ADESS
ASSOCIATION DES EXPERTS
EN SECURITÉ ET SURETÉ

Sécuriser son entreprise
Comment protéger le capital physique intellectuel et industriel

Auteur : Oz ZNAMIROWSKI

Juin 2022

ADESS
ASSOCIATION DES EXPERTS EN SECURITÉ ET SURETÉ

Table des matières

ADESS
ASSOCIATION DES EXPERTS
EN SECURITÉ ET SURETÉ

1.INTRODUCTION

Le développement des nouvelles menaces qui sont liées à la mondialisation et aux nouvelles technologies doivent impulser le surgissement d'un vrai paradigme de la sécurité globale.
Le contexte géopolitique, le développement du terrorisme ont contribué à cela autant que l'explosion du cybercrime et de l'espionnage industriel.

Ce guide a pour objectif de conseiller les organisations dans la protection de leur patrimoine humain, matériel et immatériel.

Le document s'adresse aux Directions Générales, Direction Sécurité Sûreté, DAF, DRH, services techniques, moyens généraux, afin d'implémenter les bonnes pratiques sécurité sûreté dans les processus des entreprises et anticiper la gestion des risques, des crises et des atteintes, agir pour en diminuer ou supprimer les effets, les conséquences.

L'irruption au centre des préoccupations publiques des menaces, des risques anciens et nouveaux (conflits de haute intensité, guerres asymétriques, terrorisme international, cybercrime, catastrophes naturelles, crises sanitaires internationales, crime organisé et réseaux mafieux à l'efficacité renforcée grâce aux nouvelles technologies et à l'effacement progressif des frontières nationales, etc.) nécessitent la mise en œuvre de moyens.

Ce guide comporte des recommandations sur les moyens d'ordre organisationnels, techniques et humains à appréhender afin de planifier une stratégie d'anticipation et de prévention sécurité sûreté pour les entreprises et organisations de toutes tailles.

Nous avons tenté de balayer un maximum d'aspects, peut- être insuffisamment pour certains experts auprès desquels nous nous excusons par avance.

Vous souhaitant une bonne lecture

2.LES GRANDES FONCTIONS DE L'ENTREPRISE ET LEURS LIENS AVEC LA SECURITE ET LA SÛRETE

Les défis s'imposent indistinctement aux directeurs de sécurité sûreté des entreprises : le besoin de légitimité interne, en adaptant son discours à ses interlocuteurs, le besoin d'agilité, en s'adaptant à un environnement mouvant, et le besoin de capital social, en mobilisant des ressources externes à partir de son réseau de relations personnelles.
La capacité de l'entreprise à répondre à ces défis déterminera en grande partie l'efficacité de son dispositif de sécurité et de sûreté.

Fonctions administratives

Direction Générale L'employeur
- Politique de sécurité sûreté
- Obligation de sécurité et de résultat

DRH
- Programme général de formation dont sécurité sûreté
- Réglement intérieur

Direction Administrative et Financière
- Assistance juridique
- Dossier assurance (dont contrat assistance)
- Financement des investissements sécurité sûreté

Fonctions techniques et de soutien

Direction Production
- Protection du process contre la malveillance
- Secrets de fabrication
- Prototypes...

Direction Technique Maintenance Travaux
- Mise en place et maintenance des moyens de protection
- Premier niveau d'intervention sur les moyens de protection
- Maintenance et suivi des installations fixes incendie, etc.

Services et moyens Généraux
- Fonction accueil et parfois service de sécurité
- Propreté, service courrier, parc auto...
- Lien avec la prévention situationnelle

La chaîne logistique

Service Achats

Achats et stockage de produits sensibles (valeur ou danger)

Fiche de Donnée de Sécurité

Achats des produits et services de sécurité sûreté

Service Expéditions

Stockage et expéditions des produits sensibles

Le service de sécurité incendie

Service de sécurité Incendie

Prévention:

Conformité électrique, permis feu (travaux par points chauds), maîtrise du process, comportement humain...

Protection:

Détection, intervention, extinction, compartimentage, désenfumage.

Réglementation applicable:

Code du travail, code de l'envirronnement, code de la construction et de l'habitation, normes.

Documents techniques unifiés

Référentiels techniques APSAD, moyens de secours, installations fixes, dispositions constructives...

Référentiels organisationnels APSAD R6 et R8

Les autres services

Service Informatique
- Cybersécurité
- Accueil et flux des données sûreté

Bureau d'études Service Projets
- Intégration de la prévention dès le stade projet
- "Combattre les risques à la sources" Art L 4121-2 Code du Travail

Fonction « International »
- Risques "Pays"
- Sûreté sécurité des expatriés et missionnaires

Service Communication
- Informations classifiées
- Circuit de notoriété

Les partenaires sociaux

Instances Représentatives du Personnel

Le Comité Social et Economique (CSE) est une instance représentative du personnel qui succède aux anciennes instances représentatives suivantes : délégués du personnel, comité hygiène sécurité et conditions de travail et comité d'entreprise.

les rôles du CSE

D'exprimer les réclamations, individuelles et collectives, des salariés de l'entreprise.

De veiller à l'application des réglementations du travail dans l'entreprise.

De promouvoir la santé, la sécurité sur le lieu de travail.

Il doit être consulté avant toute décision d'aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail et, notamment, avant toute transformation importante des postes de travail.

3.MENER UNE POLITIQUE SECURITE SÛRETE

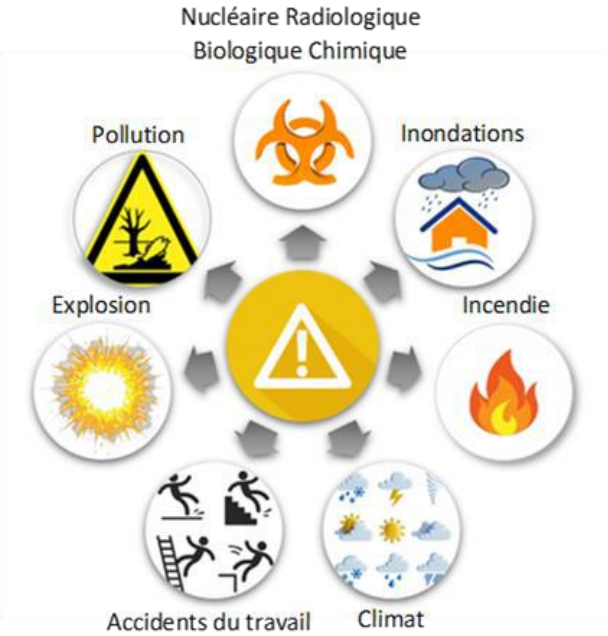
Une politique de sécurité-sûreté est un plan d'action défini pour préserver l'intégrité et la pérennité de l'entreprise. Elle reflète la vision stratégique de la direction de l'organisme :

- ⇨ Définir la doctrine et la politique de sécurité-sûreté
- ⇨ Identifier le cadre de référence de la sécurité-sûreté (chartes, instruction, standards)
- ⇨ Mettre en œuvre la conformité réglementaire et suivre les non-conformités
- ⇨ Gérer les dérogations et les mesures compensatoires (réglementation et doctrine interne)
- ⇨ Piloter un dispositif de veille réglementaire, normatif, technique et organisationnel
- ⇨ Gérer les relations institutionnelles avec les autorités étatiques et locales (DREAL, inspection du travail, commissions de sécurité, référents sûreté, etc.)

Le manque d'anticipation, la défiance, les négligences et la méconnaissance des règles en vigueur ou de leur non-respect peuvent avoir un impact sur le capital humain, matériel et immatériel de l'entreprise.

Atteintes malveillantes Sûreté

Atteintes accidentelles Sécurité



*L'incendie peut être volontaire et entrer dans le périmètre des atteintes malveillantes

Les enjeux résident donc dans :

- Le fait d'assurer la sécurité des personnes
- La protection et la sauvegarde de l'outil de travail
- L'assurance de la continuité d'activités
- Le fait de prévenir les risques inhérents de responsabilité
- Le respect des obligations réglementaires et contractuelles, des règles de l'art

3.1 Assurer la sauvegarde du patrimoine humain, matériel et immatériel des organisations

A la suite d'une analyse ou d'un audit de risques, certaines données sont essentielles à prendre en compte. Elles serviront de "données d'entrée" à la composition du service de surveillance et/ou de télésécurité.

Les principaux éléments analytiques sont les suivants :

- Activité principale : Préciser l'activité principale du site en se servant des classes de risques liées aux marchandises ou à l'activité.
- Environnement : Evaluer tout ce qui entoure le site (isolement, voisinage, milieu urbain…)
- Accessibilité : Préciser les issues principales, les issues secondaires, les accès par destruction des parois et les éventuels accès par des locaux adjacents.
- Présence : Préciser le nombre de personne sur le site (personnel, personne externe) et les habitudes sur le site : présence de travailleur isolé, horaires…
- Les points d'accès sur l'emprise industrielle, l'étude des flux et l'organisation des contrôles d'accès pour les personnels permanents ou temporaires, les visiteurs, les entreprises extérieures, les livraisons et expéditions (dont celles de substances dangereuses) ainsi que les secours ;
- Les scénarios de risques significatifs d'atteinte à des cibles vis-à-vis desquels l'(les) agent(s) de sécurité a(ont) des missions en matière de dissuasion, d'identification d'une situation anormale (dès le stade des signaux faibles), d'analyse et également de réaction

- Le temps de résistance mécanique des couches successives (périphérie, périmétrie, ponctuelle) associé aux délais de détection d'une intrusion et de transmission d'une alarme afin d'équilibrer son "équation de la sûreté"
- Les interactions de la surveillance humaine avec les technologies de détection ou les moyens d'assistance en place tels que la vidéosurveillance, les drones, les robots…
- Les moyens de maîtrise des risques accidentels (dispositifs fixes d'extinction ou de refroidissement, réseau incendie et sources d'énergie de secours par exemple) faisant l'objet d'une surveillance renforcée afin d'assurer la protection physique de ces points névralgiques
- Les périodes de fonctionnement normal (journée, quarts de production…), d'arrêt de l'activité et de chantiers, les situations d'urgence (plan d'opération interne - POI) ou de crise de manière plus générale
- Les modalités de surveillance et d'intervention par les mêmes ressources vis-à-vis des risques incendie et techniques
- Les modalités de contrôle opérationnel des moyens de maîtrise des risques
- Particularité d'exploitation du système : Le mode d'exploitation doit être défini en accord avec le client :

- Les besoins d'accès des utilisateurs
- Les niveaux d'autorisation pour chacun d'eux
- Si le système doit être en surveillance totale ou partielle
- Si, en cas d'intrusion, des moyens doivent être mis en œuvre pour interpeller l'intrus ou une levée de doute audio ou vidéo

Particularités du site :

Analyse des valeurs déclarées par le client et liste des secteurs sensibles :
Pour faire le lien avec la seconde partie de l'analyse il est nécessaire d'établir une liste numérotée, précisant la localisation des différents secteurs sensibles présents sur le site.

Trois Critères liés à chaque secteur sensible

1. Désignation du secteur sensible :

Identifier le(s) secteur(s) sensible(s) et préciser ses dimensions et les localisations (se référencer à un plan).

2. Définition des zones de localisation de valeurs :

Reformuler ce qui pour le client est considéré comme valeur.
Formaliser les zones de localisation de valeur.
Préciser la surface (en m²) couverte par les valeurs à l'intérieur du secteur sensible.

3. Scénarios retenus de pénétration et de circulation :

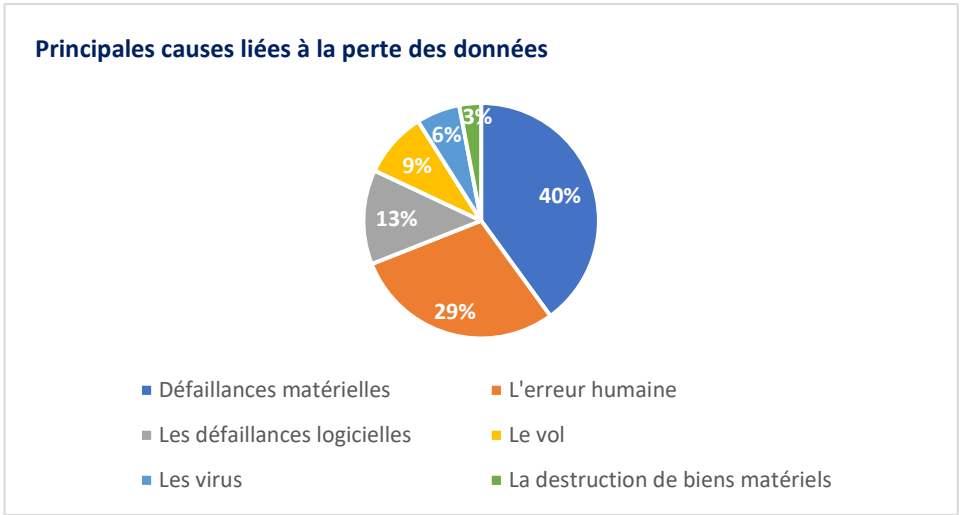
Les scénarios doivent tenir compte au minimum des cheminements permettant l'accès par les chemins normaux aux secteurs sensibles et sont plus ou moins nombreux et complexe en fonction de ceci.
Ils peuvent comprendre des pénétrations via les ouvrants qui seront retenus pour les identifier et associés aux scenarios.

Quelques chiffres

Source CNPP

La France est le troisième pays le plus touché dans l'UE, d'après un baromètre du ransomware publié le lundi 30 mai 2022

Cybermalveillance.gouv.fr-bilan-2021



SSMSI Etat 4001

Service statistique ministériel de la sécurité intérieure

	2021	2020	2019
Menaces ou chantage pour extorsion de fonds	17 210	16 316	16 131
Menaces ou chantage dans un autre but	145 020	126 200	125 175
Cambriolages de locaux industriels, commerciaux ou financiers	55 536	69 833	72 257
Vols à la tire	118 606	120 075	168 056
Vols avec entrée par ruse en tous lieux	8 464	7 254	8 898
Vols simples sur chantiers	12 215	11 625	13 657
Autres vols simples contre les établissements privés et publics	50 261	49 990	65 188
Recels	35 318	37 105	42 735
Incendies volontaires contre des biens publics	5 253	5 224	7 178
Incendies volontaires contre des biens privés	24 708	28 433	32 263
Atteintes à l'environnement	3 702	3 581	3 262
Attentats explosifs contre les biens publics	60	66	55
Attentats explosifs contre les biens privés	233	186	189
Contrefaçons et fraudes industrielles et commerciales	2 744	2 072	2 599
Escroqueries et abus de confiance	317 474	273 304	260 368
Séquestrations	4 798	4 192	4 211

Les chiffres clés officiels de 2020 (édition 2021) des **Services d'incendie et de secours** font état des interventions suivantes, en milieu professionnel :

- **6296** incendies constatés dans des ERP (établissements recevant du public),
- **4275** feux dans des entrepôts et locaux industriels,
- **3525** incendies de locaux artisanaux et agricoles.
  Sans compter les **incendies déclarés dans les bureaux**…
- 4% des accidents sont causés par des actes de malveillance (source **Bureau d'Analyse des Risques et Pollutions Industrielles -BARPI**)
- Selon le "Traité Pratique de Sûreté Malveillance" du **CNPP** :
  77% des accidents liés à la malveillance se caractérise par un incendie.
- 7 entreprises sur 10, c'est le taux d'entreprises ayant fermé définitivement leur porte à la suite d'un incident majeur lié à un incendie (source **Institut National de Recherche et de Sécurité –INRS**)

Le risque incendie en entreprise est souvent lié à 2 facteurs principaux :

1. Le premier concerne généralement un manque d'anticipation, avec un manque d'évaluation des risques, l'absence d'un plan d'évacuation et d'équipements adaptés ou une négligence dans le contrôle des matériels de sécurité.
2. Le second facteur concerne le manque de formation et d'information du personnel. Les consignes sont souvent méconnues, et les sessions de formation et les exercices de mise en situation n'ont pas été organisés comme il se doit.

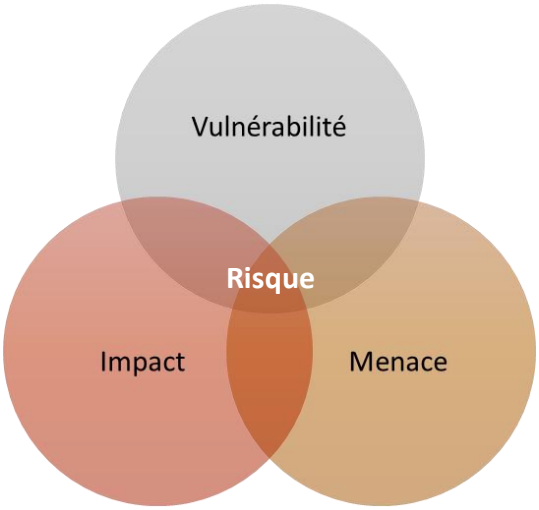
4.ANALYSE ET PREVENTION DE RISQUES

4.1 Qu'est-ce qu'un risque

Un risque est un événement dont la survenance est incertaine, mais qui, en cas de matérialisation, pourra causer des dommages aux personnes physiques ou morales ainsi qu'aux biens matériels ou immatériels (image de marque, informations, etc.).
Un risque qui est peu probable aujourd'hui peut devenir probable demain, très probable après-demain, et certain une semaine plus tard.
Il est primordial de garder en tête que c'est le temps et de nombreux autres facteurs qui vont renforcer la probabilité d'occurrence du risque qui aura été identifié.

4.2 Qu'est-ce qu'une menace

Une menace est quant à elle un risque dont la probabilité de survenance est extrêmement forte du fait des circonstances et/ou des vulnérabilités qui auront été identifiées.



4.3 Prévenir les risques dans une entreprise

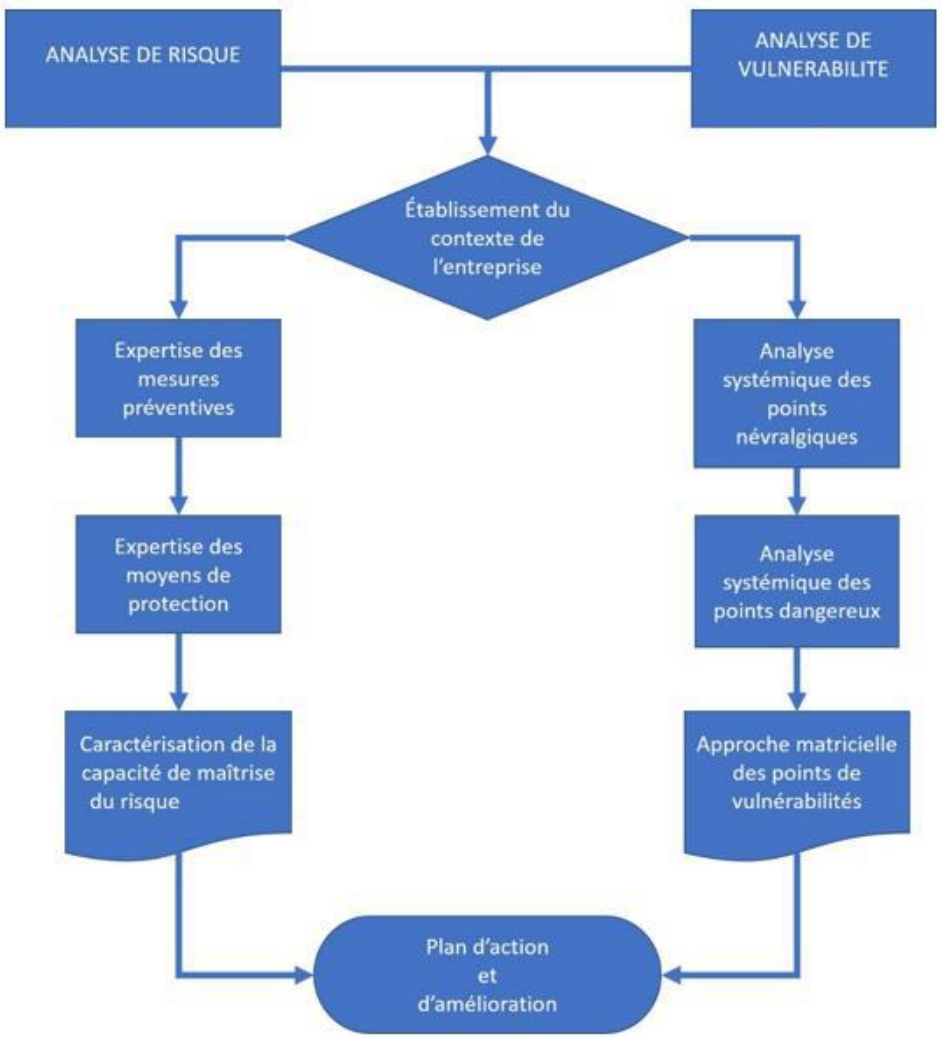
Il existe de nombreux risques que les entreprises peuvent rencontrer.
La maîtrise de ces risques constitue en premier lieu un outil de gestion permettant à l'organisation de concentrer ses ressources sur ses objectifs et enjeux stratégiques.

L'analyse de risques est une démarche dont les conclusions permettent la conception et d'établir un devis.
Pour les cas complexes, il est conseillé de faire réaliser un diagnostic, de rédiger un cahier des charges fonctionnelles et d'obtenir l'accord de l'assureur.

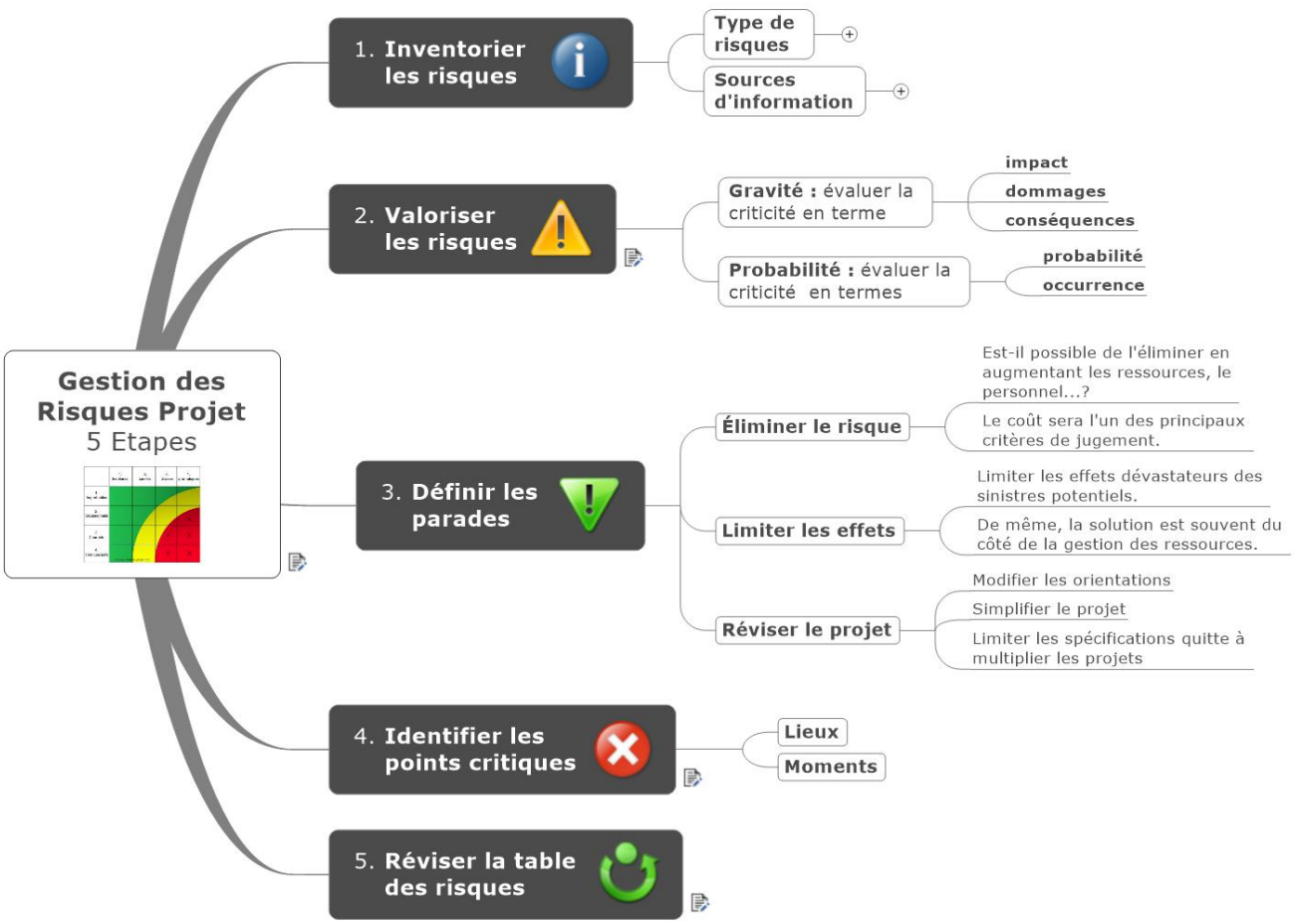
• **L'identification du risque** consiste, compte tenu des éléments recueillis, à déterminer et à élaborer tous les scénarios pouvant conduire à la survenance du risque.

• **L'analyse du risque** a pour objet la qualification des effets non désirés à l'aide d'éléments de référence, des connaissances techniques et des retours d'expérience dont dispose le chargé de sécurité sûreté.
L'analyse doit être effectuée sous un angle systémique liée à l'organisation.

•**L'analyse de vulnérabilité** consiste à déterminer la vulnérabilité vis-à-vis du risque incendie ou des menaces de malveillance en intégrant le résultat de la première étape et en estimant les conséquences sur le fonctionnement du site et sur la pérennité de l'activité.



• **L'évaluation du risque** constitue une appréciation des résultats de l'analyse en comparaison d'une part aux objectifs de l'entreprise, aux obligations réglementaires de l'établissement et aux niveaux de gravité des effets non désirés.
Les scénarios d'incendie ou de malveillance les plus probables compte tenu de l'audit de l'existant permettent ainsi d'estimer les probables conséquences sur la pérennité de l'activité du site et de l'exploitation.



4.4 Les grands principes de la gestion des risques

- ⇨ Identifier les évènements de risques potentiels.
- ⇨ Evaluer en quantifiant l'impact et la survenance de l'évènement de risque.
- ⇨ Gestion des risques : Mise en place de mesures opérationnelles et stratégiques pour éviter et/ou réduire l'impact et la survenance.
- ⇨ Contrôle des risques : Contrôler/Surveiller le niveau des risques, l'application des mesures de gestion.

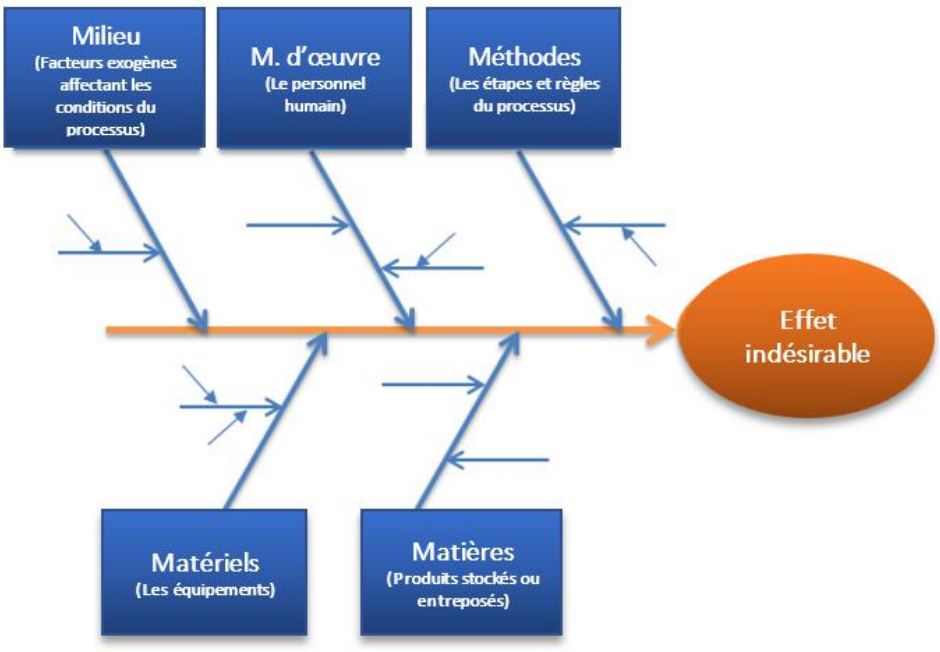
4.5 Les points essentiels pour la mise en œuvre d'un système de management des risques

1- Réaliser une évaluation des risques : identifier les cibles de son entreprise, les scénarios de malveillance et de dangers potentiels.

2- Mise en œuvre des moyens de protections :

- ⇨ Moyens humains (ex. : gardiennage),
- ⇨ Technique (ex : vidéosurveillance, système de sécurité incendie, etc.),
- ⇨ Organisationnels (procédures, information et formation du personnel, exercices d'évacuation ou de confinement, …)

3- Assurer une veille permanente et contrôler régulièrement les moyens de protection mis en place.



La Méthode AMDEC : Analyse des Modes de Défaillance, de leurs Effets, et de leur Criticité

La méthode AMDEC est un outil qualité d'analyse préventive permettant d'identifier et de traiter les causes potentielles de défauts et de défaillance avant qu'ils ne surviennent.

La méthode AMDEC est une méthode rigoureuse de travail très efficace grâce à la mise en commun des informations et données.

Elle est menée en groupe et permet à chaque participant d'y apporter ses propres expériences et connaissances.

La méthode AMDEC se déploie en 4 étapes :

- La préparation
- La décomposition fonctionnelle
- La phase d'analyse
- La mise en place et le suivi des plans d'actions

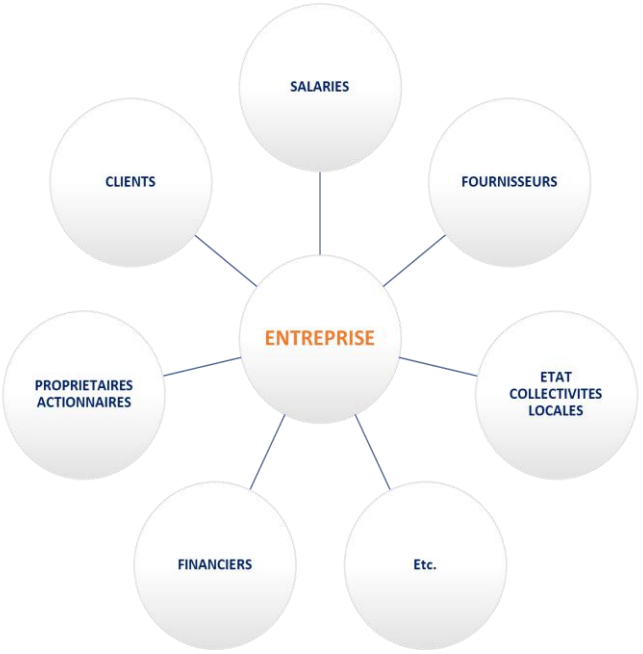
Schéma d'audit

L'étude des sites, des procédures ou d'une situation particulière vont aboutir à l'émission de solutions innovantes qui ramèneront les risques à un niveau acceptable.

5.GESTION DE CRISE ET CONTINUITE D'ACTIVITE

5.1 Qu'est-ce qu'une crise en entreprise

Une crise est une situation d'urgence qui survient brutalement et avec intensité.
Elle a un caractère limité dans la durée mais son impact peut s'étendre dans le temps.
La situation peut aller jusqu'à menacer la pérennité de l'entreprise ou, changer profondément ses façons de faire.
Elle affecte l'entreprise, ses parties prenantes, ses employés, ses clients et ses revenus.
La crise touche l'ensemble de l'entreprise et prend donc plusieurs dimensions qui interagissent en créant une situation complexe.



