MINISTÈRE
DES ARMÉES
ET DES ANCIENS
COMBATTANTS

Liberté
Égalité
Fraternité

Guide pratique

Gestion de la sûreté

à l'usage des PME et des ETI de la BITD

SOMMAIRE

AVANT-PROPOS

La **prise de conscience du recours croissant aux actions hybrides** et aux **ingérences** – telles que l'espionnage, le sabotage, la guerre économique, les cyber-attaques ou les atteintes à la réputation – est **désormais avérée. Ces menaces ciblent notamment les petites et moyennes entreprises** (PME) et les **entreprises de taille intermédiaire** (ETI) de la base industrielle et technologique de défense (BITD). En effet, celles-ci sont souvent jugées plus vulnérables que les grands groupes industriels dont elles sont un maillon essentiel de la chaîne de sous-traitance. Dépositaires de savoir-faire critiques et indispensables à la souveraineté nationale, ces entreprises constituent des cibles privilégiées pour les services de renseignement étrangers, mouvements contestataires ou compétiteurs économiques dans un contexte géopolitique particulièrement tendu.

En complément du domaine cyber qui est de plus en plus un vecteur d'attaque, **les entreprises de la BITD sont confrontées à une recrudescence des attaques classiques** dont les modes opératoires visent à **exploiter les vulnérabilités des entreprises et de leurs collaborateurs** à travers une **combinaison entre interactions humaines et actions physiques ciblées.** L'ingénierie sociale, en particulier via les réseaux sociaux, est exploitée pour repérer et approcher des collaborateurs aux postes stratégiques afin d'obtenir des accès ou des informations sensibles. Cette phase de repérage constitue fréquemment un préalable à des intrusions dans les locaux, visant le vol de documents ou de supports liés à des savoir-faire spécifiques, voire des actions de sabotage.

La mise en place de mesures de protection est indispensable, car l'atteinte d'un seul sous-traitant peut remettre en cause l'intégrité d'un programme de défense dans son ensemble. Or, les **PME et ETI de la BITD ne disposent pas toujours des repères nécessaires pour déployer un dispositif de sûreté[1] adapté à leur structure.** Partant de ce constat, le bureau « expertise protection sûreté » du Centre du conseil, de la prévention et des inspections (CCPI) de la DRSD a engagé une démarche visant à synthétiser les notions essentielles de la sûreté et, surtout, à proposer un **canevas permettant la mise en œuvre d'un dispositif de sûreté initial**, susceptible d'être renforcé ultérieurement selon les besoins et les capacités des entreprises concernées.

Ce guide pratique dédié à la **gestion de la sûreté** propose aux dirigeants un **cadre le plus pragmatique possible**, leur permettant de **transformer les exigences de sûreté** en un véritable **levier de compétitivité**. Pour sortir de la perception de centre de coût souvent attribué à la structure de sûreté, ce guide contribuera à la protection des actifs stratégiques, au maintien et au **renforcement de la confiance** des donneurs d'ordre et des clients, tout en garantissant la pérennité de l'entreprise face à des adversaires déterminés.

Le **général de corps d'armée Aymeric Bonnemaison**
Directeur du renseignement et de la sécurité de la défense

[1] La sûreté concerne la prévention et la lutte contre la malveillance. La sécurité concerne la prévention et la lutte contre les risques accidentels, naturels et technologiques (définitions dans le glossaire p 74).

PRÉFACE

En juin 2024 je remettais au Président de la République mon rapport relatif à la sécurité économique des entreprises françaises, qu'il m'avait commandé un an auparavant. Ce rapport classifié a permis notamment de mettre en évidence le besoin urgent de renforcer la protection des actifs stratégiques des entreprises françaises dans un contexte mondial fragile, incertain où les ingérences étrangères se multiplient. Renforcer la protection, « Protect France », tout en restant attractif, « Choose France », telle était la conclusion finale du rapport.

Le manque voire l'absence de connaissances de nombreux dirigeants, en particulier dans les PME, quant aux mesures organisationnelles, techniques et humaines à mettre en place pour veiller à la protection de leur entreprise et de leur activité, ainsi que la perception fréquente de la sûreté comme uniquement un centre de coût, constitue une vulnérabilité, pour elles-mêmes d'abord, et évidemment pour le pays.

Ce guide pratique de gestion de la sûreté pour les PME/ETI de l'industrie de défense élaboré par la DRSD, s'inscrit pleinement dans l'esprit de ce rapport : faire connaitre les risques pour mieux s'en protéger. Son idée maîtresse est de démontrer que la sûreté pour une entreprise doit être considérée comme un *business partner* et que sa prise en compte dans le business plan ne doit pas être sous-estimée. En effet, lorsqu'elle est alignée sur les objectifs stratégiques de l'entreprise, la sûreté devient un facteur de compétitivité. En plus d'augmenter la confiance des clients et des partenaires, elle devient un élément discriminant, une plus-value, notamment dans des secteurs d'activité tout particulièrement sensibles de la base industrielle et technologique de défense.

Construit de manière à être rendu accessible, ce guide permet à un dirigeant, quel que soit son niveau de connaissance et de maîtrise des fondamentaux de la sûreté, de déployer et de mieux appréhender un dispositif initial de sûreté au sein de son entreprise.

Monsieur Geoffroy Roux de Bézieux
Président d'honneur du MEDEF et président de Notus technologies

INTRODUCTION

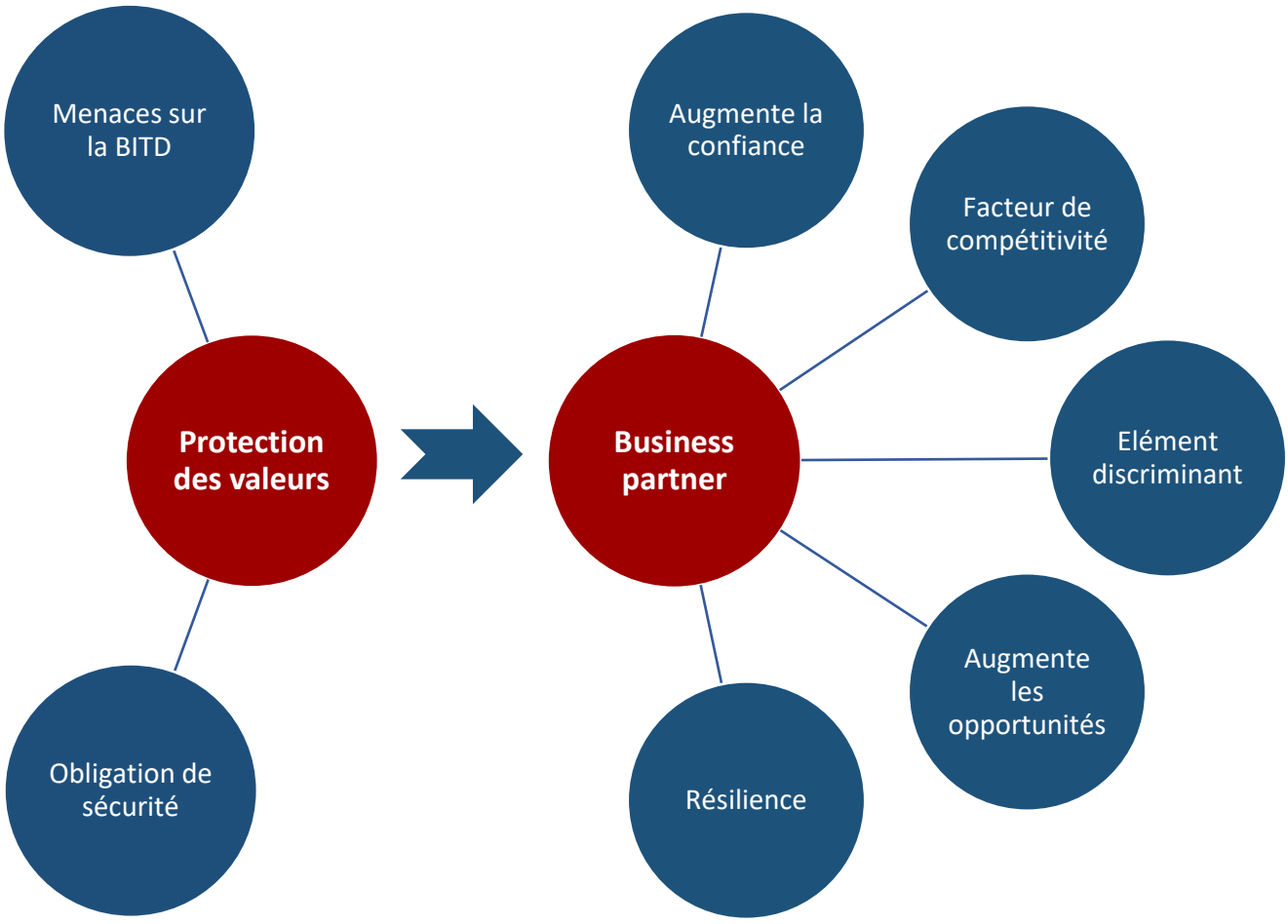
POURQUOI METTRE EN ŒUVRE UNE POLITIQUE DE SÛRETÉ AU SEIN DE VOTRE ENTREPRISE

L'actualité et les faits démontrent **l'intensification des menaces visant la BITD et entre autres ses savoir-faire**, parfois critiques et essentiels à la souveraineté nationale.

L'article L4121-1 du code du travail instaure envers le dirigeant d'une entreprise une **obligation de sécurité envers ses salariés**, avec la mise en œuvre de **moyens renforcés** selon la jurisprudence *Air France* de 2015.

Par ailleurs, les services achats des grandes entreprises de la BITD, voire de certaines administrations, **intègrent** dorénavant pleinement la **sûreté comme un critère discriminant** dans le choix d'un fournisseur. À l'instar de la cybersécurité, les exigences en matière de sûreté physique sont aujourd'hui progressivement formalisées et intégrées aux relations contractuelles.

Lorsqu'elle est alignée avec la stratégie, l'activité et le fonctionnement de l'entreprise, la **sûreté contribue directement à sa performance globale**, non seulement en assurant la **protection de ses actifs** et sa **résilience**, mais également en **contribuant à la compétitivité** en favorisant les opportunités commerciales ainsi qu'en **renforçant la confiance** des clients et des partenaires. La sûreté s'impose désormais comme un véritable ***business partner*** **de l'entreprise**.



OBJECTIF DE CE GUIDE

Il existe de nombreuses normes[2] et référentiels[3] relatifs à la gestion de la sûreté. Toutefois, ces derniers sont davantage adaptés aux grandes entreprises et peuvent s'avérer complexes à appréhender et à déployer pour des structures de taille plus modeste. L'objectif est donc ici **d'accompagner les PME et les ETI de la BITD en mettant à leur disposition un document clé en main dédié à la gestion globale de leur sûreté**. Celui-ci s'articule autour de 2 volets complémentaires :

- Une **partie théorique** présentant les fondamentaux de la sûreté : sa définition, ses grands principes, ainsi que les différents domaines dans lesquels elle s'applique et leurs composantes, etc.
- Une **partie didactique** destinée à faciliter la mise en œuvre concrète de la sûreté au sein de l'entreprise, en s'appuyant sur une démarche éprouvée du monde de l'entreprise, à savoir la méthode d'amélioration continue PDCA (plan, do, check, act).

Afin de **permettre au lecteur d'aller à l'essentiel et de faciliter la priorisation**, ces 2 parties sont scindées en **2 catégories hiérarchisées**, tant pour le contenu théorique que les actions de mise en œuvre :

- Les informations et mesures « pour commencer », correspondant aux fondamentaux à maîtriser et aux actions prioritaires à engager
- Les informations et mesures « pour aller plus loin », destinées à approfondir et renforcer le dispositif initial.

En revanche, ce guide **ne traite pas des contraintes réglementaires** spécifiques liées à la protection du secret de la défense nationale (PSDN), la protection du potentiel scientifique et technique (PPST) et la sécurité des activités d'importance vitale (SAIV).

[2] Norme NF **ISO 22300** concernant le vocabulaire lié à la sécurité et la résilience ; NF **ISO 22340** concernant les lignes directrices pour une architecture et un cadre de sûreté préventive de l'entreprise ; NF **ISO 22342** lié aux lignes directrices pour l'élaboration d'un plan de sûreté destiné à un organisme ; NF ISO 31000 concernant le management du risque ; **AFNOR SPEC 2404** pour plan de sûreté et les exigences opérationnelles.

[3] **Traité pratique de sûreté malveillance** du CNPP ; référentiel **1302** sur le système de management de la sûreté du CNPP ; référentiel APSAD **D83** du CNPP sur le contrôle d'accès ; référentiel APSAD **R31** du CNPP concernant la télésurveillance ; référentiel APSAD **R81** du CNPP sur la détection d'intrusion ; référentiel APSAD **R82** du CNPP sur la vidéosurveillance ; les **29 fiches pratiques de la sécurité économique** du SISSE ; le **jeu des 8 familles d'atteintes à la sécurité économique** de l'IHEMI.

PARTIE 1 – GÉNÉRALITÉS SUR LA SÛRETÉ

Fiche 1 : grands principes

Fiche 2 : gouvernance de la sûreté

Fiche 3 : système de management de la sûreté

Fiche 4 : sûreté du personnel

Fiche 5 : sûreté physique des valeurs

Fiche 6 : sécurité des informations

FICHE 1 – GRANDS PRINCIPES

La démarche de sûreté repose sur un socle de principes structurants qui permettent à l'entreprise de protéger efficacement ses actifs stratégiques, de manière adaptée et pérenne, contre les actes de malveillance présentant un risque.

UNE SÛRETÉ INTEGRÉE À LA STRATEGIE ET AU FONCTIONNEMENT DE L'ENTREPRISE

La sûreté doit être **intégrée à la stratégie et au fonctionnement de l'entreprise**, être au service de son activité et contribuer à sa performance globale. Pour cela, elle doit assurer la sûreté de ses valeurs : son personnel, son patrimoine matériel (installations, matériels, produits, etc.) et immatériel (informations, réputation, savoir-faire). Elle peut et doit être un *business partner* de l'entreprise.

UN ENGAGEMENT CLAIR DE LA DIRECTION

La **direction doit valider et incarner la gouvernance de la sûreté**, en définissant notamment sa politique générale de sûreté et son organisation. Cet engagement est indispensable pour garantir la légitimité, le financement et l'efficacité de la démarche.

UNE ARCHITECTURE DE SÛRETÉ COHÉRENTE ET ADAPTÉE

L'objectif est d'établir une architecture de sûreté, cohérente et adaptée à l'entreprise, fondée sur une **stratégie globale** reposant sur le principe de **défense en profondeur des valeurs** et s'appuyant sur des **barrières successives**. Toutes les mesures associées, de nature humaine, organisationnelle et technique (HOT), doivent être parfaitement adaptées, complémentaires, homogènes et redondantes, afin de se prémunir des risques liés aux menaces et aux vulnérabilités identifiées.

Cette défense en profondeur des valeurs doit permettre de **répondre à l'équation de sûreté**, à savoir : le temps de freinage doit être strictement supérieur aux temps cumulés de détection, de traitement de l'alarme et d'intervention.

Cette architecture de sûreté **repose sur une gouvernance dédiée** qui va s'appuyer sur un **système de management de la sûreté** structuré autour de **trois domaines fondamentaux** : la sûreté du personnel, la sûreté physique et la sécurité des informations. L'ensemble des mesures mises en œuvre doit, par ailleurs, être conforme au cadre réglementaire en vigueur, notamment le RGPD, le code de la sécurité intérieure et le code du travail.

UNE GESTION DU RISQUE SÛRETÉ CENTRÉE SUR LA MALVEILLANCE

Le management du risque sûreté s'appuie sur les grands principes de l'ISO 31000 relatifs au management des risques, en se concentrant plus spécifiquement sur le **risque de malveillance**. Cette approche permet d'identifier, d'évaluer et de traiter les menaces et les vulnérabilités pouvant présenter un risque pour les actifs stratégiques de l'entreprise.

UNE RESPONSABILITÉ INDIVIDUELLE AU PROFIT DU COLLECTIF ET DE L'ENTREPRISE

La sûreté ne repose pas uniquement sur les experts ou les responsables : elle est **l'affaire de chacun des collaborateurs**. Chaque personnel, quel que soit son rôle, contribue à la vigilance collective et à la protection des valeurs. La confidentialité de certaines mesures et dispositifs de sûreté constitue, par ailleurs, une condition essentielle à leur efficacité.

L'importance de la sensibilisation du personnel, impulsée par les dirigeants, est cruciale en termes de sûreté. Elle encourage la remontée des signaux faibles et permet même d'entraver des attaques de faibles complexités.

UNE CHAÎNE DONT LA FORCE DÉPEND DU MAILLON LE PLUS FAIBLE

La **sûreté** doit être appréhendée comme une chaîne dont la **solidité dépend de son maillon le plus fragile**. La moindre vulnérabilité, même ponctuelle, qu'elle soit humaine, organisationnelle ou technique, est susceptible de remettre en cause l'ensemble du dispositif. Cette représentation met en évidence la nécessité d'une vigilance permanente à tous les niveaux.

UNE DÉMARCHE FONDÉE SUR L'AMELIORATION CONTINUE

La sûreté s'inscrit dans une logique d'amélioration continue pouvant s'incarner dans le processus de PDCA (Plan, Do, Check, Act) consistant à évaluer régulièrement la situation, adapter les dispositifs, contrôler leur efficacité, mettre à jour les procédures et assurer une veille permanente. Cette dynamique améliore la résilience de l'entreprise face à des menaces en constante évolution.

