 Rabie Ethani 1416 correspondant au 25 septembre 1995 relative à la protection du patrimoine public et à la sécurité des personnes qui lui sont liées**.**
- Décret exécutif n° **93** – **206** du 6 Rabie Ethani 1414 correspondant au 22 septembre 1993 relatif à la prévention et à la surveillance dans les institutions, administrations et organismes publics ainsi que dans les entreprises publiques économiques.
- Décret exécutif n° **93** – **222** du 16 Rabie Ethani 1414 correspondant au 2 octobre 1993 fixant le statut et la rémunération des agents et chefs de groupe de prévention et de sécurité**.**
- Décret exécutif n° **96** – **158** du 16 Dhou El Hidja 1416 correspondant au 4 mai 1996 fixant les conditions d'application des dispositions de sureté interne d'établissement**.**
- Décret exécutif n° **98** – **410** du 18 Chaâbane 1419 correspondant au **7** décembre 1998 portant création, attributions et organisation des bureaux ministériels de la sureté interne d'établissement**,** modifié et complété par le décret exécutif n° **18**–**50** du 12 Joumada El Oula 1439 correspondant au 30 janvier 2018 **.**
- Arrêté du 13 Rabie El Aouel 1423 correspondant au 26 mai 2002 fixant la composition et fonctionnement du bureau ministériel de la sureté interne d'établissement au niveau du ministère de l'enseignement supérieur et de la recherche scientifique**.**

Sur le plan international et contrairement à la sécurité, la **sûreté en entreprise** n'est pas encore normée… mais cela devrait très prochainement changer avec le projet de norme managériale ISO 22342 sur le plan de sûreté (Sécurité et résilience - Sûreté préventive - Lignes directrices pour l'élaboration d'un plan de sûreté destiné à un organisme). Cette norme donne des lignes directrices pour l'implémentation d'un plan de sûreté dont la structure inclut les recommandations pour une architecture de sûreté préventive. Ainsi, le plan de sûreté peut être intégré efficacement dans un système de management existant. L'intégration des processus de management du risque de l'organisme au modèle de plan de sûreté, contribue à une gestion appropriée de la sûreté. Ce plan de sûreté est conçu pour attribuer l'imputabilité et la responsabilité de même pour guider la mise en œuvre des contrôles afin de protéger l'organisme contre les risques de sûreté.

## 2. Le concept en Sûreté et sécurité

Les termes "sûreté" et "sécurité" sont souvent utilisés de manière interchangeable, comme s'ils signifiaient la même chose. Ils font en effet toutes deux références à la protection des biens et des personnes. La notion de sûreté n'est pas aussi précisée que celle de sécurité parce que par nature, son domaine est plus diffus, plus fluctuant, plus évolutif, reposant sur la complexité du comportement humain, mais aussi sur l'affirmation et le respect des libertés publiques fondamentales. Mais la principale différence réside dans l'intentionnalité des menaces. Les actes malveillants intentionnels relèvent de la sûreté alors que les accidents s'apparentent à la sécurité. Par ailleurs, on utilise couramment le terme de sécurité pour englober les deux concepts.

La confusion entre la sécurité et la sûreté n'est pas sans conséquences sur les choix de solutions pour faire face aux menaces. Cette confusion peut engendrer la mise en œuvre de moyens inefficaces, inadaptés et couteux. Seule la mise en place d'une politique de sécurité qui englobe les problématiques de sécurité et de sûreté apportera une réponse efficace aux risques.

Les différents acteurs du secteur définissent la sûreté comme l'ensemble des activités et mesures prises pour prévenir et lutter contre les risques liés à la malveillance (risques d'origine humaine).

Par opposition, la sécurité couvre quant à elle les mesures visant à circonvenir les risques d'origine accidentelle (risque technologique, biologique, incendie, gaz...) ou chroniques (risque biologique, chimique…). La sûreté est donc liée à la notion d'accident volontaire alors que la sécurité fait référence à des accidents d'origine involontaire. Désormais la conception d'un dispositif global de sécurité du public doit intégrer les notions de sécurité (prévention d'un événement non intentionnel) et de sûreté (prévention d'un acte intentionnel) en prenant soin que les impératifs de l'un ne contrarient pas les obligations de l'autre, tout en recherchant les complémentarités et synergies opérationnelles nécessaires entre eux.