Une situation de crise implique quatre issues possibles :

1. La disparition d'une partie ou de la totalité de l'entreprise en raison des pertes financières :
⇨ La mauvaise image de l'entreprise demeure après fermeture de l'une de ses agences : altération de la confiance en la marque.
2. L'évolution de l'entreprise vers le haut
⇨ Résilience de l'entreprise : La crise va donner l'opportunité au dirigeant de donner un sens nouveau à son entreprise, prise de conscience de la ou les problématiques.
⇨ Il existe différents types d'innovation :
   - Stratégique, consistant en la création d'un business model.
   - Structurelle, dans le but de modifier l'organisation.
   - Systémique, en modifiant les méthodes et processus.
   - Scientifique, en implémentant les résultats d'avancées scientifiques dans de nouveaux produits.
   - Sociale, afin de faire évoluer la culture d'entreprise.

3. L'évolution de l'entreprise vers le bas
4. Le retour au Statu Quo :

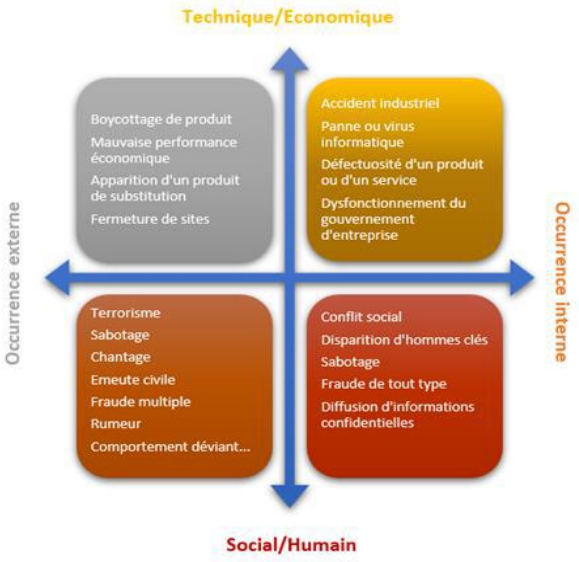
⇨ Auto-persuasion de la capacité de l'entreprise à faire face à toutes les situations.
⇨ Refus de la remise en question de l'organisation et donc des décisions du dirigeant.
⇨ Refus de modifier l'organisation de l'entreprise par manque de visions et en raison de décisions irréversibles qui pourraient exposer l'entreprise à de nouveaux risques.

5.2 Les types de crise

Elles peuvent être d'ordres politique, économique, sanitaire, social, climatique, opérationnel, cyber, réputationnel, etc.

Ou être l'occurrence de circonstances internes ou externes, d'actes volontaires ou involontaires :

⇨ Le décès d'une personne clé de l'entreprise
⇨ La défectuosité d'un produit
⇨ La diffusion d'informations compromettantes
⇨ Un accident industriel
⇨ Un effondrement boursier
⇨ Une catastrophe naturelle
⇨ Pandémie/Sanitaire
⇨ Des conflits internes
⇨ Une attaque informatique
⇨ Une panne informatique
⇨ Terrorisme
⇨ Instabilité politique
⇨ Guerre
⇨ Etc.

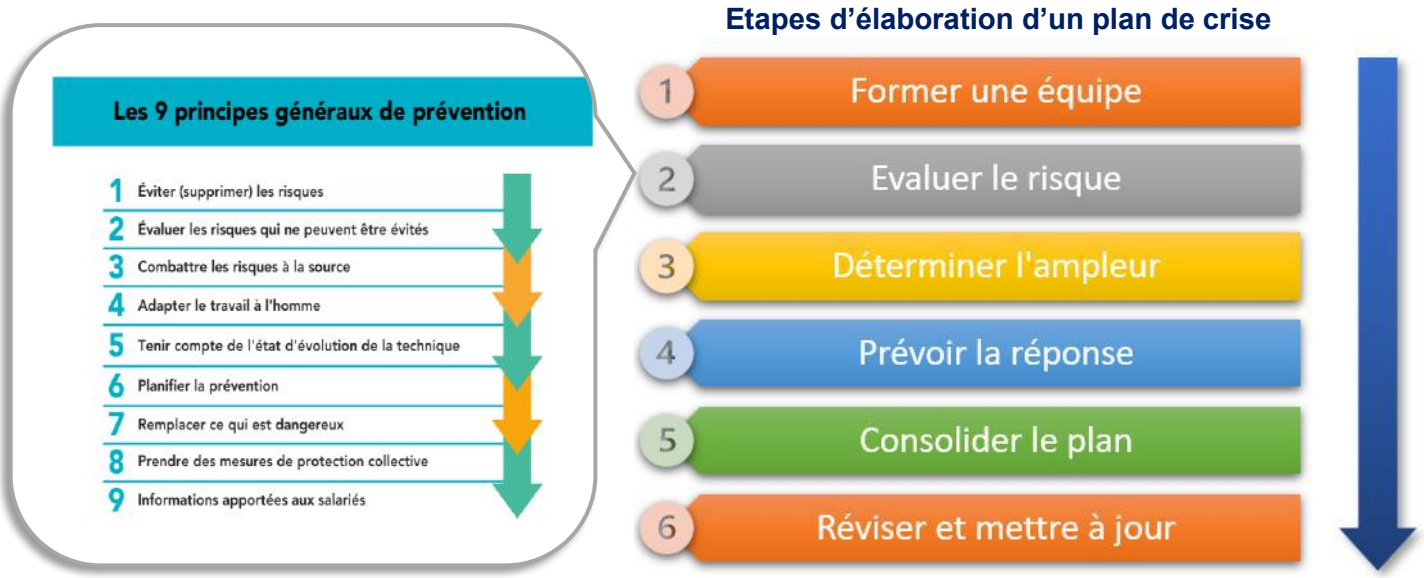


Gérer une crise en entreprise

La gestion de crise se compose à la fois d'une organisation, de techniques et de moyens qui doivent permettre à une entreprise ou une institution de faire face à une situation d'urgence pour maintenir ou augmenter la productivité pendant et après une crise.
Les dirigeants et les responsables des départements clés doivent anticiper une réaction via plusieurs scénarios de crise pour protéger au mieux la structure, ses activités et réduire ses effets nocifs.

5.3 Le plan de gestion de crise

Le plan de crise défini le rôle et la fonction de chacun tout au long d'une crise, afin de réduire les temps d'arrêt, de prendre les mesures adéquates et assurer le plus rapidement possible la résolution des problèmes.
Un plan de crise consiste à élaborer des scénarios de crises et des réponses à celles-ci qui seront implémentés dans les procédures d'urgence de l'entreprise.
Il devra être transmis aux personnes désignées en fonction des responsabilités, testé et évalué régulièrement pour le faire évoluer si besoin.



L.4121-2 du Code du travail

Le plan de gestion de crise doit inclure :

- Les protocoles
- La chaine de responsabilités
- Les contacts
- Les mesures préétablies
- Les outils à disposition
- Les canaux de communication

Fonctions du plan de gestion de crise d'entreprise

- Aide à maintenir une bonne réputation auprès de vos clients, concurrents et leaders du secteur pendant et après une crise.
- Améliore la sécurité, la santé et le bien-être de tous ceux qui travaillent pour l'entreprise et ceux qui collaborent avec elle.
- Il apporte la tranquillité d'esprit en tant qu'employeur et entreprise : être prêt à faire face à toute situation qui se présentera.
- Augmente la productivité pendant et après une crise : chacun connaîtra son rôle et sa fonction tout au long d'une crise, ce qui permettra de réduire les temps d'arrêt, de prendre davantage de mesures et de résoudre plus rapidement les problèmes.

Comment créer un plan de gestion de crise ?

- Identifier les types de crises possibles (crise financière, crise des ressources humaines, crise organisationnelle, crise technologique, crise naturelle, crise épidémiologique, etc.)
- Déterminer l'impact de chaque type de crise sur votre entreprise.
- Réfléchir aux mesures qui devront être prises pour résoudre chaque type de crise.
- Décider qui sera impliqué dans les actions que vous devez prendre dans chaque scénario.
- Élaborer des plans de résolution pour chaque type de crise.
- Former tous ceux qui doivent se familiariser avec vos plans.
- Réexaminer et mettre à jour vos plans régulièrement et si nécessaire.

Liste des tâches d'un plan de gestion de crise

Il y a deux principaux acteurs internes à l'entreprise dans la gestion de crise

- La direction en charge des décisions stratégiques, des grandes directives.
- Les salariés, collaborateurs de l'entreprise qui, à différents niveaux vont proposer et/ou appliquer les décisions opérationnelles.

5.4 La cellule de crise

La composition de la cellule de crise doit être déterminée en amont, dans le plan de crise.
La plupart du temps, les participants sont les membres du personnel, qui peuvent être épaulés par des intervenants externes.

On y trouve généralement :

- Les dirigeants, et éventuellement, les principaux managers de l'entreprise
- Les responsables de la communication (externe, interne et de crise)
- Les responsables des services juridiques et financiers
- Des professionnels externes, le cas échéant (professionnels de la gestion de crise, consultant en communication, avocat, etc.)

Il est important de limiter le nombre de participants à la cellule de crise.
Elle doit appartenir à un groupe restreint et pérenne pour éviter la perte de savoir-faire, les fuites éventuelles ou les disparités de visions.

5.5 Anticiper et gérer une crise

Avant

- ⇨ Créer un plan de gestion des crises
- ⇨ Prévoir et prévenir les risques par la préparation des équipes via des formations et des exercices de simulation.
- ⇨ Être en veille constante de son environnement :
  - La concurrence : que fait-elle ?
  - Les médias : que disent-ils ?
  - Les détracteurs : que pensent-ils ?
  - L'atmosphère politique et sociale : quels sont les enjeux ?
  - L'ambiance au sein de l'entreprise : quels sont les conflits ?

Pendant

- ⇨ Evaluation des risques
  - Impact que la situation pourrait avoir sur l'entreprise, ses employés et ses clients
- ⇨ Décision des actions à mettre en œuvre
- ⇨ Communication entre les parties prenantes
- ⇨ Résolution de la crise, gestion du plan de résolution choisi, des effets immédiats de l'événement et de tout effet nouveau ou aggravant qui pourrait survenir.

L'après

- ⇨ Conditions du retour à la normale des activités de l'entreprise et analyse des effets de la crise.
- ⇨ Rester en contact avec ses salariés, clients ou fournisseurs et rester disponible pour répondre aux questions : Envoyer des mises à jour proactives à ces parties.
- ⇨ Examiner et analyser le plan de gestion de crise et la manière dont il a été mis en œuvre.
  - Comment se sont déroulées les communications de crise ?
  - Votre public a-t-il eu des questions ou des préoccupations auxquelles vous avez négligé de répondre ?

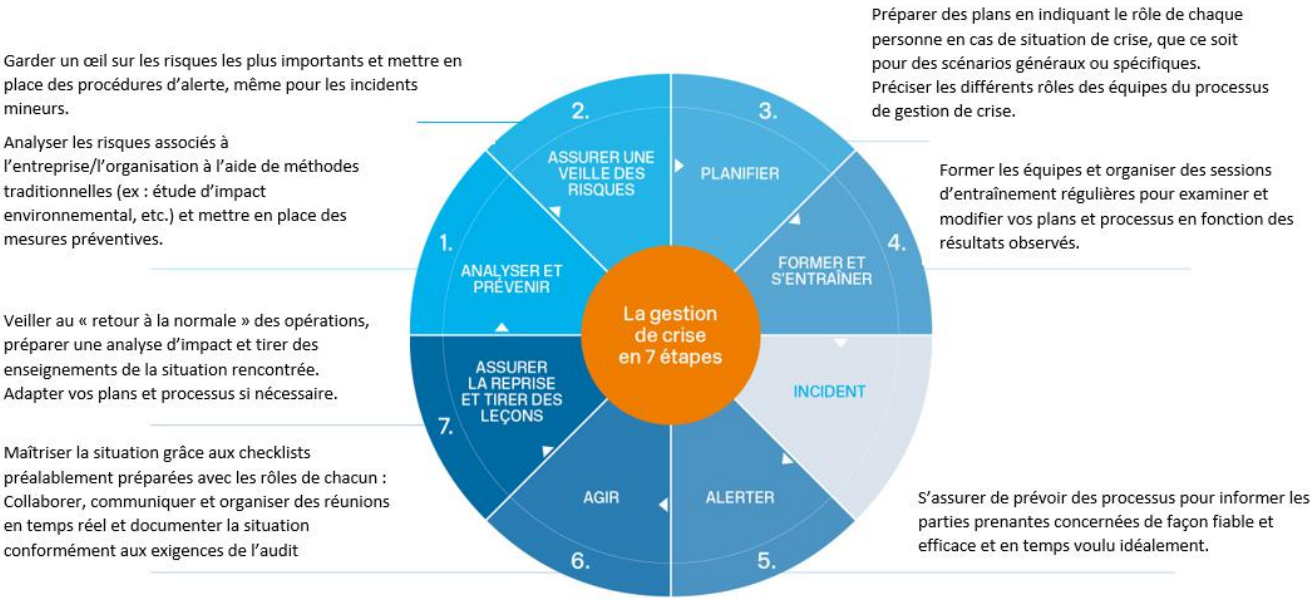
5.6 Bilan d'après crise

« RETEX », le retour d'expérience est un outil managérial précieux.
Après une crise, il est essentiel pour les entreprises et les équipes d'analyser ce qui a émergé durant cette période particulière : difficultés, forces, nouveautés…

Quel objectif ?

Tirer les leçons qui s'imposent pour mieux aller de l'avant, accroitre les connaissances et la résilience.

5.7 La gestion de crise en 7 étapes



6.MISE EN CONFORMITE REGLEMENTAIRE, DOCUMENTAIRE ET ORGANISATIONELLE

6.1 Le document unique d'évaluation des risques professionnels

L'évaluation des risques : votre rôle d'employeur vous impose tout d'abord d'évaluer les situations à risques au sein de l'entreprise, tout particulièrement en cas de présence de produits combustibles.

Cela passe notamment par l'identification des sources possibles d'inflammation (thermique, électrique, mécanique, etc.).

C'est d'ailleurs à partir de ce travail que vous serez en mesure d'éditer et de mettre à jour le document unique d'évaluation des risques professionnels (DUEvRP), servant de base à la mise en place d'actions, de contrôles, de formations et de procédures adaptés.

Le document unique d'évaluation des risques professionnels doit permettre à l'employeur de lister tous les risques liés à son activité de façon exhaustive. Il doit être réalisé en tenant compte de toutes les familles de risques dans lesquelles sont prévues des actions préventives.
En cas d'accident du travail ou de maladie professionnelle, le document unique d'évaluation des risques professionnels doit permettre de démontrer que le risque qui est à l'origine d'un AT (Accident de travail) /MP (Maladie professionnelle) a bien été identifié et qu'une prévention a bien été définie.
Sans cela, la responsabilité de l'employeur sera engagée.

Le DUEvRP devra être conservé pendant (au moins) 40 ans

Dorénavant, le document unique d'évaluation des risques professionnels (DUEvRP), ainsi que ses versions successives, devront être conservés par l'employeur pendant au moins 40 ans et mis à disposition des travailleurs et de toute personne et instance pouvant justifier d'un intérêt à y avoir accès.

Dans ce cadre, il devra faire l'objet d'un dépôt dématérialisé sur un portail numérique administré par un organisme géré par les organisations professionnelles d'employeurs représentatives au niveau national et interprofessionnel.

Ce portail devra impérativement préserver la confidentialité des données contenues dans le DUEvRP : l'accès à ce document sera restreint via une procédure d'authentification sécurisée, ouverte aux seules personnes et instances habilitées à déposer et mettre à jour le document sur le portail, ainsi qu'à celles justifiant d'un intérêt à y avoir accès.

L'obligation de dépôt dématérialisé s'appliquera :

- ⇨ À compter du 1er juillet 2023 pour les entreprises dont l'effectif est supérieur ou égal à 150 salariés ;
- ⇨ Au plus tard à compter du 1er juillet 2024 pour les entreprises de moins de 150 salariés.

Pour finir, l'employeur devra transmettre le DUEvRP au service de prévention et de santé au travail auquel il adhère à chacune de ses mises à jour.

Les risques encourus

1 Inspection du travail

En cas de contrôle, d'accident du travail ou de maladie professionnelle, l'Inspection du Travail vous demandera de démontrer que vous avez bien mis en place toutes les mesures de prévention pour protéger la santé physique et mentale de votre personnel.

Vous devrez également démontrer que vous avez bien répondu à votre obligation de formation et d'information auprès de vos salariés.

2 Prud'hommes

En cas de conflit lié à la Santé Sécurité au Travail, un salarié pourra saisir le tribunal des prud'hommes pour demander réparation de son préjudice.

3 Sanctions civiles et pénales

En cas d'accident du travail, de maladie professionnelle, la responsabilité de l'employeur peut être engagée.

Il s'expose à des sanctions civiles et pénales.

La faute inexcusable de l'employeur peut également être retenue à son encontre.

6.2 Le plan de prévention des risques et plan de particulier de sécurité et de protection (PPSPS)

Ce que dit la loi : *Article R4512-6 et Article R4512-7 et Article R4512-8 et Article R4512-9*

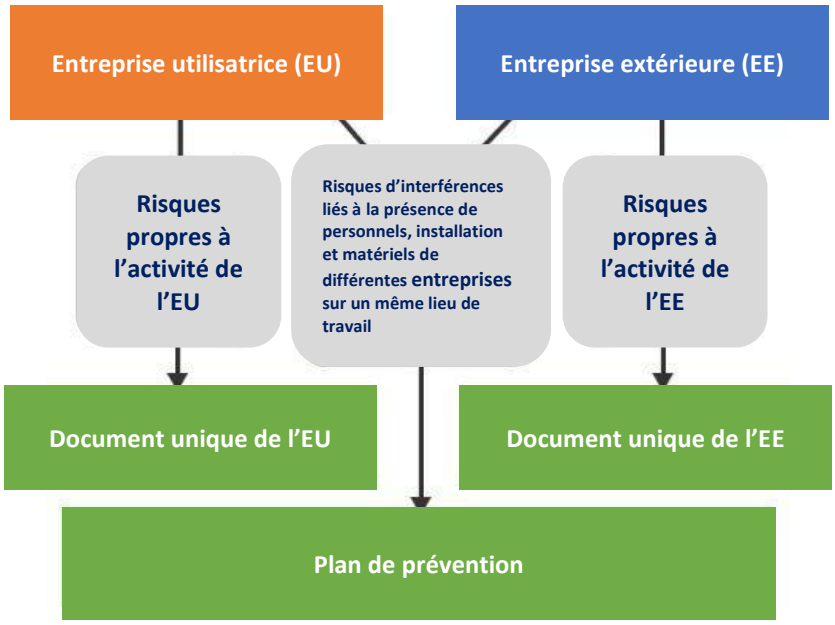
Lorsque deux entreprises travaillent en coactivité, elles établissent un plan de prévention selon certaines conditions. Lors de l'inspection commune préalable, les chefs des entreprises utilisatrices et extérieures procèdent en commun à une analyse des risques pouvant résulter de l'interférence entre les activités, installations et matériels.

Lorsque ces risques existent, les employeurs arrêtent d'un commun accord, avant le début des travaux, un plan de prévention définissant les mesures prises par chaque entreprise en vue de prévenir ces risques.

Article L4532-9

Sur les chantiers soumis à l'obligation d'établir un plan général de coordination, chaque entreprise, y compris les entreprises sous-traitantes, appelée à intervenir à un moment quelconque des travaux, établit, avant le début des travaux, un Plan Particulier de Sécurité et de Protection de la Santé (PPSPS). Ce plan est communiqué au coordonnateur.

Toute entreprise appelée à exécuter seule des travaux dont la durée et le volume prévus excèdent certains seuils établit également ce plan. Elle le communique au maître d'ouvrage.



6.3 Protocole de sécurité

Le protocole de sécurité est un document écrit qui remplace le plan de prévention.

Il doit contenir toutes les informations utiles pour l'évaluation des risques des opérations de chargement et déchargement ainsi que les mesures de prévention et de sécurité qui doivent être observées.

Le cadre réglementaire du protocole de sécurité est constitué des articles R. 4515-1 à R. 4515-11 du Code du travail.

Les rubriques du protocole de sécurité

- les matériels et engins spécifiques utilisés pour le chargement ou le déchargement ;

- les moyens de secours en cas d'accident ou d'incident ;

- l'identité du responsable désigné par l'entreprise d'accueil, auquel l'employeur délègue, le cas échéant, ses attributions.

Concernant l'entreprise d'accueil, on doit retrouver :

- Les consignes de sécurité, particulièrement celles qui concernent l'opération de chargement et de déchargement
- Le lieu de livraison ou de prise en charge, les modalités d'accès et de stationnement aux postes de chargement ou de déchargement accompagnées d'un plan et des consignes de circulation
- Les matériels et engins spécifiques utilisés pour le chargement ou le déchargement
- Les moyens de secours en cas d'incident ou d'accident
- L'identité du responsable désigné par l'entreprise d'accueil

Concernant le transporteur, il doit contenir :

- Les caractéristiques du véhicule, son aménagement et ses équipements
- La nature et le conditionnement de la marchandise
- Les précautions particulières résultant de la nature des substances ou produits transportés, notamment celles imposées par la réglementation relative au transport de matières dangereuses.

						
Casque	Chaussures ou bottes	Vêtement de travail	Lunettes	Visière	Masque	Protection auditive
❑	❑	❑	❑	❑	❑	❑

❑ Port de tout autre équipement de protection
Préciser .....
Respecter la signalisation routière sur le site (limitation de vitesse, interdiction de stationnement,...)

Hygiène	Interdiction	Consignes
❑ Le lavage des mains est fortement conseillé après l'opération de chargement ou de déchargement. ❑ Autre.....	❑ De fumer et de vapoter à l'intérieur des bâtiments. ❑ D'évoluer dans la zone d'action des matériels de manutention. ❑ De monter sur le marchepied des véhicules pendant les manœuvres. ❑ Autre.....	❑ Les ouvertures et fermetures des portes de remorques ou camions doivent s'effectuer véhicule à l'arrêt, moteur coupé, frein à main serré, câle sous les roues tractrices. ❑ Autre.....

Sécurité pour le transport de matières dangereuses

Présence de matières dangereuses ? ❑ Oui ❑ Non

Si oui, en préciser la nature

.....

.....

.....

Numéro ADR .....

Procédure et cheminement de l'opération
(à la charge de l'entreprise)

❑ affichage des panneaux de signalisation obligatoire
❑ contrôle de la certification / habilitation du chauffeur
❑ documents de bords à présenter
❑ dispositif de fermeture des vannes (vérification de l'étanchéité des raccords ou vannes après dépotage)
❑ branchement et identification des flexibles
❑ récupération des polluants et élimination
❑ branchement des dispositifs d'élimination de l'électricité statique

Caractéristiques des produits

❑ 	CMR	❑ 	Corrosif	❑ 	Inflammable
❑ 	Toxique	❑ 	Gaz sous pression	❑ 	Comburant
❑ 	Nocif Irritant	❑ 	Explosif	❑ 	Dangereux pour le milieu aquatique

Précautions à prendre en fonction de la nature du produit :

Dispositions générales

En accord avec les prescriptions des articles R 4515-4 à R 4515-11 du Code du Travail, les parties signataires s'engagent à tenir à jour le présent protocole de sécurité en fonction des modifications qui pourraient intervenir pendant la durée de la prestation.
Le transporteur s'engage à transmettre toutes les informations nécessaires au bon déroulement de l'opération à tout nouveau chauffeur amené à pénétrer sur le site.
Les signataires s'engagent à respecter les prescriptions du présent protocole ainsi que celles figurant dans les documents joints.
Toute information modifiant ce protocole sera annexé ou donnera lieu à la rédaction d'un nouveau protocole.

Le responsable du service dans lequel s'effectue l'opération de chargement ou de chargement	Le responsable de l'entreprise de transport	Cachet de l''entreprise d'accueil
Nom..... Date..... Signature	Nom..... Date..... Signature	Cachet

6.4 Elaboration des consignes de sécurité incendie

L'élaboration des consignes de sécurité incendie : autrefois limitée aux entreprises de plus de 50 salariés, l'obligation d'éditer des consignes incendie selon la norme NF EN ISO 7010 concerne désormais tous les établissements.

Pour être conforme, ce document doit notamment indiquer les équipements d'extinction disponibles, les moyens d'alerte ainsi que le nom des personnes en charge de contacter les pompiers en cas de départ de feu.

Les articles R232-12-1 à -29 du Code du Travail prévoient l'obligation pour les entreprises de mettre en place des dispositifs pour lutter contre l'incendie et les explosions au sein de leurs locaux.

De plus, il invoque de sensibiliser les ressources humaines aux différents risques encourus.

Cependant, 1 Français sur 4 n'est pas formé dans ce sens, soit environ 6,5 millions d'employés.

Et 1 Français sur 3 ignore tout des mesures anti-incendie sur son lieu de travail.

7.PREVOIR, PLANIFIER ET SUIVRE LA MAINTENANCE DES INSTALLATIONS

La maintenance préventive consiste en la vérification et l'entretien complet des installations et des systèmes de sûreté et de sécurité, afin de maintenir leur bon fonctionnement, dans le respect des règlements et normes en vigueur.

Une maintenance préventive régulière permet ainsi de réduire la probabilité de défaillance des installations et de minimiser les opérations de maintenance corrective.

Lors de ces opérations de maintenance préventive, chaque équipement constituant le système est ainsi marqué d'un code barre d'indentification et de localisation permettant de tracer les prestations préventives réalisées. L'ensemble de ces rapports de visites préventives et actions correctives menées sont consultables dans le registre de sûreté et/ou de sécurité.

Vérifier et ajuster, si besoin, les contrats de maintenance en fonction de l'importance des installations en cas de maintenance corrective, afin de maîtriser les délais d'intervention des mainteneurs pour ne pas vulnérabiliser l'entreprise et son organisation.

8.RISQUE MALVEILLANCE

En fonction de sa localisation et de son environnement, un site peut devenir potentiellement une cible d'actes de malveillance.

Ainsi, les standards de sûreté d'un site ne seront pas les mêmes si celui-ci est situé dans une zone industrielle, une zone résidentielle, en pleine campagne, etc.

L'environnement et le voisinage du site peuvent aussi augmenter le risque de malveillance avec par exemple la présence d'un site sensible à proximité.

8.1 Eléments d'attractivité

La nature et les caractéristiques spécifiques d'un site vont motiver son attractivité aux yeux d'auteurs d'actes de malveillance.

L'attractivité peut être déterminée grâce à plusieurs types de facteurs :

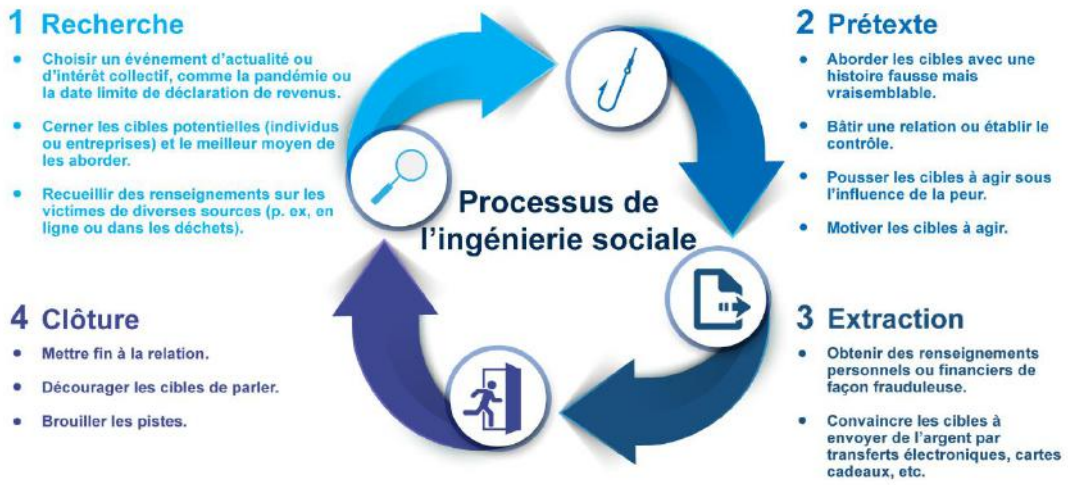
- Le pays que l'entreprise représente (ex. pays géopolitiquement instable)
- L'emploi qu'elle génère ou qu'elle affecte
- L'image qu'elle représente (cf. activisme)
- Le savoir qu'elle détient (ex. secret industriel, technologie, etc.)
- Les valeurs présentes (numéraires, matières premières, matériels, produits, etc.)
- Les usagers présents plus ou moins attractifs (VIP, membres du COMEX, etc.)
- Etc.

Le sous-traitant d'une entreprise aux activités sensibles peut rendre un de ses sites particulièrement attractif.

Dans un contexte concurrentiel où l'intelligence économique devient un enjeu stratégique, le fait de s'en prendre à un sous-traitant (par nature plus vulnérable qu'un grand groupe) devient monnaie courante.

8.2 L'ingénierie sociale (*social engineering* en anglais)

L'ingénierie sociale est, dans le contexte de la sécurité de l'information, une pratique de manipulation psychologique à des fins d'escroquerie.
Les pratiques du piratage psychologique exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles des individus ou organisations pour obtenir quelque chose frauduleusement (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.).
En utilisant ses connaissances, son charisme, son sens de l'imposture ou son culot, l'attaquant cherche à abuser de la confiance, de l'ignorance et de la crédulité de sa cible pour obtenir ce qu'il souhaite.