FICHE 2 – GOUVERNANCE DE LA SÛRETÉ

Pour commencer

- Généralités
- Domaines concernés par la sûreté
- Responsable sûreté

Pour aller plus loin

- Politique générale de sûreté
- Plan de sûreté
- Structure de sûreté au niveau de la société
- Schéma directeur de sûreté
- Revue de direction sûreté

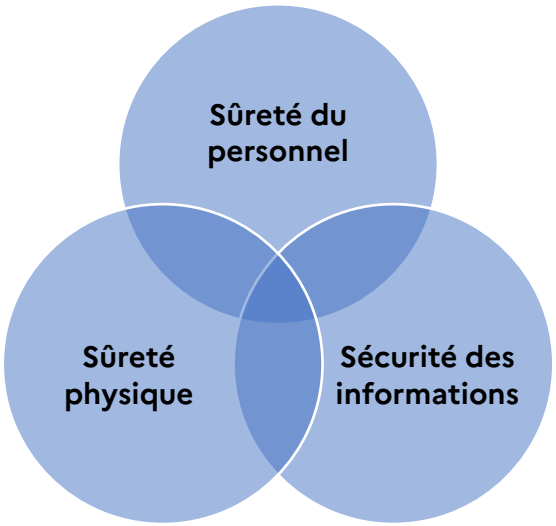
POUR COMMENCER

GÉNÉRALITÉS

La gouvernance de la sûreté est l'**engagement stratégique de la direction** qui définit la **vision** et les **objectifs**, détermine les **rôles** et les **responsabilités**, alloue les **ressources nécessaires** et imprime la **culture de sûreté** nécessaire pour protéger les valeurs de l'entreprise. Il s'agit du « **quoi** » et du « **pourquoi** ». Elle concrétise cet engagement en fixant les **politiques** et en assurant la légitimité de la sûreté au cœur des décisions et processus de l'organisation.

Enfin, en termes de pilotage et de contrôle, elle s'assure de la cohérence des pratiques et garantit que les **dispositifs de sûreté sont alignés sur les objectifs stratégiques** et les priorités opérationnelles de l'entreprise, spécifiquement via une revue de direction.

DOMAINES CONCERNÉS PAR LA SÛRETÉ



La sûreté concerne **3 grands domaines** :

- La **sûreté du personnel**, comprenant principalement la sûreté physique des collaborateurs. Elle s'attache également à s'assurer de l'éligibilité et l'aptitude du personnel, des sous-traitants et de l'ensemble des parties prenantes à accéder aux actifs stratégiques de l'entreprise pendant toute la durée de leur emploi ou de leur mission. De plus, elle comprend l'instauration d'une culture de sûreté au sein de l'entreprise
- La **sûreté physique**, dont l'objectif est de s'assurer de la protection physique des valeurs détenues ou gérées par l'entreprise afin de se prémunir d'un risque lié à des menaces et des vulnérabilités
- La **sécurité des informations**, dont l'objectif est de garantir la disponibilité, la confidentialité, l'intégrité et la traçabilité (DCIT) des informations de l'entreprise ainsi que celles qui lui sont confiées.

L'ensemble de ces domaines forme une chaîne de sûreté dont l'interdépendance est forte. La vulnérabilité d'une composante d'un seul des domaines peut compromettre l'efficacité de l'ensemble du dispositif.

RESPONSABLE SÛRETÉ

Le **responsable sûreté** est généralement le dirigeant, le responsable des moyens généraux, le responsable QHSE voire le responsable des ressources humaines. Autrement dit, la sûreté est généralement une mission secondaire. Parfois, en fonction de la structure de l'entreprise et du secteur d'activité, le responsable sûreté est à temps plein sur cette fonction.

Pour exercer ses responsabilités et remplir ses missions, **le responsable sûreté doit pouvoir disposer** :

- Du **positionnement hiérarchique** adapté, avec entre autres un accès aisé, si possible direct, à la direction de l'entreprise
- De l'**autorité nécessaire**
- Des **ressources adéquates** pour gérer et diriger la sûreté, notamment en termes de disponibilité. Selon la taille de l'établissement, le responsable sûreté peut exercer d'autres fonctions au sein de l'entreprise. De plus, il est possible pour celui-ci de disposer de plusieurs personnes sous sa responsabilité
- Des **compétences** requises
- Idéalement, d'un **adjoint** afin d'assurer la continuité de la fonction lors de ses absences.

Le responsable sûreté peut recevoir une **délégation de pouvoir** du dirigeant. Dans ce cadre, cela nécessite qu'il dispose de l'autorité et surtout des moyens pour exercer cette responsabilité. Cependant, le dirigeant et la direction restent comptable du résultat du travail délégué.

Il est nécessaire de définir et d'attribuer clairement les rôles et les responsabilités. Le responsable sûreté doit être identifié et connu des salariés de l'entreprise.

POUR ALLER PLUS LOIN

POLITIQUE GÉNÉRALE DE SÛRETÉ

La politique générale de sûreté **fixe officiellement les orientations stratégiques de la direction en termes de sûreté**. Elle explique le **« quoi »** et le **« pourquoi »**.
Elle doit principalement comprendre :

- La définition d'une **gouvernance de la sûreté** claire et structurée, précisant les rôles, les responsabilités et les imputabilités à tous les niveaux de l'organisation
- Les **objectifs de sûreté** mesurables et cohérents avec les enjeux de l'organisation, et déployer éventuellement un schéma directeur de sûreté permettant de les atteindre dans une logique d'amélioration continue
- La **conformité avec les exigences légales** et réglementaires applicables, ainsi qu'aux normes et bonnes pratiques en vigueur
- L'élaboration et le maintien d'une **documentation formalisée liée à la sûreté**, incluant notamment le plan de sûreté, un éventuel schéma directeur sûreté, les procédures et les consignes opérationnelles
- L'instauration d'une **politique de sensibilisation aux risques sûreté** afin de promouvoir une culture de sûreté partagée, fondée sur la sensibilisation, la formation et la responsabilisation de tous
- La mise en place d'une **revue de direction sûreté**, permettant d'évaluer la pertinence, l'adéquation et l'efficacité du dispositif de sûreté, et de définir les axes d'amélioration.

Un exemple de politique générale de sûreté est présenté en annexe 5.

Dans le but de renforcer la confiance des partenaires de l'entreprise (clients, prestataires), il est possible de leur partager (en mode consultation) cette politique générale de sûreté.

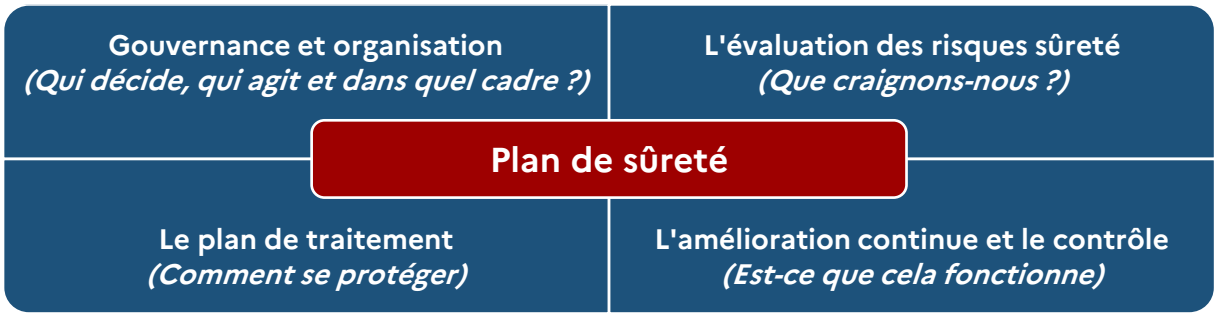
PLAN DE SÛRETÉ

Le plan de sûreté est le document de référence qui décrit « **comment** » **une entreprise protège activement ses valeurs par rapport aux risques sûreté** et s'assure de son efficacité. Il ne s'agit pas d'une simple liste de mesures techniques et organisationnelles, mais d'une stratégie globale qui explique comment l'entreprise **identifie ses risques, décide de les traiter et réagit en cas de crise**.

Le plan de sûreté répond à trois finalités :

- **Protéger les valeurs stratégiques de l'entreprise**, à savoir son personnel, son patrimoine matériel (installations, matériels, produits…) et immatériel (les informations, l'e-réputation)
- **Démontrer la maîtrise des risques**. Il prouve aux dirigeants, aux assureurs, aux clients et aux autorités la rigueur avec laquelle la gestion des risques est traitée au sein de l'entreprise, en définissant clairement les risques auxquelles elle est soumise, les responsabilités de chacun pour s'en protéger, les ressources mobilisées ainsi que les règles mises en œuvre
- **Structurer la réponse face à l'imprévu**. Les menaces évoluant vite, le plan impose une approche agile : il permet non seulement de prévenir les risques connus, mais aussi de réagir rapidement et de manière coordonnée face à des situations inédites ou de crise.

Il comprend 4 grandes parties :



Un exemple de plan de sûreté est présenté en annexe 6.

STRUCTURE DE SÛRETÉ AU NIVEAU DE LA SOCIÉTÉ

Lorsqu'une entreprise possède plusieurs établissements, il peut être pertinent, en complément des responsables sûreté locaux, de nommer un **responsable sûreté central**. Cette fonction permet d'incarner la sûreté au niveau de l'entreprise, de définir une politique commune, de diffuser une culture de sûreté partagée et de capitaliser sur les bonnes pratiques issues de chaque site. Cette fonction peut être occupée par un collaborateur au niveau central ayant déjà d'autres fonctions, ou par un des responsables sûreté d'établissement.

Ce rôle garantit également une cohérence durable entre les orientations de la direction et les enjeux de sûreté rencontrés par les différents établissements.

SCHÉMA DIRECTEUR DE SÛRETÉ

Appelé aussi « plan stratégique de sûreté », le schéma directeur de sûreté **fixe la vision de la sûreté** pour l'entreprise **à moyen terme** (3 à 5 ans). Il détermine la feuille de route pour sa mise en œuvre avec les grands objectifs de sûreté à atteindre par la direction.

REVUE DE DIRECTION SÛRETÉ

Idéalement effectuée annuellement, la revue de direction a pour objectif de s'assurer de la pertinence, l'adéquation et l'efficacité du système de management de la sûreté pour atteindre les objectifs fixés dans la politique générale de sûreté.

Pour cela, elle va devoir : **Vérifier** **Évaluer** **S'assurer** **Décider**

1. **Vérifier l'adéquation** entre la stratégie de l'entreprise et les enjeux de sûreté
2. **Évaluer l'efficacité** du dispositif global de sûreté
3. **S'assurer** que les ressources, les compétences et l'organisation sont **suffisantes**
4. **Décider** des orientations, arbitrages et **priorités** pour l'année à venir.

La revue de direction sûreté peut également avoir lieu si un événement majeur survient (incident grave, changement de contexte, crise, etc.) ou si une évolution importante impacte les risques ou les missions de l'entreprise.

Un PV de revue de direction sûreté est rédigé à l'issue, permettant principalement d'attester des décisions prises, de permettre un suivi régulier, mais également de démontrer l'engagement de la direction en matière de sûreté.

Un exemple de revue de direction sûreté est présentée en annexe 7.

FICHE 3 – SYSTÈME DE MANAGEMENT DE LA SÛRETÉ

Pour commencer

- Généralités
- Généralités sur le management du risque sûreté
- Le règlement intérieur avec des éléments de sûreté

Pour aller plus loin

- Connaissance de l'environnement interne/externe
- Identification des valeurs
- Évaluation des risques sûreté
- Maîtrise et traitement des risques sûreté
- Surveillance, contrôle et réexamen des risques sûreté
- Procédures de sûreté
- Dispositif de veille
- Plan de continuité d'activité (PCA) / plan de reprise d'activité (PRA)
- Plan de gestion de crise

POUR COMMENCER

GÉNÉRALITÉS

Le système de management de la sûreté (SMS) est l'**outil opérationnel et méthodologique** qui permet de **mettre en œuvre le plan de sûreté** visant à protéger le patrimoine humain, matériel et immatériel de l'entreprise contre les actes de malveillance, en d'autres termes le « **comment** ». Il s'agit d'un ensemble de processus, de **procédures** et de pratiques fonctionnant en **cycle d'amélioration continue**. Ce cycle comprend les étapes suivantes :

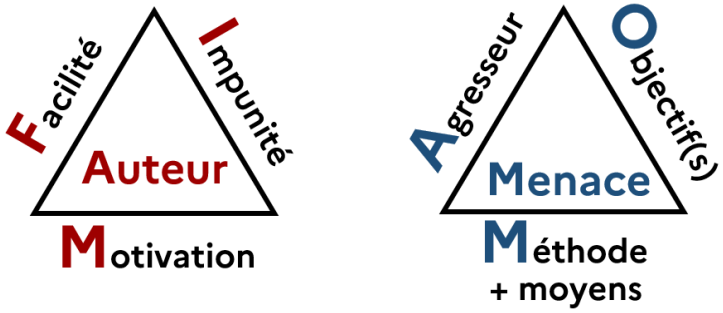
- Une **analyse de risques** où les valeurs sont clairement identifiées au sein de l'entreprise et son environnement, ainsi que les menaces, les vulnérabilités et les risques associés
- La mise en œuvre de **mesures de traitement** concernant les risques identifiés comme devant l'être
- La **surveillance et le contrôle** de ces risques et des mesures mises en place
- L'**amélioration continue** de l'ensemble du processus.

GÉNÉRALITÉS SUR LE MANAGEMENT DU RISQUE SÛRETÉ

Basé sur les **conditions de passage à l'acte d'un malveillant**, à savoir sa motivation, la facilité d'action et l'impunité potentielle, la **stratégie de sûreté a pour objectif** de dissuader, alerter, bloquer ou à défaut, freiner, réagir et intervenir, limiter ou au mieux supprimer les effets et les conséquences des dommages potentiels.

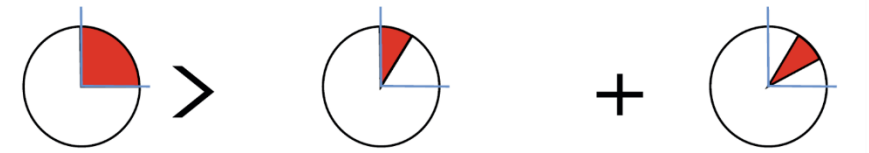
Une **menace se caractérise par 3 éléments** devant être réunis :

- Un auteur, qui peut être d'origine interne ou externe, d'opportunité ou professionnel, agir seul ou avec un complice
- Un objectif, qui peut être un bien matériel ou immatériel, ainsi qu'une personne
- Une méthode et des moyens d'action.



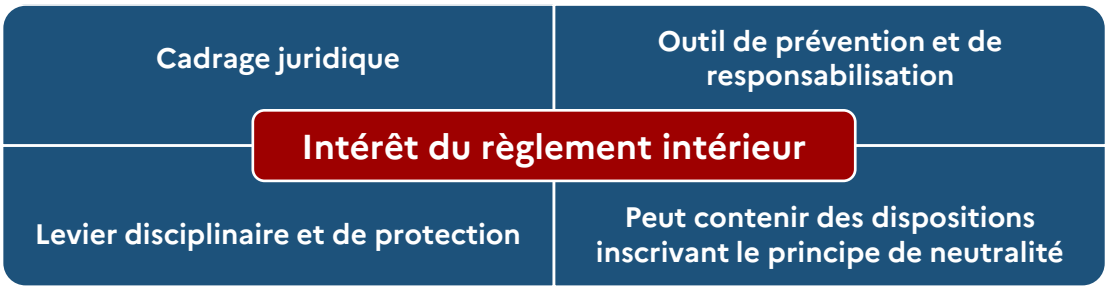
La **stratégie de sûreté repose sur la mise en œuvre d'une défense en profondeur des valeurs** s'appuyant sur des **barrières successives** allant de la périphérie, la périmétrie, à la volumétrie. Les mesures associées, d'ordres humaines, organisationnelles et techniques, doivent être cohérentes, adaptées, homogènes, redondantes et complémentaires.

Cette **défense en profondeur des valeurs doit permettre de répondre à l'équation de sûreté**, à savoir : le temps de freinage doit être strictement supérieur aux temps cumulés de détection, de traitement de l'alarme et d'intervention.



LE RÈGLEMENT INTERIEUR AVEC DES ÉLÉMENTS DE SÛRETÉ

Même s'il n'est obligatoire que pour les entreprises d'au moins 50 salariés, il est fortement recommandé de le mettre en place dans toutes les entreprises de par le fait qu'il permet de poser des notions de base de la sûreté tout en étant un **véritable levier et une protection juridique pour le dirigeant**.



Le règlement intérieur présente plusieurs intérêts en termes de sûreté pour le dirigeant :

- **Il définit un cadrage juridique** permettant de protéger les valeurs de l'entreprise en officialisant et en rendant opposable les règles spécifiques de sûreté applicables au sein de l'entreprise, dont les conditions d'accès au site et aux locaux, la cybersécurité, les dispositifs de vidéosurveillance, etc.
- C'est un **outil de prévention et de responsabilisation** en matière de santé et de sécurité au travail, notamment au travers d'obligations et d'instauration d'une culture de sûreté et de sécurité
- C'est un **levier disciplinaire et de protection** en établissant des échelles de sanctions en cas de manquement aux règles établies et en étant opposable
- Il peut également contenir des dispositions inscrivant le **principe de neutralité** et restreignant la manifestation des convictions, mais seulement sous certaines conditions strictement définies.

Quelques **points de vigilance** existent pour le dirigeant concernant le règlement intérieur. Celui-ci doit être **conforme aux lois et règlements** en vigueur ainsi qu'aux accords et conventions collectives applicables. Il doit également **être accessible** aux salariés, régulièrement mis à jour, et rester **équilibré et proportionné** aux besoins de l'entreprise. Enfin, il ne doit pas contenir de restrictions injustifiées aux droits et libertés individuelles.