Les concepts de la sûreté comportent notamment : la défense en profondeur, une attitude de prudence et de pessimisme dans l'étude des accidents possibles, un retour d'expérience systématique, des études probabilistes de sûreté. Dans l'ensemble, on constate que les concepts ont nettement évolué depuis les premières études de sûreté. Le domaine de la sûreté n'a acquis sa légitimité et sa maturité actuelle que de façon progressive.

## 3. Le risque en sûreté internes des établissements

Bon nombre d'entreprises ne font pas la différence entre la sécurité qui représente les risques accidentels et la sûreté qui traite des risques découlant d'un acte de malveillance. Il devient primordial et même vital pour ces entreprises d'approcher encore plus cette notion, en vue d'une meilleure appréciation du risque qu'elles encourent, pour mieux y faire face, et aussi pour garantir la compétitivité mais aussi le développement de l'entreprise.

Dans le domaine de la sûreté, la nature du risque est d'origine humaine. Cela sous-entend qu'à tout moment, l'intelligence de celui qui veut nuire entre en jeu. Cette intelligence est à considérer au sens de la capacité à analyser la situation donnée et donc d'une capacité à inventer, à imaginer une nouvelle façon de faire, à contourner, à mettre à défaut des dispositifs existants. La logique de « course » entre attaquants et défenseurs contribue ainsi à l'instabilité du niveau de risque.

L'évolution du contexte a aussi son importance. L'environnement social, économique et/ou politique dans laquelle évolue l'organisation peut modifier le risque (terrorisme, vol, vandalisme, sabotage…). Par exemple une société, où règnent des conflits sociaux, est plus sujette à des actes de vandalisme voire de vol qu'une entreprise ou règne un climat de sérénité et de dialogue.

### 3.1. Catégories des menaces en sûreté internes des établissements

Les menaces en sûreté au sens de « manifestations intentionnelles d'un danger » sont traditionnellement réparties en trois catégories de cibles :

**-Intégrité physique et morale des personnes**

Par définition, l'intégrité désigne l'état d'un objet qui est entier, c'est-à-dire n'ayant subi aucune dégradation. Le respect de l'intégrité physique implique le droit à la vie et le droit au respect du corps. Le respect de l'intégrité morale implique le respect de la dignité humaine , le droit à l'honneur, le respect de la vie privée…etc.

L'intégrité est aussi une valeur humaine très appréciée dans la société. En effet, une personne intègre est quelqu'un qui ne se laisse pas corrompre et donc qualifiée de fiable. En effet, au quotidien, les entreprises font face à des problèmes tels que le détournement de leurs clients, les vols et braquages organisés par leurs propres employés ou encore la vente aux concurrents de leurs secrets professionnels. Comment y remédier, donc ? En engageant des collaborateurs intègres.

**-Atteinte aux biens matériels,**

**Le vol** : est le fait de prendre, sans autorisation, un bien ou une chose appartenant à une personne. L'auteur conscience de l'acte commis, car Il agit dans le but de s'enlever la chose d'autrui.

**Le vandalisme** est le fait de porter atteinte volontairement aux biens privés ou publics sans motif légitime.

**L'abus de confiance** est le fait pour une personne, à qui a été remis de l'argent ou un bien, de détourner l'usage de ce bien à son profit ou pour un usage frauduleux. Ce bien peut être une somme d'argent, une marchandise, un chèque, un fichier de données.

**L'escroquerie** consiste pour l'escroc à obtenir un bien, un service ou de l'argent par une tromperie (faux nom, manœuvres frauduleuses...