8.3 Les environnements et contextes extérieurs de l'entreprise

En fonction de son activité et de son implantation, l'entreprise doit faire face à des risques inhérents aux environnements et aux contextes extérieurs.
L'étude des environnements contribue à la stratégie et la mise en œuvre des moyens organisationnels, techniques et humains adéquates (résistance et sensibilité des systèmes exposés à la faune et au climat, délais d'intervention si isolé, accessibilité du site, chemin de fuite ou de pénétration, instabilité politique, concurrence etc.

a) **Environnement Naturel/Urbain**
   a. Accessibilité (route, autoroutes, train, cours d'eau, …) = Facteur aggravant d'une menace ou d'une solution de repli pour les malfaiteurs/Délais d'intervention des secours, du prestataire et des forces de sécurité
   b. Isolement (Rural, Urbain, …) = Proie facile +délais d'intervention
   c. Climatologie (Brouillard, neige, …) = Contrainte pour mise en œuvre de détection

b) **Environnement Socio-Économique**
   a. Contexte Social : Analyse de la délinquance et Contexte social et sociétal
   b. Contexte Géopolitique : Pays d'implantation, Implantation, Relations extérieures
   c. Contexte Économique : Analyse et Risques du marché

c) **Environnement législatif et règlementaire**
   a. Code du travail – Art. L4121-1

⇨ « L'employeur prend les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs »

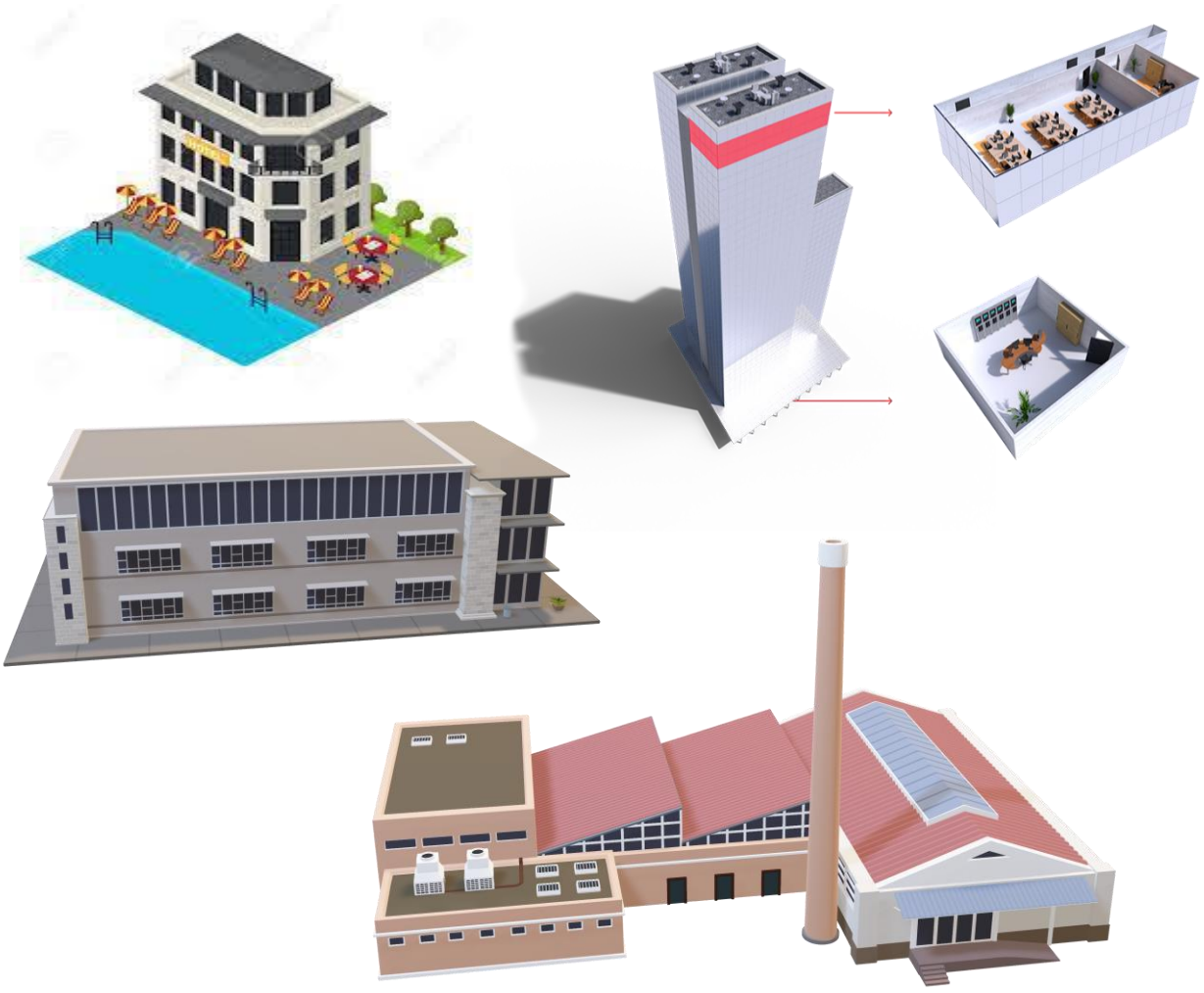
⇨

Connaître les classifications règlementaires de l'entreprise

a. Code de l'environnement – ICPE-Sites SEVESO – Autorisation préfectorale pour l'exploiter – DREAL-DRIRE
b. Code de la construction et de l'habitation (ERP, IGH, …) – Menace Incendie – DDSIS (Direction Départemental Des Services D'Incendie Et De Secours)

⇨ Base de la prévention des risques technologiques et incendie

c. Règlementations privées (APSAD)
d. Règlementations spécifiques de sûreté (Secteurs d'Activités d'Importance Vitale, Etudes de Sûreté et de Sécurité Publique, Code de la Sécurité Intérieure, CNIL, Code pénal, …)



Environnement naturel

FLORE
- Forêt?
- Terre cultivées?

FAUNE
- Espèces protégées?
- Gibiers? (donc chasseurs)

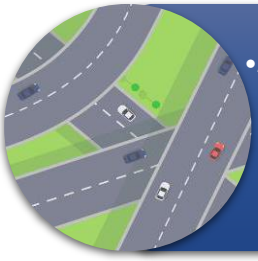
HYDROLOGIE
- Cours d'eau?
- Marais?
- Littoral?

TOPOLOGIE
- En hauteur?
- Encaissé?

CLIMATOLOGIE
- Brouillard?
- Précipitations?

GEOLOGIE
- Carrières?

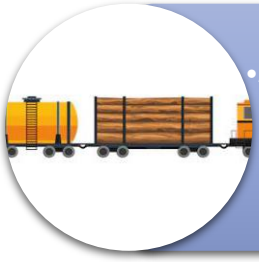
Environnement de desserte



- Autoroute?

- Autre réseau routier?

- Voies navigables?



- Accès marchandises par voie ferrée?

- Transports en commun?

Environnement socio-économique

ACTIVITE COMMERCIALE

- Grande distribution?
- Commerces à forte attractivité de la malveillance?

ACTIVITE INDUSTRIELLE

- ICPE ?
- SEVESO ?

ZONE

- Rurale?
- Urbaine?
- Périurbaine?

HABITAT

- Résidentiel?
- Cités sensibles?

DELINQUANCE

- Délinquance itinérante?
- Les causes: Facteurs endogènes, facteurs individuels, facteurs exogènes, facteurs sociaux
- Typologies des actes
- Evolution en volume
- Evolution des modes opératoires

EVENEMENTIEL

- Enceintes sportives ou de spectacles?
- Evènements prévisibles?

Contexte géopolitique

IMPLANTATIONS OU MISSIONS

- Nationales
- Européènnes, mondiales

PAYS D'IMPLANTATIONS

- Distance physiques, liaisons
- Culture, exposition à des risques "pays"

RELATIONS DES PAYS AVEC LA FRANCE

- Partenariats(économiques, militaires, etc.)
- Francophonie
- Tensions et/ou hostilité

Contexte économique

ANALYSE DU MARCHE

- Nature de la production
- Marché "protégé" (défense, OIV)
- Stabilité ou incertitude
- Concurrences loyales

RISQUES DU MARCHE

- Espionnage industriel
- Sabotages, destructions
- Compromission de personnels
- Vols d'informations (physiques ou numériques)
- Désinformation

8.4 Analyse et gestion des flux

Une entreprise est un ensemble complexe de moyens et de fonctions, elle peut se représenter schématiquement par :

- Des flux entrants subissant un processus de transformation, de traitement…
- Des flux sortants : produits finis, services, …

Il y a risque dès qu'il y a croisement de flux.

L'étude et l'analyse de ce flux doit être attentive, afin de favoriser ou de permettre le cas échéant, des cloisonnements, des moyens de traçabilité (pour les fournisseurs, les clients), des stockages appropriés (conservation et péremption),

Le flux énergies et fluides

En amont (approvisionnement)

Qu'il s'agisse d'une entreprise de services ou de production, d'une administration ou d'une collectivité, ce flux (énergies) est généralement celui qui permet de faire fonctionner toute la structure.

Plusieurs points viennent à l'esprit :

- L'électricité pour l'alimentation principale mais aussi secondaire (groupe électrogène…)
- Le gaz
- L'eau
- Le carburant (fuel, essence, charbon, gasoil, etc.)
- L'oxygène pour les centres hospitaliers

Les atteintes peuvent être des coupures, des sabotages, des détournements, des dénaturations, des pollutions, des incendies, etc… Les points sensibles sont les postes de livraisons, de transformation, de détente, de stockage ou de production des gaz comprimés, les réseaux de distribution.

En aval (les rebuts et les déchets)

- Les eaux de production et/ou les eaux usées
- Les déchets papier
- Les déchets industriels
- Les déchets courants
- Les rejets atmosphériques

Une vigilance particulière est parfois nécessaire. Ces déchets peuvent constituer une cible.
Les déchets papiers peuvent être volés et analysés dans le cadre de l'espionnage.
Les déchets industriels peuvent être détournés, déversés ou dispersés pour porter atteinte à l'image de l'entreprise, etc.

Il convient donc de connaître leur contenu, leur destination et leur parcours pour éviter les pollutions, les incendies, des dispersions, des analyses, etc.

Le flux finance

Ce flux peut se présenter sous deux formes :

A l'état fiduciaire (encaissement de liquidités, et donc transfert et transport de fonds) ;
A l'état scriptural (moyen de payement électronique, virements, écritures comptables, etc.

Dans le premier cas, on pense à des appropriations avec ou sans violence, par ruse ou par chantage. Mais dans le second cas, cela peut prendre des formes plus subtiles comme la falsification ou le détournement, le blanchiment…

Le flux information, communication

Ces informations pour se véhiculer passent encore et toujours par l'oral que ce soit lors de réunions de travail, de débriefings pour donner suite à des rendez-vous professionnels et commerciaux, de déplacements, de pauses café, etc.

Dans chaque structure, il doit exister une hiérarchie de l'information qui distingue les informations selon leurs types et leurs destinataires.

Ces informations peuvent être soit :

- ⇨ Orale (lors de réunions ou de conférences)
- ⇨ Papier (notes, documents commerciaux, rapport technique)
- ⇨ Informatiques

Les menaces qui pèsent sur l'information dans chaque structure commencent par l'appropriation plus ou moins licite de celle-ci.

- ⇨ L'intrusion logique (ou informatique : virus, cheval de Troie, etc.)
- ⇨ Les interceptions et écoutes
- ⇨ Le vol de support (document papier, ordinateur portable…)
- ⇨ Le recueil, l'analyse et le recoupement de sources dites « ouvertes »
- ⇨ La rumeur, la désinformation
- ⇨ La manipulation de personnes…

Les points sensibles peuvent être les fichiers (informatique ou papier), les terminaux, les sous-répartiteurs, les photocopieurs, imprimantes, les conversations en milieu public, les secrétariats, les accueils …

- Informations blanches : disponible en libre-service
- Information grise : nécessite des actions de renseignements, parfois à la limite de la légalité
- Information noire : nécessite des actions de recherche illicites.

Le flux rebut et déchet

Eaux usées, déchets papiers, déchets banals, déchets industriels spéciaux, rejet atmosphérique.

En Sécurité comme en Sûreté le croisement des flux entraîne des situations de vulnérabilités.
3 objectifs recherchés :

1. Eviter les points de croisement de flux, notamment à la conception des process (intégration de la prévention).
2. Diminuer le nombre de points de croisement (réorganisation des process existants).
3. Connaître les points résiduels de croisement de flux pour effectuer une surveillance.

Les principaux auteurs d'actes de malveillance peuvent être :

- Un riverain
- Un employé mécontent
- Un concurrent
- Un délinquant
- Un criminel
- Un Cyber criminel
- Un membre du grand banditisme
- Un activiste (ex. association, ONG, etc.)
- Un terroriste
- Un mouvement de protestation (syndicat, association ou ONG)
- Un fraudeur : arnaque au président
- Un état
- Etc.

Prendre en considération que la menace peut très souvent avoir pour provenance une source interne (collaborateurs, prestataires, sous-traitants, etc.).

Plus de la moitié des actes de malveillance présente une complicité interne volontaire ou involontaire : par exemple, il arrive souvent que par manque de vigilance, un employé se rende complice de divulgation des informations sensibles.

Il faut prendre en compte l'interactivité des flux.

Catégories de flux	Risques
Humain (Employés, visiteurs, fournisseurs, sous-traitants)	**L'humain devient menace** : intrusion, sabotage, espionnage, vol, agression, etc. **L'humain devient cible** : harcèlement, viol, agression, enlèvement, vol, voie de fait, chantage, etc.
Finances (Argent matériel, immatériel : virement, …)	**Atteintes** : Vol par ruse, détournement, blanchiment, vol à main armée, escroquerie, etc.
Produits, biens et marchandises (Matières premières, consommables, déchets, etc.)	**Atteintes :** Démarque inconnue, braquage, etc. Ils sont une cible potentielle, mais peuvent devenir un vecteur de menace. ⇨ Protection des produits alimentaires contre la contamination intentionnelle ou l'adultération par des agents biologiques, chimiques, physiques ou radiologiques introduits dans le but de causer des dommages. ⇨ Colis piégés.
Energies et fluides (Électricité, gaz, eau, et fluides très spécifiques, ex : oxygène dans les hôpitaux)	**Atteintes** : Coupure électrique, détournements, incendie, pollution, … **Points sensibles** : Poste de livraison, zone de stockage, zone de transformation, …
Informations et de communications ⇨ Communication interne **:** doc commerciale, rapport technique, … ⇨ Communication externe **:** pub, presse, exposition, … ⇨ Information blanche **:** Disponible en libre accès. ⇨ Information grise : Nécessite des recherches à la limite de la légalité. ⇨ Information noire : Nécessite des recherches illégales.	**Atteintes :** Piratage industriel, fichiers, terminaux, gestion des codes et des clés, …

8.5 Les atouts de la démarche partenariale

1. Communication :

- ⇨ Mettre en place des relations de proximité avec les responsables de la sécurité sûreté des sites mitoyens ou voisins de façon à générer une dynamique contre la malveillance éventuelle.
- ⇨ Entretenir des contacts avec la collectivité locale pour l'entretien, la surveillance des espaces publics susceptibles de générer des usages déviants, la maintenance de l'éclairage public, de la voirie, etc. Participation si besoin aux *CLSPD (Conseil Local de Sécurité de Prévention et de Délinquance).
- ⇨ Assurer la relation partenariale avec les SDIS, forces de sécurité police, gendarmerie, municipale.

2. La mutualisation :

- ⇨ Nécessité de s'inscrire dans la logique d'une coproduction de la sécurité ;
- ⇨ Mutualiser les expertises, les ressources et les savoirs faire des différents intervenants ;
- ⇨ Une connaissance plus fine des caractéristiques locales de la délinquance permet d'orienter les actions dans le domaine de la sécurité de l'entreprise.

*Le Conseil local de sécurité et de prévention de la délinquance (CLSPD) est une instance française chargée de la coordination locale du contrat local de sécurité (CLS) ou de la stratégie territoriale de sécurité et de prévention de la délinquance (STSPD).
Il réunit, selon le territoire, l'ensemble des acteurs prenant part à l'application des politiques de sécurité et de prévention de la délinquance.
Le CLSPD est présidé par le Maire de la commune ou le président de l'intercommunalité.
Un CLSPD comprend un collège d'élus désignés par le président, un collège de représentants de l'État désignés par le préfet et un collège composé de professionnels confrontés aux manifestations de la délinquance.
Le CLSPD doit généralement permettre de réunir le Préfet et le Procureur de la République, ou leurs représentants, le Directeur départemental de la sécurité publique, le commissaire de la circonscription de sécurité publique dont dépend la commune, Le Chef de la police municipale, le commandant de groupement de gendarmerie, le commandant de compagnie ou commandant de brigade de gendarmerie dont dépend la commune, le président du conseil général ou son représentant, les représentants des administrations de l'État désignés par le Préfet, des représentants d'associations, établissements ou organismes œuvrant notamment dans les domaines de la prévention, de la sécurité, de l'aide aux victimes, du logement, des transports collectifs, de l'action sociale, ou des activités économiques, etc.
La composition peut varier en fonction des besoins et des problématiques rencontrées localement, la liste des acteurs invités à siéger au CLSPD est, en principe, inscrite dans le règlement intérieur du CLSPD.

Le CLSPD est régi par l'article L. 132-4 du code de la sécurité intérieure, le décret du 17 juillet 2002 et plusieurs circulaires.

8.6 Identifier les risques de sûreté malveillance de son entreprise

L'approche classique commence par une évaluation et une hiérarchisation minutieuse des risques, des menaces et des vulnérabilités du site.

1.Identification des valeurs à protéger dans son établissement en accord avec la compagnie d'assurance.

2.Prise en compte des exigences particulières de l'assureur (Conseil), qui connait l'importance des valeurs à protéger.

3.Analyse des risques définissant les besoins, en mettant en évidence les « valeurs » et leurs vulnérabilités.

L'analyse doit prendre en compte :

- L'accessibilité du bâtiment.
- La protection mécanique existante.
- Les systèmes de contrôle d'accès existants.
- Les systèmes de détections existants.
- La localisation des différents secteurs sensibles présents sur le site.
- La délimitation des zones de localisation de valeurs dans les secteurs sensibles.
- Les personnes habilitées à accéder dans les zones de valeurs et les secteurs sensibles (jours, plages horaires).
- L'évaluation des niveaux de résistance des diverses parois, issues et ouvrants.
- L'importance des éléments de valeur ou les conséquences d'un éventuel sinistre dans ces secteurs (donnée par l'assurance).
- Les scénarios vraisemblables de pénétrations et de circulations dans les locaux.
- Le mode d'exploitation des locaux (utilisation partielle, etc.).
- Les conditions d'environnement du site (Isolement, voisinage, sinistralité du site).
- Les phénomènes physiques susceptibles d'altérer le fonctionnement des matériels (températures, foudre, vibrations, humidité, électromagnétisme, etc.).
- Les phénomènes animaux susceptibles d'altérer le fonctionnement des matériels (oiseaux, rongeurs, sangliers, etc.).
- Les contrats de maintenance (délais et plages horaires d'interventions en cas de panne, d'arrachage ou de détérioration des installations).

Ce tour d'horizon permet ensuite de définir un zonage plus ou moins complexe et formalisé, qui se compose de plusieurs cercles concentriques :

La zone périphérique porte sur la délimitation du terrain et sa clôture, placée aussi loin que possible du bâtiment.
Elle passe, entre autres, par des barrières à infrarouge, des capteurs de vibrations ou des géophones.

La zone périmétrique concerne l'enveloppe extérieure du bâtiment (murs, toits, issues, fenêtres) et requiert notamment des détecteurs d'ouverture, de choc ou de bris de glace, le barreaudage des fenêtres.

La zone de valeur définie l'intérieur des locaux, le dispositif de surveillance est souvent couplé avec un système de contrôle d'accès.

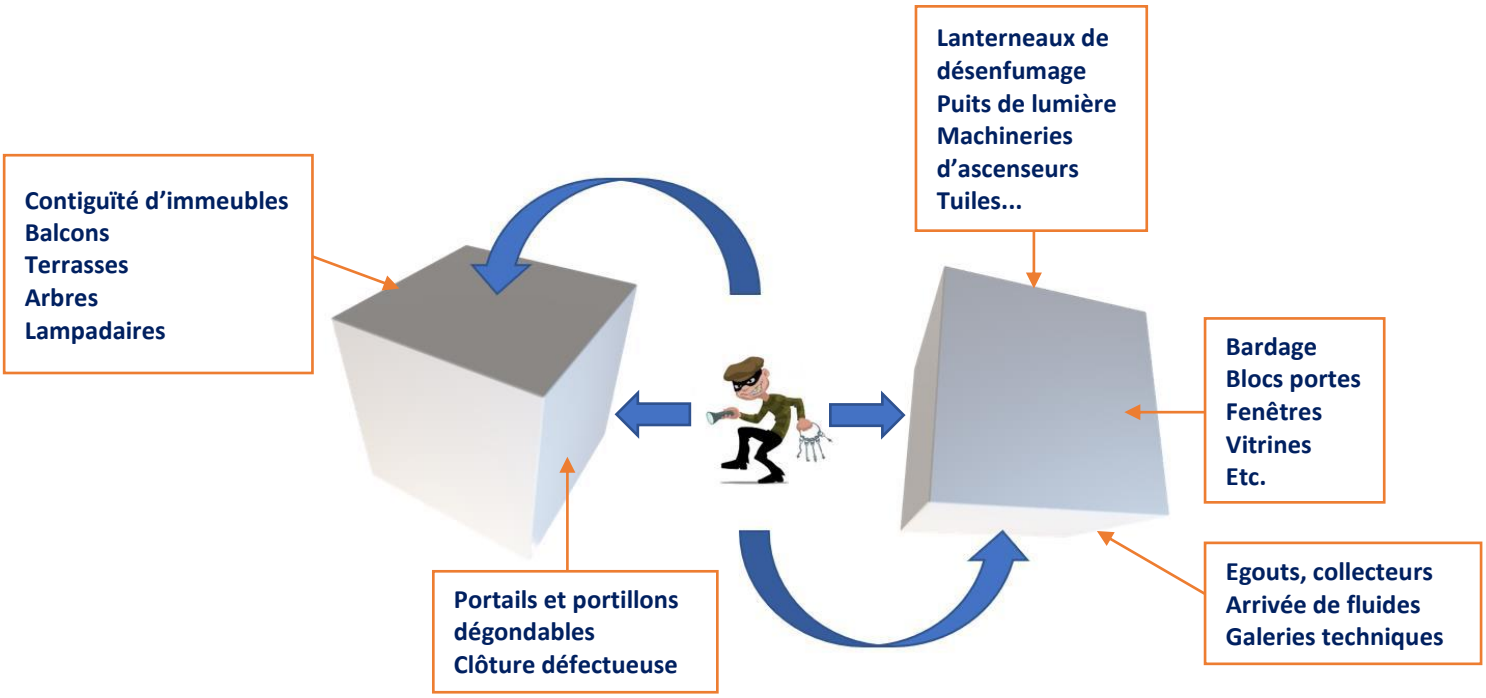
8.7 Concept de protection des 3 cubes

Protection périphérique (délimite la zone extérieure) ;
Il peut s'agir d'une clôture, d'un grillage, d'un mur, etc.

Protection périmétrique (généralement, l'enveloppe du bâtiment) ;
Il s'agit des parois, des portes, des surfaces vitrées.

Protection intérieure (zone concernée et les valeurs à protéger).
Il s'agit d'un coffre-fort, d'une pièce spécifiquement protégée, de tout élément physique protégeant directement les valeurs ou ralentissant leur prise (système de fixation par exemple).
Les cubes doivent être continus et constitués d'éléments de protection de niveau homogène.
La valeur d'un système de sécurité est égale à celle de l'élément le plus faible du système.
Pour concevoir un bon système, considérer les approches par le toit et les égouts.

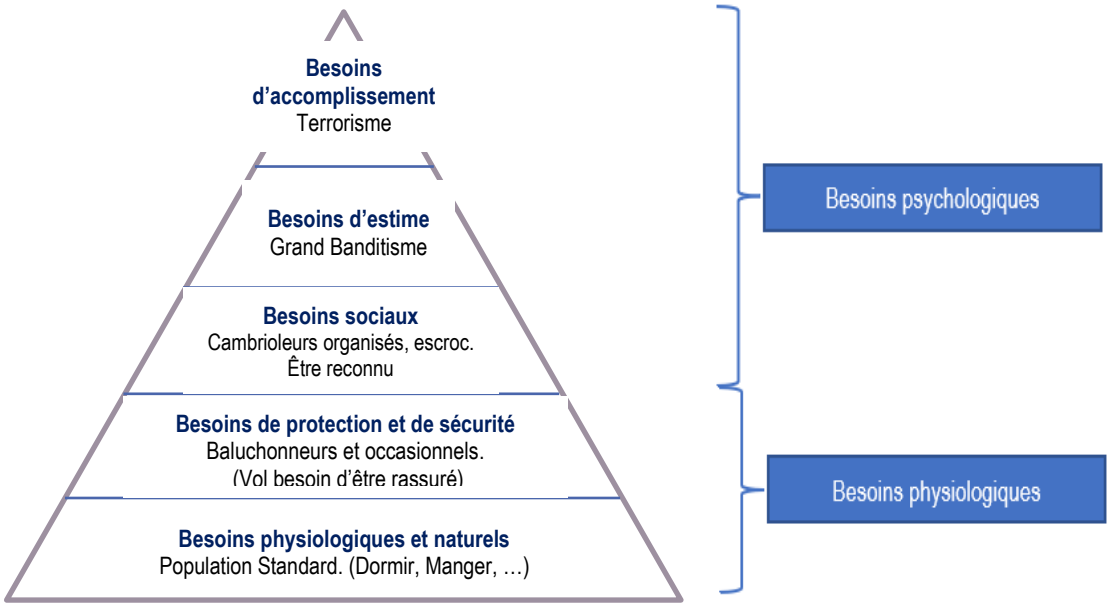
La prise en compte des accès par le haut et par le bas est schématiquement représentée par trois volumes à 6 faces (Nord, Est, Sud, Ouest, les toitures et les sous-sols).
Nonobstant les intrusions par des points d'accès identifiés, afin d'avoir une approche structurée des vulnérabilités du site, il sera pertinent d'intégrer des scénarios d'intrusion en fonction des points d'accès pouvant exister par : les sous-sols et galeries techniques, les égouts, les collecteurs, par l'arrivée de fluides.
La contigüité d'immeubles peut favoriser des scénarios d'intrusion par les toits, terrasses, les lanterneaux de désenfumage, par les puits de lumière, les machineries d'ascenseurs, les tuiles, etc.



Un zonage de sûreté permet de représenter visuellement la criticité des espaces, avec 4 types de zones distinctes.

8.8 Compréhension de la motivation

Les motivations du passage à l'acte de malveillance peuvent être expliquées par un déséquilibre des besoins physiologiques ou psychologiques présentée dans la pyramide de MASLOW ci-dessous.



La frustration d'un besoin peut engendrer de la malveillance ou de l'agressivité avec passage à l'acte.

Prévenir la menace et se protéger contre l'agresseur :

L'agresseur cherche à atteindre un/des objectifs par un/des modes ou moyens d'actions

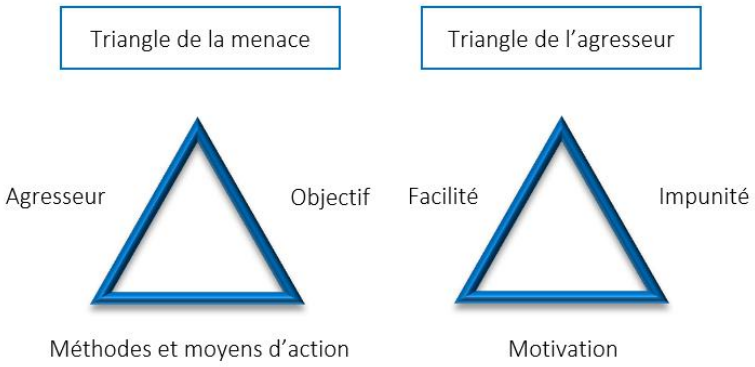
- ⇨ Triangle de la menace

Tout comportement humain repose sur une/des motivations qui associées à la facilité et à l'impunité déclenchent l'agression (malveillance)

- ⇨ Triangle du passage à l'acte (de l'agresseur)

La menace peut très souvent avoir pour provenance une source interne (collaborateurs, prestataires, sous-traitants, etc.).

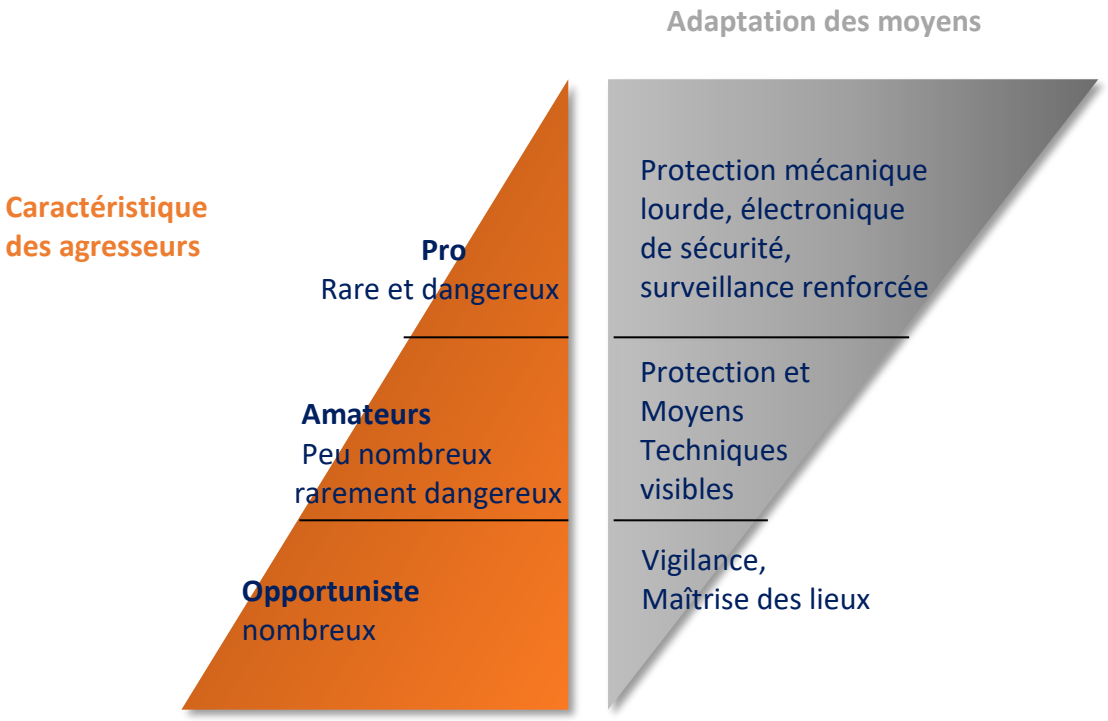
- ⇨ Plus de la moitié des actes de malveillance présente une complicité interne volontaire ou involontaire.



Conditions du passage à l'acte

Facilité : Absence de contrôle ou filtrage, Valeurs non rangées, absence de clôtures/barrières.
Impunité : Absence de règlement intérieur, manque de signalisation.
Motivation : Pyramide de Maslow.

Hiérarchisation des auteurs



9.LA PREVENTION SITUATIONNELLE

Cette approche a pour objectif de prévenir les actes contraires aux normes (crime, délit, incivilité) en limitant les opportunités (perçues par leurs auteurs) de les commettre, en augmentant le risque perçu d'être arrêtés et/ou en réduisant au minimum les avantages escomptés.
La prévention situationnelle désigne des mesures qui visent à supprimer ou à réduire ces opportunités en modifiant les circonstances dans lesquelles ces infractions pourraient être commises.

Pour réduire les conditions du passage à l'acte malveillant :

Augmenter l'effort	Augmenter les risques	Réduire les gains	Réduire les excuses
La protection des cibles	Le contrôle des flux	Le déplacement des cibles	Mise en place de règles
Le contrôle des accès	La surveillance formelle	L'identification des biens	Mise en place de signalétiques
La dissuasion des délinquants	La surveillance par les employés	La réduction des tentations	Rappel des règles de comportements
Le contrôle des facilitateurs	La surveillance naturelle	La suppression des bénéfices	Campagne de communication

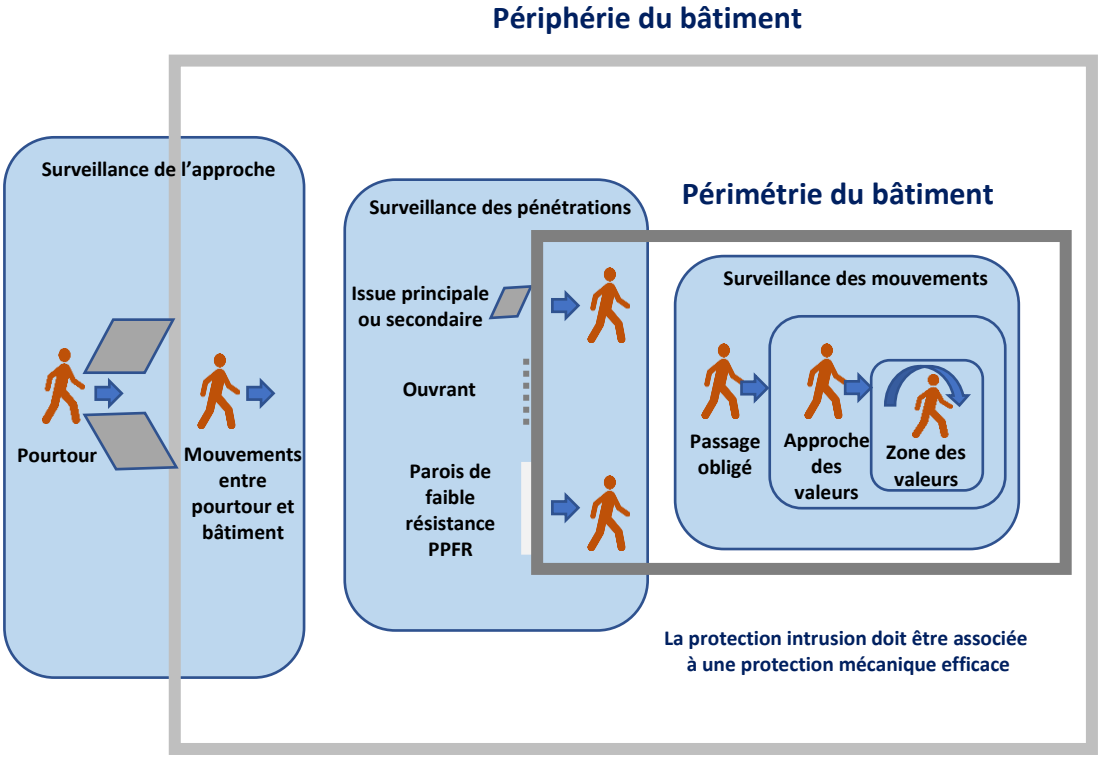
En fonction du délit à éviter, et des ressources à sa disposition, la prévention situationnelle privilégiera une action visant à :

- Augmenter les efforts perçus
- Augmenter les risques perçus
- Réduire les gains escomptés
- Réduire les incitations : il s'agit, au travers de diverses techniques de réduire les incitations à passer à l'acte.
- Empêcher toute justification : il s'agit d'empêcher l'auteur de justifier son acte, en promouvant notamment des injonctions et des interdictions de faire.