En plus du règlement intérieur, d'autres documents en lien avec la sûreté et la sécurité existent : le document unique d'évaluation des risques professionnels (DUERP), le plan de prévention et le protocole de sécurité.

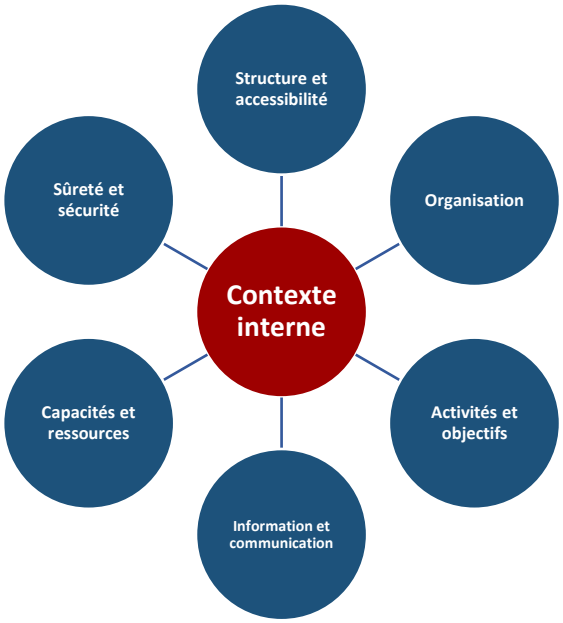
POUR ALLER PLUS LOIN

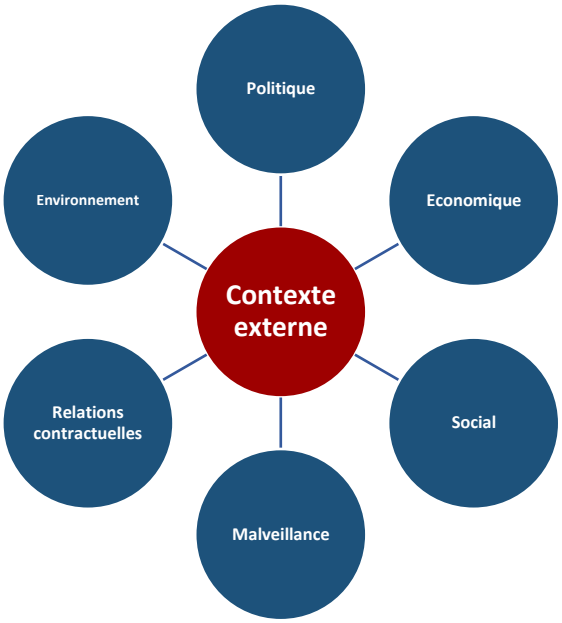
CONNAISSANCE DE L'ENVIRONNEMENT INTERNE/EXTERNE

Avant de pouvoir effectuer une analyse de risques sûreté, il est tout d'abord nécessaire de bien connaître son entreprise et l'environnement interne comme externe dans lequel elle évolue. Pour cela, il faut principalement étudier les thèmes suivants :

- **Pour le contexte interne** :
  - **Structure et accessibilité** : configuration du site, plans, accès, zonages, fluides, etc.
  - **Organisation** : gouvernance, responsabilité, organisation, recrutement, sensibilisation à la sûreté, etc.
  - **Activités et objectifs** : secteur d'activité, objectif de l'entreprise, stratégies, valeurs, flux, sous-traitants, prestataires, histoire et culture d'entreprise, etc.
  - **Information et communication** : moyens, procédures, culture interne, etc.
  - **Capacités et ressources** : stock, moyens de secours, etc.
  - **Sûreté et sécurité** : type d'installation, exigences légales et réglementaires voire assurancielles, moyens et dispositifs de protection mécanique et électronique, dispositifs de contrôle d'accès, moyens humains, sécurité et sûreté informatique, historique des incidents de sécurité et de sûreté, plans de sécurisation, chaîne d'alerte, rôles et responsabilités, dans la sûreté et la sécurité, etc.

- **Pour le contexte externe** :
  - **Politique** : conflits externes et internes, stabilité des institutions, etc.
  - **Économique** : taux de chômage, démographie, etc.
  - **Social** : population au voisinage, conflits sociaux, niveau d'activisme, communautés, image et notoriété de l'organisation, etc.
  - **Malveillance** : présence policière, actes de délinquance aux alentours, groupes criminels ou terroristes, etc.
  - **Relations contractuelles** : relations avec les parties prenantes externes, dont les sous-traitants et les clients, leurs perceptions et leurs valeurs
  - **Environnement** : exposition à un aléa naturel ou industriel et technologique, circulation et flux.





Pour aller plus loin, il est possible de se référer à l'étape 1 du guide pratique d'analyse de risques coécrit par la DRSD et la direction de la protection des installations, moyens et activités de la défense (DPID), publié en 2023 et disponible sur le site internet de la DRSD.

IDENTIFICATION DES VALEURS

Il est nécessaire de procéder à l'inventaire des valeurs que possède l'entreprise afin d'être en mesure d'apprécier les actifs pouvant être considérés comme prioritaires.

Une valeur est un **bien**, une **personne**, une **information matérielle ou immatérielle**, un **savoir-faire** qui revêt un caractère précieux, voire indispensable (pour l'activité, le fonctionnement et la pérennité de l'entreprise) et vulnérable du fait de son prix, de son attrait commercial, de son coût, de son délai de remplacement ou de son caractère unique.

Les valeurs peuvent être regroupées au sein des catégories suivantes :

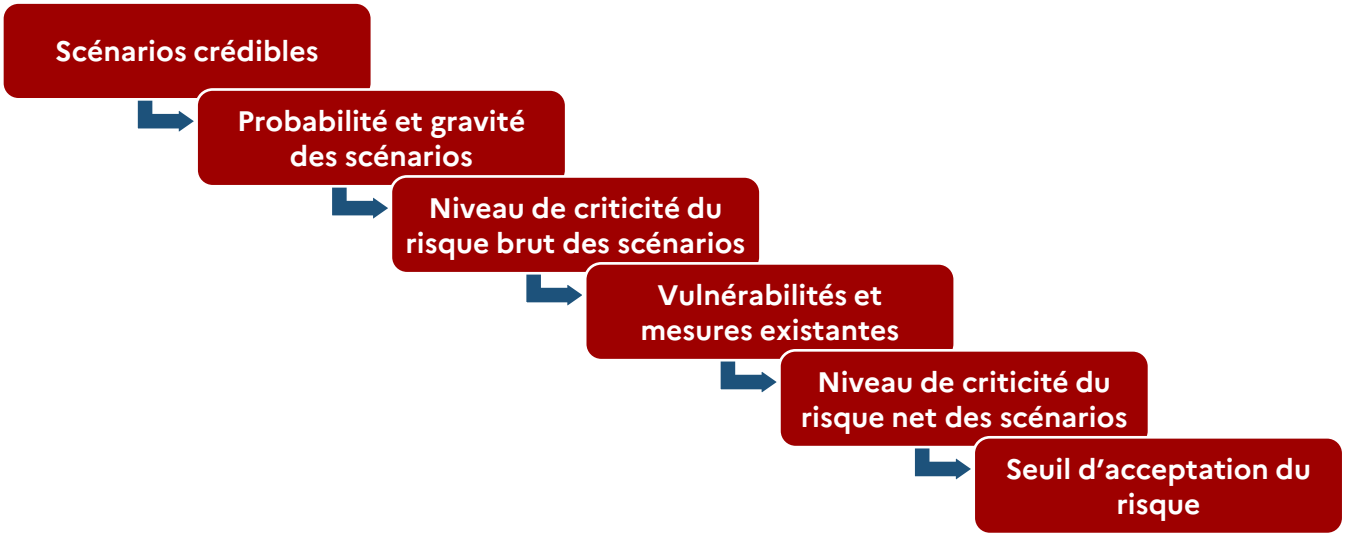
- Les **ressources humaines** : personnel interne détenant un savoir-faire stratégique, etc.
- Les **ressources intellectuelles** : informations sensibles qu'elles soient RH, commerciales ou technologiques, etc.
- Les **systèmes d'information** : serveurs, réseaux, applications, logiciels, etc.
- L'**image** : réputation, confiance des partenaires, confidentialité, stratégie, etc.
- Les **infrastructures** : bâtiments, bureaux, zones de stockage, zones de production, points sensibles, etc.
- Les **prestations externes** : sous-traitant, partenaires ou fournisseurs critiques, etc.
- Les **matériels et capacités** : équipements, liquidités et trésorerie, stocks intermédiaires et de produits finis, matériels, outils spéciaux, machines, services, etc.
- Les **transports** : énergies, fluides, déchets, etc.

VALEURS							
Ressources humaines	Ressources intellectuelles	Systèmes d'informations	Image	Infrastructures	Prestations externes	Matériels et capacités	Transports

Pour aller plus loin, il est possible de se référer à l'étape 2 du guide pratique d'analyse de risques coécrit par la DRSD et la DPID.

ÉVALUATION DES RISQUES SÛRETÉ

La phase d'évaluation des risques sûreté se déroule en 6 étapes. Elle comprend la réalisation d'une cotation et d'une cartographie du niveau de criticité des scénarios de risques sûreté auxquels l'entreprise est exposée.



1. **Étudier des scénarios crédibles pour l'entreprise**
2. **Déterminer la probabilité et la gravité des scénarios** :
    - La probabilité correspond à une probabilité d'occurrence d'une source de menace ou d'un aléa. Elle est facilement mesurable quand il s'agit de sinistres statistiquement connus. Lorsqu'il s'agit d'une menace provenant d'une intention humaine, il est possible d'évaluer la probabilité en considérant la crédibilité d'un scénario à partir des antécédents d'incident (sur le site, le secteur d'activité et l'environnement géographique) et la faisabilité d'un scénario à partir du niveau de technicité et de ressources des auteurs
    - Pour chaque scénario, il sera nécessaire de recenser leur gravité donc d'identifier les impacts potentiels sur l'entreprise et son environnement. Il existe **plusieurs types d'impacts** : humain et social, financier et juridique, image, opérationnel et sur l'environnement

3. **Déterminer le niveau de criticité du risque brut des scénarios** :
    - Le risque brut est le risque identifié pour l'entreprise dont l'évaluation de la criticité se fait avant la prise en compte des moyens de maîtrise. Il correspond à un niveau de criticité brut du risque
    - Le niveau de criticité du risque peut être déterminé pour calculer un risque brut par la **combinaison entre la probabilité et la gravité**
    - Cela permettra de cartographier et de hiérarchiser les scénarios pertinents sur une matrice des risques

4. **Identifier les vulnérabilités de l'entreprise et les mesures existantes** :
    - Une vulnérabilité correspond à une faiblesse connue de l'entreprise susceptible d'être exploitée par des menaces ou d'augmenter l'exposition aux risques. Les vulnérabilités peuvent être regroupées dans les catégories suivantes : matériel, logiciel, réseau, organisme et partenaire, personnel et infrastructure
    - Les mesures de sûreté existantes sont toutes les mesures déjà mises en place ou prévues dans le but de réduire l'exposition de l'entreprise à une menace ou un aléa. Il existe des **mesures de prévention**, visant à diminuer la probabilité d'une menace, et des **mesures de protection** visant à réduire, diminuer ou contenir les effets d'un risque après sa survenue
    - Cela permettra de prendre la décision de traitement du risque la plus adaptée. Ces données seront utiles pour déterminer le niveau de criticité du risque net durant l'étape suivante

5. **Déterminer le niveau de criticité du risque net des scénarios** :
    - Il est nécessaire de pondérer le risque brut en appréciant les mesures de sûreté existantes et les vulnérabilités de l'entreprise. Cette pondération permet de déterminer le niveau de criticité du risque net qui devra être considéré lors de la décision de traitement du risque
    - Un risque net peut être un risque significatif confirmé (le niveau de criticité net est supérieur au seuil d'acceptabilité) ou un risque significatif maîtrisé (le niveau de criticité net est inférieur au seuil d'acceptabilité)

6. **Déterminer le seuil d'acceptation du risque** :
    - Le seuil d'acceptation du risque doit être déterminé afin d'identifier les risques significatifs maîtrisés et les risques significatifs confirmés. Ce seuil a pour but d'aider à la prise de décision en matière d'ordre de priorité et de traitement du risque.

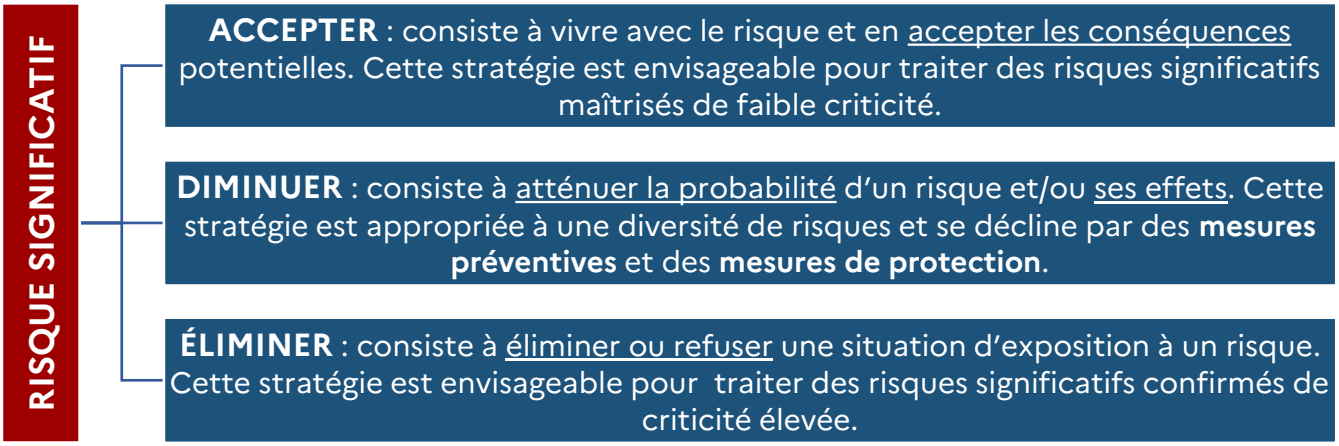
Pour aller plus loin, il est possible de se référer aux étapes 3 à 8 du guide pratique d'analyse de risques coécrit par la DRSD et la DPID.

MAÎTRISE ET TRAITEMENT DES RISQUES SÛRETÉ

La phase de maîtrise et de traitement des risques se déroule en 2 étapes. Elle consiste à prioriser les risques établis lors de la phase d'évaluation des risques puis de déterminer des mesures de traitement.

Le traitement du risque est un processus générique destiné à modifier un risque et pouvant inclure :

- Un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque
- La prise ou l'augmentation d'un risque en vue de saisir une opportunité
- L'élimination de la source d'une menace ou d'un aléa
- Une modification de la probabilité
- Une modification des conséquences
- Un partage du risque avec une ou plusieurs autres parties incluant des contrats et un financement du risque
- Un maintien du risque fondé sur une décision argumentée.



Il est désormais nécessaire de **définir une stratégie de traitement du risque** en choisissant des mesures de sûreté adaptées pour **accepter**, **éliminer** ou **diminuer les risques**. Ces stratégies ne s'excluent pas mutuellement et peuvent être mises en œuvre simultanément.

Les **mesures de prévention** sont des dispositifs ou des actions propres **à diminuer la probabilité d'occurrence** d'un risque, au moyen de solutions organisationnelles, techniques et humaines. Voici quelques exemples :

- Actions sur les **infrastructures** : protection physique (bloc-porte, barrière, etc.), protection juridique, surveillance humaine, dispositif techniques (contrôle d'accès, détection d'intrusion, vidéosurveillance, détection incendie…), etc.
- Actions sur les **systèmes d'information** : politique de sécurité des systèmes d'informations, mises à jour régulières, gestion des authentifications, cloisonnement des réseaux, surveillance des réseaux, etc.
- Actions sur les **fournisseurs** : augmentation des stocks stratégiques, diversification des fournisseurs de la chaîne logistique, etc.
- Actions sur les **ressources humaines** : sensibilisation et mesures comportementales, exercices de simulation, formation aux risques sûreté, etc. Les **actions de sensibilisation aux risques sûreté** et l'instauration d'une **culture de sûreté** ont un caractère particulièrement **important** dans le dispositif global de protection des valeurs de l'entreprise.

Les **mesures de protection** sont des dispositifs ou des actions propres à **diminuer, réduire ou contenir les effets d'un risque après sa survenue**. Les moyens de protection agissent sur la diminution des conséquences du risque, au moyen de solutions organisationnelles, techniques et humaines. En voici quelques exemples :

- Actions sur les **infrastructures** : protection physique, dispositif technique (contrôle d'accès, détection d'intrusion, vidéosurveillance, protection incendie, etc.), utilisation d'un site alternatif, processus alternatifs, etc.
- Actions sur les **systèmes d'information** : moyens de communication de secours, restitution des sauvegardes, fonctionnement dégradé, etc.
- Actions sur les **fournisseurs** : approvisionnement par un fournisseur alternatif, etc.
- Actions sur les **ressources humaines** : utilisation du télétravail, dispositif d'intervention, etc.

Pour aller plus loin, il est possible de se référer aux étapes 9 et 10 du guide pratique d'analyse de risques coécrit par la DRSD et la DPID.

Dans le cadre de la maîtrise d'un risque, les cas particuliers de la continuité et reprise d'activité ainsi que de la gestion de crise sont abordés plus spécifiquement ultérieurement.