**-Atteinte aux biens immatériels**

D'un point de vue général, le capital immatériel est composé du capital humain (ressources humaines, potentiel de développement et savoir attaché), du capital relationnel (relation durable avec des fournisseurs, clients et partenaires économiques) et du capital structurel. Les principaux actifs immatériels de l'entreprise peuvent être le brevet, la marque (de fabrique, de commerce, de service ou le nom de l'entreprise), la dénomination sociale (le nom officiel donné à la société au moment de son immatriculation : c'est l'élément qui permet de l'identifier et de l'individualiser), le savoir-faire (connaissances techniques industrielles, organisationnelles ou commerciales d'une entreprise et aux procédés ou formules de fabrication), …etc.

## 3.2. Analyse des risques en sûreté interne des établissements

Toute entreprise doit procéder à une analyse de risque pour identifier et prévenir les risques de malveillance en tenant compte des équipements de sûreté existants et des mesures opérationnelles déjà en place, tout en garantissant le niveau de sécurité des installations.

Les principales étapes pour analyser des risques sont les suivantes :

1. Identifier les risques de l'entreprise selon le type d'activité, la faisabilité et les enjeux (vandalisme, vols, fraudes, agressions, cambriolages, employés déloyaux, espionnage industriel, braquages…etc.).
2. Identifier les sources de risques internes.
3. Analyser les mesures de sûreté adoptées et leur efficacité du point de vue humain, organisationnel, technologique et procédural.
4. Élaborer la liste de tous les risques relevés et les conséquences pour l'entreprise.
5. Présenter des scénarios possibles et leur niveau de probabilité.
6. Rédiger la liste de priorité des mesures à entreprendre avec leur niveau d'urgence.

# 4. Système de Management de la Sûreté Interne d'Etablissement (SMSIE)

Le management de la sûreté est un vaste sujet qu'il est toujours nécessaire d'aborder humblement étant donné la diversité, la complexité et l'instabilité qui le caractérisent.

D'un point de vue collectif, la sûreté a pour but de garantir la pérennité de l'entreprise et la protection des collaborateurs. Elle s'inscrit dans le cadre d'une politique de management des risques visant à faire décroître les menaces et les actes de malveillance (intrusions, vols, corruption, terrorisme, fraudes et vols de données, intrusions dans les systèmes d'information, etc.) sont autant de menaces qui peuvent devenir mortelles pour toute entreprise qui sous-estime l'impact de ces attaques.

Un Système de Management de la Sûreté Interne d'Etablissement (SMSIE) est avant toute chose de préparer l'entreprise à faire face à tout incident sécuritaire et à protéger par tous les moyens possibles son patrimoine humain et matériel. Chaque entreprise organise sa sûreté en fonction de son domaine d'activité, de son périmètre géographique opérationnel et aussi de sa culture interne.

## 4.1. Conséquences des menaces

Toute entreprise doit se prémunir des risques de malveillance qui pourraient l'impacter, ainsi que de leurs conséquences qui peuvent être*:*

- des conséquences internes : dues aux pertes humaines, à la perte de l'outil de production ou à celles d'informations capitales à la poursuite des activités, à la dégradation de son image.
- des conséquences externes : dues à la perte de crédibilité auprès de ses clients, à la dégradation de son image, à l'interdiction administrative d'exploiter un site de production à la poursuite judiciaire, etc.

Pour tous ses enjeux majeurs, elle doit s'armer afin de de prévenir efficacement tous ses risques. Elle doit donc pouvoir mettre en place un système de management global. Ce process permet de structurer son organisation afin notamment :

- d'identifier tous les dangers et menaces potentielles pour les biens matériels et immatériel dont la protection du savoir-faire, le personnel, et ses partenaires (clients, fournisseurs…) ;
- d'argumenter le niveau de maitrise suffisant mis en œuvre face à ces dangers/menaces et de viser une amélioration et une adaptation constante du niveau sécurité ;
- de définir l'implication dans le système de management global du personnel à tous les niveaux de l'organisation ;
- de garantir, aux diverses parties prenantes, le fonctionnement efficace d'une organisation structurée permettant une maitrise des risques.

## 4.2. Évaluation de la menace

Pour les auteurs des actes de malveillance, le facteur le plus influent dans le choix de la cible est ce qu'on pourrait appeler la « probabilité de succès ». C'est pour cette raison que les menaces internes présentent toujours un risque plus élevé de nuire que les menaces extérieures.