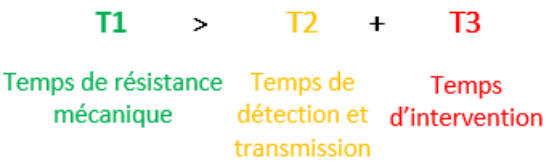
10.LES SYSTEMES DE SÛRETE

10.1 Rôle d'une installation de détection intrusion

Une installation de détection d'intrusion a pour objectif la surveillance des éléments de valeur (biens, mobiliers, fonds et valeurs, ainsi que les produits et documents).
Elle est destinée à détecter et à signaler l'approche, la pénétration et/ou le déplacement d'un intrus dans le site, les secteurs sensibles ou les zones de localisation de valeurs et selon les besoins, permet de déclencher une intervention.



La protection d'un site contre les cambriolages doit d'abord être assurée par une protection mécanique efficace constituée de dispositifs résistants à l'effraction, tels que : murs, verrous, serrures, portes, volets, barreaudage des fenêtres, etc.
La surveillance par un système électronique de détection d'intrusion vient en complément de la protection mécanique.
Plus la durée de l'acte de malveillance est courte, plus la détection doit être précoce ;
La résistance des éléments de protection mécanique accroît cette durée.
La résistance mécanique doit représenter un élément non seulement dissuasif mais également retardateur.



Le temps de résistance à l'effraction doit être supérieur au temps de détection et transmission + du temps d'intervention (service de sécurité, intervenant sur alarme, forces de l'ordre).

10.2 Les moyens de protection mécanique

1ère ligne de défense pour tout système de sécurité, la protection mécanique est un **ensemble d'obstacles physiques**, généralement passifs, retardant ou empêchant la pénétration dans un site protégé.
Un système de sûreté ne peut exister efficacement que s'il y a d'abord une protection physique.

Objectifs de la protection mécanique :

- **Interdire l'accès ou ralentir la pénétration** (clôture, portail, fossé, mur, haie vive, bloc porte, serrure, borne escamotable, herse…)
- **Détecter les pénétrations** (détecteurs, vidéosurveillance)
- **Donner l'alerte** (un cri, une alarme)
- **Retenir les valeurs** (avec un coffre)
- **Intervenir** (levée de doute par le service de sécurité sur site, ou la société de télésurveillance, puis appel des forces de l'ordre)
- **Dissuader l'agresseur potentiel**.

Caractéristiques des obstacles :

Ils doivent nécessiter :

- Du temps
- Du matériel
- Des savoir-faire

Buts/Objectifs pratiques :

- Dissuader l'agresseur
- Empêcher l'agresseur
- Retarder l'agresseur
- Retenir les valeurs

Type d'agresseur	Savoir-faire	Outillage	Temps d'action
Opportuniste	Aucun	Aucun	≤ 3 min
Occasionnel	Attaque basique Peu de connaissance	Léger et facile à transporter	3 à 5 min
Organisé	Attaque préparée Connaissance des produits	Adapté aux méthodes d'attaque	10 min
Expérimenté	Attaque élaborée et préparée Connaissance approfondie des produits	Adapté aux méthodes d'attaque et performant	15 min
Bande organisée	Attaque élaborée et préparée Connaissance approfondie des produits	Méthode experte performante et moyens d'actions importants	> 15 min

Source CNPP

10.3 Le contrôle d'accès

Le contrôle d'accès désigne les différentes solutions techniques qui permettent de sécuriser et gérer les accès physiques à un bâtiment ou un site, ou les accès logiques à un système d'information.
On distingue ainsi le contrôle d'accès physique et le contrôle d'accès logique.
Le contrôle d'accès permet de savoir Qui ? Où ? Par où ? Combien ? et Quand ? un individu est autorisé ou interdit d'accès et parfois des véhicules.
Un système de contrôle d'accès est constitué d'un ensemble de moyens qui permettent d'autoriser les entrées et les sorties de zones sensibles (points névralgiques) aux seules personnes qui ont le droit d'accès.


Caméra


Lecteurs de badges


Pavé numérique


Lecteurs biométriques


Valideurs de tickets


Collecteurs de jetons


Lecteurs de codes-barre

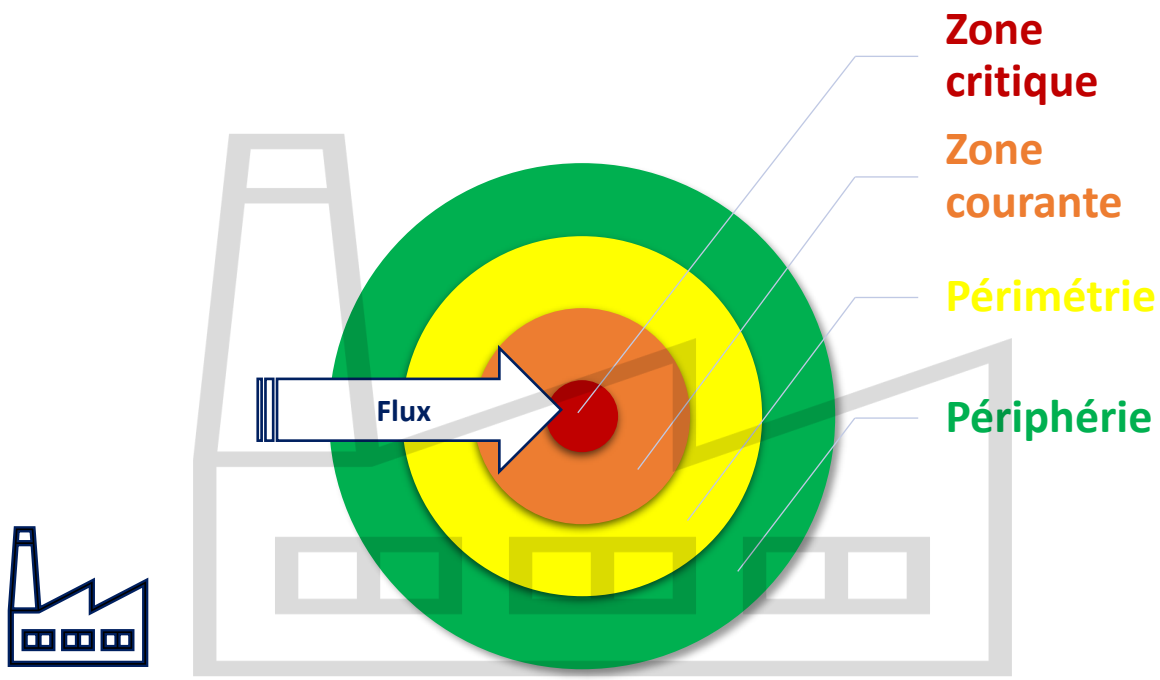

Compteur de passages


Lecteurs de plaques d'immatriculation

Objectifs du contrôle d'accès

La canalisation des flux en périphérie, périmétrie, zone courante et zone critique :

- ⇨ Contrôler la circulation dans les zones sensibles de l'établissement
- ⇨ Limiter les déplacements des personnes non autorisées
- ⇨ Maîtriser les flux par catégorie de personnes



Identification et authentification

L'identification : Le sujet désirant un accès à une ressource doit avant tout s'identifier, c'est-à-dire qu'il doit annoncer qui il est (Digicode, badge d'accès, etc.).
Authentification : Après l'identification, le sujet doit prouver son identité (Caméra, biométrie, mot de passe).

1/Fonction identification :

Classe 0 : Pas d'identification effective (bouton poussoir, contact, détecteur de mouvement…) ;
Classe 1 : Information mémorisée (code personnel, mot de passe mémorisé au clavier…) ;
Classe 2 : Identifiant personnalisé ou caractéristique biométrique (carte magnétique, carte de proximité, carte à puce, caractéristiques biométriques…) ;
Classe 3 : Combinaison de l'identifiant personnalisé ou caractéristique biométrique, et de l'information mémorisée (identification personnalisée et confirmation par code personnel ou mot de passe).

On peut distinguer trois familles principales d'identifiants :

1. Codes mnémoniques : l'usager saisit un code qui est comparé à ceux de la base de données du système. Il n'a pas à apporter d'élément physique. Cela supprime les problèmes de gestion des identifiants par un service de sécurité (stocks, pertes, oublis, etc.)
2. Cartes et badges : Une carte est un objet que l'on porte avec soi et que l'on présente sur demande. Un badge est un objet que l'on affiche spontanément sans qu'il y ait de demande préalable (badge visiteur, par exemple).
3. Biométrique : (empreintes digitales, morphologie de la main, reconnaissance faciale, reconnaissance rétinienne, de l'iris, vocale, de la signature…). Ces dispositifs permettent la reconnaissance de certaines caractéristiques propres à chaque individu. L'usager se présente au lecteur, qui mesure les caractéristiques et les transmets à l'unité de traitement pour comparaison avec celles contenues dans la base de données.

2/Fonction traitement

Elle contient toutes les bases de données nécessaires pour l'exploitation du système.
Elle réalise aussi toutes les fonctions secondaires d'interface entre les fonctions d'identification des usagers, de verrouillage des points d'accès, ainsi que pour les communications avec l'extérieur du système.

Les bases de données répertoriées sont :

- ⇨ Les points d'accès
- ⇨ Les usagers
- ⇨ Les grilles horaires
- ⇨ Les niveaux d'accès
- ⇨ L'enregistrement des évènements
- ⇨ L'intervention
- ⇨ Le traitement fonctionnel
- ⇨ Gestion des lecteurs

3/Fonction verrouillage :

La troisième fonction est une fonction de blocage. Cette fonction permet de limiter la libre circulation de personnes dans les locaux "sensibles", en plaçant les obstacles mécaniques (barrières) sur les accès aux bâtiments.

On retrouve :

- ⇨ Les gâches électriques
- ⇨ Les verrous motorisés
- ⇨ Les ventouses électromagnétiques

10.4 RGPD-CNIL

Le développement des technologies facilite ces contrôles mais permet aussi de collecter bien plus d'informations sur les personnes concernées.
Des limites à leur utilisation sont donc indispensables pour préserver les droits et libertés de chacun.

Les informations ne sont accessibles qu'aux membres habilités des services gérant le personnel, la paie, ou la sécurité.
L'employeur doit prévoir des mesures pour assurer la sécurité des informations concernant ses salariés et éviter que des personnes qui n'ont pas qualité pour y accéder puissent en prendre connaissance.
Ainsi, il doit prévoir des habilitations pour les accès informatiques avec une traçabilité des actions effectuées (savoir qui se connecte à quoi, quand et pour quoi faire).

Une étude des risques sur la sécurité des données est également souhaitable afin de définir les mesures les mieux adaptées, notamment lorsqu'un dispositif biométrique est mis en place.

Le contrôle d'accès biométrique doit faire l'objet d'une analyse d'impact sur la protection des données (AIPD). Cette démarche permet d'identifier les risques associés aux données personnelles concernées par le dispositif, et à en réduire soit la vraisemblance soit la gravité.
L'aide du fournisseur, de l'intégrateur ou de l'installateur du dispositif peut être utile.
Dans ces situations, l'employeur doit privilégier le stockage du gabarit biométrique de l'employé sur un support individuel.

Si l'organisme a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en œuvre de ce dispositif.
L'employeur doit inscrire ce dispositif de contrôle dans son registre des activités de traitement de données.

Suite à l'entrée en application du RGPD, les normes adoptées par la CNIL n'ont plus de valeur juridique depuis le 25 mai 2018. Dans l'attente de la production de référentiels RGPD, les responsables de traitement peuvent s'en inspirer pour orienter leurs premières actions de conformité.

Norme Simplifiée n°42 (sans biométrie), pour le traitement automatisé d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de restauration, et les accès visiteurs.

Autorisation Unique 052 (données biométriques stockées sur badge), pour le contrôle des accès à l'entrée et dans les locaux faisant l'objet d'une restriction de circulation et pour le contrôle des accès à des appareils et applications informatiques.

Autorisation Unique 053 (données biométriques stockées dans un serveur) pour le contrôle des accès à l'entrée et dans les locaux faisant l'objet d'une restriction de circulation et pour le contrôle des accès à des appareils et applications informatiques.

Cadre juridique :

Principe de proportionnalité
Art. L1121-1 du code du travail. Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

Recueil d'informations sur le salarié
Art. L1221-9 du code du travail. Aucune information concernant personnellement un candidat à un emploi ne peut être collectée par un dispositif qui n'a été porté préalablement à sa connaissance.
Art. L1222-4 du code du travail. Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.

Information et la consultation préalable du comité d'entreprise
Art. L.2323-32 du code du travail. Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci.

10.5 Détection intrusion

Insuffisante en elle-même, la détection d'intrusion doit s'appuyer et être complémentaire avec la protection mécanique, sous peine de voir son efficacité grandement diminuée.
La détection électronique consiste en une mise en œuvre de moyens décelant et réagissant à des changements d'états dans les zones, accès ou objets à surveiller.

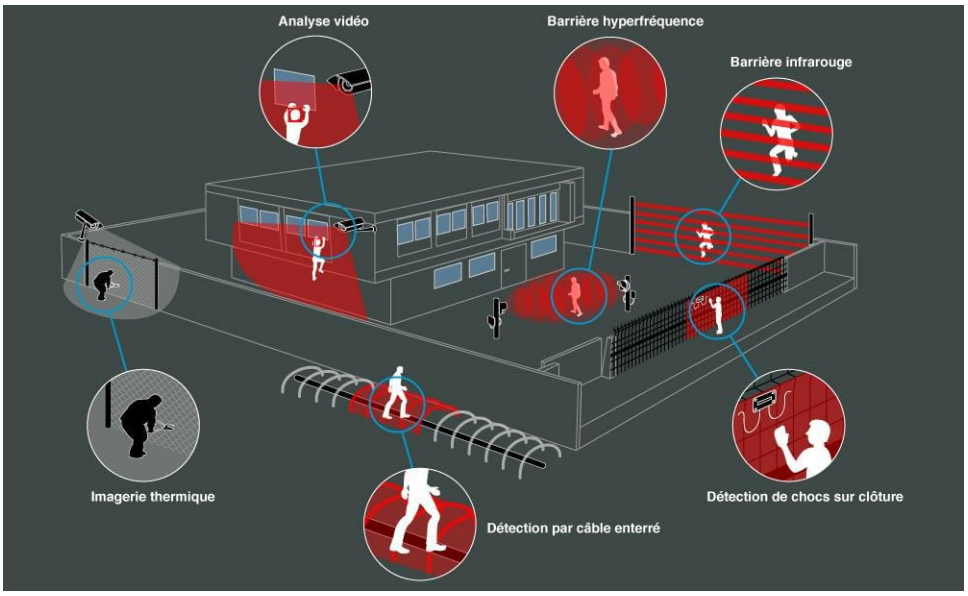
Lorsqu'un détecteur anti-intrusion se déclenche (mouvement ou ouverture ou choc), une alerte est alors envoyée au PC de sécurité du site ou du télésurveilleur afin qu'une levée de doute soit effectuée soit physiquement par un agent de sécurité ou soit vidéo et/ou audio.

Il existe de nombreuses manières de détecter une intrusion

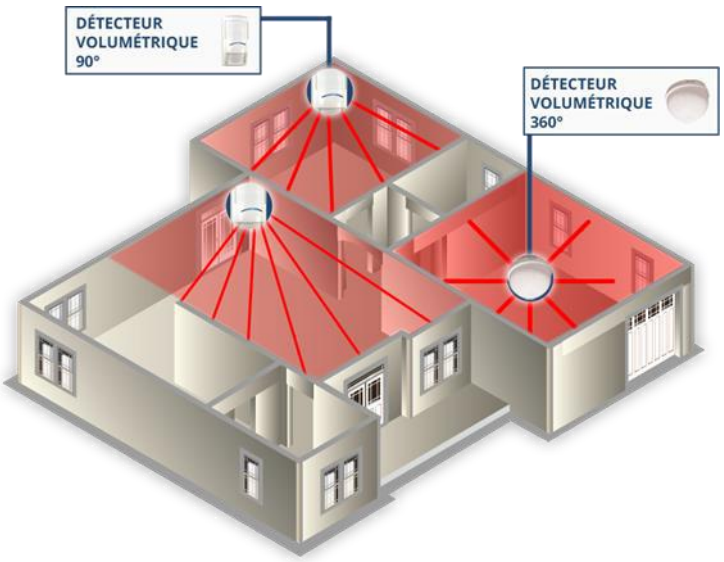
Les dispositifs les plus connus sont les détecteurs d'ouvertures, les détecteurs de choc et les détecteurs de mouvement et de passage sans fil ou avec fil, les barrières infrarouges qui déclenchent une alerte lorsqu'elles sont franchies.
Il est également possible de détecter une intrusion via un choc contre une fenêtre ou via l'utilisation de sabots sous une porte.

Le système doit détecter toute intrusion humaine au plus tôt dans le périmètre surveillé :

- Au moment de la tentative d'intrusion
- Dès l'intrusion réalisée
- Avant d'être neutralisé ou détruit
- Au pire, en cas de destruction ou de neutralisation, une alarme d'autoprotection doit être générée (sécurité positive).



Une panne du système ou d'un élément de la chaîne locale doit déclencher une information de défaut.



10.6 Vidéosurveillance-Vidéoprotection

Vidéoprotection, vidéosurveillance, quelle différence ?

Les dispositifs de vidéoprotection filment la voie publique et les lieux ouverts au public : rue, gare, centre commercial, zone marchande, piscine etc.

Les dispositifs de vidéosurveillance filment les lieux non ouverts au public : réserve d'un magasin, entrepôts, copropriété fermée etc.

Les dispositifs permettent d'assurer la sûreté d'une entité par la visualisation de zones observées en direct (action) ou en différé (réaction). Elle permet la surveillance et l'identification :

- ⇨ D'individus
- ⇨ De véhicules
- ⇨ D'objets

Objectif : Captation des images d'un espace défini avec ou sans enregistrement.
Zone de couverture : Périmétrique et/ou volumétrique
Lieu d'implantation : Dans les zones ouvertes au public, les lieux professionnels ou privés.

La vidéosurveillance ou la vidéoprotection a plusieurs fonctions, elle permet :

- ⇨ D'apprécier les situations,
- ⇨ De dissuader d'un passage à l'acte,
- ⇨ De détecter tout événement ou comportement anormal,
- ⇨ D'identifier un individu ou un véhicule et fournir des éléments aux enquêteurs.

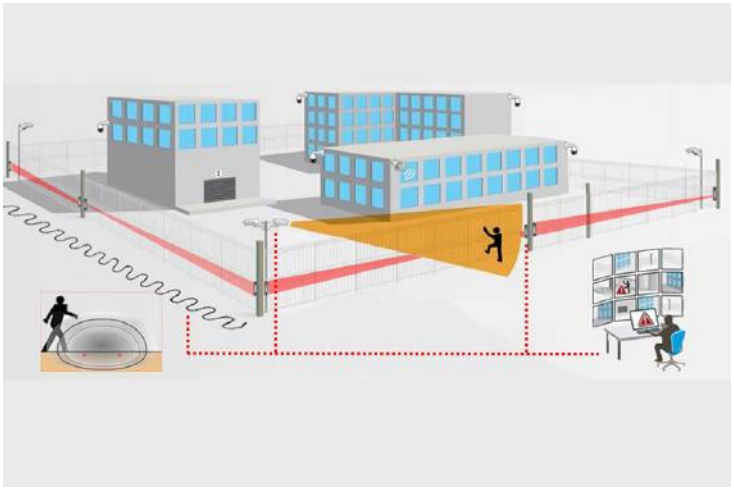
Une installation de vidéosurveillance permettra de déceler des situations anormales ou interdites, avant d'entamer une démarche de conception, il, importe d'identifier et préciser le rôle que jouera le système au sein de l'ensemble des mesures de sécurité.

- ⇨ Aider à la surveillance
- ⇨ Identifier l'origine d'un acte de malveillance
- ⇨ Lever de doute en cas d'alarme
- ⇨ Assister le contrôle de flux
- ⇨ Détecter le déplacement d'objets ou d'individus
- ⇨ Contribuer à la gestion de l'activité

Il s'agit d'un outil performant qui s'inscrit dans un plan d'ensemble de sûreté dont elle n'est qu'un des éléments et dans lequel l'homme se doit d'être présent, actif et réactif.
Le Code de la sécurité intérieure (CSI) précise les cas dans lesquels l'installation d'un système de vidéoprotection est soumise à autorisation préfectorale.

Conseils pour l'implantation

- La caméra doit être placée de manière à ne pas pouvoir être manipulée ou masquée facilement.
- Le câblage ne doit pas être apparent et accessible.
- Pour les caméras extérieures penser à les équiper d'un boitier garantissant l'étanchéité.
- Attention aux tolérances de température pour les caméras extérieures, en fonction de la région d'installation.
- Nettoyer régulièrement les caméras pour optimiser la qualité des enregistrements.
- Penser à positionner des caméras en plan large pour visualiser une scène sans oublier une captation en plan étroit au niveau des zones de passages obligées (entrée- accueil - caisses) pour réaliser de la reconnaissance d'individu.
- Privilégier un mode de fonctionnement à la détection en période d'inactivité sur le lieu de travail, vous économiserez de la mémoire d'enregistrement et les activations seront plus faciles à repérer.
- Prendre en considération de nombreux critères environnementaux, comme l'éclairage (phares, soleil), la vitesse de déplacement des objets ou personnes filmées, la végétation et son développement....
- Un enregistrement de mauvaise qualité ne peut pas être amélioré par la suite.
- Eviter la compression des images qui sont enregistrées car l'exploitation sera moins efficace voire impossible.
- La qualité de la lumière sur la zone à vidéoprotéger ou vidéosurveiller doit être prise en compte.
- L'activation de spots à la détection de mouvements améliorera le rendu de l'enregistrement, va créer une gêne pour le délinquant, permettra aux forces de l'ordre une intervention plus efficace et en cas de prise en main à distance sera un bon moyen de communiquer encore des renseignements à la police ou à la gendarmerie.
- L'enregistreur doit impérativement être installé à l'abris des regards dans un lieu protégé pour éviter sa destruction volontaire ou son vol lorsqu'un acte de malveillance est commis.
- Réfléchir aux éventuelles évolutions du système vidéo car les enregistreurs permettent la connexion de 4, 8, 16 ou 32 caméras (Le terme voie est employé). Il est parfois judicieux de pouvoir faire évoluer son matériel à moindre frais.



CNIL/RGPD Vos obligations légales :

Lorsque vous décidez de mettre en place un système de vidéos surveillance ou de vidéoprotection vous devez respecter certaines obligations.

Si le dispositif est installé sur la voie publique ou dans un lieu ouvert au public, il faudra faire une déclaration auprès de la préfecture et ce en rédigeant l'imprimé CERFA N°13806*03 et joindre les documents utiles.

- ⇨ Particularité pour les banques il s'agit de l'imprimé CERFA 14095-02

Après étude de la commission départementale de la conformité du système à la réglementation en vigueur, une autorisation sera accordée par le préfet.

- ⇨ En cas de modification de l'installation, il faudra en aviser cette commission.

La durée de conservation des données enregistrées est comprise entre 0 et 30 jours.
En fonction de l'activité, une réflexion doit être apportée à la durée.

Il est obligatoire d'informer les employés et les visiteurs avant qu'elles ne rentrent dans un espace vidéo protégé via un affichage visible par le public sur lequel sera mentionné le moyen de contacter la personne en charge de l'accès aux images.
Pour les systèmes vidéosurveillance qui filment un lieu non ouvert au public (lieux de stockage, zones dédiées au personnel, salle de coffre etc.) : aucune déclaration à la CNIL n'est nécessaire.

Attention !

Demander conseil et assistance à votre Délégué à la protection des données (DPO), si vous en avez un.
Vérifier, en fonction de votre projet, si vous devez effectuer une analyse d'impact sur la protection des données (AIPD).
Inscrire votre fichier dans le Registre des activités de traitement tenu par votre société.
Informer vos employés et visiteurs des conditions dans lesquelles vous traitez leurs données.
Prévoir des mesures de sécurité adaptées au regard des risques.
Si le dispositif conduit à "la surveillance systématique à grande échelle d'une zone accessible au public", une analyse d'impact doit être effectuée.

Quelle est la loi qui régit l'usage de la vidéo surveillance ?

Loi informatique et libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004, puis par la loi du 20 juin 2018 relative à la protection des données personnelles et réécrite par l'ordonnance n° 2018-1125 du 12 décembre 2018 applicable au 1er juin 2019. Lieu public ou lieu privé ouvert au public.

10.7 Les drones

La sécurité privée combine les moyens traditionnels et les outils technologiques.
La vidéo surveillance a ainsi permis de surveiller un site depuis un poste de contrôle.
Les systèmes de drones ajoutent l'atout de la mobilité aux caméras fixes, afin de projeter un œil déporté dans tous les endroits, quelque soit la taille du site.

Conditions d'utilisation restrictives

Les capacités d'observation discrète, d'acquisition et de transmission de données en masse posent les questions du respect de la vie privée et des libertés individuelles.

Cadre réglementaire général

- Les conditions d'utilisation,
- Les exigences pour les opérateurs,
- Les équipements du drone,
- Les conditions de télé pilotage,
- Les conditions d'insertion des drones dans l'espace aérien.

Des interdictions absolues de survol sont en vigueur pour les aérodromes, les sites sensibles ainsi qu'une interdiction générale pour la ville de Paris.
Globalement, la technologie est très avancée mais le droit est très restrictif.

10.8 Approche méthodologique des installations des systèmes de sûreté

Pour garantir une installation de chacun des systèmes de vidéosurveillance/vidéoprotection, de contrôle d'accès et de détection intrusion adaptée à ses besoins, une démarche méthodique, ordonnée et systématique doit être appliquée à toutes les installations comprises en **4 phases** :

Phase 1 : Analyse de risque

- Consiste à cerner les besoins, à partir de l'identification claire des valeurs importantes pour le demandeur (et éventuellement le prescripteur), des menaces, des scénarios associés, du contexte, de l'environnement dans lesquels sont situées ces valeurs (vulnérabilité) et des autres contraintes éventuelles.

Phase 2 : Conception

- Consiste à proposer les solutions techniques aptes à répondre aux besoins identifiés en phase 1 en fournissant le niveau de surveillance adapté aux scénarios et aux valeurs dans le respect des règles applicables, avec prise en compte des contraintes économiques.
- L'offre proposée par l'installateur matérialise cette phase.

Phase 3 : Réalisation de l'installation

- Débute à la réception de la commande par l'installateur. Elle comporte la réalisation de l'installation, le contrôle et la mise en service, la formation, l'assistance des utilisateurs et la réception de l'installation.
- Sa conclusion se matérialise par la remise du dossier technique de l'installation réalisée comprenant le PV de réception et l'établissement de la déclaration correspondante.

Phase 4 : Maintenance

- Correspond à toute la période d'activité de l'installation.
- Elle a pour objet de maintenir en bon état le système installé et de veiller à son adaptation au besoin dans le respect des exigences de la règle.

10.9 Préconisations face à la menace malveillante

- Création ou renforcement de la fonction sûreté
- Mener une étude pour le site en prenant en compte les menaces particulières du secteur d'activité
- Déplacement des équipements sensibles et réorganisation des stockages
- Mise en place de mesures préventives pour éviter les atteintes au milieu naturel
- Sensibilisation et formation du personnel
- Ajout ou renforcement de protections mécaniques (Clôtures, grillage, serrure, etc.)
- Ajout ou renforcement de la surveillance humaine
- Ajout ou renforcement de la détection électronique anti-intrusion, vidéosurveillance/vidéoprotection, télésurveillance
- Ajout ou renforcement des systèmes de contrôle d'accès (identification et authentification dans les zones sensibles)

Mais surtout
Lien avec les services de tutelles (Municipalité, SDIS, Sécurité Civile, Police/Gendarmerie.)

ORGANISATION

- Désigner un responsable sûreté, connu de l'ensemble des salariés, chargé de la rédaction des procédures et du contrôle de la mise en œuvre.
- Prendre en compte les risques liés à l'environnement immédiat : le voisinage, les bâtiments adjacents, etc.
- Identifier les flux d'entrées et de sorties au sein de l'entreprise (personnes, informations, marchandises, fluides/énergies, etc.).

- Hiérarchiser les zones à protéger en fonction des risques, des acteurs, du fonctionnement de l'entreprise, et adapter les mesures de sécurité en conséquence. Eviter de placer les zones les plus sensibles dans des locaux trop vulnérables.
- Réglementer l'accès aux différentes zones en fonction des nécessités réelles de chacun.
- Établir un journal des incidents, des reports et alertes.
- Sensibiliser régulièrement les personnels aux règles de sécurité du site et prévoir les formations adaptées en y associant les sociétés prestataires de services et les partenaires aux dispositifs internes de protection des locaux.
- Évaluer périodiquement la performance du système de contrôle d'accès : audits internes, exercices, tests d'intrusion, vérification des délais d'intervention, etc.
- Centraliser les systèmes de sûreté (contrôle d'accès, détection d'intrusion, vidéo surveillance) au sein du poste central de sécurité sous la supervision du responsable de la sûreté.
- Prévoir une gestion rigoureuse des clés et badges d'accès.

11.MISE EN PLACE ET ORGANISATION DE LA SURVEILLANCE DES RISQUES DE L'ENTREPRISE

11.1 Organisation humaine de la Surveillance

Missions et moyens du service de surveillance (surveillance de l'ensemble du site, contrôle d'accès applicable à l'établissement et aux locaux, enregistrement des alarmes, diffusion des alarmes et alertes, consignes spécifiques et générales, interventions (levées de doute et intervention sur alarme, rondes), accueil des secours, mesures d'urgences(POI(SEVESO), vol à main armée, attentats, intoxications …etc.), la formation pratique tutorée en binôme…etc.),exercices et tests archivés dans le registre de surveillance.

11.2 Composantes techniques et organisationnelles liées à la Surveillance

Gestion des flux (consigne décrit : règle de circulation (obligations & interdictions), règles à respecter, infos obligatoires).

Installation concourant à la protection du site et à la détection d'évènements participant à la maîtrise des vulnérabilités dans :

- ⇨ Le domaine incendie : *D.I, protection par sprinklers, asservissement de fermeture des *PCF.
- ⇨ Le domaine technique : Détection/coupure/mise en sécurité.
- ⇨ Le domaine Sûreté/Malveillance : les moyens pour dissuader, retarder, détecter et intervenir.

11.3 Suivi, maintien et amélioration de la Surveillance

Moyens matériels (suivi & disponibilité des moyens matériels, entretien des équipements (maintenance préventive planifiée, contrôleur de ronde, DATI, Main courante, consignes, plans, dispositifs permettant de recevoir les informations d'alarme, des moyens de diffusion de l'alarme et moyens d'alerte, système portatif de réception des alarmes…)

Intervention rapide suite à tous dysfonctionnements d'une fonction de surveillance (mise en place d'une gestion en mode dégradé, définir le délai maxi acceptable de la perte de fonction (conséquences des vulnérabilités identifiées & coûts des mesures compensatoires),

Être en capacité de présenter l'état du suivi et de la maintenance des installations de la surveillance.