SURVEILLANCE, CONTRÔLE ET RÉEXAMEN DES RISQUES SÛRETÉ

La **surveillance** correspond à la vérification, la supervision, l'observation critique ou la détermination de l'état du risque dans le but d'identifier continûment des changements par rapport au niveau de performance exigé ou attendu. La surveillance peut s'appliquer à un cadre organisationnel de management du risque, un processus de management du risque, un risque ou un moyen de maîtrise du risque.

Dans ce cadre, il est **utile de définir des indicateurs de sûreté**, permettant ainsi un **meilleur pilotage** de la sûreté au sein de l'entreprise, mais surtout de **mettre en évidence la valeur ajoutée de la sûreté à la performance de l'entreprise** :

- **Indicateurs de suivi d'activité**, permettant de recenser en termes de **quantité** les actions liées à la sûreté réalisées, par exemple :
  - Nombre de rondes effectuées
  - Nombre d'incidents constatés
  - Nombre d'audits de sûreté réalisés (interne et externe)
  - Nombre de badges délivrés (nouveaux collaborateurs, visiteurs)
  - Nombre de collaborateurs sensibilisés à la sûreté
  - Nombre d'alarmes intempestives
  - Nombre d'opérations de maintenance préventive et corrective
  - Nombre d'écarts des prestataires de sécurité privée par rapport au contrat
  - Nombre d'accompagnements en sûreté pour des projets de nouveau contrat
  - Nombre de vols (ordinateur, matière première, outil, produit fini)
  - etc.
- **Indicateurs de performance** (KPI)[4], permettant de caractériser, en termes de **qualité**, l'**efficacité** des actions et mesures de sûreté par rapport aux objectifs stratégiques et opérationnels fixés, par exemple :
  - Pourcentage des personnes sensibilisés par an
  - Nombre de remontée de faits de sûreté d'initiative par les collaborateurs
  - Conformité à certaines exigences de sûreté (assurance, réglementaire, etc.)
  - Temps moyen de levée de doute et d'intervention en cas de détection d'intrusion
  - Diminution du nombre d'alarmes intempestives
  - Nombre de faits de sûreté détectés et déjoués
  - Taux de non-conformité dans les audits de sûreté (interne et externe)
  - Diminution du nombre de faits de sûreté (dégradation, vol, etc.)
  - Pourcentage de satisfaction des partenaires (clients, prestataires, collaborateurs, etc.) par rapport à la sûreté
  - Baisse du nombre d'écarts des prestataires de sécurité privée par rapport au contrat, etc.

[4] *Key Performance Indicator* : indicateur clé de performance (définition dans le glossaire p 72).

- **Indicateurs de retour sur investissement** (ROI)[5], permettant de mettre en avant la performance de la sûreté en valeur économique ou stratégique pour l'entreprise, par exemple :
    - Coût des incidents évités : estimation financière des pertes (matérielles, données, arrêt de production) qui auraient eu lieu sans les dispositifs mis en place, comparée au coût de ces dispositifs, voire aux pertes des années précédentes avant la mise en place de ces dispositifs
    - Nombre d'appels d'offres (sensibles) auxquels l'entreprise est éligible grâce aux dispositifs de sûreté
    - Nombre de contrats remportés où la sûreté a été un facteur discriminant
    - Gain de continuité d'activité : montant du chiffre d'affaires préservé grâce à la reprise d'activité après un sinistre, etc.

Afin de prendre du recul et de s'assurer, dans une logique d'amélioration continue, que les dispositifs de sûreté mis en œuvre au sein de l'entreprise soient adaptés, opérationnels et appliqués, mais également d'identifier des vulnérabilités, il est **nécessaire de réaliser de manière périodique des audits de sûreté internes et externes**.

L'audit de sûreté externe offre l'avantage d'avoir un regard extérieur. Néanmoins, il **permet à une entité tierce l'accès à des informations sensibles et stratégiques** de l'entreprise. Il est donc nécessaire de prendre des précautions et d'avoir une vigilance toute particulière. Dans ce cadre, voici plusieurs points d'attention :

- **La sélection rigoureuse du prestataire** : référence, indépendance par rapport à des fournisseurs ou concurrents, qualifications, etc.
- **Le cadrage juridique et contractuel** : accord de confidentialité (NDA), définition du périmètre de l'audit, propriété des données et du rapport
- **La protection des données et des accès** : principe du moindre privilège, anonymisation des données quand cela est possible, accompagnement permanent sur le site
- **La gestion de la restitution** : rapport sécurisé (chiffrement, canaux sécurisés), destinataires limités, destruction des données à la fin de la mission.

PROCÉDURES DE SÛRETÉ

Une procédure de sûreté a pour but de **définir « comment » mettre en œuvre un objectif spécifique** avec des mesures humaines, organisationnelles et techniques.

La formalisation d'une procédure permet entre autres de :

- **La pérenniser dans le temps**, c'est tout particulièrement utile en cas de changement de la seule personne ayant connaissance de l'information (cas d'un départ de l'entreprise par exemple)
- **Éviter les éventuelles approximations** dans l'application des consignes
- Enfin d'avoir des **sanctions associées** en cas de non-respect de ces consignes.

[5] *Return On Investment* : indicateur de retour sur investissement (définition dans le glossaire p 72).

Les **principales procédures de sûreté sont** :

- Consignes globales et spécifiques de sûreté
- Gestion des visiteurs
- Gestion des accès, des flux, dont l'ouverture et la fermeture du site en temps normal et lors des périodes de fermeture annuelle
- Gestion des livreurs, prestataires, stagiaires/apprentis/alternants et du courrier
- Traitement des incidents (remontée et gestion de l'information en interne et en externe, RETEX, etc.)
- Politique de protection de l'information
- Consignes de communication en externe à l'entreprise et de discrétion professionnelle
- Procédure de sûreté liée à la mobilité nationale et internationale
- Fiches réflexes en cas d'événement sûreté
- Gestion des clés et des badges
- Procédure en cas d'élévation de la menace
- Fonctionnement en mode dégradé, etc.

Certaines des procédures de sûreté sont détaillées en annexe 8.

DISPOSITIF DE VEILLE

Un dispositif de veille est un processus continu et itératif de surveillance active de l'environnement d'une entreprise visant à collecter, analyser et **diffuser l'information pertinente afin d'anticiper les évolutions et réduire l'incertitude dans la prise de décision**.

Il existe **différents types de veilles** se distinguant selon leur périmètre de surveillance. Les principaux sont :

- **La veille stratégique** : elle surveille l'environnement global (géopolitique, tendances de fond) pour éclairer les décisions à long terme
- **La veille concurrentielle** : elle analyse les actions, forces et faiblesses des concurrents actuels et potentiels
- **La veille technologique** : elle suit les innovations, brevets et nouvelles technologies susceptibles d'impacter le secteur
- **La veille réglementaire et normative** : elle surveille les évolutions légales et les normes pour assurer la conformité
- **La veille réputationnelle** : elle surveille l'image de l'entreprise et les discussions la concernant sur le web et les réseaux sociaux.

L'intérêt pour une entreprise réside dans sa capacité à transformer l'importante source d'information disponible et reçue, aussi appelée « infobésité », en connaissance actionnable. Cela permet de détecter les opportunités et les menaces avant les concurrents, de sécuriser les décisions stratégiques, d'innover en s'appuyant sur l'existant et de protéger son patrimoine immatériel face à la guerre économique. Dans un monde VICA (Volatile, Incertain, Complexe, Ambigu), la veille confère un **avantage concurrentiel** décisif en offrant **un temps d'avance**.

PLAN DE CONTINUITÉ D'ACTIVITÉ / PLAN DE REPRISE D'ACTIVITÉ

Alors que le management du risque et son plan de traitement visent à protéger les valeurs de l'entreprise et réduire l'impact du risque, disposer d'un **plan de continuité d'activité** (PCA) et d'un **plan de reprise d'activité** (PRA) permet de **prévoir des solutions permettant de poursuivre ou de maintenir les activités critiques**, et ainsi garantir la pérennité de l'entreprise. Cette capacité de réponse consiste en la mise en œuvre de solutions flexibles et robustes préétablies, par des acteurs formés.

En vue de rédiger un PCA et un PRA, il est nécessaire de :

- Définir le périmètre des PCA/PRA
- D'élaborer les PCA puis les PRA
- De définir le processus d'activation des PCA/PRA
- D'effectuer un maintien en conditions opérationnelles (MCO).

Pour aller plus loin, il est possible de se référer à l'outil-guide pratique d'élaboration et de mise en œuvre des PCA ainsi qu'à sa méthode flash établis par la DRSD en 2025, disponibles sur le site internet de la DRSD.

PLAN DE GESTION DE CRISE

La crise est une situation globalement imprévisible où les faits recueillis permettent de constater que les **processus et l'organisation habituelle mis en place ne permettent plus d'absorber la totalité des impacts** rencontrés et la multiplicité des **parties prenantes** concernées, impliquées ou à informer.

Une crise peut se définir grâce à **8 caractéristiques** fondamentales :

- Incertitude
- Perturbation
- Urgence et pression temporelle
- Impacts multiples
- Parties prenantes
- Émotion et attractivité des médias
- Point de rupture
- Cinétique[6].

[6] Une crise se caractérise également par son mouvement, son évolution constante. Il est en revanche impossible de modéliser par anticipation cette cinétique, car les situations chaotiques ne respectent pas de schéma directeur préétabli et linéaire.

Il s'agit d'une **posture dérogatoire** où l'objectif est alors d'assurer la pérennité de l'entreprise dans un contexte dégradé, imprévu et évolutif.
Il s'agit donc pour cela de **gérer** :

- **Les impacts actuels**, futurs et potentiels au niveau des personnes, de l'environnement, des activités, de la réputation et du droit
- **Les parties prenantes** impactées, impliquées et à informer, notamment leurs attentes.

Dans ce cadre, le plan de gestion de crise repose sur **4 piliers** :

- **Organisation** de la gestion de crise : pilotage de la crise, fonctions permanentes (communication, RH, juridique), fonctions mobilisables (experts métiers, etc.), fonctions organisationnelles (secrétariat, etc.)
- **Processus** de gestion de crise : alerte, mobilisation, pilotage, démobilisation et RETEX
- **Méthode AGIR** : Afficher les faits, Gérer les impacts, Identifier les parties prenantes (impactées, impliquées et à informer) et Répondre par un plan d'action
- Supports de crise.

Pour aller plus loin, il est possible de se référer au guide de survie face à la crise publié par la DRSD en 2024 et disponible sur son site internet.

FICHE 4 – SÛRETÉ DU PERSONNEL

Pour commencer

- Définition
- Quelques procédures clés
- Procédure en cas de déplacement à l'international

Pour aller plus loin

- Procédures organisationnelles permettant de renforcer la sûreté du personnel

POUR COMMENCER

DÉFINITION

Le **premier objectif** du domaine de la sûreté du personnel est de **garantir la sûreté des collaborateurs**. S'il constitue une valeur essentielle à protéger, il peut également représenter une source potentielle de menace, volontaire ou non. Il est donc nécessaire d'assurer la protection des personnes entre elles et contre elles-mêmes. Dans cette logique, le **second objectif** consiste à **vérifier l'éligibilité et l'aptitude du personnel**, des sous-traitants et de l'ensemble des parties prenantes **à accéder aux actifs stratégiques de l'entreprise**, et ce pendant toute la durée de leur emploi ou de leur mission.

Il est donc nécessaire :

- **D'instaurer une culture de sûreté**, l'action de chacun permettant de contribuer à la sûreté globale de l'entreprise et de ses collaborateurs
- En plus de la **mise en œuvre de certaines procédures organisationnelles, d'entretenir des échanges de qualité et régulier** avec le service des ressources humaines (RH) de l'entreprise et des autres fonctions supports (juridique, achat, etc.).

QUELQUES PROCÉDURES CLÉS

Certaines procédures organisationnelles liées à la sûreté du personnel sont particulièrement importantes :

- **Consignes relatives à la sûreté** avec un renvoi vers le règlement intérieur
- **Circuit arrivée et départ d'un collaborateur de l'entreprise**. Ce circuit permet de s'assurer que certains messages clés sont transmis, tant à l'arrivée qu'au départ d'un collaborateur, mais également que certains matériels ont bien été restitués lors du départ (badge d'accès, ordinateur portable) ou certaines actions bien effectuées (clôture du compte informatique, retrait des droits d'accès au site, etc.)
- **Gestion des visiteurs**
- **Sensibilisation initiale, puis régulière**, et adaptée du **personnel** et des **prestataires aux risques de sûreté** et aux bons gestes à adopter

- **Gestion du personnel temporaire** (stagiaires, alternants, apprentis et intérimaires). Cela comprend notamment la désignation d'un tuteur, la relecture des rapports de stage/thèse, des accès réduits aux locaux, l'intégration d'une clause de confidentialité dans les conventions, etc.

PROCÉDURE EN CAS DE DÉPLACEMENT À L'INTERNATIONAL

L'article L4121-1 du code du travail instaure envers le dirigeant d'une entreprise une **obligation de sécurité envers ses salariés,** même s'ils sont en mission à l'étranger, avec la mise en œuvre de **moyens renforcés** selon la jurisprudence *Air France* de 2015. En fonction des pays et des risques associés, des **mesures adaptées doivent donc être déployées**, à savoir :

- Des **mesures de prévention** : information sur les risques, processus voyage interne, formation sur les bonnes pratiques, protocole de sécurité (interdiction d'aller dans certaines zones), gestion des données (messagerie de communication spécifique, VPN, stockage des données uniquement et strictement nécessaires), etc.
- Et des **mesures de protection** : téléphone et ordinateur « blanchis », assurance voyage dédiée et adaptée (rapatriement, frais médicaux), véhicule blindé, protection rapprochée, kit de secourisme, etc.

Il est systématiquement recommandé de :

- **Suivre les conseils mis à disposition** sur le site conseils-aux-voyageurs du ministère de l'Europe et des Affaires étrangères (MEAE)
- S'inscrire sur le fil d'Ariane du MEAE permettant de recevoir des alertes durant les voyages.

La jurisprudence *Abidjan*, issue d'un arrêt de la Cour de cassation du 7 décembre 2011, a mis en lumière l'extension de l'obligation de sécurité de l'employeur à la **vie privée** en déplacement à l'international.

En cas d'expatriation, des éléments complémentaires sont à prendre en compte.

POUR ALLER PLUS LOIN

PROCÉDURES ORGANISATIONNELLES PERMETTANT DE RENFORCER LA SÛRETÉ DU PERSONNEL

Les procédures organisationnelles suivantes permettent de renforcer la sûreté du personnel :

- Définition des **critères d'éligibilité et d'adéquation** du personnel pour **accéder aux actifs** de l'entreprise
- **Vérification périodique** de l'adéquation des accréditations à certains actifs (accès administrateur au système d'information, accès à certains locaux sensibles, etc.)
- **Vérification de certains éléments lors du recrutement** d'un nouveau collaborateur, surtout pour ceux amenés à occuper un poste sensible, en respectant le cadre légal
- **Gestion de visites de délégations**, notamment étrangères, appelée « parcours de notoriété »[7]
- Identification **d'indicateurs de sûreté** (indicateur d'activité, KPI et ROI) spécifiques à la sûreté du personnel (pourcentage des personnes sensibilisées par an, nombre de remontée de faits de sûreté d'initiative par les collaborateurs, etc.)
- Consignes de **communication externe** (consignes lors d'événement extérieur telles que des salons, la validation des contenus diffusés en dehors de l'établissement, etc.)
- Consignes de **discrétion**, entre autres dans les lieux publics et la **vigilance sur les réseaux sociaux**
- **Réalisation de fiches réflexes à l'attention des collaborateurs par rapport à des faits de sûreté** : intrusion, individu suspect, véhicule suspect, alerte à la bombe, survol de drone, etc.
- Instauration d'un **complément dans l'adresse e-mail** (.ext par exemple) permettant à un extérieur à l'entreprise d'**identifier un personnel temporaire** (prestataire, stagiaire, apprenti, alternant)
- Dans certains cas particuliers, la réglementation peut imposer la réalisation d'une enquête administrative préalable pour la personne souhaitant accéder à une zone spécifique comme l'accès à une zone protégée (ZP), un point d'importance vitale (PIV), une zone réservée (ZR) ou une zone à régime restrictif (ZRR).

[7] Pour plus de détails, voir la fiche « parcours de notoriété » établie en 2025 par la DRSD.

FICHE 5 – SÛRETÉ PHYSIQUE DES VALEURS

Pour commencer

- Définition
- Généralités
- Protection mécanique
- Contrôle d'accès
- Détection d'intrusion
- Vidéosurveillance

Pour aller plus loin

- Surveillance humaine
- Complément sur la protection mécanique
- Complément sur le contrôle d'accès
- Complément sur la détection d'intrusion
- Complément sur la vidéosurveillance
- Anticipation

POUR COMMENCER

DÉFINITION

L'objectif du domaine de la sûreté physique de l'entreprise est de s'assurer de la **protection physique des valeurs détenues ou gérées par l'entreprise afin de se prémunir d'un risque lié à des menaces et des vulnérabilités**. Ces valeurs peuvent être une personne, un bien matériel (installation, matériel, produit, etc.) ou immatériel (plan, document, etc.).

Il est donc nécessaire :

- D'identifier les zones **où les valeurs sont détenues**
- De **protéger les zones** identifiées avec des mesures adaptées aux risques auxquels elles sont soumises, les mesures étant d'ordre humain, organisationnel et technique
- D'**intégrer la sûreté par défaut** (principe de *security by default*) et **en anticipation** le plus en amont possible pour tout projet de construction/rénovation (principe de *security by design*).