L'évaluation de la menace a pour objectif d'identifier une menace existante ou émergente avant qu'elle ne se transforme en acte de violence, puis de gérer efficacement le risque potentiel qui en résulte en mettant en œuvre une politique de prévention des risques efficace.

## 4.3. La fonction 'sûreté' dans l'entreprise.

Le directeur sûreté utilise en permanence de la stratégie. Il doit être doté d'une certaine capacité à faire face à l'imprévu. C'est le nouveau domaine de la sûreté globale, sans limite bien définie mais qui va au-delà de la simple conformité aux textes et aux jurisprudences.

Un système de management des risques est la gestion nécessitant des interactions entre plusieurs acteurs de l'entreprise dans le but d'améliorer les performances d'une entreprise et pour cela la sûreté est un levier. Il est nécessaire d'avoir une approche globale, d'anticipation et de prévention des risques professionnels. C'est une démarche qui oblige à anticiper les changements, à augmenter la réactivité et la performance de l'entreprise dans la prévention des risques, de limiter les dysfonctionnements de l'entreprise, d'assurer une cohérence globale avec les autres démarches de management.

Le service sûreté va assurer la prévention et la protection des salariés des entreprises, favoriser et pérenniser les bonnes pratiques, améliorer la motivation et sensibiliser le personnel sur le respect des procédures de travail et donner un moyen de contrôle de la gestion en place. Pour cela, le service sûreté va devoir se donner des objectifs accessibles et mesurables.

## 4.4. Culture de sûreté

La culture de sûreté n'est pas une propriété de chaque individu, mais une caractéristique d'un groupe ou de l'ensemble de l'organisation. Un individu peut, dans son activité, avoir une attitude générale plus ou moins attentive à la sûreté. Mais parler de culture, c'est se référer à des manières de faire et des manières de penser qui sont partagées au sein d'un collectif.

Une culture en sûreté peut se fonder sur les étapes suivantes :

a) En faisant connaître les normes de sûreté pertinentes dans l'organisation;

b) En effectuant une analyse des risques des procédures appliquées;

c) En établissant des règles et procédures appropriées et en observant les prescriptions réglementaires pour maintenir les risques au minimum;

d) En évaluant périodiquement le respect de ces règles et procédures;

e) En formant périodiquement le personnel selon un programme établi afin qu'il applique les règles et les procédures correctement;

f) Par la discussion du programme établi au sein du personnel formé;

g) En mettant périodiquement à jour les programmes de formation et en les coordonnant avec les prescriptions des organismes juridiques et de réglementation, qui vérifieront leur efficacité;

h) En diffusant et en faisant connaître les incidents et accidents effectivement survenus pour en tirer des enseignements et améliorer la culture de sûreté;

i) En demandant au personnel, par le biais d'un système d'incitations, à faire des propositions liées à la sûreté.

Enfin, La culture de sûreté reflète la place que la culture organisationnelle donne à la sûreté dans toutes les décisions, tous les services, tous les métiers, et à tous les niveaux hiérarchiques.

Enfin, on peut synthétiser l'efficacité d'un Système de Management de la Sureté (SMS) par les points essentiels :

- ✓ Réussir son évaluation initiale des risques.
- ✓ Assurer une veille règlementaire en permanence.
- ✓ Trouver une synergie suffisante avec les autres domaines du management.
- ✓ Adopter une démarche projet, la piloter et évaluer régulièrement la démarche.
- ✓ Interagir avec d'autres acteurs internes tels que la direction générale, les partenaires sociaux, le médecin du travail, la direction des ressources humaines et ou financière et si nécessaire des acteurs extérieurs comme la médecine du travail, la Caisse d'Assurance Maladie ; les forces de l'ordre dont la Police et la Gendarmerie Nationale… etc.
- ✓ Renforcer les formations, communiquer régulièrement et savoir motiver le personnel et reconnaitre la contribution de chacun.
- ✓ Choisir des indicateurs pertinents et savoir réagir aux dérives.