***D.I :** Détection Incendie
***PCF :** Porte Coupe-Feu

11.4 Installations concourant à la protection du site et à la détection des évènements

Les moyens de détections et de protection des installations peuvent être associés :

Au domaine incendie (détection incendie, protection des sprinklers, asservissement des PCF…)
Au domaine technique (des asservissements « détection/coupure-mise en sécurité »)

Au domaine de la sûreté malveillance
- Dissuader
- Retarder
- Détecter
- Intervenir

Les installations : Protection du site + détection des évènements
Organisation et diffusion Alarme & Alerte

⇨ **Former les personnels à la reconnaissance des alarmes.**

Alarme & alerte

Transmission par communication orale (de vive voix ou par téléphone) ou une chaine d'alarme électronique.

Détection et exploitation des alarmes Intrusion
- Détection intrusion
- Contrôle d'accès
- Vidéosurveillance
- Installations Techniques & alarmes techniques

Centralisation des alarmes : Les informations doivent être reportées vers une des zones connues et accessible de différentes personnes devant les exploiter, idéalement vers le poste de centralisation des alarmes (Accès restreint aux seules personnes autorisées).

Poste de contrôle et de surveillance (PCS)
- Détection et exploitation des alarmes
- Centralisation et exploitation des alarmes
- Confidentialité des informations à traiter
- Accès restreint aux infos et traitements associé

Moyens d'alerte : Autonomes (ligne téléphonique directe sans passage par AUTOCOM), fiables, disponibles en permanence et testés régulièrement suivant une procédure établie.

12.ETUDE DE SÛRETE ET DE SECURITE PUBLIQUE (ESSP)

Les opérations d'aménagement et de construction sont pour certaines aujourd'hui soumises à l'obligation de réaliser une étude de sûreté et de sécurité publique afin que l'aménagement urbain participe à sa hauteur à la coproduction de sécurité.
Les pratiques déjà menées montrent que la prise en compte de la sécurité, loin d'être à considérer comme une simple contrainte technique, représente une véritable plus-value pour le projet.
La réflexion sur les usages des futurs espaces publics ou collectifs, l'anticipation de la gestion ultérieure ou transitoire, l'étroite collaboration avec la maîtrise d'œuvre urbaine sont des éléments stratégiques pour y parvenir.
Elles permettent d'anticiper les risques de malveillances et d'en limiter les effets.
Elles ont pour objectif de réduire les risques de sécurité publique et de faciliter le déploiement des missions de prévention, de protection, d'intervention et d'assistance des services de sécurité publique et de secours.
Les Etudes de sûreté et de sécurité publique (ESSP) sont réalisées par des tiers, les ESSP sont évaluées par le référent sûreté avant d'être validées par la sous-commission départementale de sécurité publique.

Code de l'urbanisme Article R114-1

Sont soumis à l'étude de sécurité publique prévue à l'article L. 114-1 :

1° Lorsqu'elle est située dans une agglomération de plus de 100 000 habitants au sens du recensement général de la population :
a) L'opération d'aménagement qui, en une ou plusieurs phases, a pour effet de créer une surface de plancher supérieure à 70 000 mètres carrés ;
b) La création d'un établissement recevant du public de première ou de deuxième catégorie au sens de l'article R. 123-19 du code de la construction et de l'habitation ainsi que les travaux et aménagements soumis à permis de construire exécutés sur un établissement recevant du public existant de première ou de deuxième catégorie ayant pour effet soit d'augmenter de plus de 10 % l'emprise au sol, soit de modifier les accès sur la voie publique.
Les dispositions ci-dessus s'appliquent également aux établissements d'enseignement du second degré de troisième catégorie ;
c) L'opération de construction ayant pour effet de créer une surface de plancher supérieure ou égale à 70 000 mètres carrés.
2° En dehors des agglomérations de plus de 100 000 habitants au sens du recensement de la population, les opérations ou travaux suivants :
a) La création d'un établissement d'enseignement du second degré de première, deuxième ou troisième catégorie au sens de l'article R. 123-19 du code de la construction et de l'habitation ;
b) La création d'une gare ferroviaire, routière ou maritime de première ou deuxième catégorie ainsi que les travaux soumis à permis de construire exécutés sur une gare existante de même catégorie et ayant pour effet soit d'augmenter de plus de 10 % l'emprise au sol, soit de modifier les accès sur la voie publique.
3° Sur l'ensemble du territoire national, la réalisation d'une opération d'aménagement ou la création d'un établissement recevant du public, situés à l'intérieur d'un périmètre délimité par arrêté motivé du

préfet ou, à Paris, du préfet de police, pris après avis du conseil local de sécurité et de prévention de la délinquance ou à défaut du conseil départemental de prévention, et excédant des seuils définis dans cet arrêté.
4° Sur l'ensemble du territoire national : celles des opérations des projets de rénovation urbaine mentionnés à l'article 8 du décret n° 2004-123 du 9 février 2004 relatif à l'Agence nationale pour la rénovation urbaine comportant la démolition d'au moins 500 logements déterminées par arrêté du préfet ou, à Paris, du préfet de police, en fonction de leurs incidences sur la protection des personnes et des biens contre les menaces et agressions.

Code de l'urbanisme Article R114-2

L'étude de sécurité publique comprend :
1° Un diagnostic précisant le contexte social et urbain et l'interaction entre le projet et son environnement immédiat ;
2° L'analyse du projet au regard des risques de sécurité publique pesant sur l'opération ;
3° Les mesures proposées, en ce qui concerne, notamment, l'aménagement des voies et espaces publics et, lorsque le projet porte sur une construction, l'implantation, la destination, la nature, l'architecture, les dimensions et l'assainissement de cette construction et l'aménagement de ses abords, pour :
a) Prévenir et réduire les risques de sécurité publique mis en évidence dans le diagnostic ;
b) Faciliter les missions des services de police, de gendarmerie et de secours.
L'étude se prononce sur l'opportunité d'installer ou non un système de vidéoprotection.
Dans les cas où une étude de sécurité publique est exigée en raison de travaux ou aménagements sur un établissement recevant du public existant, le diagnostic prévu au 1° ne porte que sur l'interaction entre le projet et son environnement immédiat. Si une étude a été réalisée depuis moins de quatre ans pour le même établissement, elle est jointe au dossier de demande de permis de construire, la nouvelle étude ne portant alors que sur la partie de l'établissement donnant lieu à modification de plus de 10 % de l'emprise au sol ou modifiant les accès sur la voie publique.

*Source Légifrance

13.LE REFERENT SÛRETE

Les référents sûreté sont des policiers ou des gendarmes, choisis pour leur bonne connaissance des modes opératoires des délinquants, capables de fournir des conseils de vigilance et de protection auprès des établissements sensibles, des commerçants à risques et des collectivités territoriales.

Le référent sûreté de la gendarmerie et de la police sont des personnels ayant bénéficié d'une formation spécifique en matière de prévention technique de la malveillance.

Ils sont présents dans chaque département, en métropole et outre-mer, appuyés localement par des correspondants sûreté.

Quel est leur rôle ?

- La sensibilisation à la prévention technique de la malveillance : conseils génériques lors de forums, salons, réunions, ou prises de contact sur site.
- La consultation de sûreté : conseils formulés oralement au demandeur.
- Le diagnostic de sûreté : document écrit comportant des préconisations de sûreté humaines, organisationnelles et techniques sur un site exposé à un risque particulier.
- L'audit de sûreté : étude écrite approfondie élaborant une stratégie de mise en sûreté globale sur un site présentant un intérêt stratégique et opérationnel pour la gendarmerie et l'Etat.
- Les Etudes de Sûreté et de Sécurité Publique (ESSP) sont évaluées par le référent sûreté avant d'être validées par la sous-commission départementale de sécurité publique.
- Le diagnostic de vidéoprotection : le référent sûreté peut conseiller les collectivités territoriales dans la mise en place d'un dispositif de vidéoprotection. Son avis est requis pour l'attribution d'une subvention du fonds interministériel de prévention de la délinquance.
- La prévention des tueries de masse ou des actes terroristes : le référent sûreté évalue les dispositifs existants ou dispense des conseils permettant de renforcer la protection des sites.
- La sécurité du transport de fonds : le référent sûreté représente la gendarmerie au sein des commissions départementales de sécurité des transports de fonds.

14.REGLEMENT, CLAUSES, REGISTRES, CONSIGNES, BREVET ET PROCEDURES

14.1 Le règlement intérieur

Le règlement intérieur est un document créé par l'employeur **(Articles L1321-1 à L1321-6 du code du travail)**.
Il est le pouvoir normatif et disciplinaire de l'entreprise, ce qui n'est pas notifié peut-être considéré comme autorisé.

Procédure de mise en place du règlement intérieur

Etape 1	**Consultation, des représentants du personnel** CSE ou CE, DP, CHSCT	
Etape 2 Communication du règlement intérieur à l'inspection du travail	**Simultanément**	**Etape 3** Dépôt au conseil de prud'hommes et affichage dans l'entreprise
Etape 4	**Entrée en vigueur** 1 mois à compter de l'accomplissement des étapes 2 et 3	

Depuis le 1er janvier 2020, un **règlement intérieur** doit être établi dans les entreprises et établissements employant au moins **50 salariés** (c. trav. art. L. 1311-2).
Le seuil de 50 salariés doit avoir été atteint pendant 12 mois consécutifs.
Avant cette date, l'obligation concernant les entreprises de plus de 20 salariés.

Dans les entreprises employant moins de 50 salariés, l'établissement d'un règlement intérieur est facultatif.

Il fixe les règles de conduite dans l'entreprise en matière de santé et de sécurité.
Il définit aussi les règles concernant la discipline et notamment la nature et l'échelle des sanctions que peut prendre l'employeur.
Une sanction disciplinaire autre qu'un licenciement ne peut être prononcée que contre un salarié que si elle est prévue par le règlement intérieur.

Le règlement intérieur doit contenir exclusivement :

- Les mesures d'application de la réglementation en matière de santé et de sécurité dans l'entreprise ou l'établissement
- Les conditions dans lesquelles les salariés peuvent être appelés à participer, à la demande de l'employeur, au rétablissement des conditions de travail protectrices de la santé et de la sécurité, quand elles apparaissent compromises ;
- Les règles générales et permanentes relatives à la discipline et, notamment, la nature et l'échelle des sanctions disciplinaires que peut prendre l'employeur.

S'agissant des sanctions disciplinaires -autres que le licenciement disciplinaire, le règlement intérieur fixe les règles générales et permanentes relatives à la discipline, notamment la nature des sanctions applicables aux salariés et l'échelle des sanctions.

Les sanctions disciplinaires peuvent consister en :

- Un blâme,
- Un avertissement oral,
- Un avertissement écrit,
- Une mutation disciplinaire,
- Une rétrogradation,
- Une mise à pied disciplinaire.

Le degré et la nature de la sanction varie en fonction de la gravité des faits devant être sanctionnés.

- Une sanction autre que le licenciement ne peut être prononcée contre un salarié que si elle est prévue par le règlement intérieur ;
- Une mise à pied disciplinaire prévue par le règlement n'est licite que si ce règlement en précise la durée maximale.

Depuis le décret du 20 octobre 2016, l'article R 1321-1 du Code du travail dispose que « Le règlement intérieur est porté, par tout moyen, à la connaissance des personnes ayant accès aux lieux de travail ou aux locaux où se fait l'embauche ».
Ainsi, les salariés se verront appliqués valablement le règlement intérieur dès l'instant où ils en ont eu connaissance, par tous moyens, dans les locaux de l'entreprise.
L'information peut donc se faire par n'importe quel procédé désormais.

14.2 Le livret d'accueil sécurité

Le livret d'accueil sécurité constitue un outil indispensable pour les salariés présents et pour accueillir au mieux le nouveau salarié.
Il permet notamment de regrouper les informations délivrées lors de l'accueil du nouvel embauché.

Ainsi le code du travail précise que : L'employeur informe les travailleurs sur les risques pour leur santé et leur sécurité d'une manière compréhensible pour chacun. Cette information ainsi que la formation à la sécurité sont dispensées lors de l'embauche et chaque fois que nécessaire.
Tout nouvel embauché doit recevoir, à la fois, un accueil et une formation à la sécurité au poste.
Le code du travail parle de formation pratique et appropriée (Article L4141-2 du code du travail).
Pour les salariés (CDD et CDI), les intérimaires, les stagiaires, apprentis, c'est au dirigeant ou au Référent Sécurité et Santé au Travail de s'organiser pour qu'ils aient les informations utiles à la préservation de leur santé au travail.

Bon nombre d'entreprises répondent à leurs obligations en matière de sécurité et santé au travail, mais n'ont pas le temps de former les salariés aux consignes de sécurité définies dans le document unique et ses annexes.

Lors de l'embauche, elles omettent généralement de préciser l'existence du document unique, du règlement intérieur, ou bien le lieu où peuvent être consultés les affichages obligatoires.

Le dirigeant a une obligation d'information et de formation concernant les règles de sécurité qui doivent être appliquées dans l'entreprise. Pour cela, il doit logiquement s'appuyer sur le contenu du document unique, si celui-ci a été établi avec soin.

Dans les faits, bon nombre de dirigeants négligent cette formation par manque de temps, à tel point que les salariés ne connaissent même pas, la plupart du temps, l'existence du document unique pourtant prépondérant pour la sécurité du personnel.

Le livret d'accueil, correctement réalisé, contient une quantité d'informations utiles permettant de se substituer à la formation obligatoire concernant la sécurité au poste de travail et plus généralement dans l'entreprise si le dirigeant se rend compte qu'il ne pourra, personnellement, dispenser une formation en bonne et due forme.

Le livret d'accueil sécurité permet au salarié d'avoir accès aux informations suivantes. Présentation et organigramme de l'entreprise, nombre de salariés par type de poste, comment réagir lorsqu'une défaillance liée à la sécurité est constatée, où et comment consulter le DUER, analyse de la pénibilité, des RPS, où et comment consulter le règlement intérieur, que faire en cas d'incendie, que faire en cas d'accident du travail d'un autre salarié, risque routier, règles de vigilance au travail. Ces informations, non exhaustives, donnent néanmoins un aperçu de ce que doit contenir le livret d'accueil sécurité.

Code du travail
Article L4141-2
Version en vigueur depuis le 01 mai 2008
L'employeur organise une formation pratique et appropriée à la sécurité au bénéfice :
1° Des travailleurs qu'il embauche ;
2° Des travailleurs qui changent de poste de travail ou de technique ;
3° Des salariés temporaires, à l'exception de ceux auxquels il est fait appel en vue de l'exécution de travaux urgents nécessités par des mesures de sécurité et déjà dotés de la qualification nécessaire à cette intervention ;
4° A la demande du médecin du travail, des travailleurs qui reprennent leur activité après un arrêt de travail d'une durée d'au moins vingt et un jours.
Cette formation est répétée périodiquement dans des conditions déterminées par voie réglementaire ou par convention ou accord collectif de travail.

Article R4141-2
L'employeur informe les travailleurs sur les risques pour leur santé et leur sécurité d'une manière compréhensible pour chacun.
Cette information ainsi que la formation à la sécurité sont dispensées lors de l'embauche et chaque fois que nécessaire.

14.3 Le registre santé sécurité au travail

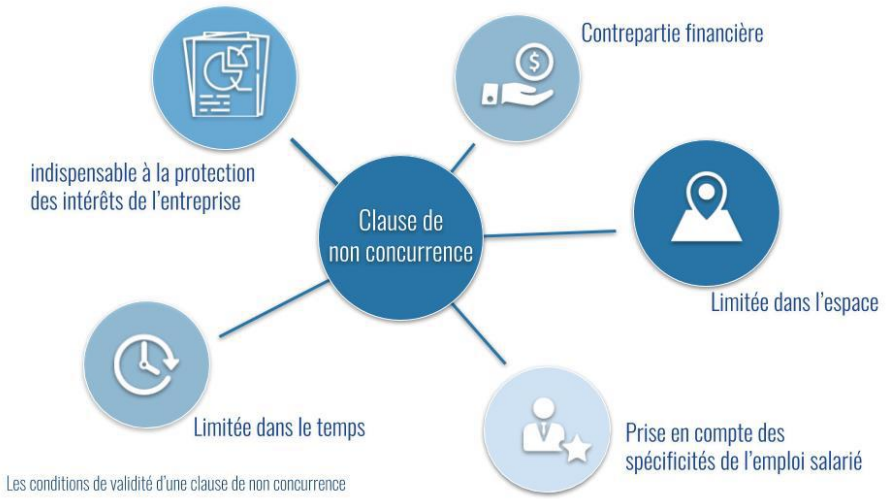
Le Registre de santé et sécurité au travail contient les observations et suggestions des agents relatives à la prévention de risques professionnels et à l'amélioration des conditions de **travail** (art 3.1 du décret n°85-603 du 10 juin 1985 modifié).

Depuis la parution du décret du 03 février 2012, le registre « d'hygiène et de sécurité » est dénommé registre de « santé et de sécurité au travail ». Seule l'appellation a été modifiée, le contenu et la finalité du registre ne changent pas.
Le registre, prévu par la réglementation (art. 3-1 du décret n°85-603 du 10 juin 1985 modifié), est un outil mis à disposition de tous les agents et des usagers des sites dans chaque service ou bâtiment.
Ce registre est destiné à signaler toute observation et/ou suggestion relative à l'amélioration de la santé, de la sécurité et des conditions de travail. Il est consulté régulièrement et tenu à jour par l'assistant de prévention et / ou le conseiller de prévention en relation avec l'autorité territoriale. Il est mis à la disposition de l'ACFI (Agent Chargé de la Fonction d'Inspection dans le domaine de la santé et de la sécurité au travail) et du CT/CSE.
Le Comité d'Hygiène, de Sécurité et des Conditions de Travail, à défaut le Comité Technique (CT) est tenu informé des observations et suggestions consignées sur le registre (article 48 du décret n°85-603 du 10 juin 1985 modifié).

14.4 Clause de non-concurrence

1/ Le principe
La clause de non-concurrence vise à limiter la liberté d'un salarié d'exercer, après la rupture de son contrat, des fonctions équivalentes chez un concurrent ou à son propre compte.

2/ Les critères de validité
La validité d'une clause de non-concurrence est liée au respect de cinq conditions cumulatives. S'il en manque une, la clause est frappée de nullité.



Les conditions de validité d'une clause de non concurrence

Être indispensable à la protection des intérêts légitimes de l'entreprise
L'obligation de non-concurrence ne peut pas être généralisée. Elle peut être imposée à des salariés dont les connaissances techniques ou commerciales risqueraient de causer à l'employeur un préjudice important si elles étaient mises au service d'une entreprise concurrente. Il en va de même si les fonctions du salarié l'ont amené à être en contact direct et suivi avec la clientèle.

Être limitée dans le temps
L'atteinte à la liberté du travail du salarié ne peut être générale. Elle doit donc être proportionnée au risque posé par le départ du salarié.
Être limitée dans l'espace
Le secteur géographique où s'applique l'interdiction de concurrence doit être précisément défini sous peine d'entraîner la nullité de la clause de non-concurrence. Il faut en effet que le salarié connaisse dès la conclusion de son contrat les endroits où il lui sera temporairement impossible de retravailler.

Tenir compte des spécificités de l'emploi du salarié
Le salarié ne doit pas se retrouver dans l'impossibilité absolue d'exercer une activité professionnelle conforme à ses aptitudes et connaissances générales et à sa formation professionnelle. C'est pourquoi la clause de non-concurrence doit précisément définir les interdits faits au salarié après la rupture de

son contrat de travail, sachant que cette restriction doit être en relation avec l'activité de l'entreprise mais aussi avec celle du salarié.

Comporter une contrepartie financière

La clause de non-concurrence doit prévoir une contrepartie financière (ou indemnité compensatrice) pour le salarié. L'employeur verse une indemnité au salarié en contrepartie de son engagement à ne pas lui faire concurrence. Si le salarié ne respecte plus la clause, l'employeur peut interrompre le versement de la contrepartie.

Cette contrepartie est due quel que soit l'auteur de la rupture (employeur ou salarié) ou les circonstances de la rupture. Il n'est donc pas possible d'exclure de contrepartie financière en cas de démission du salarié ou en cas de licenciement pour faute grave ou lourde.

Cette contrepartie peut prendre la forme d'un capital ou d'une rente, elle doit être versée après la rupture du contrat de travail, et non pendant son exécution. La contrepartie doit être raisonnable, une contrepartie dérisoire équivaut à une absence de contrepartie financière, et n'est donc pas valable. Son montant est compris entre le quart et la moitié du salaire mensuel moyen versé au salarié.

14.5 La clause de confidentialité

La clause de confidentialité interdit au salarié de divulguer certaines informations qui lui ont été communiquées pendant son travail.

Le secret doit être gardé non seulement à l'égard des personnes extérieures à l'entreprise, mais aussi en interne.

Lorsque des professionnels concluent un contrat commercial, un partenariat ou tout autre type de contrat, ils peuvent être amenés à communiquer des informations dites “sensibles” sur leurs entreprises (identité des clients, stratégie commerciale, situation économique et financière de l’entreprise, secret de fabrique, savoir-faire, etc.).
La divulgation de ces données à des tiers pourrait compromettre ou nuire au développement de leur entreprise.
Pour se protéger de ce risque, les parties peuvent insérer une clause de confidentialité à leur contrat commercial.

La clause de confidentialité doit être distinguée de la clause de non-concurrence qui vise à limiter la possibilité pour une entreprise d’exercer une activité similaire à celle de son partenaire commercial.

La clause de confidentialité peut-être :

- ⇨ Bilatérale : c’est le cas si les deux partenaires s’échangent des données secrètes. Ici, l’obligation de confidentialité s’applique aux deux parties.
- ⇨ Unilatérale : c’est l’hypothèse où un seul des partenaires communique des informations sensibles. Alors, l’obligation ne s’applique qu’à une seule des parties.

Cette obligation de confidentialité s’applique pendant toute la durée de l’exécution du contrat.
Toutefois, la clause de confidentialité peut aussi s’appliquer dans le cadre des négociations précontractuelles, notamment dans le cas où les pourparlers n'aboutiraient pas à la conclusion d’un contrat.
A ce stade des négociations, puisqu’aucun contrat n’est encore conclu entre les parties, on ne parle pas de clause de confidentialité mais d’accords de confidentialité.

Bon à savoir : même si le terme « accord » suppose une certaine réciprocité entre les parties, il existe aussi des accords de confidentialité unilatéraux.
Par ailleurs, la clause de confidentialité peut aussi continuer de s’appliquer même une fois que le contrat a pris fin (on dit qu’il a été exécuté).

14.6 Agir en temps utile pour protéger la confidentialité de l’information

L’entreprise qui souhaite protéger ses secrets d’affaires, veillera à intervenir en temps utile pour ce faire. Elle veillera notamment à :

- Ne pas attendre l’entrée en fonction du sous-traitant pour lui faire signer un accord de non-divulgation ;
- Ne pas attendre pour demander à l’employé qui démissionne de restituer tous les documents confidentiels en sa possession (restituer l’ordinateur de travail, clôturer ses comptes d’accès, etc.).

Former ses travailleurs à respecter les informations confidentielles

Le salarié est *ipso facto* tenu par une obligation de confidentialité, du fait de son contrat de travail. Cependant, si le travailleur évente le secret par mégarde, le manque de formation pourra être imputé à son employeur.
Il est donc utile de fournir une formation à ceux des travailleurs qui sont en contact avec des informations confidentielles. Il s'agit notamment d'éviter :

- Que les techniciens laissent traîner sur des serveurs non-sécurisés (voir, sur leur site internet), des informations sensibles
- Que les commerciaux ne communiquent trop d'informations pour convaincre un client potentiel
- Que les chercheurs de l'entreprise ne publient des informations sensibles, même dans des publications scientifiques.

Contrôler l'accès aux informations confidentielles

L'entreprise veillera à contrôler *l'accès interne* aux informations confidentielles. Ceci implique de :

- Restreindre l'accès physique à certains sites (badges, clefs, …)
- Restreindre l'accès à certains fichiers informatiques (profils individuels, temps de connexion limité aux données confidentielles, …)
- Éviter qu'une personne (travailleur ou tiers) n'ait accès à *l'intégralité* d'un procédé ou d'une formule si ceci n'est pas nécessaire à la réalisation de son travail.

L'entreprise veillera également à contrôler *l'accès externe* aux informations confidentielles. L'espionnage industriel est une réalité. Toute entreprise se doit de sécuriser ses données (pare-feu, anti-virus, cryptage, …) et de former ses travailleurs à exercer la meilleure des vigilances en ligne.

Recenser les informations confidentielles

Toutes les informations ne sont pas confidentielles. Or, seul le « vol » de données *confidentielles* est sanctionné ; les autres informations sont dans le domaine public et peuvent être véhiculées librement. Afin de protéger au mieux ses secrets d'affaire et éviter toute contestation devant le Tribunal en cas d'éventuel procès il est recommandé d'identifier clairement *a priori* les données qui sont considérées comme confidentielles.

Ceci peut se faire de plusieurs manières :

- Faire porter la mention « confidentiel » sur tel ou tel document ;
- Consigner précisément les informations les plus importantes dans un registre interne sur les secrets d'affaires.

Contrôler la chaîne de production

Conclure des accords de non-divulgation est indispensable, mais ne suffit pas toujours.
Il est utile de se réserver le droit de vérifier que celui qui s'engage à respecter la confidentialité des données qui lui sont confiées prend effectivement toutes les précautions nécessaires, pour ce faire Il est donc conseillé de se réserver le droit d'auditer les précautions prises par ses sous-traitants (en termes contractuels ou d'organisation interne).

Revoir régulièrement la politique de protection de l'entreprise

Trop souvent, la protection de secrets d'affaires n'est examinée qu'à des moments charnières de la vie d'une société (ex. : création, lancement d'un nouveau partenariat, mise en place de nouvelles infrastructures informatiques, etc.).

Or, au fur et à mesure, les activités et méthodes de production de l'entreprise évoluent. Les procédures de protection doivent être adaptées. Idéalement, l'entreprise veillera à :

- Assurer un suivi régulier et un réexamen au moins annuel des procédures de protection ;
- Confier la responsabilité de la protection des secrets d'affaires à une personne ou à une équipe précise (éventuellement par l'intervention d'équipes pluridisciplinaires (juriste, technicien, informaticien, etc.).

14.7 Charte informatique

La charte informatique est un instrument juridique qui définit les conditions générales d'utilisation des systèmes d'information et de communication, de l'accès à Internet, aux divers réseaux et systèmes d'information de l'entreprise ou encore à ses services multimédias.
La mise en place d'une charte informatique dans une entreprise permet de fixer les règles d'utilisation des outils informatiques par les salariés, mais aussi de prévoir des sanctions en cas de violation de ces règles. Sa mise en œuvre est par ailleurs recommandée par la Commission Nationale de l'Informatique et des Libertés (CNIL).
Généralement intégrée au règlement intérieur de la société (ou rajoutée en annexe de ce règlement), la charte informatique peut aussi être intégrée au contrat de travail (la première solution est toutefois préférée).

14.8 Protéger la propriété industrielle de son activité

Ne pas se faire voler une idée, une marque, un concept innovant ou un modèle, pouvoir en bénéficier en exclusivité en France, voire à l'étranger, asseoir sa réputation ou encore combattre la contrefaçon, sont autant de raisons de protéger ce qui fait la spécificité de votre entreprise.
Il s'agit de protéger des actifs dits immatériels : avancée scientifique, création esthétique, identité visuelle, dénomination sociale de l'entreprise, etc.

La propriété industrielle vise à protéger et à valoriser les inventions, les innovations et les créations. Pour bénéficier de cette protection, une création doit faire l'objet d'un dépôt auprès de l'INPI.

Qu'est-ce que la propriété industrielle ?

La propriété industrielle constitue l'une des deux composantes de la propriété intellectuelle avec la propriété littéraire et artistique.
La propriété industrielle a pour objet de protéger et valoriser les inventions techniques telles que la création d'un nouveau procédé ou d'un produit innovant ou bien les créations ornementales telles que les dessins et modèles ou encore les signes distinctifs tels que les marques, les noms de domaine, les dénominations sociales.
La protection offerte par la propriété industrielle consiste à conférer à un créateur un monopole d'exploitation de son œuvre pendant une certaine durée.

Comment protéger une création grâce à la propriété industrielle ?

La protection offerte par les droits de propriété industrielle nécessite d'effectuer un dépôt.
Les inventions, les créations et les innovations ne peuvent faire l'objet d'une protection au titre de la propriété industrielle qu'après accomplissement de cette formalité par l'auteur de l'invention, de la création ou de l'innovation. Les dépôts de marque, de brevet ou de dessin et modèle s'effectuent auprès de l'Institut nationale de la propriété industrielle (INPI).
Le créateur d'une invention ou d'une innovation, d'une marque ou d'un modèle bénéficie, après ce dépôt, des droits de propriété industrielle sur son œuvre : il peut alors l'exploiter de manière exclusive, la protéger de toute utilisation ou reproduction par un tiers et en tirer des revenus.

Les différents types de dépôts auprès de l'INPI

Pour protéger une innovation technique telle qu'un procédé ou un produit, son créateur doit déposer un brevet auprès de l'INPI. Ce dépôt lui confère alors des titres de propriété industrielle sur sa création. Ces titres permettent au créateur de bénéficier d'un monopole d'exploitation de sa création pendant vingt ans.
Une marque peut aussi faire l'objet d'un dépôt auprès de l'INPI. Le créateur d'une marque s'assure ainsi de préserver le monopole du nom de sa marque pendant dix ans renouvelables.
Pour protéger un dessin ou un modèle, son auteur peut déposer son œuvre auprès de l'INPI. Ce dépôt lui offre alors un monopole d'exploitation pendant une durée de cinq ans renouvelables.
Le dépôt d'un brevet, d'une marque ou encore d'un dessin donne lieu au paiement, par l'auteur, d'une redevance annuelle dont le montant diffère selon la nature du dépôt.
Source JDN

Organisationnel

Comment protéger son savoir et ses idées ?

- ⇨ Identifier, parmi les différents titres de propriété intellectuelle (brevets, marques, dessins et modèles, droits d'auteur, etc.) ceux qui sont les mieux adaptés pour protéger et valoriser ses innovations, ses produits ou ses créations immatérielles.
- ⇨ Avant de déposer une marque, un dessin et modèle ou un brevet, vérifier auprès de l'Institut national de la propriété industrielle (INPI) la disponibilité du droit à protéger (recherches d'antériorité) pour s'assurer du caractère nouveau de la création. Examiner la nécessité de se faire assister d'un conseil en propriété intellectuelle.
- ⇨ Identifier les marchés (national, communautaire, international), présents et futurs, sur lesquels protéger ses droits. Si des droits sont présents à l'international, se renseigner auprès du réseau d'experts à l'international (Douanes, INPI, Business France, conseillers du commerce extérieur, CCI Innovation, etc.).
- ⇨ Enregistrer ses droits auprès des offices compétents (INPI, l'Office de l'Union européenne pour la propriété intellectuelle, EUIPO ; l'Office européen des brevets, OEB ; l'Organisation mondiale de la propriété intellectuelle, OMPI).
- ⇨ Faire enregistrer les noms de domaine liés aux titres et à l'activité commerciale auprès de l'Agence française pour le nommage sur internet en coopération (AFNIC).

Quelles démarches adopter pour se prémunir de la contrefaçon ?

- ⇨ Mettre en place une veille, notamment sur internet, afin de détecter et de se prémunir des contrefaçons.
- ⇨ Déposer une demande d'intervention auprès des Douanes qui permettra de mettre en retenue des marchandises suspectées d'être contrefaisantes et d'alerter le propriétaire du droit. Cette demande gratuite est valable un an renouvelable.
- ⇨ Protéger ses créations par une confidentialité stricte des documents relatifs aux droits et aux produits : signature de clauses de confidentialité, protection physique et numérique des documents, etc.
- ⇨ Faire immédiatement opposition auprès de l'INPI, ou de tout autre office compétent, dès qu'une personne dépose un droit déjà détenu par l'entreprise. Examiner sans délai la nécessité de se faire assister d'un avocat ou d'un conseil en propriété intellectuelle.

Quelle attitude adopter en cas de contrefaçon ?