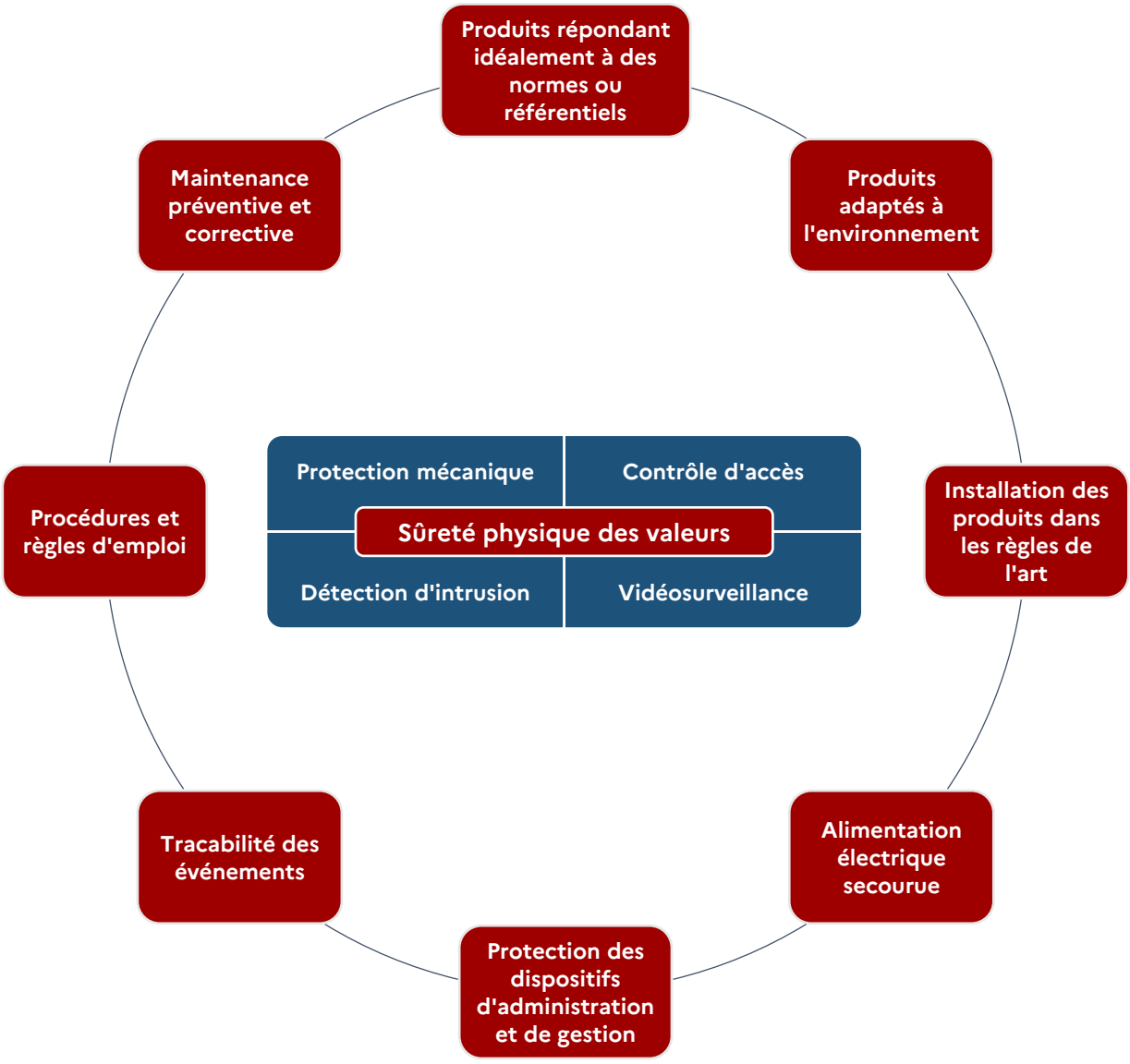
GÉNÉRALITÉS

Comme évoqué précédemment :

- La **défense en profondeur des valeurs** repose sur des barrières successives (périphérie, périmétrie et volumétrie) où toutes les mesures **humaines, organisationnelles et techniques** (HOT) sont parfaitement complémentaires, homogènes et redondantes, de manière à se prémunir des risques liés aux menaces et aux vulnérabilités identifiés
- Cette **défense en profondeur des valeurs doit permettre de répondre à l'équation de sûreté**
- L'**objectif** est de dissuader, alerter, bloquer ou à défaut freiner, réagir et intervenir, limiter ou au mieux supprimer les conséquences des dommages potentiels
- Les mesures doivent se **conformer à la réglementation en vigueur**.

Les mesures techniques regroupent : la **protection mécanique** (PM), le **contrôle d'accès**, la **détection d'intrusion** et la **vidéosurveillance** (CADIVS). L'ensemble de ces dispositifs nécessite :

- Le choix de produits répondant idéalement à des normes ou référentiels
- Des produits **adaptés à l'environnement**, notamment en cas de zone fortement exposée aux vents, de zone montagneuse, de bord de mer, etc.
- Leur installation selon les **règles de l'art**, idéalement en se conformant aux différents référentiels (certaines entreprises pouvant être certifiées)
- Une alimentation électrique **secourue** (batterie, onduleur, groupe électrogène, etc.) dans le but d'assurer la continuité de fonctionnement en cas de coupure électrique
- La protection des dispositifs d'administration et de gestion (poste administrateur, poste de gestion des droits, etc.)
- La possibilité d'assurer la **traçabilité** des événements
- Des **procédures et règles d'emploi**
- L'instauration d'une politique de **maintenance** préventive et corrective de ces dispositifs.



LA PROTECTION MÉCANIQUE

La protection mécanique constitue le **socle indispensable et minimal de défense** de tout dispositif de sûreté, en érigeant une série d'obstacles physiques successifs destinés à dissuader, bloquer ou à défaut freiner toute action de malveillance.

Les **principaux dispositifs de protection mécanique sont** les suivants :

- **Clôtures** :
  - L'objectif principal est de délimiter la propriété et de protéger le site d'une intrusion. Elles peuvent également permettre d'empêcher les vues depuis l'extérieur
  - Il existe plusieurs types de clôtures : pleines, grillagées (simple torsion, soudé, etc.), treillis soudés, barreaudées, mixtes, avec ou sans soubassement
- **Points d'accès au niveau d'une clôture** : **portails** (véhicule) et **portillons** (piéton). Ils peuvent être pivotants ou coulissants, à un ou deux vantaux, et à ouverture manuelle ou motorisée
- **Parois de bâtiments** (murs) :
  - Il s'agit de la protection principale d'un bâtiment
  - Il existe des parois de résistance mécanique faible ou correcte. Le niveau dépend principalement de la structure des parois : bois, carreaux de plâtre, bardage simple ou double peau, parpaing creux ou plein, brique creuse ou pleine, béton armé, etc.
- **Vitrage** :
  - Il existe différents types de vitrages répondant à différentes finalités : résistant au vandalisme, à l'effraction, à l'attaque par balle, à l'explosion, etc.
  - Il est nécessaire de prendre en compte la fixation du vitrage en plus du vitrage lui-même
- **Volet** :
  - Il s'agit d'une protection supplémentaire à un vitrage
  - On peut retrouver des volets de type battant, persienne, roulant, coulissant ou pliant
- **Rideau ou grille métallique**. Ils apportent également une protection supplémentaire à un vitrage ou un accès
- **Points d'accès au niveau d'un bâtiment** : les **blocs-portes**, appelés couramment « **portes** ». Ils peuvent être de plusieurs types : en bois, métallique, PVC, etc., mais également à âme creuse, pleine ou alvéolaire. Certains permettent une **unicité de passage** (tourniquet, passage non gardé couramment appelé PNG)
- **Dispositifs de verrouillage** (serrure et verrou) :
  - Ils permettent de protéger et restreindre l'accès à une zone, et notamment d'éviter un accès à une zone d'une personne n'y étant pas autorisée
  - Il existe différentes catégories de serrures mécaniques : intégrée ou rapportée, multipoints, antipanique, à sûreté mécanique ou à sûreté électronique, etc.

Cependant, la protection mécanique d'une valeur n'est pas suffisante seule. Elle nécessite d'être complétée par un dispositif de contrôle d'accès.

LE CONTRÔLE D'ACCÈS

Le dispositif de contrôle d'accès est une des **composantes majeures** de la protection d'une valeur. En effet, il permet la **gestion des flux** (personnes, véhicules) **accédant aux valeurs de l'entreprise** (site, bâtiment, local, voire système d'information). La grande majorité des intrusions se fait d'ailleurs par les accès.

Un dispositif de contrôle d'accès peut être :

- **Humain**, par un agent d'accueil ou un agent privé de sécurité, en direct ou via un interphone/vidéophone
- **Technique**, via un dispositif de clé mécanique, de clavier alphanumérique à code, de badge ou biométrique
- Ou les deux associés.

3 catégories de moyens permettent d'identifier une personne porteuse des droits d'accès :

- Ce qu'elle possède : clé mécanique ou électronique, badge, etc.
- Ce qu'elle connaît : code personnel ou collectif
- Ce qu'elle est : biométrie.

Si deux facteurs sont réunis (« je possède » et « je connais » par exemple), on parle d'**authentification**.

Ces dispositifs de contrôle d'accès **imposent de respecter certaines règles juridiques et de mise en œuvre** :

- Respect du principe de proportionnalité au but recherché et justifié
- Consultation des instances représentatives du personnel avant le déploiement
- Information du personnel sur les finalités de ces dispositifs, notamment avec une mention dans le règlement intérieur
- Respect de la protection des données à caractère personnel (durée de conservation, etc.)
- Contraintes supplémentaires concernant les dispositifs biométriques.

Afin d'assurer une bonne gestion des accès, il est nécessaire de définir des **critères de droits d'accès** en fonction des profils d'utilisateurs.

Il est possible de se référer au référentiel APSAD D83 concernant le contrôle d'accès.

La protection mécanique, associé à un dispositif de contrôle d'accès, nécessite un dispositif de détection d'intrusion en vue de pouvoir répondre à l'équation de sûreté au travers de l'identification d'une intrusion et ainsi déclencher l'élément d'intervention.

LA DÉTECTION D'INTRUSION

Le système de détection d'intrusion est **au cœur de l'équation de sûreté** permettant d'assurer la protection des valeurs. En effet, il joue le rôle clé de **surveiller les valeurs** de l'entreprise, et en cas de détection d'une intrusion, de transmettre l'alerte et d'entraîner une levée de doute, voire de déclencher une intervention.

Les **principaux dispositifs de détection d'intrusion** sont les suivants :

- Barrière (à infrarouge ou à hyperfréquence)
- Détecteur sur clôture
- Contacteur d'ouverture
- Détecteur volumétrique (à infrarouge passif, à hyperfréquence, double technologie)
- Détecteur de choc
- Détecteur de bris de verre
- Autosurveillance
- Bouton d'alarme, etc.

Lorsqu'une intrusion est détectée, les actions suivantes sont possibles :

- **Déclenchement de certains systèmes périphériques** : activation d'une alarme (signal sonore et/ou lumineux, ces derniers pouvant être intérieurs ou extérieurs), fermeture et verrouillage de certains accès, activation d'un générateur de brouillard, etc.
- **Transmission d'une alerte**, notamment vers un poste central de sécurité ou une société de télésurveillance, en complément vers un numéro de téléphone d'astreinte interne prédéterminé
- **Levée de doute.** Elle peut se faire :
    - A **distance**, via un déclenchement successif de capteurs, une confirmation vidéo (ou une image photographique) ou un appel téléphonique
    - Par une **intervention humaine** sur site
- **Intervention**. Outre la levée de doute, elle peut avoir pour finalité de porter secours, de limiter les conséquences de l'acte malveillant ou sa tentative, de protéger les lieux et préserver les indices dans l'attente de l'arrivée des secours.

Dans le but de pouvoir répondre de manière la plus optimale à l'équation de sûreté, la détection d'intrusion doit **être la plus en amont possible**.

Pour déclencher l'intervention des forces de sécurité intérieure, il est obligatoire pour une société de télésurveillance d'avoir **au préalable effectué une levée de doute**.

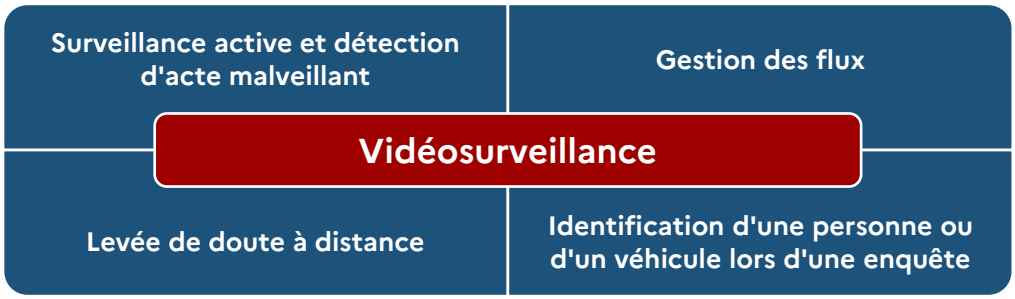
Afin de renforcer l'effet dissuasif, il est important d'apposer aux points clés du site des panneaux d'affichage « site sous alarme ».

Il est possible de se référer au référentiel APSAD R81 concernant les règles d'installation de la détection d'intrusion.

LA VIDÉOSURVEILLANCE

Le système de vidéosurveillance permet de remplir les **principaux rôles** suivants :

- Participer à la **surveillance active** des zones observées et à la détection d'un acte malveillant
- Contribuer à la gestion des flux
- Permettre la **levée de doute à distance**
- Permettre l'**identification d'une personne ou d'un véhicule** (plaque d'immatriculation) dans le cadre d'une procédure judiciaire ou administrative.



Pour installer un dispositif de **vidéosurveillance filmant l'espace ouvert au public ou les abords immédiats** de l'entreprise, il est au préalable nécessaire d'avoir une autorisation préfectorale, valable 5 ans. De plus, certaines obligations existent (information préalable, répondre à des finalités, affichage, etc.). Dans ce cadre, on parle de vidéoprotection.

On identifie **trois principaux niveaux d'exploitation** :

- Surveillance : elle permet d'effectuer une surveillance globale sommaire d'une zone
- Reconnaissance : il est possible de reconnaître une personne déjà vue auparavant
- Identification : elle permet d'identifier une personne ou une plaque d'immatriculation d'un véhicule.

Il existe de **nombreux types de caméras** : fixe ou mobile, 360° (fisheye), discrète, multicapteurs, avec intensificateur de lumière, etc.

Les images peuvent être visionnées en local ou à distance (télésurveillance ou sur smartphone), en direct ou en différé.

L'**éclairage** à proximité joue un rôle important dans la qualité du rendu de l'image.

Ces dispositifs de vidéosurveillance **imposent de respecter certaines règles juridiques et de mise en œuvre** :

- Respect du principe de proportionnalité au but recherché et justifié
- Consultation des instances représentatives du personnel avant le déploiement
- Information du personnel sur les finalités de ces dispositifs, notamment avec une mention dans le règlement intérieur
- Respect de la protection des données à caractère personnel (durée de conservation, affichage réglementaire, etc.).

Il est possible de se référer au référentiel APSAD R82 concernant les règles d'installation de la vidéosurveillance.

POUR ALLER PLUS LOIN

LA SURVEILLANCE HUMAINE

En plus des dispositifs de protection mécanique et de CADIVS, en fonction de la sensibilité et de la taille de l'entreprise, il peut être nécessaire de **disposer d'un moyen complémentaire de surveillance humaine** via la présence d'un ou de plusieurs agents privés de sécurité, permettant notamment de **réduire fortement le temps de levée de doute et d'intervention**. Les missions des agents privés de sécurité peuvent être les suivantes :

- Armer un poste central de sécurité
- Réaliser des rondes de manière régulière et aléatoire
- Procéder aux levées de doute et intervenir sur un incident.

Ce métier étant réglementé, certaines obligations incombent à la société de sécurité privée ainsi qu'à l'entreprise sollicitant cette prestation. Pour de plus amples informations, il est possible de consulter le site du CNAPS.

COMPLÉMENT SUR LA PROTECTION MÉCANIQUE

Dans le but de renforcer la protection mécanique, en plus des principaux dispositifs évoqués précédemment, il existe :

- **Dispositifs anti-stationnement** : plot métallique, barrière, mobilier urbain
- **Dispositifs anti-véhicule bélier**. Ils viennent s'installer en amont ou en aval d'un portail ou d'une clôture : bornes escamotables, herses, mobilier urbain, etc.
- **Dispositifs anti-franchissement**. Ils renforcent la lutte contre le franchissement par-dessus ou à travers une clôture, un portail, etc. : bavolets intérieurs et/ou extérieurs, barbelés, concertinas, pics de défense, etc.
- **Fossés**. Ils permettent d'éviter d'accoler un véhicule à la clôture en plus de ralentir son franchissement
- **Mobiliers urbains.** Ils offrent des obstacles complémentaires, naturels ou artificiels, tels que des jardinières, des blocs de pierre, etc.
- **Haies vives défensives**. Pouvant apporter une plus-value esthétique, elle nécessite un temps préalable avant de pouvoir être efficace. De plus, les coûts liés à l'entretien annuel sont non négligeables
- Dispositifs de renforcement d'un vitrage, **barreaudage** :
    - Il permet d'offrir une bonne résistance à l'effraction
    - Il peut être installé à l'extérieur du vitrage ou côté intérieur
- **Dispositifs de renforcement d'une porte** : le blindage pivot, la cornière anti-pinces et le protège-gonds (appelé aussi « anti-dégondage »)
- **Générateur de brouillard**. Souvent sous-estimé, il permet de remplir dans un temps très rapide un volume d'un nuage opacifiant et empêchant ainsi aux malveillants de se déplacer et de poursuivre leur action
- **Dispositifs opacifiants**. Ils peuvent être fixés au niveau d'une clôture (brise-vue) ou d'un vitrage (film opacifiant)
- **Coffres forts**, pouvant être à poser ou à encastrer
- etc.

Les sociétés d'assurance peuvent imposer certains dispositifs de protection mécaniques dans leur politique d'assurance.

COMPLÉMENT SUR LE CONTRÔLE D'ACCÈS

Afin de renforcer les dispositifs de contrôle d'accès électronique, en plus des principaux dispositifs évoqués précédemment, il est possible de **les paramétrer afin de** :

- **Limiter** :
  - Les accès à des **périodes** horaires, selon les profils
  - La **durée de validité** d'un badge, selon les profils
  - L'utilisation d'un badge en imposant un délai minimum entre deux utilisations successives du même badge sur un lecteur donné, appelé « anti pass-back temporel »
  - L'utilisation d'un badge en imposant une séquence logique stricte des points de passage de type entrée/sortie, appelé « anti pass-back géographique ». Ce cas nécessite de disposer d'un contrôle d'accès par unicité de passage sur l'ensemble des accès à la zone considérée
- **Surveiller l'état des dispositifs de verrouillage** (autosurveillance).

COMPLÉMENT SUR LA DÉTECTION D'INTRUSION

Il existe **3 types de surveillance** :

- Surveillance de l'approche
- Surveillance des pénétrations dans un bâtiment (par les murs, portes ou fenêtres)
- Surveillance des mouvements.

En vue de renforcer la détection d'intrusion, en plus des principaux dispositifs évoqués précédemment, il existe :

- Des dispositifs permettant d'assurer une **continuité de la transmission** de la communication en cas de coupure (carte GSM en plus de la connexion filaire par exemple)
- Des dispositifs de désactivation d'alarme avec un code sous contrainte.

Des restrictions de puissance des dispositifs de sirène extérieure peuvent exister, notamment dans le cadre d'arrêtés municipaux (cas par exemple de Paris).

COMPLÉMENT SUR LA VIDÉOSURVEILLANCE

Les dispositifs de vidéosurveillance peuvent présenter de **nombreuses caractéristiques complémentaires**. En effet, les caméras peuvent :

- Être analogiques ou numériques
- Disposer de leur propre alimentation électrique ou être alimentées par leur connexion (POE)
- Disposer de nombreuses options : inversion des pics de blancs, compensation du contre-jour, infrarouge, WDR, etc.
- Voir leurs images être stockées dans la caméra ou centralisées au niveau du système de vidéosurveillance
- Être reliées en hertzien ou en filaire, etc.

Dans l'idéal, il est recommandé de **privilégier des marques européennes**.

ANTICIPATION

Pour tout dispositif de protection mécanique, mais surtout pour les dispositifs de contrôle d'accès, de détection d'intrusion et de vidéosurveillance (CADIVS), il est nécessaire d'**anticiper la gestion de l'obsolescence** des dispositifs et donc de leur **renouvellement nécessaire**.

FICHE 6 – SÉCURITÉ DES INFORMATIONS

Pour commencer

- Définition
- Information, une valeur immatérielle
- Formation et sensibilisation à l'hygiène numérique
- Quelques procédures clés
- Le CERT [ED]

Pour aller plus loin

- Procédures organisationnelles permettant de renforcer la sécurité des informations

POUR COMMENCER

DÉFINITION

L'objectif du domaine de la sécurité des informations est de garantir **la disponibilité, la confidentialité, l'intégrité et la traçabilité** (DCIT) des **informations de l'entreprise** ainsi que **celles qui lui sont confiées** (celles de partenaires par exemple, de clients, etc.) **sous toutes ses formes** (documents papiers, documents numériques, conversations orales, savoir-faire). Cette protection doit être assurée tout au long du cycle de vie de l'information, en partant de sa création, son stockage, son accès, son partage/transfert, ses modifications et sa destruction.

Il est donc nécessaire de :

- **Identifier les informations détenues et celles ayant de la valeur** pour l'entreprise (stratégie, RH, finance, clients, sûreté, juridique, R&D, etc.)
- **S'assurer de l'accès à l'information** par les personnes en ayant le besoin (confidentialité)
- **Protéger ses informations** (intégrité et disponibilité).

L'INFORMATION, UNE VALEUR IMMATÉRIELLE

Comme évoqué dans la fiche sur le système de management de la sûreté et sa partie sur l'identification des valeurs de l'entreprise, **l'information est une des valeurs de l'entreprise**.

Toutes les informations n'ont pas à être protégées de la même manière. Il est donc nécessaire de catégoriser les informations et surtout d'**identifier les informations critiques** (fichiers clients, comptabilité, brevets, mots de passe administrateur, projet stratégique, etc.). La sécurité de ces informations doit être proportionnée à la valeur de l'actif et à l'impact sur l'activité et l'entreprise en cas de perte (confidentialité, intégrité ou disponibilité).

FORMATION ET SENSIBILISATION À L'HYGIÈNE NUMÉRIQUE

À l'instar de la formation et la sensibilisation aux risques sûreté, la technologie seule ne pouvant contrer l'ingénierie sociale ou la négligence, la **formation et la sensibilisation régulière à l'hygiène numérique du personnel** constituent le socle humain de toute stratégie de sécurité des informations.

Il s'agit d'instaurer une **culture de sûreté** où chaque collaborateur, du stagiaire à la direction, comprend qu'il est un maillon actif de la protection de l'entreprise et non un simple utilisateur passif. Concrètement, cela implique des formations régulières et pédagogiques, alignées sur les recommandations de l'ANSSI[8], pour apprendre à identifier les tentatives d'hameçonnage (emails suspects, urgences injustifiées, pièces jointes inattendues), à adopter des réflexes robustes (utilisation systématique d'un gestionnaire de mots de passe, activation de la double authentification, vigilance sur les supports USB) et à **signaler immédiatement tout incident ou doute** sans crainte de sanction.

QUELQUES PROCÉDURES CLÉS

Les procédures suivantes liées à la sécurité des informations sont particulièrement importantes :

- **Règles informatiques**, notamment au travers d'une charte informatique
- Règle du **besoin d'en connaître** pour l'accès aux informations
- **Activation automatique**, dès que cela est possible, des **mises à jour** des systèmes d'exploitation, des logiciels et équipements informatiques
- **Gestion des accès informatiques**, regroupant entre autres les mécanismes pour contrôler et gérer l'accès aux systèmes d'information : double authentification, mot de passe robuste et unique, accès à distance via un VPN, etc.
- Réalisation de **sauvegardes régulières** et hors ligne.

[8] Guide de la cybersécurité pour les TPE/PME en 13 questions, 2024, ANSSI.

LE CERT [ED]

Le CERT [ED] est un **centre de réponse à incident** (Computer Emergency Response Team) au **profit du secteur des entreprises de défense relevant de la DRSD**. Il contribue à :

- La prévention des incidents de sécurité informatique pour le secteur des entreprises de défense, entre autres via des actions de sensibilisation aux risques cyber
- L'analyse et au partage de l'information d'intérêt pour les entreprises de la BITD, notamment via une newsletter
- Et la coordination de la réponse aux incidents ciblant ce secteur, en coopération avec les acteurs régionaux ou nationaux de la cybersécurité.

Pour de plus d'information, il est possible d'aller sur le site du CERT [ED].

POUR ALLER PLUS LOIN

PROCÉDURES ORGANISATIONNELLES PERMETTANT DE RENFORCER LA SÉCURITÉ DES INFORMATIONS

Les procédures organisationnelles suivantes permettent de renforcer particulièrement la sécurité des informations :

- Identification d'un **responsable de la sécurité des systèmes d'information** (RSSI)
- **Politique de sécurité des systèmes d'informations** définissant les règles, les objectifs, les responsabilités, les procédures et les mesures de sécurité pour protéger les systèmes d'information (SI) d'une organisation, et au travers de laquelle la direction affirme ses exigences en matière de sécurité des SI
- **Politique de protection de l'information** comprenant l'ensemble du cycle de vie de l'information, à savoir depuis sa création, sa catégorisation (par exemple : public, interne, restreint, confidentiel), son stockage, son accès, son partage/transfert, ses modifications et sa destruction
- **Chiffrement** des données sensibles
- **Cartographie des risques cyber**
- **Gestion des incidents cyber**
- **Charte de l'usage de l'intelligence artificielle** (IA) au sein de l'entreprise
- **Gestion des comptes à privilèges** (les comptes administrateurs).

PARTIE 2 – MISE EN ŒUVRE DE LA SÛRETÉ DANS VOTRE ENTREPRISE

- Généralités

- Étape 1 : Plan / **Planifier**

- Étape 2 : Do / **Déployer**

- Étape 3 : Check / **Vérifier**

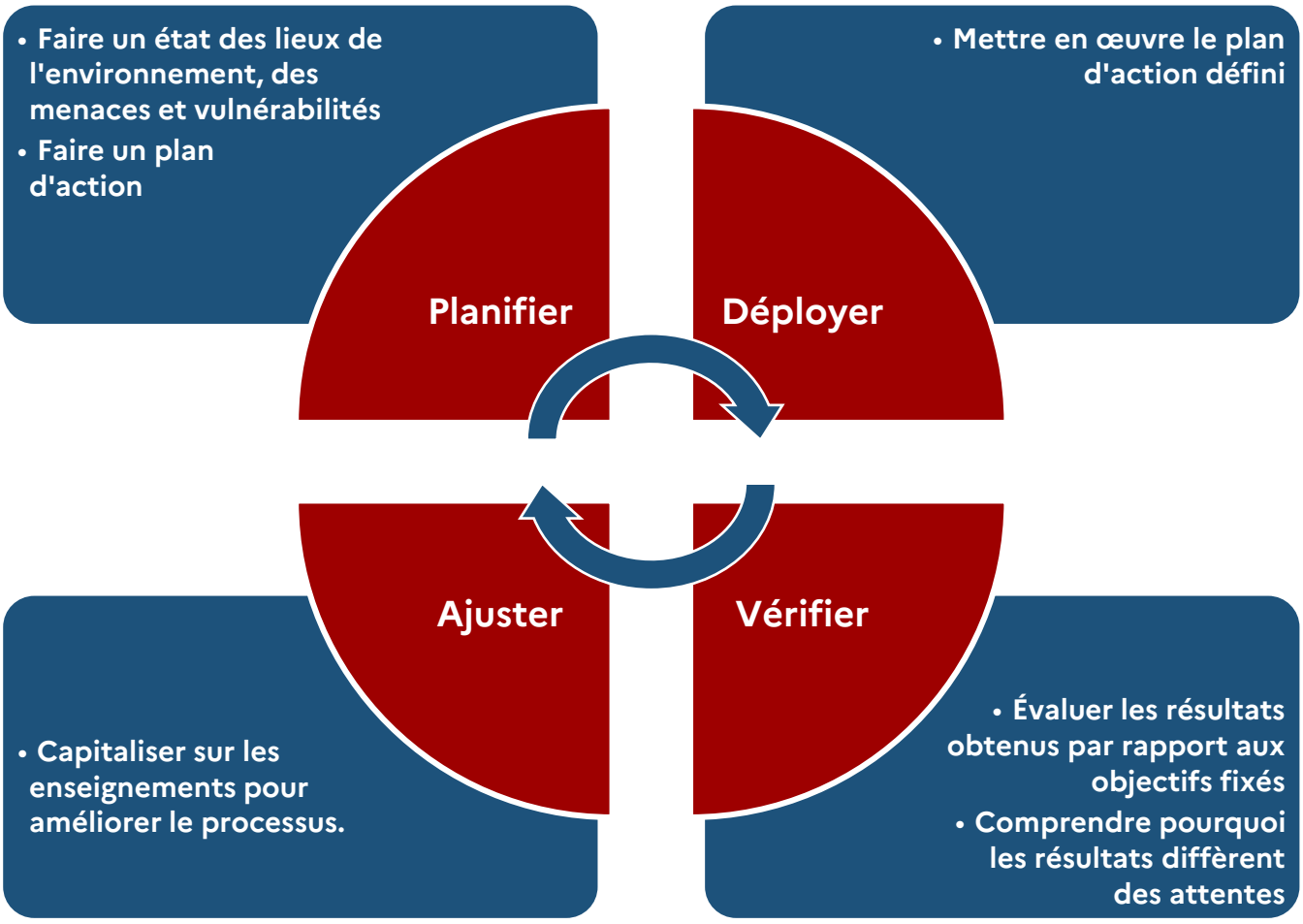
- Étape 4 : Act / **Ajuster**

GÉNÉRALITÉS

En plus **d'initier puis de déployer un dispositif de protection des valeurs** de l'entreprise, le processus PDCA (Plan, Do, Check, Act) **permet d'instaurer une amélioration continue** et une adaptabilité du dispositif de sûreté face aux menaces en constante évolution, mais également face aux changements réguliers de l'environnement interne et externe de l'entreprise (nouvelle valeur, réorganisation, contexte sécuritaire et géopolitique, nouvelle réglementation ou norme, nouvelle technologie, etc.).

Ainsi, cela permet à la sûreté d'**être à la fois dans une posture proactive** et réactive, tout en étant aligné sur la **réalité du terrain** et des menaces.

Le processus PDCA peut s'appliquer sur l'ensemble de la sûreté ou uniquement sur certains sujets spécifiques avec des boucles très courtes.



Pour rappel, afin **d'aider le lecteur à aller à l'essentiel et à prioriser**, cette partie est scindée en 2 catégories hiérarchisées :

- Les mesures « pour commencer », correspondant aux fondamentaux à maîtriser et aux actions prioritaires à engager
- Les mesures « pour aller plus loin », destinées à approfondir et renforcer le dispositif initial.

ÉTAPE 1 – PLAN / PLANIFIER

L'objectif de cette première étape est de faire un **état des lieux** de l'environnement, des menaces et vulnérabilités dans le but de fixer des orientations avec un plan d'action.

Pour commencer

- Identifier un responsable sûreté
- Identifier les valeurs
- Avoir une estimation rapide du niveau de sûreté en s'auto-évaluant
- Identifier les principaux risques liés à la sûreté
- Rédiger au moins une note relative à la sûreté (au moins le réglement intérieur)

Pour aller plus loin

- Établir plus précisément l'environnement interne et externe
- Évaluer plus precisément les risques sûreté
- Renforcer la gouvernance et le système de management de la sûreté

POUR COMMENCER

1 – IDENTIFIER UN RESPONSABLE SÛRETÉ

Avant toute chose, il est nécessaire d'identifier une personne ayant en charge la fonction sûreté au sein de l'entreprise, à savoir un responsable sûreté, même si cela ne représente qu'une faible part de son activité.

2 – IDENTIFIER LES VALEURS

Il est ensuite nécessaire de définir les valeurs, et particulièrement les **valeurs stratégiques**. On retrouve souvent comme valeur :

- **Personnel**, tant au sens large que certains profils particuliers (R&D, etc.)
- **Actifs informatiques**, tant l'infrastructure informatique que les services et logiciels (installés en local ou en cloud)
- **Stock** de matière première, de produits semi-finis et de produits finis
- Certains **outils de production**
- **Certains locaux particuliers** en plus du serveur informatique (locaux R&D, ateliers de production, zone de test, arrivée d'énergie (électricité, eau), etc.)
- **Informations stratégiques de l'entreprise** (brevet, plan de produit, contrat, cahier des charges, etc.) et celles qui lui sont confiées
- Image et **réputation** de l'entreprise.

Pour aller plus loin, il est possible de se référer à l'étape 2 du guide pratique d'analyse de risques coécrit par la DRSD et la DPID.

3 – AVOIR UNE ESTIMATION RAPIDE DU NIVEAU DE SÛRETÉ EN S'AUTO-ÉVALUANT

En vue de faire un bilan du niveau de sûreté de l'entreprise, il est possible de s'auto-évaluer à l'aide du **questionnaire d'auto-évaluation du référentiel de sûreté physique de la DGA** comprenant 13 exigences (disponible sur son site internet).

Ce référentiel a été coconstruit entre le ministère des Armées et les grands maîtres d'œuvre industriels avec le soutien du conseil des industries de défense français. Pour information, ce référentiel peut être utilisé de manière contractuelle par un donneur d'ordre vers un de ses sous-traitants dans le but d'assurer un niveau minimal de sûreté, ou par une entreprise dans le cadre d'un processus d'auto-évaluation de manière à valoriser son niveau de sûreté auprès de ses donneurs d'ordre.

4 – IDENTIFIER LES PRINCIPAUX RISQUES LIÉS A LA SÛRETÉ

Il s'agit d'identifier les 4 ou 5 grands risques auxquels l'entreprise est exposée. Par exemple :

- **Perte de produits** (matière première, produit fini) à cause d'un vol, d'une dégradation, d'un incendie, etc.
- **Dégradation de la capacité de production** du fait de la dégradation de l'outil de production, la perte du stock de matière première, une non-conformité, etc.
- **Perte d'avantage concurrentiel** suite à un vol physique de données (document papier, ordinateur), une cyberattaque, la divulgation volontaire (contre de l'argent par exemple) ou involontaire (conversation dans un lieu public, ordinateur laissé déverrouillé sans surveillance dans un train, etc.) d'un collaborateur, une non-conformité, etc.
- **Impact sur la réputation** de l'entreprise (exposition médiatique, non-conformité, etc.).

5 – RÉDIGER AU MOINS UNE NOTE RELATIVE A LA SÛRETÉ

S'il n'en existe pas déjà un, **rédiger un règlement intérieur**. Il permet de poser les bases des notions de sûreté, tout en étant un levier et une protection juridique pour le dirigeant. Il est donc nécessaire d'y **intégrer certains éléments obligatoires liés à la sûreté** (dispositif de contrôle d'accès et de vidéosurveillance). Si possible, y intégrer une charte informatique, voire une charte sur l'utilisation de l'IA.