- ⇨ Mettre en demeure le contrefacteur de cesser les actes de contrefaçon en lui envoyant un courrier lui rappelant ce qu'il encourt à enfreindre les droits de propriété intellectuelle en question.
- ⇨ Communiquer aux autorités compétentes, en particulier aux Douanes, les informations dont dispose l'entreprise sur la contrefaçon : circuit de fraude, identité des contrefacteurs, caractéristiques des marchandises contrefaites, etc.

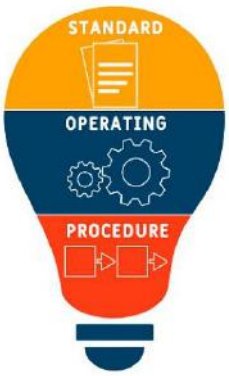
INPI : l'Institut national de la propriété industrielle, établissement public placé sous la tutelle des ministères Économiques et Financiers, est l'organisme compétent pour la délivrance des titres de propriété industrielle nationaux (marques, brevets, dessins et modèles).

EUIPO : l'Office de l'Union européenne pour la propriété intellectuelle est l'agence de l'Union européenne compétente pour l'enregistrement des marques et des dessins ou modèles valables dans les pays de l'UE.

OEB : l'Office européen des brevets offre aux inventeurs une procédure uniforme de demande de brevet, leur permettant d'obtenir une protection par brevet dans un maximum de 40 pays européens.

OMPI : l'Organisation mondiale de la propriété intellectuelle permet d'enregistrer ses marques, dessins et modèles à l'échelle internationale.

AFNIC : l'Association française pour le nommage internet en coopération est une association loi 1901 en charge de la gestion des extensions françaises d'internet.



14.9 Procédures SOP (Standard Operating Procedure) ou procédures opérationnelles normalisées

La procédure opérationnelle normalisée est une procédure de sécurité sûreté qui décrit comment affronter un risque et en réduire l'effet.
Pour évaluer le risque il faut tenir compte de deux paramètres ; mesurer le niveau de la menace, et détecter les vulnérabilités.
Une menace est une action ou un événement potentiellement négatif facilité par une vulnérabilité qui entraîne un impact indésirable sur un système ou une organisation.
Une fois ces deux éléments pris en compte on peut agir pour en diminuer ou supprimer les effets, les conséquences.
Le SOP décrit les étapes à suivre pour réduire la possibilité qu'un incident se produise et s'il se produit ce qu'il faut faire pour en limiter les conséquences.

14.10 POI ou Plan d'Opération Interne

À la demande de l'administration, pour certaines installations soumises à autorisation ou obligatoirement pour les installations soumises à servitudes, le chef d'établissement doit établir un Plan d'Opération Interne ou POI.
L'objectif du POI est de faire face à un accident et de protéger le personnel, les biens et l'environnement de l'établissement.
Le POI doit être rédigé en prenant en compte les éléments contenus dans l'étude des dangers (notamment les scénarios d'accidents) et désigne pour l'établissement, un responsable de son application et un personnel qualifié pour son exécution.
Les installations « SEVESO » doivent établir un POI avant la mise en service, le mettre à jour et les tester au maximum tous les 3 ans.

Les plans d'urgence et le POI sont des outils opérationnels d'aide à la décision utilisables en interne et par les secours extérieurs lors de la survenance d'un sinistre.

Le plan d'Opération Interne (POI) est le plan d'urgence réglementaire, au sens de l'article R.512-29 du code de l'environnement, il est applicable à certaines ICPE (Installation Classée pour la Protection de l'Environnement).

- ICPE soumise à autorisation et certains cas particuliers : entrepôts couverts de produits combustibles de plus de 50 000 m2 et dépôts de papiers et cartons de de 100 000 m3.
- Un ensemble de textes sont parus en septembre 2020 puis 2021 pour renforcer l'usage et les exigences associées au POI par suite de l'accident de Lubrizol.

Le POI décrit les règles d'organisation, les moyens en place et disponibles sur un site industriel afin de minimiser les conséquences d'un sinistre potentiellement majeur pour les personnes, l'environnement et les biens.
L'élaboration du document « POI » se fait dans une logique volontairement déterministe.
Il prend comme hypothèses l'apparition d'événements pouvant conduire à des accidents de type « scénarii majorants ».
Le POI n'a pas pour vocation dans sa structure et sa logique à être exhaustif et à fournir des éléments de réponses techniques et organisationnels à tous les accidents pouvant survenir sur un site.

Le POI se focalise donc sur la maîtrise des accidents « significatifs et représentatifs » pouvant survenir, de types incendie, explosion, épandage de produits liquides, dispersions atmosphériques de substances toxiques,...
Pour chacun de ces accidents, il sera déterminé :

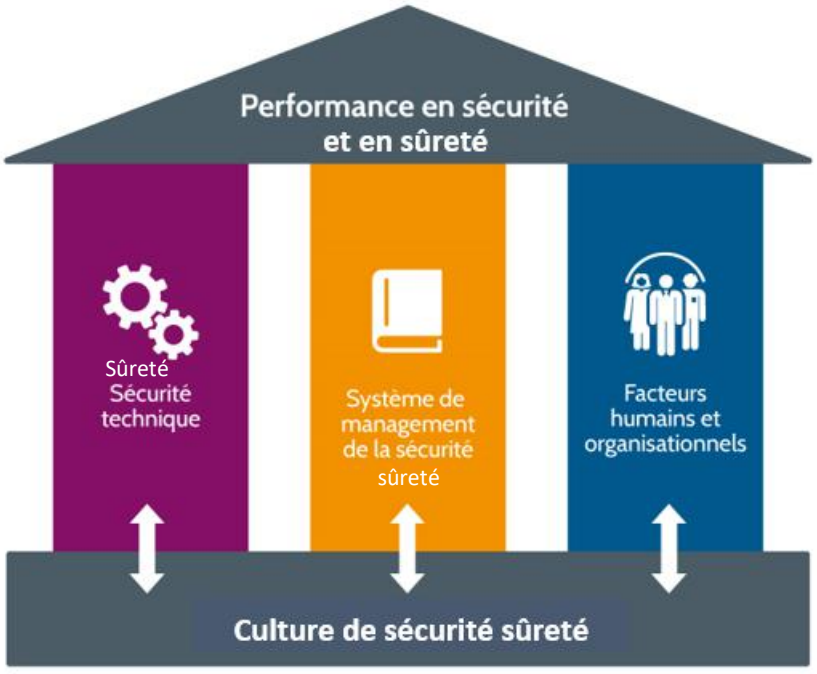
- Les modalités de détection des accidents,
- Les moyens et l'organisation à mettre en œuvre permettant la suppression ou la limitation d'accidents (extinction, confinement, etc.),
- Les extensions possibles de l'accident vers d'autres installations (dont les effets dits "dominos").

14.11 Plan de sûreté

En complément des mesures de prévoyance déjà en place pour couvrir le risque accidentel, les pouvoirs publics ont décidé de renforcer et de contrôler les mesures de sûreté sur les sites SEVESO y compris en rattachant certains d'entre eux à un SAIV (Secteur d'Activité d'Importance Vital).

Si la démarche de sûreté (gestion des actes malveillants) partage avec celle de la sécurité (gestion des actes accidentels) une logique semblable - analyse de risque initiale, rédaction de plans adaptés, préparation à la crise - l'approche en est néanmoins rendue très différente car elle repose sur la prise en compte du facteur humain et non de métriques :

- Les intentions, objectifs et modalités du passage à l'acte ont des origines de nature très différentes : vengeance, appât du gain, raisons idéologiques, revendicatives, etc.
- Leurs conséquences peuvent être non décelables sur l'instant comme les vols de produits ou d'informations sensibles ;
- Elles peuvent se dérouler dans les champs matériels et physiques, immatériels et logiques ou faire l'objet d'une combinaison des deux ;
- La conduite de l'alerte, de l'évacuation ou de la mise à l'abri du personnel peuvent être différentes des procédures de mise en sécurité de type évacuation consécutif à un accident industriel (incendie, etc.) telles que définies dans le Plan d'Opération Interne.



14.12 PPI (Plan Particulier d'Intervention)

Le plan particulier d'intervention est un dispositif local défini en France pour protéger les populations, les biens et l'environnement, pour faire face aux risques particuliers liés à l'existence d'une ou de plusieurs installations industrielles.
Le terme désigne également le document qui définit le dispositif.

14.13 Plan Particulier de Mise en Sûreté (PPMS)

Le PPMS, ou « Plan Particulier de Mise en Sûreté » est un dispositif règlementaire dont l'objectif est de mettre en place une organisation interne à l'établissement afin d'assurer la mise en sécurité de toutes les personnes présentes dans l'établissement en cas d'accident majeur externe à l'établissement.
La circulaire n° 2002-119 du 29 mai 2002 publié au BO EN Hors-Série n° 3 règlemente la mise en place du PPMS dans les établissements scolaires.

Un événement majeur est un événement d'origine naturelle, technologique ou humaine, qui cause de très graves dommages à un grand nombre de personnes, aux biens et à l'environnement.
Ce peut être une tempête, une inondation, un nuage toxique, un séisme, un accident nucléaire ou une intrusion dans l'établissement ...
L'objectif principal du PPMS est de mettre en place une organisation interne à l'établissement permettant d'assurer la sécurité des élèves et des personnels, jusqu'à la fin de l'alerte ou l'arrivée des secours

Ce plan définit notamment des lieux de confinement répartis dans le lycée, les procédures conservatoires devant être mises en place, et les conseils de gestion de la crise, dans l'attente de l'intervention des secours.

Le PPMS doit ainsi permettre de répondre aux 6 questions suivantes :

- Quand déclencher l'alerte ?
- Comment déclencher l'alerte ?
- Où et comment mettre les élèves en sûreté ?
- Comment gérer la communication avec l'extérieur ?
- Quelles consignes appliquer dans l'immédiat ?
- Quels documents et ressources sont indispensables ?

LE PLAN DE SÉCURITÉ DES ÉCOLES, DES COLLÈGES ET DES LYCÉES

Prévenir les menaces et accompagner efficacement les écoles, collèges et lycées, pour assurer la sécurité des élèves et des personnels de l'éducation nationale.

DANS LES ÉCOLES, COLLÈGES ET LYCÉES

- Organisation de 3 exercices de sécurité dont un exercice attentat-intrusion
- Apprentissage des premiers secours et gestes qui sauvent

DANS LES GENDARMERIES OU COMMISSARIATS DE POLICE

- Réseau de correspondants « Police & gendarmerie, sécurité de l'École »
- Renforcement des patrouilles mobiles

DANS LES DIRECTIONS DÉPARTEMENTALES DE L'ÉDUCATION NATIONALE

- Un référent sûreté par département
- Des correspondants « éducation nationale » dans les cellules de crise préfectorales

DANS LES PRÉFECTURES

- État-major départemental de sécurité consacré à la protection des espaces scolaires
- Un exercice cadre de gestion de crise

DANS LES RECTORATS

- Cellules académiques de gestion de crise
- Un référent sûreté par académie
- Un exercice alerte SMS à destination des directeurs d'école et des chefs d'établissement

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

14.14 Plan de Sûreté Opérationnel ou PSO

Le Plan de sûreté opérationnel est un outil indispensable à la sécurisation de ses sites et de ses collaborateurs se trouvant à l'étranger en cas d'incident sécuritaire.
Il permet d'identifier l'émergence de situations sécuritaires plus ou moins complexes, et d'adapter les mesures adoptées en fonction du niveau de risque atteint.

Votre devoir de protection en tant qu'employeur

L'employeur est tenu d'informer les salariés qu'il envoie en mission à l'étranger sur les conditions sanitaires et sécuritaires du pays. Il s'agit de mettre l'accent sur la prévention et la sensibilisation : consignes de sécurité, informations pratiques, formation interculturelle…

L'obligation d'information

L'entreprise doit garantir la sécurité de ses salariés à l'étranger. Il existe non seulement une obligation générale de sécurité édictée dans le Code du travail mais aussi une obligation de sécurité de résultat, due à l'existence du contrat de travail. Dans certains cas, le manquement à cette obligation constitue une faute inexcusable de l'employeur.

Le PSO assure la pérennité de l'entreprise y compris en temps de troubles, en protégeant ses sites et ses collaborateurs, rendant ainsi possible un retour rapide à l'activité une fois l'incident sécuritaire passé.

Il doit contenir un certain nombre d'informations :

- Cartographie et fiches signalétiques des sites et lieux d'intérêt (hôtels, points de rassemblement, etc.) ;
- Cartographie et fiches signalétiques des résidences des expatriés ;
- Numéros d'urgence (externes et internes) ;
- Liste du matériel d'évacuation ;

14.15 Sûreté des ressortissants à l'étranger

En matière de sécurité et de défense, les ministères sociaux s'appuient sur les recommandations du plan Vigipirate (SGDSN). Ce plan comporte un objectif spécifique visant à « protéger les ressortissants et les intérêts français à l'étranger ». Dans ce cadre, le service qui déclenche la mission vérifie les conditions de sécurité, en croisant plusieurs sources d'information :

⇨ Les recommandations ministérielles : le haut fonctionnaire de défense et de sécurité (HFDS) des ministères sociaux coordonne l'exécution du plan Vigipirate de vigilance, de prévention et de protection. Il peut adresser des notes d'alerte de sécurité concernant certains pays aux directions et structures des ministères sociaux ;

- ⇨ Les missions diplomatiques : elles sont les lieux de convergence de toutes les informations et capacités d'action en cas de menace à l'étranger. Elles apportent leur expertise sur chaque pays et assurent la liaison, entres autres choses, avec les ressortissants français et les autorités politiques locales. Des notes de sécurité sont produites pour informer des risques du pays ;
- ⇨ Les pages http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/ du site Internet du *MAEDI fournissent des « Conseils par pays » pour préparer votre voyage.

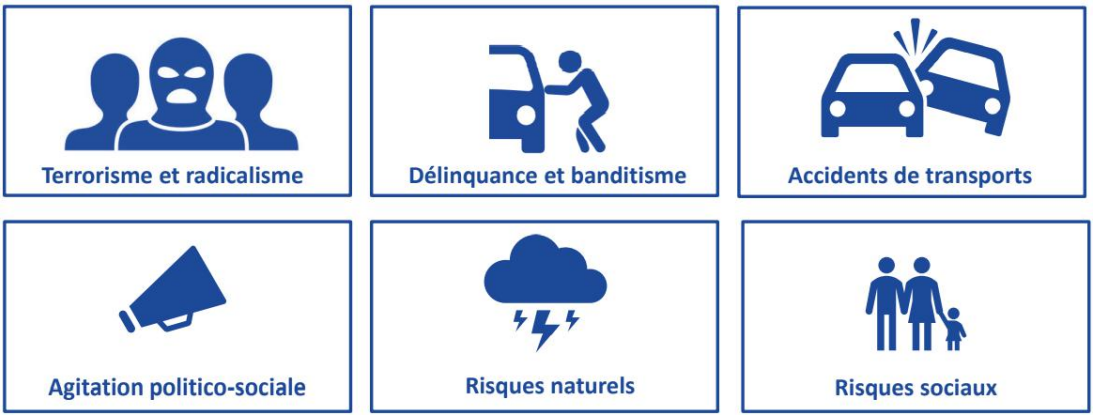
***MAEDI :** Ministère des Affaires Etrangères et du Développement International.

Gestion des risques à l'étranger : Les mesures à mettre en place

Missions professionnelles à l'étranger, détachement de salariés à l'international, expatriations… Dans un contexte d'internationalisation croissante des entreprises, les salariés deviennent de plus en plus mobiles. L'employeur est alors tenu d'informer et de protéger ses collaborateurs à l'étranger : il s'agit d'évaluer les risques encourus et de tout mettre en œuvre pour les maîtriser au mieux. La nécessité de protection de ses salariés expatriés, bien plus qu'une simple considération éthique, est une obligation : la responsabilité juridique de l'employeur est aujourd'hui bien réelle.

Bonnes pratiques et bons comportements lors de déplacements à l'étranger

- Comprendre le risque sûreté à l'international.
- Maîtriser la préparation d'un déplacement à l'étranger.
- Acquérir les bons comportements à l'étranger.
- Savoir sécuriser son déplacement.
- Appréhender la détection des anomalies et comportements atypiques ou suspects.
- Connaître les conduites à tenir en cas d'attaque.



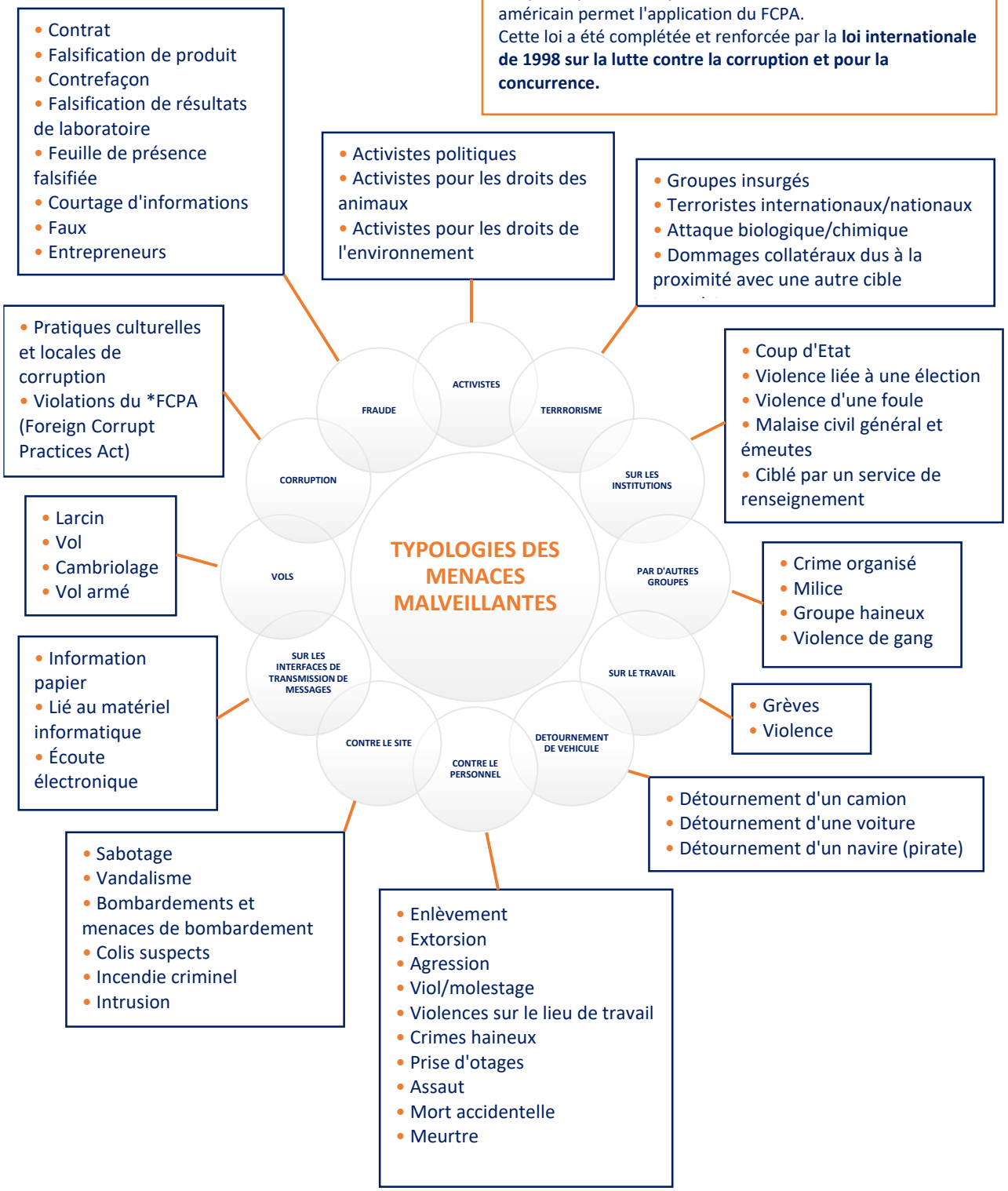
14.16 Bonne pratique de gestion du risque santé, sécurité et sûreté à l'international

		Avant le voyage	Pendant le voyage	Après le voyage
1.Politique santé et sécurité		Définir une politique : Objectif Organisation et allocation des responsabilités Plan et dispositions mis en place	Implémenter : Processus de gestion des incidents Processus garantissant la conformité	Réajuster : Revoir la politique et les processus périodiquement Adapter si nécessaire
2.Evaluation des risques et menaces identifiés		Evaluation continue des risques et menaces Sélection, implémentation et/ou ajustement des mesures de réduction des risques pour atteindre un niveau acceptable	Evaluation continue des risques et menaces Sélection, implémentation et/ou ajustement des mesures de réduction des risques pour atteindre un niveau acceptable	Evaluation continue des risques et menaces Sélection, implémentation et/ou ajustement des mesures de réduction des risques pour atteindre un niveau acceptable
3. Organisation Planification Implémentation	a. Information et conseil spécifiques : -Accès à des informations santé et sécurité avant le départ du collaborateur -Mise à disposition des guides d'information sur la destination -Accès à des alertes santé, sécurités ciblées		• Accès 24/7 à de l'expertise médicale et sécurité pendant le déplacement • Recommandations des prestataires médicaux et sécurité à l'étranger	• Accès à des conseils médicaux si la maladie s'est développée après le voyage • Accès à un soutien psychologique pos traumatique après un incident sécuritaire
	b. Formations et compétences : -Formations généralistes santé, sécurité et sûreté en déplacement -Formation premiers secours -Formation spécifique selon la destination ou la population ciblée			
	c. Aptitudes à voyager dont visite médicale : -Bilan de santé et de vaccination avant le départ		• Si nécessaire : examen ponctuel et/ou surveillance médicale	• Examen médical au retour de la mission • Procédure de validation de retour au travail après un séjour dans un pays à risque élevé
	d. Kits médicaux et sûreté : -Fourniture de kits médicaux de voyage (premiers secours, paludisme, etc.) -Vérification du stock de médicaments prescrits sous ordonnance		• Accès 24/7 à une hotline paludisme pour diagnostic et accompagnement dans le traitement	• Contrôle et réapprovisionnement des kits médicaux et sécurité de voyage après utilisation
	e. Gestion des urgences médicales et sécurité : -Définition d'un plan de gestion de crise santé et sécurité -Formation des managers et des employés aux plans d'urgence		• Accès 24/7 à une hotline santé et sécurité pour la prise en charge des urgences : hospitalisation, évacuation sanitaire, mise en sécurité	• Evaluation médicale et psychologique après le voyage • RETEX sur les cas urgents

		Avant le voyage	Pendant le voyage	Après le voyage
3. Organisation Planification Implémentation	f. Localisation et communication : -Information systématique du voyageur avant son départ avec confirmation de lecture -Identification systématique des voyageurs à destination de pays à risque -Identification systématique des déplacements à risque (VIP, nombre de collaborateurs sur le même vol, compagnie aérienne non recommandée, etc.) -Autorisation et vérification de la conformité des déplacements avec la politique de gestion des risques santé, sécurité et sûreté		• Système de localisation, géolocalisation et communication avec les voyageurs • Soutien intégré à la gestion des urgences	• Analyse statistique des déplacements à risque
4. Evaluation		• Reporting et évaluation des indicateurs de performance • Audit interne et externe • Intégration avec l'ensemble de la gestion des risques de l'entreprise (financement, actions préventives, etc.) • Intégration dans la stratégie globale de conformité		
5. Axes d'amélioration		• Implémentation des action correctives		

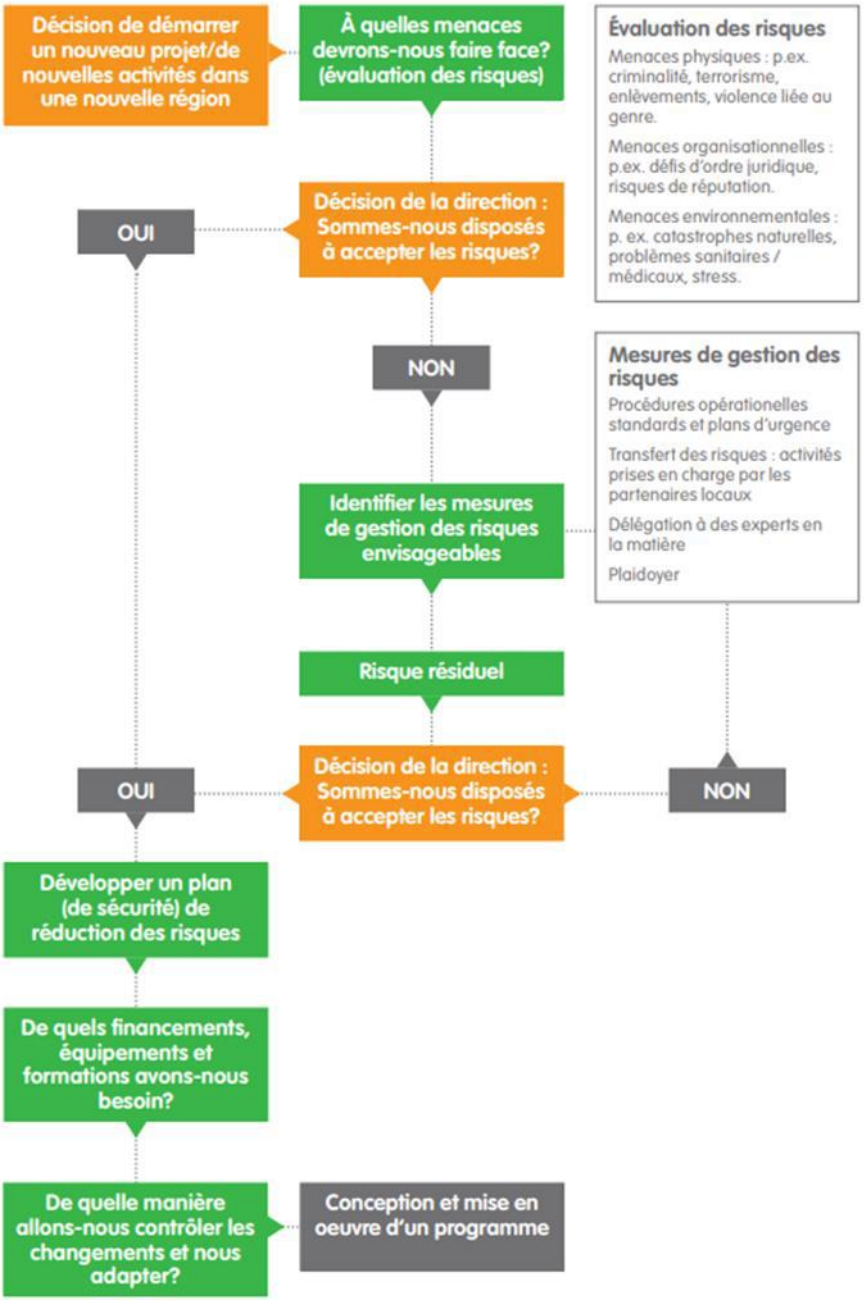
*Le **Foreign Corrupt Practices Act** (**FCPA**) est une loi fédérale américaine de 1977 pour lutter contre la corruption d'agents publics à l'étranger. Cette loi a un impact international. On parle d'extraterritorialité. Elle concerne l'ensemble des actes de corruption commis par des entreprises ou des personnes, américaines ou non, qui sont soit implantées aux États-Unis, soit simplement cotées en bourse sur le territoire américain ou qui participent d'une manière ou d'une autre à un marché financier régulé aux États-Unis. Elle est notamment mise en œuvre par l'Office of Foreign Assets Control.
Par extension, le simple fait d'avoir établi une communication téléphonique ou envoyé un courriel transitant via le territoire américain permet l'application du FCPA.
Cette loi a été complétée et renforcée par la **loi internationale de 1998 sur la lutte contre la corruption et pour la concurrence.**

Identification des menaces

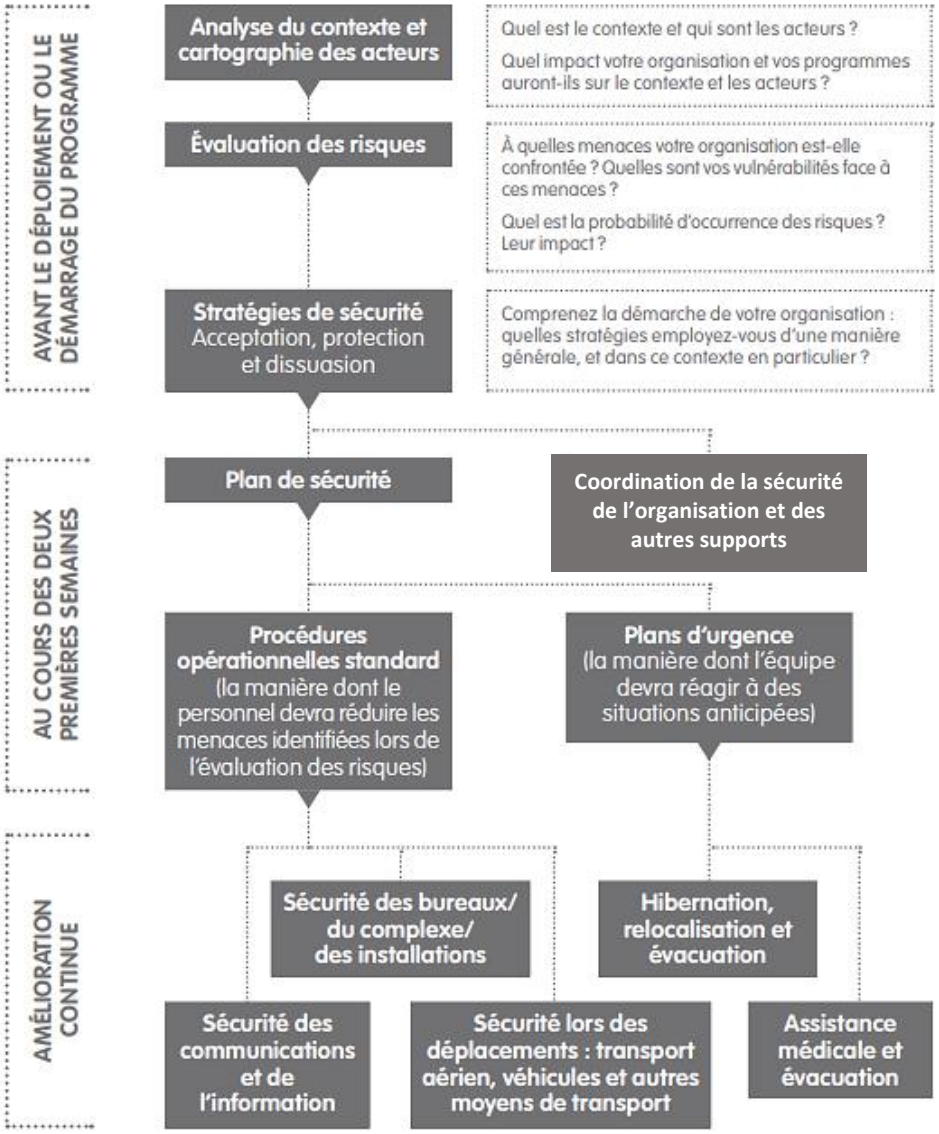


MENACES VIOLENTES	MENACES ORGANISATIONNELLES	MENACES ENVIRONNEMENTALES
Attaque armée ciblée	Risque de réputation	Risques naturels (météo, tremblements de terre, inondations, etc.)
Conflit armé non ciblé	Risque financier (système bancaire, échange de devises, vol, détournements de fonds)	Risques médicaux (possibilité pour le personnel d'avoir accès à des soins adaptés)
Enlèvement	Risque informationnel (information détenues ou émises par l'entreprise)	Risque pandémique
Terrorisme	Corruption	Risque sanitaire (maladies, nourriture, eau, stress)
Violence avec explosifs (mines anti personnels, EEI, bombardement)	Risques d'ordre juridique (permis de travail, couverture sociale, respect de la législation nationale, résistance au plaidoyer)	Accidents de la route
Piraterie routière et maritime	Risque politique	Autres types d'accidents
Violence sexuelle	Violence ou discrimination sur le lieu de travail	Incendies
Agitation civile	Défis d'ordre culturel	Autres
Violence religieuse	Autres	
Criminalité		
Guerre		
Autres		

De nombreuses entreprises se reposent le Plan d'évacuation étatique, mis en place et en œuvre par les autorités diplomatiques afin de sécuriser leurs ressortissants à l'étranger.
Néanmoins, ces dispositifs n'interviennent en majorité que lorsque la situation a atteint un point de non-retour, en dernier ressort.
A ce niveau de la crise, il est difficile d'assurer en toute sécurité et sereinement l'évacuation de l'ensemble des collaborateurs.
Le PSO propose donc l'établissement d'**un Plan d'évacuation gradué spécifique à l'entreprise**.
À chaque niveau de risque correspond un ensemble de mesures à mettre en œuvre pour préparer dans le temps et dans le calme l'ensemble des collaborateurs et leurs familles à quitter le pays.