Puis, dans l'idéal, rédiger une **note globale relative à la sûreté**, même sommaire, permettant d'intégrer des objectifs de sûreté et l'ensemble des différentes consignes et procédures liées à la sûreté, comme la gestion des visiteurs. Une mention de cette note devra apparaître dans le règlement intérieur.

Sans être une politique générale de sûreté ou un plan de sûreté, cette note globale permet de formaliser de façon succincte et de regrouper les premiers principes de la sûreté du site.

POUR ALLER PLUS LOIN

6 – ÉTABLIR PLUS PRÉCISÉMENT L'ENVIRONNEMENT INTERNE ET EXTERNE

Avant d'évaluer l'ensemble de ses risques sûreté de manière plus approfondie, il est au préalable indispensable de collecter toutes les données, informations utiles et nécessaires afin d'appréhender la globalité de l'écosystème interne et externe de l'entreprise.

L'environnement interne comprend notamment la structure et l'accessibilité, l'organisation, les activités et objectifs, les informations et la communication, les capacités et ressources, la sûreté et la sécurité.

L'environnement externe comprend quant à lui le contexte politique, économique, social, de malveillance, les relations contractuelles et l'environnement.

Pour aller plus loin, il est possible de se référer à l'étape 1 du guide pratique d'analyse de risques coécrit par la DRSD et la DPID.

7 – ÉVALUER PLUS PRÉCISÉMENT LES RISQUES SÛRETÉ

La phase d'évaluation des risques comprend la réalisation d'une cotation et d'une cartographie du niveau de criticité des scénarios de risques sûreté auxquels l'entreprise est exposée. Elle comprend **6 étapes** :

- Étudier des scénarios crédibles pour l'entreprise
- Déterminer la probabilité et la gravité des scénarios
- Déterminer le niveau de criticité du risque brut des scénarios
- Identifier les vulnérabilités de l'entreprise et les mesures existantes
- Déterminer le niveau de criticité du risque net des scénarios
- Déterminer le seuil d'acceptation du risque.

Pour aller plus loin, il est possible de se référer aux étapes 3 à 8 du guide pratique d'analyse de risques.

8 – RENFORCER LA GOUVERNANCE ET LE SYSTEME DE MANAGEMENT DE LA SÛRETÉ

Après avoir instauré un règlement intérieur et une note globale relative à la sûreté, il est nécessaire de **renforcer la gouvernance et le système de management de la sûreté**.
Pour cela :

- Remplacer la note globale relative à la sûreté précédente par :
    - Une **politique générale de sûreté** (le « quoi » et le « pourquoi »)
    - Un **plan de sûreté** (le « comment » au travers de la formalisation de l'évaluation des risques sûreté, le plan de traitement, l'amélioration continue et le contrôle)
    - Un éventuel schéma directeur de sûreté (la feuille de route pour améliorer la sûreté à moyen terme)
    - Une **revue de direction de sûreté**, au moins annuelle (« est-ce que l'on a mis en œuvre répond aux objectifs ? »)
- Définir des indicateurs de sûreté (indicateur de suivi d'activité, KPI et ROI).

ETAPE 2 – DO / DÉPLOYER

L'objectif de cette 2e étape est de mettre en œuvre le plan d'action défini.

Pour commencer

- Formaliser la fonction de responsable sûreté
- Initier une sensibilisation du personnel aux risques sûreté
- Protéger physiquement les valeurs stratégiques
- Installer un dispositif de détection d'intrusion

Pour aller plus loin

- Consolider la position du responsable sûreté
- Renforcer les procédures organisationnelles liées à la sûreté
- Développer la culture de sûreté au sein de l'entreprise
- S'assurer de la disponibilité des dispositifs techniques
- Renforcer la protection de l'établissement et de ses valeurs
- Renforcer la capacite de détection d'intrusion et de levée de doute
- Envisager la mise en place d'une surveillance humaine
- Rédiger un plan de gestion de crise
- Rédiger un plan de continuité et de reprise d'activité
- Instaurer un dispositif de veille

POUR COMMENCER

1 – FORMALISER LA FONCTION DE RESPONSABLE SÛRETÉ

La première étape de la phase 1 (Planifier) a normalement permis d'identifier une personne ayant la charge de la fonction sûreté au sein de l'entreprise, le responsable sûreté. Il est maintenant nécessaire de **formaliser cette fonction**. Pour cela, il faudra intégrer les missions de cette fonction dans la **fiche de poste** du responsable sûreté. Celui-ci devra être parfaitement identifié par l'ensemble des collaborateurs.

De plus, **désigner un adjoint** au responsable sûreté contribue à assurer la continuité de la fonction lors des absences de ce dernier.

Idéalement, ils devront **se faire connaître auprès des forces de sécurité intérieure de proximité**, à savoir l'unité de police ou de gendarmerie nationale territorialement compétente, mais également la police municipale s'il en existe une sur le secteur.

Il conviendra aussi de développer leur relation avec la personne en charge de la sécurité informatique.

2 – INITIER UNE SENSIBILISATION DU PERSONNEL AUX RISQUES SÛRETÉ

Établir une politique de sensibilisation aux risques sûreté et aux bons comportements à adopter pour l'ensemble du personnel présent sur le site, à savoir :

- Réaliser **systématiquement des sensibilisations à l'arrivée du nouveau personnel** sur le site (collaborateurs, intérimaires, alternants, stagiaires, prestataires)
- Effectuer des **rappels et recyclages périodiques** (une fois par trimestre par exemple). Ils peuvent être menés lors d'une action plus large (réunion globale du site). Idéalement, chaque collaborateur doit avoir été sensibilisé au moins une fois tous les trois ans
- Utiliser l'ensemble des **supports physiques et numériques** à la disposition du personnel pour transmettre périodiquement des messages de prévention aux risques sûreté. Diffuser et apposer par exemple les *affiches de sensibilisation aux risques sûreté* librement téléchargeables sur le site internet de la DRSD (defense.gouv.fr/drsd)
- De manière générale, **adapter le contenu, la périodicité et les canaux de diffusion** selon les activités et/ou les catégories de personnes. Justifier et expliquer au personnel les objectifs des mesures prises afin de faciliter leur acceptation et leur application et réduire les risques de contournement des dispositifs les plus contraignants
- Réaliser des **sensibilisations spécifiques pour les collaborateurs amenés à partir à l'étranger** dans le cadre de leurs missions, voire ceux qui pourraient être amenés à participer à des salons sensibles à l'avenir. S'aider si nécessaire de la Fiche *Mémo salons* librement téléchargeable sur le site de la DRSD.

3 – PROTÉGER PHYSIQUEMENT LES VALEURS STRATÉGIQUES

Les **valeurs stratégiques** identifiées précédemment doivent **bénéficier d'une protection adaptée par rapport à l'équation de sûreté**.

Concrètement, cela veut dire que **les valeurs stratégiques doivent être situées dans des locaux protégés, fermés et verrouillés** en absence du personnel autorisé et lors de la fermeture du site (les clés ne devant être ni accessibles à tous ni situées à proximité). Le niveau de protection des locaux sera en lien avec l'équation de sûreté.

Idéalement, déployer au niveau de ces valeurs stratégiques un **dispositif de contrôle des accès avec traçabilité**. Celui-ci peut se caractériser par :

- Un système de perception de la clé, stockée dans un lieu sécurisé, avec émargement dans un registre
- Ou, encore mieux, un système électronique, avec un badge par exemple.

La protection des valeurs concerne également la partie immatérielle, comme un document informatique. En cas de **partage d'information sensible en externe du réseau d'entreprise** :

- **Chiffrer les éléments** avec un logiciel adapté. Pour des informations *diffusion restreinte*, se référer à l'instruction générale interministérielle 1300 et la fiche synthétique de la DRSD disponible sur son site internet
- Pour le partage de fichiers volumineux, à défaut d'outil interne, privilégier des plateformes de transfert européennes. En cas d'échange avec des services de l'Etat français utiliser la plateforme Etatique France Transfert.

4 – INSTALLER UN DISPOSITIF DE DÉTECTION D'INTRUSION

Au niveau des **valeurs stratégiques** identifiées précédemment, il est impératif d'installer un dispositif de détection d'intrusion.

Dans ce cadre, le minimum est de disposer de :

- **Détection d'intrusion au niveau de la valeur** (surveillance des mouvements). À cet effet, les détecteurs volumétriques double technologie seront à privilégier. Idéalement, une détection préalable au niveau des **points de passage obligé** sera recherchée
- **Alarme sonore locale**
- **Alerte** vers une société de télésurveillance ou vers des numéros de téléphone préenregistrés
- **Capacité de levée de doute**, idéalement **à distance** en vue de « réduire » le délai d'intervention. Pour cela, il est possible d'avoir :
    - Une détection de mouvement avec **capteur photographique**. Il s'agit de l'option la plus accessible financièrement
    - Une **caméra de vidéosurveillance**. Elle permet d'offrir plus d'opportunité dans l'usage que le capteur photographique (souvent une meilleure identification)
    - Une intervention humaine. Celle-ci entraîne généralement un surcoût financier.

De plus, idéalement :

- Les codes d'activation de l'alarme doivent être **individuels** de manière à pouvoir assurer une traçabilité des activations/désactivations
- L'activation doit être **automatique** le soir à partir d'un horaire défini, en plus d'une activation manuelle par la dernière personne quittant l'établissement.

L'ensemble de ce dispositif nécessite la formalisation d'une **procédure** de gestion et d'utilisation.

POUR ALLER PLUS LOIN

5 – CONSOLIDER LA POSITION DU RESPONSABLE SÛRETÉ

Inciter le responsable sûreté à **renforcer ses liens avec** :

- Les **différents services de l'Etat** en fonction de l'activité : la DRSD, la direction générale de la sécurité intérieure (DGSI), la direction nationale des renseignements territoriaux (DNRT), les référents sûreté de la police ou de la gendarmerie nationale en fonction de la zone de compétence territoriale, les douanes, etc.
- **Ses pairs** : les éventuels autres responsables sûreté de l'entreprise, les responsables sûreté d'entreprises du même secteur, les entités situées à proximité, et des associations de directeurs/responsables sûreté s'il en existe à proximité.

Dans le cadre de sa relation avec la personne en charge de la sécurité informatique, il est possible de s'assurer que celui-ci soit bien abonné à la newsletter du CERT [ED].

6 – RENFORCER LES PROCÉDURES ORGANISATIONNELLES LIÉES À LA SÛRETÉ

En plus du règlement intérieur et des politiques et plans de sûreté évoqués dans la première partie (Planifier), dans le but de renforcer les mesures organisationnelles liées à la sûreté, il est nécessaire d'**établir des procédures de sûreté spécifiques** (certaines sont détaillées en annexe 8) :

- Les **consignes globales et spécifiques de sûreté**
- La gestion des accès, des flux, dont l'ouverture et la fermeture du site en temps normal et lors des périodes de fermeture annuelle
- La gestion des **visiteurs**
- La gestion des livreurs, prestataires, personnel temporaire et courrier
- La gestion des clés et des badges
- Les consignes de communication en externe à l'entreprise et de discrétion professionnelle
- La politique de **mobilité à l'international**
- La politique de protection de l'information
- Le parcours de notoriété en cas de venue de délégation
- Le traitement des incidents
- Les fiches réflexes en cas d'événement sûreté
- La procédure en cas d'élévation de la menace
- Le fonctionnement en mode dégradé, etc.

7 – DÉVELOPPER LA CULTURE DE SÛRETÉ AU SEIN DE L'ENTREPRISE

En vue de renforcer la culture de sûreté au sein de l'entreprise :

- **Solliciter l'intervention de conférenciers des services Etatiques** (DRSD, en fonction DGSI) dans le but de réaliser une action de sensibilisation du personnel, voire du comité de direction
- **Intégrer les aspects de sûreté** dans les processus métiers et les différents projets **par défaut et dès la conception** (*security by default* & *security by design*)
- Assurer un suivi des personnes ayant été sensibilisées.

8 – S'ASSURER DE LA DISPONIBILITÉ DES DISPOSITIFS TECHNIQUES

Afin de pouvoir **disposer de manière pérenne** des différents dispositifs de protection mécanique et électroniques de sûreté (CADIVS), il est impératif d'avoir pour ces derniers :

- Une **politique de maintenance préventive et corrective**
- Une **source d'alimentation secondaire** en cas de coupure électrique.

S'assurer qu'aux moins deux personnes soient formées sur le fonctionnement et la gestion des différents dispositifs électroniques de sûreté.

9 – RENFORCER LA PROTECTION DE L'ÉTABLISSEMENT ET DE SES VALEURS

Pour les valeurs les plus stratégiques et/ou exposées, **renforcer la protection physique de leur lieu de stockage et de leur accès** (par exemple par une porte renforcée, un générateur de brouillard, un second point de verrouillage, un dispositif d'authentification via un clavier alphanumérique à code, etc.).

Installer un dispositif de vidéosurveillance dans le but d'assurer une surveillance des flux de circulation du site, de certaines valeurs stratégiques et de permettre une levée de doute à distance. Idéalement, privilégier des marques européennes.

En fonction des compétiteurs de l'entreprise et notamment de leurs lois extraterritoriales, envisager de conserver les informations, au moins celles étant considérées comme stratégiques, chez un hébergeur français, sinon européen.

10 – RENFORCER LA CAPACITÉ DE DÉTECTION D'INTRUSION ET DE LEVÉE DE DOUTE

Idéalement, de manière à disposer d'une détection la plus **précoce** possible, **installer des dispositifs de détection au niveau de la périmétrie** (surveillance de pénétration).

En fonction de la sensibilité et de la taille de l'établissement, il peut également être envisagé, voire nécessaire, de **disposer** :

- D'un **moyen complémentaire de surveillance humaine** avec la présence d'un ou de plusieurs agents privés de sécurité, permettant entre autres de réduire fortement le temps de levée de doute et d'intervention
- De la détection au niveau de la périphérie (surveillance de l'approche).

11 – ENVISAGER LA MISE EN PLACE D'UNE SURVEILLANCE HUMAINE

En fonction de la sensibilité et de la taille de l'établissement, il peut être envisagé la mise en place d'une surveillance humaine via des agents privés de sécurité dans le but de renforcer :

- La dissuasion et la prévention d'un acte malveillant
- La surveillance et la garde du site, notamment via des rondes de sûreté
- Le contrôle des accès au site et la gestion des flux
- La levée de doute et l'intervention
- La gestion d'un incident de sûreté
- L'exploitation en temps réel des dispositifs de vidéosurveillance
- Le sentiment de sécurité et sûreté pour les employés et les clients.

12 – RÉDIGER UN PLAN DE GESTION DE CRISE

Il est nécessaire de rédiger un **plan de gestion de crise** permettant de définir :

- Un processus de crise (alerte, mobilisation, pilotage, sortie de crise et RETEX)
- L'organisation et le pilotage de la cellule de crise
- La méthode (AGIR)
- Les outils de crise
- La salle de crise et sa salle de back-up sur un autre site
- La formation et les exercices de crise.

Pour aller plus loin, il est possible de se référer au guide de survie face à la crise, publié par la DRSD et disponible sur son site internet.

13 – RÉDIGER UN PLAN DE CONTINUITÉ ET DE REPRISE D'ACTIVITÉ

Afin de rédiger un plan de continuité d'activité (PCA) et de reprise d'activité (PRA), il est nécessaire :

- De définir le périmètre des PCA/PRA
- D'élaborer le PCA
- D'élaborer le PRA
- De définir le processus d'activation des PCA/PRA
- D'effectuer un maintien en conditions opérationnelles.

Pour aller plus loin, il est possible de se référer à l'outil-guide pratique d'élaboration et de mise en œuvre des PCA ainsi qu'à sa méthode flash élaborés par la DRSD et disponible sur son site internet.

14 – INSTAURER UN DISPOSITIF DE VEILLE

Quel que soit le type de veille souhaitée (stratégique, concurrentielle, technologique, réglementaire ou réputationnelle), elle fonctionne selon un **cycle continu en 4 grandes étapes** :

- Définition du besoin
- Recherche et la collecte d'information
- Analyse et le traitement de l'information
- Diffusion du résultat aux acteurs concernés.

À défaut de pouvoir le faire en interne, il est possible de solliciter des prestataires externes.

ÉTAPE 3 – CHECK / VÉRIFIER

L'objectif de cette étape est **d'évaluer les résultats obtenus** par rapport aux objectifs fixés et de **comprendre pourquoi les résultats diffèrent** des attentes.

Pour commencer

- Vérifier le bon fonctionnement des mesures et des dispositifs techniques
- Évaluer les éventuels écarts par rapport aux objectifs visés

Pour aller plus loin

- Analyser finement les indicateurs de performance (KPI & ROI)
- Effectuer des audits internes et externes
- Prévoir des exercices sûreté
- Réaliser un RETEX structuré en cas d'incident de sûreté
- Anticiper l'obsolescence des dispositifs techniques

POUR COMMENCER

1 – VÉRIFIER LE BON FONCTIONNEMENT DES MESURES ET DES DISPOSITIFS TECHNIQUES

À ce stade, l'objectif est d'une part de **vérifier l'application et l'efficacité des mesures organisationnelles** en vigueur, d'autre part de contrôler techniquement les **dispositifs** installés de **protection mécanique et électronique de sûreté** (CADIVS).

Il est donc nécessaire de régulièrement :

- **Effectuer des contrôles et essais périodiques de certains dispositifs** mécaniques et électroniques de sûreté (test de l'alarme intrusion par exemple)
- **Vérifier l'historique** des différents dispositifs organisationnels (registre visiteurs par exemple) et techniques (activation/désactivation de l'alarme, log des accès aux locaux sensibles, etc.)
- **Vérifier le respect des consignes de sûreté** (verrouillage de certains accès, accompagnement des visiteurs, port du badge, etc.)
- **Analyser les incidents de sûreté mineurs** (perte de badge, etc.) afin d'identifier les récurrences.