Processus de planification de la gestion des risques



Rappel des coordonnées utiles

MAEDI :

-Twitter@conseilsVoyages
-Préparation de la mission **:** www.diplomatie.gouve.fr/fr/conseilsauxvoyageurs/
-Centre de crise et de soutien **:** alertes.cdc@diplomatie.gouv.fr
Tel : 33 (0)1 53 59 11 00
-Site internet Ariane : www.diplomatie.gouv.fr/ariane

ANSSI

www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/

SERVICE PUBLIC.FR (site internet officiel de l'administration française)

www.service-public.fr

ACRONYMES

- **ANSSI :** Agence nationale de la sécurité des systèmes d'information
- **BRHAG :** bureau ressources humaines et administration générale
- **CEAM :** carte européenne d'assurance maladie
- **DSAF :** direction des services administratifs et financiers
- **DRH :** direction des ressources humaines
- **DSI :** direction des systèmes d'information
- **HFDS :** haut fonctionnaire de défense et de sécurité
- **IAPR :** Institut d'accompagnement psychologique et de ressources
- **MAEDI :** ministère des Affaires étrangères et du Développement international
- **Ministères sociaux (MS) :** les quatre ministères, chargés respectivement des Affaires sociales et de la Santé, du Travail, de l'Emploi, de la Formation professionnelle et du Dialogue social, des Familles, de l'Enfance et des Droits des femmes, de la Jeunesse et des Sports)

15.CYBERSECURITE

15.1 Les risques liés à la mobilité

L'utilisation d'ordinateurs portables, de smartphones ou de tablettes ont rendu les déplacements professionnels et le télétravail plus simples.
Pour autant, l'utilisation de ces appareils font peser des menaces sur les informations sensibles de l'entreprise dont le vol ou la perte auraient des conséquences importantes sur ses activités.

Parmi ces risques, on trouve :

- Le piratage informatique sur un réseau wifi public ou un réseau mal sécurisé : un cyberattaquant peut rediriger ou intercepter le trafic dans le but de récupérer des informations sensibles.
  Il est également possible d'installer un malware et de prendre le contrôle des éléments physiques d'un ordinateur
- Le vol du matériel : le vol de matériel constitue un risque important pour les données de l'entreprise. Pour anticiper, la mise en place d'une sauvegarde et d'un chiffrement des données semblent être le minimum à configurer sur l'ordinateur du collaborateur.

15.2 Sensibiliser les collaborateurs

On considère que la faille de sécurité la plus importante est l'humain. Dans ce contexte, prévenir les risques via des sessions de sensibilisation et/ou de formation semble être indispensable.
Pour réduire son exposition, il est conseillé de transmettre les bonnes pratiques et les outils pour se protéger. Dans un premier temps, nous conseillons de rédiger une politique de sécurité interne. Ce document va recenser les risques auxquels votre entreprise peut faire face et comment s'en protéger.
Les collaborateurs doivent maîtriser parfaitement les outils, connaître les risques et les comportements à adopter en fonction de leur lieu de travail et des circonstances. La charte informatique de l'entité doit également intégrer les règles d'usage liées au nomadisme.

Le lieu de connexion du travailleur, qu'il soit nomade ou en situation de télétravail, est le premier environnement de risque : perte ou vol de matériel, compromission du matériel ou des informations contenues sur le matériel, accès illégitime au SI de l'entreprise, interception ou altération des informations (perte de confidentialité, d'intégrité).
Les lieux complètement ouverts au public représentent le plus fort risque : cafés, hôtels, zones d'attente pour les transports en commun…
Mais le domicile du « télétravailleur » ou l'espace de coworking présentent également un très haut niveau de risque, et quoiqu'il en soit toujours supérieur à celui encouru sur le site de l'entreprise.

15.3 Mettre en œuvre des moyens de protection physique de l'équipement d'accès nomade

L'entité doit mettre à disposition les moyens suivants pour protéger les équipements d'accès :

- Un filtre écran de confidentialité (pour les postes de travail, mais aussi pour les tablettes ou mobiles multifonction)
- Des scellés pour identifier une éventuelle compromission matérielle
- Des verrous de ports USB et RJ45 si nécessaire
- Éventuellement un câble antivol

Ensuite, intervient la protection de l'architecture globale d'un utilisateur nomade. Cette architecture se compose des éléments suivants :

- L'utilisateur nomade
- L'équipement d'accès ou poste de travail
- Le canal d'interconnexion
- La passerelle d'interconnexion
- Les ressources accessibles par les équipements nomades dans le système d'information interne de l'entreprise

*Architecture globale du nomadisme – Source : Guide de recommandation sur le nomadisme numérique ANSSI

Chaque élément doit faire l'objet d'une attention spécifique pour prévoir les mécanismes de protection adaptés et réduire les risques d'attaques potentielles.

L'utilisateur nomade : certaines catégories d'utilisateurs et certaines applications, du fait de leur sensibilité, doivent être exclues du périmètre du nomadisme. Chaque utilisateur devra être formé et sensibilisé pour limiter au maximum les situations de risque. Et idéalement, un équipement d'accès dédié sera attribué à un seul et unique utilisateur pour mieux maîtriser le risque.

L'équipement d'accès : que le terminal soit un ordinateur portable, une tablette ou un smartphone, Il est nécessaire de maîtriser complètement l'ensemble des équipements sur lesquels les utilisateurs nomades se connectent. Dans ce cadre, l'utilisation d'équipements personnels est à proscrire pour faciliter et fiabiliser le travail des équipes informatiques. Au-delà de cette première précaution indispensable, il est également nécessaire de prévoir les protections physiques pour limiter les vols et indiscrétions (filtre écran, verrou de ports, câble antivol) et de protéger au maximum les accès : contrôle d'intégrité au démarrage, chiffrement des disques, maîtrise de la connexion de supports amovibles, interdiction pour l'opérateur d'apporter des modifications aux moyens de connexion, verrouillage automatique de session en cas d'inactivité.

Le canal d'interconnexion : il s'agit du lien entre l'équipement d'accès et le SI de l'entreprise. Il est composé de :

- Un client logiciel situé sur l'équipement d'accès ;
- Un tunnel d'interconnexion VPN ;
- Un équipement de terminaison VPN.

Tous les flux en provenance et à destination de l'équipement d'accès doivent être maîtrisés. Il est donc important d'utiliser des mécanismes robustes de chiffrement, d'authentification et d'intégrité pour la mise en place du canal d'interconnexion d'un équipement d'accès nomade. Il est également impératif que l'utilisateur nomade ne puisse pas utiliser sa connexion réseau locale pour d'autres flux que ceux nécessaires à l'établissement du tunnel VPN.

15.4 Les authentifications

L'objectif est de s'assurer d'une part que l'utilisateur nomade est bien connecté sur un poste maîtrisé par l'entité, et d'autre part de vérifier l'identité et les droits d'accès de l'utilisateur avant sa connexion au SI interne de l'entreprise.
Plusieurs authentifications sont donc requises. En premier lieu l'utilisateur doit être authentifié sur son équipement d'accès, au démarrage de celui-ci.
Ensuite, l'équipement d'accès et l'utilisateur nomade doivent s'authentifier sur le SI de l'entité.
La DMZ (DMZ, signifie en anglais **D**e**M**ilitarized **Z**one, et en français **zone démilitarisée**) correspond à un sous-réseau, séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local. Les services susceptibles d'être accédés depuis Internet seront situés en DMZ, et tous les flux en provenance d'Internet sont redirigés par défaut vers la DMZ par le firewall. Le pare-feu bloquera donc les accès au réseau local à partir de la DMZ pour garantir la sécurité. En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local. Il est donc conseillé de prévoir des équipements physiquement dédiés au nomadisme dans la DMZ entrante ou a minima un cloisonnement logique performant.

15.5 Les ressources du système d'information de l'entreprise

Il est important de ne pas exposer d'applications métiers directement sur Internet pour conserver la maîtrise de l'information et le besoin de confidentialité. La connexion aux différentes applications métiers ne doit être possible que depuis le tunnel VPN, y compris la messagerie et malgré une demande importante et insistante des utilisateurs.
Il en est de même pour les applications internes déployées dans le Cloud.

15.6 L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)

Acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV).
Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

15.7 La Norme ISO 27001

La certification AFAQ ISO/IEC 27001 démontre que vous avez mis en place un Système de management de la sécurité de l'information (SMSI) efficace construit sur la base de la norme internationale de référence, l'ISO 27001.
Elle définit une méthodologie pour identifier les cybermenaces, maîtriser les risques associés aux informations cruciales de votre organisation, mettre en place les mesures de protection appropriées afin d'assurer la confidentialité, la disponibilité et l'intégrité de l'information.

16.SECURITE INCENDIE

La réglementation incendie participe à la sécurité des biens et des personnes dans les locaux commerciaux, industriels, d'habitation, les établissements recevant du public.

Les règles et les normes varient en fonction du type d'établissement concerné.

16.1 Réglementation de sécurité incendie

La réglementation en matière de sécurité incendie est la référence pour garantir la sécurité d'un établissement.

Il est indispensable de bien connaître les normes en vigueur, et ce dans le but d'éviter tout risque pour les personnes en cas de non-conformité.

Plusieurs typologies d'établissements sont concernés par ces réglementations : établissements recevant du public, habitations, écoles ou encore bureaux… il est donc d'autant plus important de les connaître pour être aux normes au regard de la loi.
La réglementation en matière de sécurité incendie est très vaste et est mise à jour régulièrement.

DIFFÉRENTS TEXTES ET NORMES DE SÉCURITÉ INCENDIE DANS LES ERT ET LES ERP

16.2 La réglementation incendie dans les ERT

Pour les établissements recevant des travailleurs (ERT), il convient de consulter les consignes de sécurité incendie dans le code du travail, complété par des textes satellites, appartenant par exemple au code de la construction et de l'habitation. Le code du travail se prononce sur la formation des personnels en incendie et la présence au moins d'un des membres du personnel ayant suivi un stage de sauveteur secouriste du travail (SST). Il n'existe pas de formation incendie obligatoire à proprement parlé, mais la formation des personnels à la sécurité incendie relève de l'obligation de l'employeur.

De même un exercice doit être effectué au moins tous les 6 mois pour permettre aux salariés d'acquérir les bons réflexes.

Les dates des exercices incendie ainsi que les éventuelles observations doivent être notées dans le registre sécurité de l'entreprise.

Le code du travail désigne l'employeur comme responsable du respect de la réglementation incendie au sein de son entreprise, au service de la protection des salariés.

Dans les ERT recevant également du publique la réglementation prévue au titre du code du travail est complétée par l'ensemble des normes ERP, généralement plus strictes.

16.2 La sécurité incendie dans les ERP

Dans les établissements recevant du public (ou ERP) s'appliquent les règles précisées dans le Code de la Construction et de l'habitation, dans le Code du Travail, dans le Code de l'Urbanisme et dans un ensemble de textes et circulaires complémentaires. Les mesures de sécurité incendie à mettre en œuvre dépendent ainsi d'une classification stricte des ERP.

Les normes ERP distinguent ainsi les ERP disposant d'un service d'hébergement, maisons accueillant des personnes âgées par exemple, ou établissement scolaire doté d'un internat (catégorie J), les établissements scolaires à accueil de jour (catégorie R), les administrations, les banques, les bureaux (catégorie W), etc. Chaque catégorie se doit de respecter la réglementation incendie propre à son type d'ERP, en tenant compte du nombre de personnes accueillies.

16.3 Les consignes de sécurité dans les IGH

Les IGH désignent les immeubles d'habitation dont la hauteur est comprise entre 28 et 50 mètres. Les dispositions de protection incendie prévues par la loi comprennent les obligations de vérification par des organismes agréés, les documents de contrôle à tenir à jour et à disposition, l'implantation et l'environnement des bâtiments, dont le volume de protection et les voies permettant l'accès des secours, les normes de construction.

Ces normes s'appliquent en particulier à la stabilité au feu, au statut des parois contiguës à d'autres constructions, au comportement des façades face au feu, ainsi qu'aux caractéristiques des couvertures.

La réglementation sur les immeubles à usage d'habitation précise les équipements à prévoir et la responsabilité des propriétaires et syndics.

En particulier, les normes visent à réglementer l'implantation des extincteurs, ainsi que la signalétique de protection incendie, qu'il s'agisse des plans d'évacuation des locaux ou des plans d'intervention, destinés eux aux secours.

Dans un feu, les fumées représentent un danger majeur de par leur opacité, leur chaleur, leur toxicité, leur risque d'explosion ainsi que leur mobilité.

Les incendies entraînent trois grands types de pathologies, les brûlures, les traumatismes liées à la chute de matériaux et à la fuite des victimes et les intoxications aux fumées.

Pendant très longtemps le risque toxique des fumées d'incendie a été sous-estimé.

80% des décès sont en relation avec l'inhalation de fumées toxiques.

16.4 Conséquences d'un incendie

LES CONSÉQUENCES HUMAINES

C'est la conséquence la plus grave qui puisse survenir. Un incendie peut provoquer **une intoxication par gaz et fumées, des brûlures, l'asphyxie et diverses blessures** qui pourraient survenir avec l'écroulement des structures. Des handicaps et surtout des décès peuvent en résulter.

Le stress et l'angoisse ressentis au moment du sinistre sont d'autres conséquences que l'on peut constater.

LES CONSÉQUENCES FINANCIÈRES

Un incendie peut également avoir des conséquences importantes sur le plan financier, tant du côté **du salarié que de l'entreprise elle-même**. La baisse d'activité ou la fermeture définitive de l'établissement peuvent être à l'origine de nombreuses pertes d'emplois.

Le chef d'entreprise subit lui aussi de lourdes conséquences, notamment au niveau de l'indemnisation des victimes, la reconstruction des locaux, le remplacement des équipements, l'arrêt temporaire ou définitif de l'activité et de la production et bien d'autres encore.

LES CRAINTES DE FERMETURE DE LA SOCIÉTÉ

Généralement, un incendie est source d'**importants dégâts pour une société**. Si cette dernière échappe à l'arrêt définitif de l'activité, il faut tout de même se préparer à une fermeture temporaire qui va impacter l'exploitation, la production et de facto la rentabilité.

LES CONSÉQUENCES AU NIVEAU DES OUTILS

L'incendie peut également engendrer la perte de données importantes de la société, notamment des **données informatiques, mais aussi leurs supports physiques**. Une autre conséquence grave est la **destruction du stock et la perte d'outils de production**. L'image de la société peut en être affectée, entraînant à son tour la perte de clients et de certains partenaires.

LES CONSÉQUENCES ÉCONOMIQUES

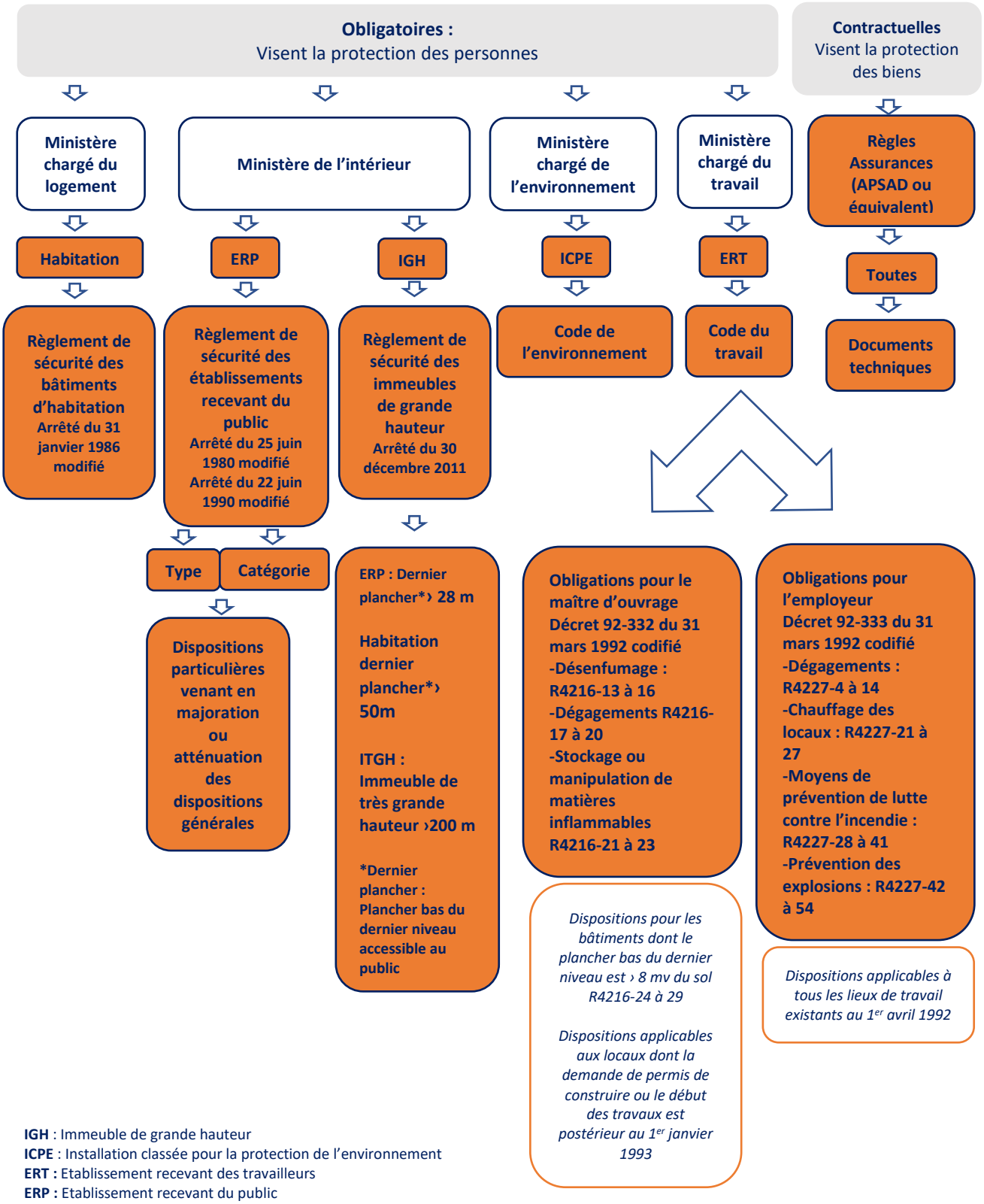
Au niveau économique, les conséquences d'un incendie sont souvent irrémédiables. Certaines études affirment que près de 70 % des entreprises victimes d'incendies ont cessé leurs activités et l'ensemble du personnel s'est retrouvé au chômage (source INRS).

LES CONSÉQUENCES ENVIRONNEMENTALES

L'impact environnemental d'un incendie en entreprise n'est pas des moindres. Il est notamment lié à **la pollution de l'air provoquée par la fumée, les gaz,** les produits utilisés par les extincteurs pour éteindre le feu, etc. Et c'est sans compter la pollution visuelle et les déchets parfois non destructibles provoqués par les flammes.

Incendie de l'usine Lubrizol à Rouen

16.5 Dispositions réglementaires et normatives de la sécurité incendie



IGH : Immeuble de grande hauteur
ICPE : Installation classée pour la protection de l'environnement
ERT : Etablissement recevant des travailleurs
ERP : Etablissement recevant du public

17.ENTREPOSAGE DE PRODUITS DANGEREUX

Par négligence, méconnaissance des règles et manque d'espace dévolu, le stockage de produits dangereux ne s'opère pas toujours dans les règles de l'art et pourtant il représente un risque élevé en incendie, explosion, pour la santé des personnes et l'environnement.

La grande variété de produits utilisés nécessite un stockage adéquat en raison :

- ⇨ Des différents états et natures des produits (solide, liquide, inflammable, comburant, toxique…),
- ⇨ Des volumes stockés,
- ⇨ Des matériaux d'emballage.

17.1 Produits dangereux

Ciment, peintures, vernis, diluants, aérosols sont dangereux et présentent des risques pour la santé et la sécurité du bâtiment (nocifs, irritants, inflammables, explosifs)

Stocker les produits dans un lieu suffisamment ventilé car ils présentent des risques d'inflammabilité ou d'explosion, donc toujours stocker les produits au frais, et à l'abri de la lumière ou de sources de chaleur.

Les ciments étant considérés comme des mélanges dangereux, ils doivent être mis en œuvre en respectant les règles générales de prévention prévues par le Code du travail pour les agents chimiques dangereux (articles R. 4412-1 à R. 4412-57)

Les incompatibilités de stockage des produits chimiques : certains produits peuvent réagir les uns avec les autres, provoquant parfois des explosions, des incendies, des projections ou des émissions de gaz dangereux.

Ces matières incompatibles doivent donc être séparés physiquement.

Des produits réagissent violemment avec l'eau : ils doivent donc être entreposés de façon à ce que tout contact avec de l'eau soit impossible, même lors d'inondation (P223, H260, H261, EUH014, EUH029).

Les produits inflammables doivent être stockés à part dans une enceinte dédiée et constamment ventilée.

Article R.5132-66 du Code de la santé publique : Les substances ou préparations dangereuses mentionnées à l'article R. 5132-58, à savoir, très toxiques, toxiques, cancérogènes, tératogènes ou mutagènes, doivent être placées dans des armoires fermées à clef ou dans des locaux où n'ont pas librement accès les personnes étrangères à l'établissement. En aucun cas, il ne doit être introduit dans les armoires et locaux des produits destinés à l'alimentation de l'homme ou des animaux.
Dans ces armoires ou locaux, les substances ou préparations mentionnées plus haut, doivent être détenues séparément des autres substances ou préparations, notamment de celles relevant des autres catégories (très toxiques, toxiques, nocives, corrosives, irritantes, sensibilisantes, cancérogènes, mutagènes).

Article R.5132-68 du Code de la santé publique et préconisations de l'INRS : Les substances ou préparations dangereuses (acides et bases), mentionnées à l'article R. 5132-67, détenues en vue de leur mise sur le marché ou de leur emploi, sont conservées séparément des autres substances ou préparations.

17.2 Quels sont les risques

Accident, pollutions environnementales, contusions, plaies, brûlures chimiques, intoxication, incendie, explosion.

On peut considérer qu'un stockage est non-adapté lorsque :

- Il est exposé à la chaleur, l'humidité, la lumière et aux intempéries
- La température ambiante est inappropriée à la nature et aux conditions de stockage du produit
- Il est mal rangé : en hauteur, non étiqueté, avec des produits incompatibles, sur des étalages surchargés…
- Le local est mal conçu
- La durée de stockage est excessive

Les armoires de sécurité coupe-feu sont la solution optimale pour le stockage des produits chimiques, toxiques, des peintures et vernis, des produits polluants ou inflammables en toute sécurité et en conformité avec la législation.
Les armoires de sécurité offrent une solution d'entreposage suivant la quantité de matières à stocker.

17.3 Conditions et suivi d'installation des armoires coupe-feu

- L'armoire doit être sécurisée contre le basculement
- Le lieu d'installation doit être à l'abri du gel et sec, température ambiante de +5 °C à +30 °C
- Les armoires coupe-feu doivent être protégées contre l'eau, la pénétration d'humidité et les éclaboussures
- Le sol/mur doivent être adaptés (charge admissible, classification)
- Le ventilateur, le détecteur de fumée et les piles doivent être contrôlés deux fois par an, vérifier si une procédure et un planning de vérification ont été établis.
- Mise en place et affichage de notice d'information concernant la manipulation des produits dangereux et le port des EPI (Equipements de Protection Individuelle)

17.4 Les moyens de prévention

- Fiche de données de sécurité,
- Étiquetage,
- Mesures organisationnelles,
- Règles de stockage,
- Stockage minimum au poste de travail,
- Local de stockage extérieur,
- Rangement,
- Extincteurs,
- Installation de lutte incendie,
- Système de désenfumage,
- Ventilation,
- Équipements de protection individuelle.
- Demander systématiquement au fournisseur de joindre la fiche de données de sécurité au produit
- Prendre connaissance de l'étiquetage du produit (notamment sur les précautions d'emploi et de stockage)

17.5 Mettre en place des mesures organisationnelles

- Gestion des stocks et des flux entrants et sortants, séparation des produits incompatibles, rayonnages non surchargés, contrôle d'accès, règles de déstockage et d'élimination des produits inutiles et périmés
- Regrouper les produits de même nature à l'aide de leurs étiquetages
- Stocker une quantité minimum et nécessaire de produits aux postes de travail

Disposer d'un local de stockage de préférence à l'extérieur à une dizaine de mètre du bâtiment, afin de limiter la propagation d'un éventuel incendie et faciliter l'intervention des secours, à défaut :

- Disposer d'un local de stockage au même niveau que le laboratoire ou l'atelier (afin d'éviter les passages difficiles : escaliers, sous-sol mais aussi en hauteur…)
- Assurer un rangement et une conception du local de stockage optimale pour éviter la création de risques supplémentaires (chutes, réactions dangereuses)
- Equiper le local de moyens de prévention et de lutte contre l'incendie (extincteurs adaptés, installation de lutte incendie, système de désenfumage…) et contre les déversements accidentels (rétentions, produit absorbant)
- Assurer une ventilation et un conditionnement d'air adéquat
- Mettre à disposition immédiate du personnel les moyens de traitement appropriés (douche de sécurité, lave œil…)
- Se munir des équipements de protection individuelle systématiquement lors de la manipulation et du transfert du produit (protections individuelles : gants, lunettes…informer les salariés + affichage des règles)
- Informer les salariés sur les risques chimiques encourus et les moyens de s'en prémunir (précautions et mesures à respecter en cas d'incident et/ou d'accident)
- Ne pas stocker d'aliments ou boissons dans les réfrigérateurs, congélateurs, chambres froides et étuve où sont stockés des produits chimiques et vice-versa (risques d'intoxications, d'anoxie, d'incendie et d'explosion)

18.LES ACTEURS DE LA SECURITE ET DE LA SÛRETE

L'employeur est l'acteur principal de la prévention des risques professionnels.
Avec l'appui d'une équipe compétente, il doit assurer la sécurité et préserver la santé physique et mentale de ses salariés.
Il a également la possibilité de solliciter des spécialistes externes à l'entreprise, Il peut s'agir d'acteurs locaux, institutionnels ou étatiques.

18.1 Au niveau de l'État

Police Nationale	Ministère de l'Intérieur =>DGPN (sous autorité du Directeur Général de la Police National)	❖ Mission d'assistance ❖ Mission de prévention auprès des maires et du CLSPD (Conseil local de sécurité et de prévention de la délinquance) ❖ Mission judiciaire (crimes et délits) ❖ Mission de maintien et de rétablissement de l'ordre.	C'est la Direction Centrale de la Sécurité Publique (DCSP) qui est en charge de la mission d'ordre public dans les agglomérations (hors agglomération, elle est confiée à la gendarmerie).	Ses missions sont multiples : Une action préventive et répressive essentielle dans la lutte contre l'insécurité routière ; La lutte contre la toxicomanie et les trafics de stupéfiants ; La prévention et la dissuasion de la délinquance par une présence active et visible sur la voie publique.
Gendarmerie	Ministère de l'intérieur	Idem que la Police Nationale	Agit hors agglomération	Chaque groupement de gendarmerie départementale dispose d'un référent sûreté. Il agit quotidiennement au profit des collectivités territoriales, des entreprises et des particuliers afin de leur apporter une expertise et des conseils en matière de prévention technique de la malveillance.
Police Municipale	Maire	Veille à appliquer : ❖ Des arrêtés municipaux, ❖ À la tranquillité et ❖ La salubrité publique	Elle est régie par : ❖ Code générale des collectivités territoriales ❖ Code de procédure pénale ❖ Livre 5 du Code de Sécurité Intérieure	Le Policier **Municipal** qui exerce toujours en uniforme, a pour **mission** la prévention et la surveillance du bon ordre, de la tranquillité, de la sécurité et de la salubrité publiques. Il agit sous autorité du maire et possède des pouvoirs de **police** administrative mais aussi de **police** judiciaire.
La Douane	Ministère de l'Économie et des Finances	❖ Mission fiscale (tabacs, alcool, droits de douane) ❖ Mission de soutien à la compétitivité économique des entreprises ❖ Mission de protection et de sécurité		➢ Le chargé de sûreté devra connaître les douaniers de son ressors, notamment par rapport à la validation du statut d'OEA (Opérateur Économique agrée) avec deux autorisations : C1 et S2

La DGSI : Direction Générale de la Sécurité Intérieure	Ministère de l'Intérieur	❖ Contre-espionnage ❖ Anti-terrorisme et extrémismes violents ❖ Protection du patrimoine économique	Rapprochement entre la Direction Centrale des Renseignements Généraux (DCRG) et la Direction de la Sécurité du Territoire (DST)	➢ Le chargé de sûreté devra connaître l'inspecteur DRSD de son ressors, en vue d'audit ou conseils.
La DRSD : Direction du Renseignement et de la Sécurité de la Défense	Ministère de la Défense	❖ La contre-ingérence ❖ Prévention et lutte contre les menaces (Terrorisme, Espionnage, Sabotage, Subversion, Crime organisé.)	Assumer ses responsabilités en matière de sécurité du personnel, des informations, des matériels et des installations sensibles	En charge de l'inspection des PIV (points d'importance vitale)
La CNIL : Commission Nationale de l'Information et des Libertés	Institué par la loi 78-17 du 06 janvier 1978 relative à l'informatique et modifiée par la loi du 06 août 2004	❖ Informer, Conseiller ❖ Réguler et recenser les fichiers ❖ Contrôler et sanctionner	C'est une autorité administrative indépendante. Elle délivre des avis, examine des projets de loi et décide des mesures à prendre en cas de non-respect de la loi. Elle ne délivre plus d'autorisations depuis la création de la RGPD sauf en ANCM (Agence nationale de sécurité du médicament) par ex.	<u>Pour contrôler les applications informatiques, la CNIL peut</u> : ➢ Accéder à tous les locaux professionnels ➢ Demander communication de tout document nécessaire et d'en prendre copie ➢ Recueillir tout renseignement utile ➢ Accéder aux programmes informatiques et aux données La CNIL peut prononcer diverses sanctions graduées : avertissement, mise en demeure, sanction pécuniaire pouvant atteindre 300 000€, ou encore retirer une autorisation.
La DGCCRF : Direction Générale de la Concurrence, de Consommation et de la Répression des Fraudes	Ministère de l'Économie	<u>Elle régule</u> : ❖ La concurrence des marchés, ❖ Assure la protection économique du consommateur, ❖ Préserve la sécurité physique et la santé du consommateur		La **DGCCRF** veille à assurer la qualité que les consommateurs sont en droit d'attendre d'un produit – alimentaire ou non-alimentaire – ou d'un service (règles d'étiquetage, de composition et de dénomination des marchandises, **contrôle des falsifications et tromperies**).
L'INPI : Institut National de la Propriété Industrielle		❖ Recevoir, examiner et délivrer les titres de propriété industrielles ❖ Tenir les registres ❖ Diffuser l'information ❖ Élaborer le droit de la propriété industrielle		<u>Composée de</u> : ➢ Membres de droit (Maire/Préfet, …) ➢ Membres élus et désignés par arrêté par le préfet

SGDSN Secrétariat Général de la Défense et de la Sécurité Nationale	1er Ministre	❖ Anticipe risques et menaces ❖ Prépare réponses aux crises ❖ Protège secret défense ❖ Assurer la cyberdéfense ❖ Contrôle exportations de matériels de guerre		Le secrétariat général de la Défense et de la Sécurité nationale est un organisme interministériel placé sous l'autorité du Premier ministre français. Il est chargé d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Il fixe la posture VIGIPIRATE
ANSSI Agence Nationale de la Sécurité des Systèmes d'Information		❖ Elle est chargée de détectée et d'alerter s'il y a la présence d'attaques informatiques. Elle veille notamment à la protection de l'État concernant leurs données informatiques.		Service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.
DREAL Direction Régionale de l'Environnement, de l'Aménagement et du Logement	Les directions régionales de l'Environnement, de l'Aménagement et du Logement sont des services déconcentrés de l'État français, sous tutelle commune du ministère de la Transition écologique et solidaire et du ministère de la Cohésion des territoires	Lutter contre le changement climatique et réduire les émissions de gaz à effet de serre dans les domaines industriel et routier Assurer la sécurité des habitants et de l'ensemble des acteurs économiques vis à vis de l'ensemble des risques Réduire la pollution de l'air et de l'eau, préserver la santé et l'environnement, pour préserver et reconquérir le patrimoine naturel Mettre fin à la banalisation des paysages et à l'érosion de la biodiversité, promouvoir la ville durable et intégrer les enjeux environnementaux et industriels dans une politique concertée régionale d'aménagement du territoire	Elle est régie par le code de l'environnement et le code de l'urbanisme.	Reprenant l'ensemble des compétences jusqu'alors dévolues aux DRIRE, DIREN et DRE, les DREAL ont pour rôle l'élaboration et la mise en œuvre des politiques de l'État en matière d'environnement, de développement et d'aménagement durables. Code de l'environnement Registre de l'ICPE : Art L511-1 + R. 541-43 et R. 541-46 du code de l'environnement (Abrogé à compter du 1er janvier 2022)

		Répondre aux besoins élevés en logement Impulser un nouveau modèle de développement économique respectueux de l'environnement		
Le fil d'Ariane	Ministère des affaires étrangères et du développement international	Ariane permet à tout ressortissant français, lors d'un voyage à l'étranger pour des motifs touristiques ou professionnels, de se signaler gratuitement et facilement auprès du ministère des Affaires étrangères et du Développement international (MAEDI).		Une fois son voyage enregistré sur Ariane, le ressortissant français : ➢ Recevra des recommandations de sécurité par SMS ou courriels si la situation dans le pays le justifie. ➢ Sera contacté en cas de crise dans le pays de destination

18.2 Les autorités départementales et locales

Le Préfet	Art. 72 de la constitution du 4 octobre 1958 dispose que le préfet : Représentant de l'État et chacun des membres du gouvernement dans le respect des lois et le contrôle administratif	6 missions prioritaires : 1. Représentation de l'État et la communication 2. La sécurité des personnes et des biens 3. Le service au public et la délivrance des titres 4. Le respect de la légalité et l'État de droit 5. L'intégration sociale et la lutte contre les exclusions 6. L'administration du territoire et le développement économique	Dans le dép. ou la région, il : ➢ Est le dépositaire de l'autorité de l'État ➢ A la charge de l'ordre public ➢ Représente le 1er Ministre et chacun des ministres ➢ Veille à l'exécution des règlements et décisions gouvernementales ➢ Arrête le projet stratégique de l'État dans la région (PASE) ➢ Préside de droit toutes les commissions administratives en région
Le Maire	A la fois agent de la commune et agent de l'État. Le Maire et ses adjoints sont officiers de police judiciaires (OPJ)	Ses missions sont variées : ❖ Représenter la commune en justice ❖ Passer les marchés, signer les contrats ❖ Préparer le budget et gérer le patrimoine Il dispose d'une police municipale	➢ Il est l'autorité de police compétente dans les ERP où se trouve l'établissement. Pour cela, il va consulter la CCDSA puis notifie un PV portant avis de la commission et de sa décision. ➢ Il dispose également du Plan communal de Sauvegarde dans le cas d'un évènement de sécurité civile.

CCDSA Commission Consultative Départementale de Sécurité et d'Accessibilité	Sous l'autorité du Préfet	La CCDSA exerce sa mission dans les domaines de : ❖ La sécurité contre les risques incendie et de panique dans les ERP/IGH ❖ L'accessibilité aux personnes handicapées ❖ La protection des forêts contre incendies ❖ L'homologation des enceintes recevant des manifestations sportives, musicales, etc. ❖ La sécurité des infrastructures et systèmes de transport ❖ Les études de sûreté et de sécurité publique	Elle effectue des visites périodiques de sécurité dans les ERP. Commission de sécurité Cela donne lieu à des rapports et des propositions d'avis. Code de la construction et de l'habitation ERP : R143-2+R123-19+GN1+GN8 IGH : R122-2+R122-5

18.3 Les acteurs du monde de l'entreprise

Inspection du travail		❖ Mission de contrôle et de conseil sur les dispositions légales et règlementaires auprès des chefs d'établissement ❖ Veiller à l'application des dispositions légales et règlementaires du travail ❖ Protection de l'intégrité physique des travailleurs ❖ Elle est régie par le Code du travail	La modification d'un Règlement Intérieur doit leur parvenir. Les inspecteurs sont habilités à pénétrer à tout moment dans les établissements. En cas de situation dangereuse, dresse un PV à l'employeur et transmet au procureur de la République, Copie au préfet. Code du travail Articles L.4121-1 à L4121-5 (principes généraux de prévention) Articles L 4111-1 à L 4831-1 (santé et sécurité au travail) Articles R 4227-1 à R 4227-57 (Chapitre VII : Risques d'incendies et d'explosions et évacuation) Articles R4121-1 à R4822-1 (Santé et sécurité au travail) Obligation générale d'information et de formation (Articles R4141-1 à R4141-20)
CARSAT Contrôleur de la Caisse d'Assurance Retraite et de la Santé au Travail	Organisme de droit privé	Mission de service public, son rôle est de : ❖ Convaincre en matière de prévention ❖ Convaincre de progresser ❖ Voire contraindre	Il a un droit d'entrée, de visite et d'enquête dans les établissements

Huissier de justice		Mission est de constater des preuves, propos ou faits dans des situations de menace pour l'entreprise Chargé de signifier les actes de procédures et d'exécuter les décisions de justice, l'huissier est un véritable allié pour les entreprises. À la demande des dirigeants, il peut intervenir dans de nombreux cas de figure pour sécuriser la vie de l'entreprise, ou faire appliquer la loi.	Un acte d'huissier est un acte rédigé, signé et signifié par un huissier de justice. ... Différents types d'actes peuvent être réalisés et signifiés par un huissier. Ce sont par exemple : assignation, mise en demeure, sommation, signification d'une décision ou d'un acte de procédure, etc.
CNAPS Conseil National des Activités Privées de Sécurité	Ministère de l'intérieur Il est un organisme de contrôle et de régulation	Le **conseil national des activités privées de sécurité**, ou **CNAPS**, est un service français de police administrative, rattaché au ministère de l'Intérieur et constitué sous la forme d'un établissement public administratif. Il est chargé de la délivrance, pour le compte de l'État, des autorisations d'exercice dans le secteur de la sécurité privée, du contrôle des acteurs (personnes physiques ou morales) de la sécurité privée et d'une mission de conseil à la profession.	Le CNAPS est un organisme de contrôle et de régulation de certaines professions de sécurité privée régies par le **livre VI du Code de la sécurité intérieure**. Le CNAPS est chargé, au nom de l'État, de l'agrément et du contrôle des professions de sécurité privée suivantes : ❖ Gardiennage ou surveillance humaine pouvant inclure l'utilisation de moyens électroniques ; ❖ Gardiennage ou surveillance humaine pouvant inclure l'utilisation de moyens électroniques avec arme des catégories B et D ; ❖ Agent cynophile ; ❖ Opérateur de vidéo protection ; ❖ Sûreté aéroportuaire ; ❖ Transport de fonds ; ❖ Maintenance et gestion de distributeurs automatiques de billets (DAB) ; ❖ Protection physique des personnes ; ❖ Recherches privées ; ❖ Protection des navires ; ❖ Formation aux activités privées de sécurité.

19.DOCUMENTATION

19.1 Référentiels APSAD

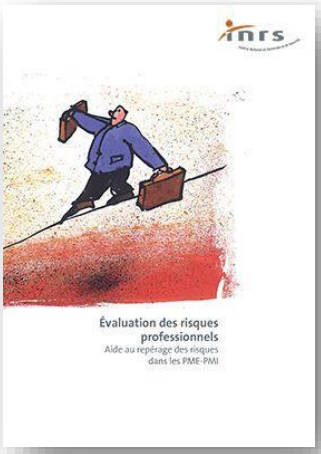
Titre		Date d'édition
Référentiel APSAD R1	Extinction automatique à eau, type sprinkleur – Règle d'installation	Mars 2015
Référentiel APSAD D2	Brouillard d'eau – Guide pour l'installation des systèmes de protection incendie par brouillard d'eau Existe en version anglaise	Novembre 2007
Référentiel APSAD R4	Extincteurs portatifs et mobiles – Règle d'installation	Novembre 2016
Référentiel APSAD R5	Robinets d'incendie armés et postes d'incendie additivés – Règle d'installation et de maintenance	Septembre 2018
Référentiel APSAD R6	Maîtrise du risque incendie et du risque industriel – Règle d'organisation	Janvier 2019
Référentiel APSAD R7	Détection automatique d'incendie – Règle d'installation	Février 2014
Référentiel APSAD R8	Surveillance des risques opérationnels – Règle d'organisation pour les risques d'incendie, de malveillance et techniques	Novembre 2010
Référentiel D9	Défense extérieure contre l'incendie – Guide pratique pour le dimensionnement des besoins en eau	Septembre 2001
Référentiel D9A	Défense extérieure contre l'incendie – Guide pratique pour le dimensionnement des rétentions des eaux d'extinction	Août 2004
Référentiel APSAD R11	Analyse de risque et de vulnérabilité incendie – Règle pour la réalisation de missions d'audit prévention et de conseil incendie Existe en version anglaise	Novembre 2014
Référentiel APSAD R12	Extinction automatique à mousse haut foisonnement – Règle d'installation	Avril 2014
Référentiel APSAD R13	Extinction automatique à gaz – Règle d'installation	Octobre 2019
Référentiel APSAD D14-A	Panneaux sandwichs et comportement au feu – Document technique pour la mise en œuvre Existe en version anglaise	Juin 2009
Référentiel APSAD R15	Ouvrages séparatifs coupe-feu – Règle de construction	Février 2009
Référentiel APSAD R16	Fermetures coupe-feu – Règle d'installation	Août 2007
Référentiel APSAD R17	Désenfumage naturel – Règle d'installation	Mars 2010

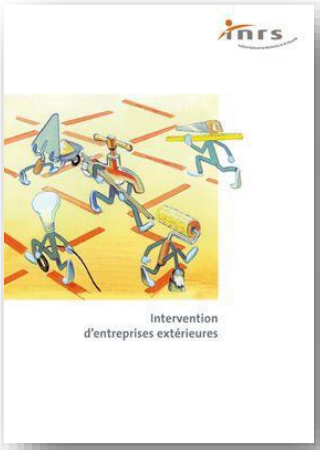
Titre		Date d'édition
Référentiel APSAD D18	Installations électriques – Document technique pour la réalisation des missions de vérification et de prévention	Septembre 2013
Référentiel APSAD D19	Thermographie infrarouge – Document technique pour le contrôle d'installations électriques	Juin 2019
Référentiel APSAD D20	Procédés photovoltaïques – Document technique pour la sécurité des bâtiments Existe en version anglaise	Février 2013
Référentiel APSAD R31	Télésurveillance – Règle de prescription	Septembre 2017
Référentiel APSAD D32	Cybersécurité – Document technique pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique	Juin 2017
Référentiel APSAD R81	Détection d'intrusion – Règle d'installation	Septembre 2015
Référentiel APSAD R82	Vidéosurveillance – Règle d'installation	Février 2016
Référentiel APSAD D83	Contrôle d'accès – Document technique pour la conception et l'installation	Novembre 2012
Référentiel CNPP 1008	Surveillance des risques – Méthode et outils pour le pilotage du management de sûreté malveillance	Mars 2018
Référentiel CNPP 6109	Expertise préalable – Guide pour la réalisation des missions d'identification et de valorisation des biens	Juin 2013
Référentiel CNPP 6011	Analyse de risque et de vulnérabilité – Méthode pour l'incendie ou la malveillance	Février 2018
Référentiel CNPP 7011	Analyse de vulnérabilité – Méthode pour le risque de responsabilité civile	Novembre 2014
Référentiel CNPP 8011	Analyse de risque et de vulnérabilité – Méthode pour les risques liés aux équipements et installations	Avril 2018
Référentiel CNPP 9011	Analyse de vulnérabilité – Food defense ou méthode pour réduire le risque de malveillance dans la chaîne alimentaire	Juin 2016
Référentiel CNPP 1302	Systèmes de management de la sûreté – Lutte contre la malveillance et la prévention des menaces	Septembre 2009

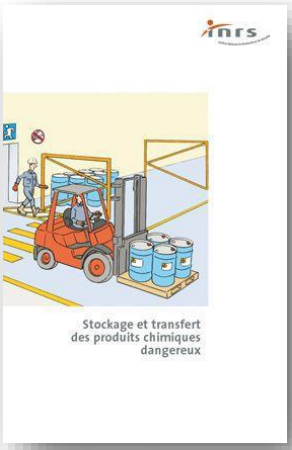
19.2 Ouvrages de référence (liste non exhaustive)

19.3 Guides utiles de référence téléchargeables gratuitement (liste non exhaustive)

INRS

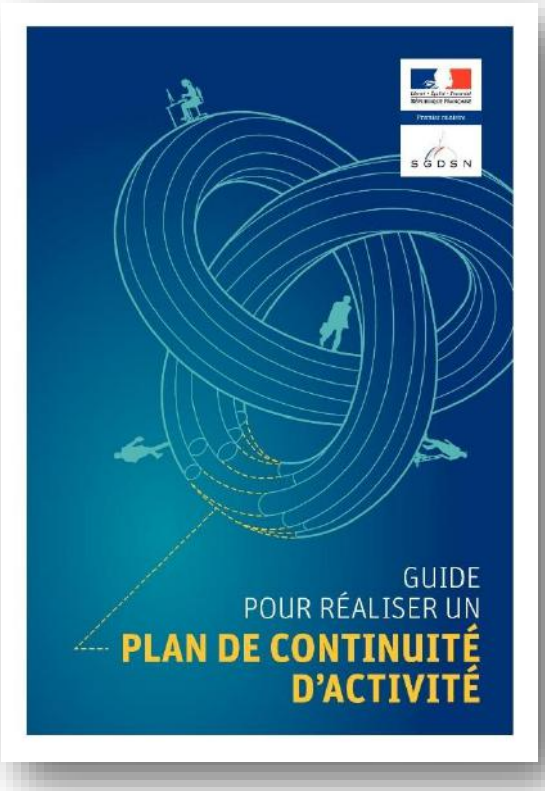




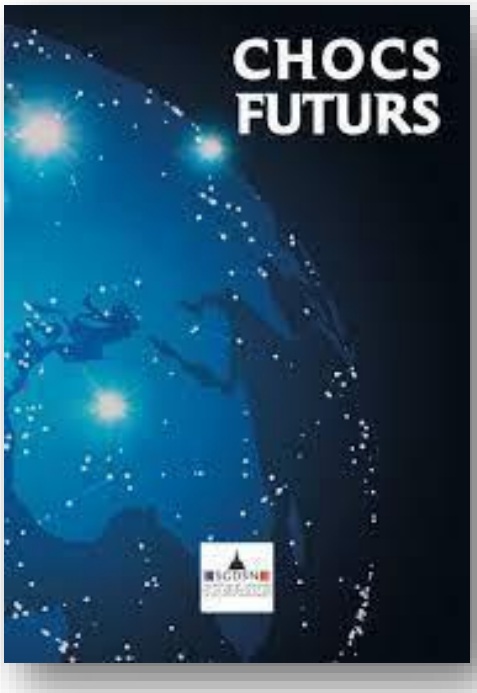


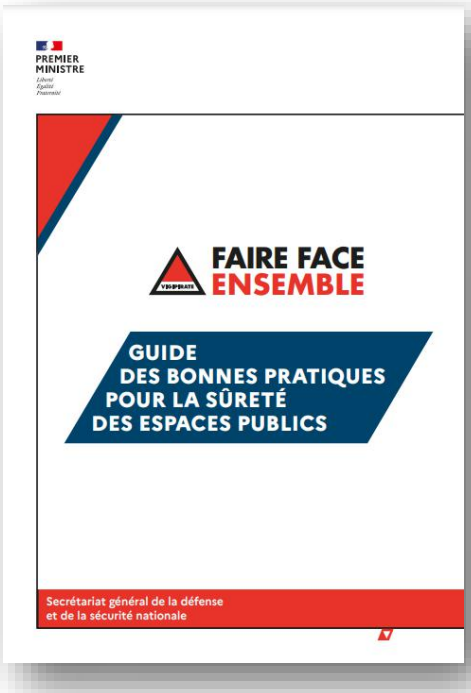
INERIS

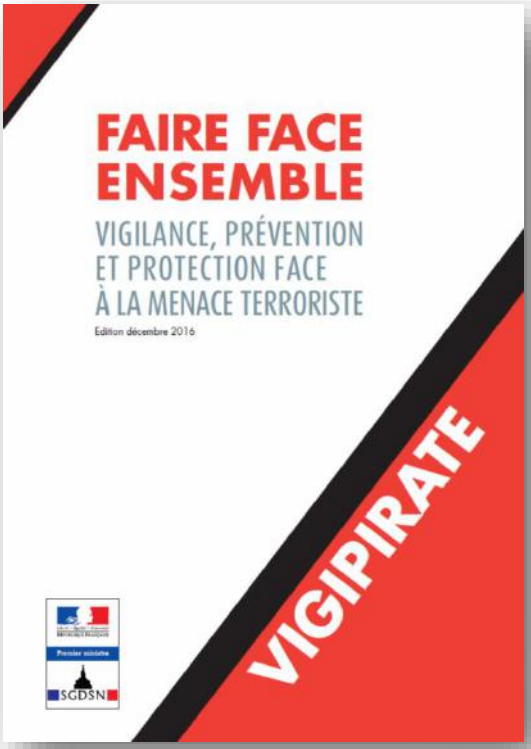
SGDSN

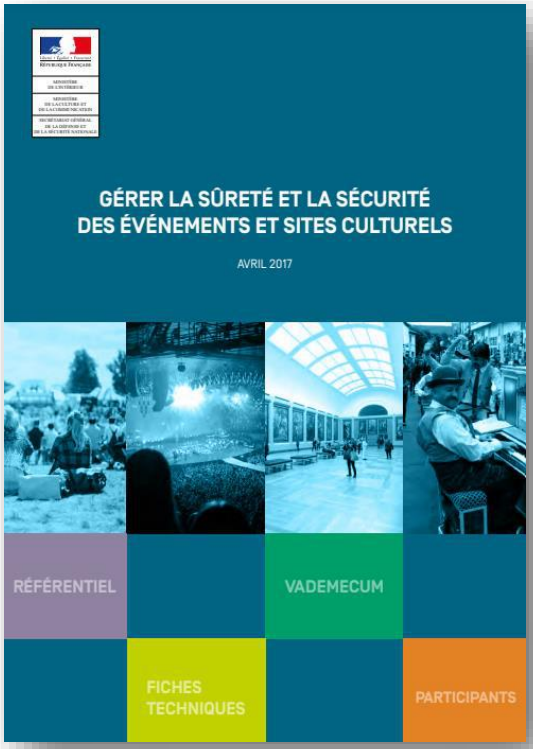


SGDSN

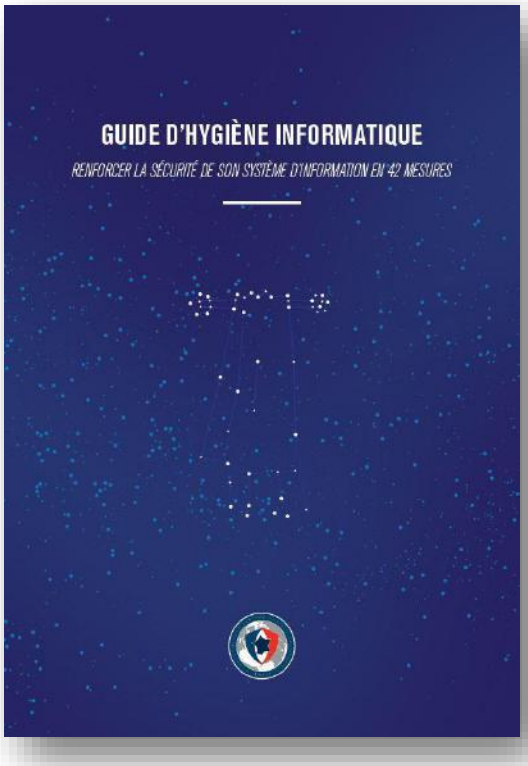


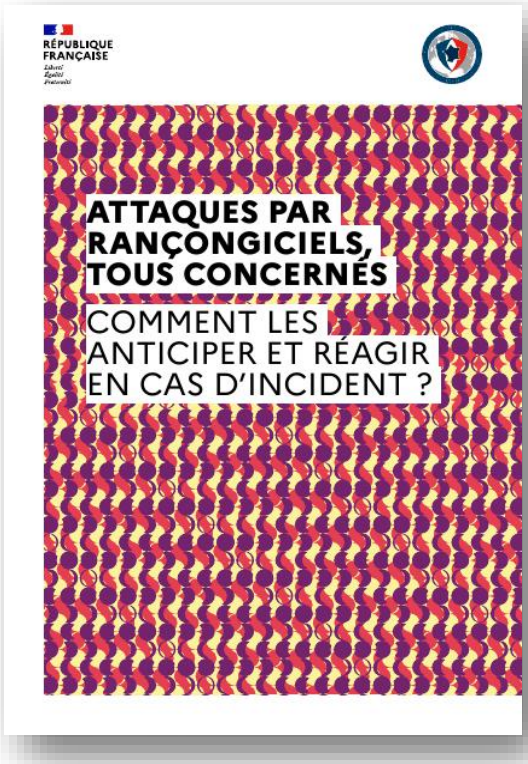



FAIRE FACE ENSEMBLE
VIGILANCE, PRÉVENTION ET PROTECTION FACE À LA MENACE TERRORISTE
Édition décembre 2016
VIGIPIRATE
SGDSN

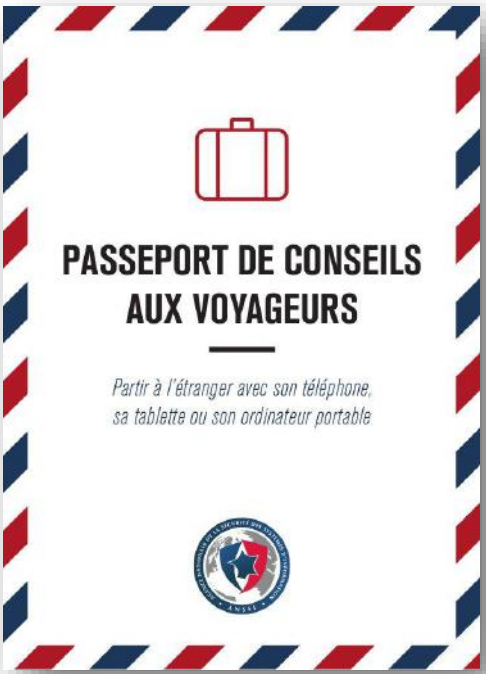

GÉRER LA SÛRETÉ ET LA SÉCURITÉ DES ÉVÉNEMENTS ET SITES CULTURELS
AVRIL 2017
RÉFÉRENTIEL
VADEMECUM
FICHES TECHNIQUES
PARTICIPANTS

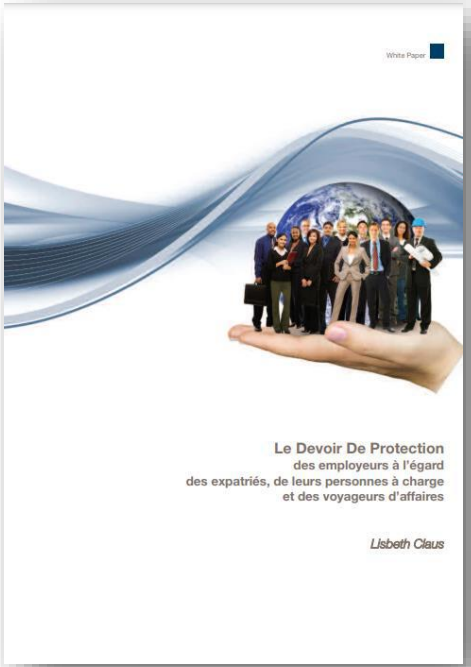
ANSSI


GUIDE D'HYGIÈNE INFORMATIQUE
RENFORCER LA SÉCURITÉ DE SON SYSTÈME D'INFORMATION EN 42 MESURES

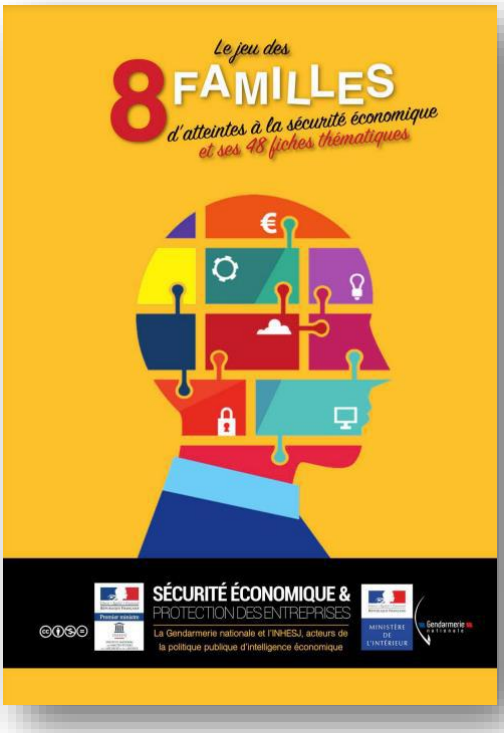

RÉPUBLIQUE FRANÇAISE
ATTAQUES PAR RANÇONGICIELS, TOUS CONCERNÉS
COMMENT LES ANTICIPER ET RÉAGIR EN CAS D'INCIDENT ?

International SOS

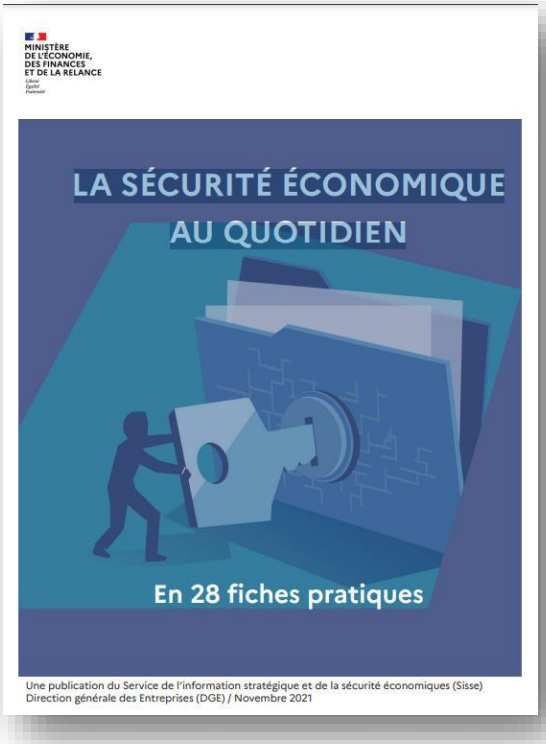




INHESJ



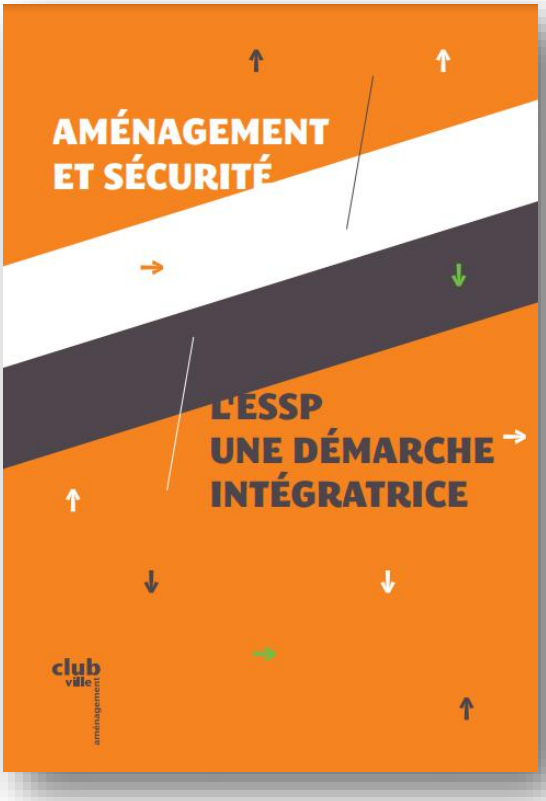
SISSE



MEDEF

CDSE

Club ville aménagement



19.4 Liens

https://www.inrs.fr/media.html?refINRS=ED%206336
https://www.inrs.fr/media.html?refINRS=ED%20990
https://www.inrs.fr/dms/inrs/CataloguePapier/ED/TI-TJ-20/tj20.pdf
https://www.inrs.fr/media.html?refINRS=ED%20840
https://www.inrs.fr/media.html?refINRS=ED%20941
https://www.inrs.fr/media.html?refINRS=ED%20753
https://www.inrs.fr/dms/inrs/CataloguePapier/ED/TI-ED-6230/ed6230.pdf
https://www.actu-environnement.com/media/pdf/dossiers/790-guide-vulnerabilite.pdf
http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf
http://www.sgdsn.gouv.fr/uploads/2017/04/sgdsn-document-prospectives-v5-bd.pdf
http://www.sgdsn.gouv.fr/uploads/2021/12/guide-unique-de-sensibilation-vigipirate-pact-num-v7.pdf2
http://www.sgdsn.gouv.fr/uploads/2017/01/plan-vigipirate-gp-bd.pdf
http://www.sgdsn.gouv.fr/uploads/2017/02/guide-bonnes-pratiques-surete-des-festivals-et-rassemblements-culturels.pdf
https://www.culture.gouv.fr/content/download/161242/file/Referentiel_Securite_Culture_web.pdf?inLanguage=fre-FR
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf
https://www.ssi.gouv.fr/uploads/2014/09/anssi_passeport_2019_1.0.pdf
https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf
https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf
https://www.aftm.fr/wp-content/uploads/2010/06/internationalsos_etude_devoir_de_protection_des_employeurs2009.pdf
http://www.ioe-emp.org/fileadmin/ioe_documents/publications/Policy%20Areas/osh/FR/_2014-10__Intl_SOS_-_Guide_mondial_de_reference_-_Sante_surete_et_securite_des_missions_et_deplacements_professionnels.pdf
https://www.ihemi.fr/sites/default/files/pages/files/2020-01/48_fiches_kit_secu-eco.pdf
https://sisse.entreprises.gouv.fr/files_sisse/files/outils/fiches/la-securite-economique-au-quotidien-en-28-fiches.pdf
https://www.medef.com/fr/content/commande-publique-guide-pratique-sur-la-protection-des-informations-sensibles-des-entreprises
https://www.cdse.fr/IMG/pdf/cdse_livre_blanc_2022_web-2.pdf
https://www.cdse.fr/IMG/pdf/opinionway_-_barometre_cdse_-_axa_-_synthese_etude.pdf
https://club-ville-amenagement.org/wp-content/uploads/essp_brochure.pdf

ADESS

ASSOCIATION DES EXPERTS
EN SECURITÉ ET SURETÉ

4 allée des Augustins -92 390 - Villeneuve la Garenne

06 32 29 67 62

contact@adess-france.fr

https://adess-france.fr

Association déclarée RCS 882 714 165 000 17

N°RNA W922 017 481

Code APE 9492Z