2 – ÉVALUER LES ÉVENTUELS ÉCARTS PAR RAPPORT AUX OBJECTIFS VISÉS

Faire le bilan de l'activité de sûreté, et des éventuels indicateurs de performance, par rapport aux objectifs visés. Identifier les raisons des éventuels écarts.

En cas d'incident de sûreté, effectuer un rapide RETEX de manière à comprendre les causes de ces incidents.

Il est possible de réaliser un tableau de bord dans le but d'en faciliter le suivi.

POUR ALLER PLUS LOIN

3 – ANALYSER FINEMENT LES INDICATEURS DE PERFORMANCE (KPI & ROI)

Analyser **finement les différents indicateurs de performance** (KPI) par **rapport aux objectifs visés** dans le plan de sûreté, et les éventuels indicateurs de retour sur investissement (ROI).

Étudier les différentes **causes** en cas d'absence d'atteinte des objectifs.

4 – EFFECTUER DES AUDITS INTERNES ET EXTERNES

Dans le but de prendre du recul et de s'assurer, dans une logique d'amélioration continue, que les dispositifs de sûreté mis en œuvre au sein de l'entreprise sont adaptés, opérationnels et appliqués, mais également d'identifier des vulnérabilités, il est **nécessaire de réaliser de manière périodique des contrôles et audits de sûreté internes et externes**.

Dans le cadre d'un audit de sûreté externe, il est important d'avoir plusieurs points d'attention : la sélection rigoureuse du prestataire, le cadrage juridique et contractuel, la protection des données et des accès, et la gestion de la restitution. Les **mêmes points de vigilance seront à prendre en compte en cas de sollicitation d'un prestataire externe pour un accompagnement** sur la montée en puissance du dispositif de sûreté.

5 – PRÉVOIR DES EXERCICES SÛRETÉ

Afin de **tester les mesures et dispositifs** humains, organisationnels et techniques de l'entreprise lors d'un incident de sûreté, réaliser des exercices de sûreté **de manière progressive**, d'abord sur table avant d'aller éventuellement et progressivement vers un exercice en grandeur nature. Pour ce dernier, il sera possible d'associer les différentes forces de sécurité intérieure et de secours situées à proximité.

Dans le même esprit, en fonction de la sensibilité et de la taille de l'établissement, il peut être envisagé de réaliser un test d'intrusion et des mises en situation, notamment pour tester les éventuels agents de sécurité privés présents.

6 – RÉALISER UN RETEX STRUCTURÉ EN CAS D'INCIDENT DE SÛRETÉ

En cas d'incident de sûreté, effectuer une analyse et un retour d'expérience (RETEX) approfondis, non pas pour chercher un éventuel coupable, mais davantage pour **comprendre les causes de l'incident**, les éventuelles défaillances matérielles et organisationnelles, ou les lacunes dans la sensibilisation et la formation, afin d'**adapter les processus et dispositifs en place**.

En complément, il sera utile de réaliser un bilan précis et global de l'ensemble des différents incidents de sûreté.

7 – ANTICIPER L'OBSOLESCENCE DES DISPOSITIFS TECHNIQUES

Pour tout dispositif de protection mécanique, mais surtout pour les dispositifs électroniques de sûreté (les CADIVS), il est nécessaire d'**anticiper la gestion de l'obsolescence** des dispositifs et donc de leurs **renouvellements nécessaires**.

ÉTAPE 4 – ACT / AJUSTER

L'objectif de cette étape est de capitaliser sur les enseignements dans le but d'améliorer le processus.

Pour commencer

- Instaurer des points sûreté réguliers
- Réparer les dispositifs de protection défectueux
- Renforcer au besoin la sensibilisation aux risques sûreté
- Mettre à jour les procédures de sûreté

Pour aller plus loin

- Réaliser une revue de direction sûreté

POUR COMMENCER

1 – INSTAURER DES POINTS SÛRETÉ RÉGULIERS

L'idée ici **est d'initier une routine régulière** (par exemple une fois par trimestre), même si elle est peu structurée et assez courte (1 h), permettant de prendre du recul et de faire un point sur la sûreté **avec la direction et les partenaires clés** de l'entreprise.

Cela sera l'occasion de faire un bilan concernant ce qui fonctionne, les vulnérabilités et les actions à mettre en œuvre, etc.

2 – RÉPARER LES DISPOSITIFS DE PROTECTION DÉFECTUEUX

Dans la continuité des contrôles et essais périodiques, dès qu'un dispositif de protection mécanique ou électronique de sûreté (CADIVS) est défectueux, il est **impératif de le réparer le plus tôt possible**, idéalement dans le cadre d'un contrat de maintenance corrective.

3 – RENFORCER AU BESOIN LA SENSIBILISATION AUX RISQUES SÛRETÉ

Effectuer des **rappels** lorsque des **consignes ou procédures de sûreté ne sont pas respectées** par le personnel ou les prestataires, tant au travers de *feedback* individuel que des communications de sensibilisation plus globales sous différentes formes (mail, affiche, réunion, etc.).

4 – METTRE À JOUR LES PROCÉDURES DE SÛRETÉ

Il est nécessaire de procéder aux mises à jour légères des procédures de sûreté lorsque le besoin apparaît. Le personnel en sera alors informé.

POUR ALLER PLUS LOIN

5 – RÉALISER UNE REVUE DE DIRECTION SÛRETÉ

Idéalement effectuée annuellement, mais également après un événement majeur ou une évolution importante des risques ou de l'entreprise, la revue de direction a pour objectif de **s'assurer de la pertinence, l'adéquation et l'efficacité** du système de management de la sûreté et pour atteindre les objectifs visés dans la politique générale de sûreté.

À cet effet, elle va :

1. **Vérifier l'adéquation** entre la stratégie de l'entreprise et les enjeux de sûreté (analyse du contexte interne et externe, des enjeux, mise à jour de l'évaluation des risques de sûreté, etc.)
2. **Évaluer l'efficacité** du dispositif global de sûreté (bilan des incidents de sûreté, RETEX, indicateurs de sûreté, résultats des audits, satisfaction des parties intéressées, etc.)
3. **S'assurer** que les ressources, les compétences et l'organisation **sont suffisantes**
4. **Décider** des orientations, arbitrages et **priorités** pour l'année à venir (mise à jour des procédures, plan d'action éventuel, etc.).

Un exemple de revue de direction sûreté est présentée en annexe 7.

ANNEXES

- Annexe 1 : **time line des 15 actions à mener pour commencer**
- Annexe 2 : **time line des actions à mener pour aller plus loin**
- Annexe 3 : **les dix règles élémentaires de la sûreté**
- Annexe 4 : **principale documentation liée à la sûreté**
- Annexe 5 : **trame de la politique générale de sûreté**
- Annexe 6 : **trame du plan de sûreté**
- Annexe 7 : **trame de la revue de direction sûreté**
- Annexe 8 : **détail de certaines procédures de sûreté**
- Annexe 9 : **glossaire**
- Annexe 10 : **bibliographie**

ANNEXE 1 – TIME LINE DES 15 ACTIONS À MENER POUR COMMENCER

	LISTE DES ACTIONS À MENER	À faire	En cours	Fait	Référence (Page)
PLANIFIER	Identifier un responsable sûreté	☐	☐	☐	47
	Identifier les valeurs	☐	☐	☐	47
	Avoir une estimation rapide du niveau de sûreté en s'auto-évaluant	☐	☐	☐	48
	Identifier les principaux risques liés à la sûreté	☐	☐	☐	48
	Rédiger au moins une note relative à la sûreté (RI)	☐	☐	☐	48
DEPLOYER	Formaliser la fonction de responsable sûreté	☐	☐	☐	50
	Initier une sensibilisation du personnel aux risques sûreté	☐	☐	☐	51
	Protéger physiquement les valeurs stratégiques	☐	☐	☐	51
	Installer un dispositif de détection d'intrusion	☐	☐	☐	52
VERIFIER	Vérifier le bon fonctionnement des mesures et des dispositifs techniques	☐	☐	☐	56
	Evaluer les éventuels écarts par rapport aux objectifs visés	☐	☐	☐	56
AJUSTER	Instaurer des points sûreté réguliers	☐	☐	☐	58
	Réparer les dispositifs de protection défectueux	☐	☐	☐	58
	Renforcer au besoin la sensibilisation aux risques sûreté	☐	☐	☐	58
	Mettre à jour les procédures de sûreté	☐	☐	☐	58

Pour chacune des actions à mettre en œuvre, il est possible de se référer à :

- La page de la partie 2 (PDCA) indiquée à droite
- La partie 1 du guide, plus théorique, pour avoir plus de détails.

ANNEXE 2 – TIME LINE DES ACTIONS À MENER POUR ALLER PLUS LOIN

	LISTE DES ACTIONS À MENER	À faire	En cours	Fait	Référence (Page)
PLANIFIER	Établir plus précisément l'environnement interne et externe	☐	☐	☐	49
	Évaluer plus précisément les risques sûreté	☐	☐	☐	49
	Renforcer la gouvernance et le système de management de la sûreté	☐	☐	☐	49
DEPLOYER	Consolider la position du responsable sûreté	☐	☐	☐	53
	Renforcer les procédures organisationnelles liées à la sûreté	☐	☐	☐	53
	Développer la culture de sûreté au sein de l'entreprise	☐	☐	☐	53
	S'assurer de la disponibilité des dispositifs techniques	☐	☐	☐	54
	Renforcer la protection de l'établissement et de ses valeurs	☐	☐	☐	54
	Renforcer la capacité de détection d'intrusion et de levée de doute	☐	☐	☐	54
	Envisager la mise en place d'une surveillance humaine	☐	☐	☐	54
	Rédiger un plan de gestion de crise	☐	☐	☐	55
	Rédiger un plan de continuité et reprise d'activité	☐	☐	☐	55
	Instaurer un dispositif de veille	☐	☐	☐	55
VERIFIER	Analyser finement les indicateurs de performance (KPI & ROI)	☐	☐	☐	57
	Effectuer des audits internes et externes	☐	☐	☐	57
	Prévoir des exercices sûreté	☐	☐	☐	57
	Réaliser un RETEX structuré en cas d'incident de sûreté	☐	☐	☐	57
	Anticiper l'obsolescence des dispositifs techniques	☐	☐	☐	57
AJUSTER	Réaliser une revue de direction sûreté	☐	☐	☐	59

ANNEXE 3 – LES 10 RÈGLES ÉLÉMENTAIRES DE LA SÛRETÉ

1. **Soyez concerné par la sûreté**, elle n'est pas que l'affaire des autres.
2. **Connaissez et respectez les règles** et consignes de sûreté de votre entreprise.
3. Signalez immédiatement au responsable sûreté ou sécurité tout incident ou fait inhabituel. Ne pensez pas qu'une autre personne le fera à votre place.
4. **Verrouillez systématiquement votre session informatique** dès que vous quittez votre bureau, même pour une courte absence.
5. **Utilisez un mot de passe robuste et différent** pour chaque accès informatique. Enregistrez le dans un gestionnaire de mot de passe.
6. **Restez discret** sur les mesures de sûreté et le fonctionnement de votre entreprise.
7. En déplacement, **évitez d'évoquer des sujets professionnels** et restez discret dans vos lectures.
8. En déplacement, conservez avec vous votre ordinateur portable.
9. En déplacement, **privilégiez les prises secteurs** pour recharger vos appareils.
10. En déplacement, ne vous connectez pas aux réseaux Wifi publics et utilisez un VPN.

ANNEXE 4 – PRINCIPALE DOCUMENTATION LIÉE À LA SÛRETÉ

Pour commencer

- **Fiche de poste du responsable sûreté** (même si en temps partiel sur cette fonction)
- Le **règlement intérieur** avec des éléments de sûreté
- Une **éventuelle note relative à la sûreté** (qui sera abbrogée une fois la politique générale de sûreté et le plan de sûreté établis)

Pour aller plus loin

- **Politique générale de sûreté** (cf. annexe 5)
- **Plan de sûreté** comprenant notamment l'analyse de risques, le plan de traitement, les indicateurs sûreté, etc. (cf. annexe 6)
- **Procédures de sûreté** : consignes globales et spécifiques, circuit arrivée/départ d'un collaborateur, sensibilisation aux risques sûreté, gestion des visiteurs, parcours de notoriété, gestion des prestataires et des livreurs, gestion des stagiaires/apprentis/alternants, gestion des flux, gestion des accès, traitement des incidents, fiches réflexes en cas d'incident, protection de l'information, consignes de communications et de discrétion, mobilité nationale et internationale, gestion des clés/badges, politique de maintenance préventive et corrective, ouverture/fermeture du site, charte informatique, politique de sécurité des systèmes d'informations, etc. (cf. partie 1 et annexe 8)
- **PCA/PRA** (cf. guide de la DRSD)
- **Plan de gestion de crise** (cf. guide de la DRSD)
- Éventuel **schéma directeur de sûreté**
- **Revue de direction sûreté** (cf. annexe 7)

ANNEXE 5 – TRAME DE POLITIQUE GÉNÉRALE DE SÛRETÉ

1. GOUVERNANCE DE LA SÛRETÉ

Au sein de l'établissement, un **responsable sûreté** est formellement désigné. Son existence et son rôle sont connus de tous. Il est en charge de la protection du patrimoine humain, matériel et immatériel. Il est responsable de la mise en œuvre opérationnelle de cette politique générale de sûreté. Il n'est pas responsable de la sécurité incendie.

2. LES OBJECTIFS DE SÛRETÉ

La sûreté doit être **alignée sur la stratégie et le fonctionnement de l'entreprise**, être au service de son activité et contribuer à sa performance globale. Elle doit assurer la protection de ses valeurs, à savoir son personnel, son patrimoine matériel (installations, matériels, produits…) et immatériel (les informations, l'e-réputation). Elle doit être un *business partner* de l'entreprise.

Pour cela, en collaboration avec l'ensemble des représentants des métiers de l'entreprise, dans le but de se prémunir des risques liés aux menaces et aux vulnérabilités identifiées, elle établit une stratégie globale de sûreté reposant sur le principe de **défense en profondeur des valeurs**, permettant de répondre à l'équation de sûreté, et s'appuyant sur des barrières successives où toutes les mesures humaines, organisationnelles et techniques sont parfaitement adaptées, complémentaires, homogènes et redondantes.

Incarnant la gouvernance de la sûreté, la direction inscrit la sûreté dans une démarche d'**amélioration continue**.

Au besoin, un schéma directeur de sûreté est mis en œuvre afin de combler l'écart entre le niveau de protection actuel et celui fixé par la direction.

3. CONFORMITÉ AVEC LES EXIGENCES LÉGALES ET RÉGLEMENTAIRES

L'ensemble des règles et dispositifs en lien avec la sûreté doit être **conforme avec les exigences légales** et réglementaires applicables.

4. CORPUS DOCUMENTAIRE LIÉ A LA SÛRETÉ

Le règlement intérieur indique les règles essentielles de sûreté et précise les sanctions applicables en cas de non-respect des règles de disciplines.

Les règles, procédures et consignes liées à la sûreté sont formalisées dans une documentation mise à jour régulièrement.

5. CULTURE DE SÛRETÉ

La sûreté ne repose pas uniquement sur les experts ou les responsables : elle est l'**affaire de chacun des collaborateurs**. Chaque personnel, quel que soit son rôle, contribue à la vigilance collective et à la protection des valeurs. Il est donc nécessaire de mettre en œuvre une **politique de sensibilisation aux risques sûreté** afin de promouvoir, dès l'arrivée sur site puis de manière régulière, une culture de sûreté partagée, fondée sur la sensibilisation, la formation et la responsabilisation de tous, que cela soit les collaborateurs ou les prestataires réguliers.

Dans le but de **renforcer la confiance des partenaires** de l'entreprise (clients, prestataires), il est possible de leur partager (en mode consultation) cette politique générale de sûreté.

6. LA REVUE DE DIRECTION SÛRETÉ

En vue de **s'assurer de la pertinence, l'adéquation et l'efficacité** du système de management de la sûreté pour **atteindre les objectifs visés** dans cette politique générale de sûreté, il est instauré une revue de direction sûreté au minimum annuelle. À cet effet, elle devra :

- Vérifier l'adéquation entre la stratégie de l'entreprise et les enjeux de sûreté
- Évaluer l'efficacité du dispositif global de sûreté
- S'assurer que les ressources, les compétences et l'organisation sont suffisantes
- Décider des orientations, arbitrages et priorités pour l'année à venir.

ANNEXE 6 – TRAME DU PLAN DE SÛRETÉ

Si existant au sein de l'entreprise, un **marquage de classification de protection adaptée doit lui être appliqué** (restreint, confidentiel entreprise, etc.).

Cette trame comprend 4 parties.

1. LA GOUVERNANCE ET L'ORGANISATION – *Qui décide, qui agit et dans quel cadre ?*
Cette partie va rappeler certains points clés définis dans la politique générale de sûreté (rôle et responsabilité, engagement de la direction, objectifs de sûreté, conformité avec les exigences réglementaires, revue de direction, etc.).

Un **responsable** de l'élaboration et de la mise en œuvre de ce plan de sûreté est formellement désigné, il doit en rendre compte à la direction générale de l'entreprise.

Cette partie définit également les ressources (budget, personnel, outils) nécessaires allouées.

2. L'ÉVALUATION DES RISQUES SÛRETÉ – *Que craignons-nous ?*
Il s'agit de la partie analyse du plan de sûreté. Après avoir **identifié les valeurs** de l'entreprise dans son environnement externe et interne, cette partie comprend la réalisation d'une **cotation et d'une cartographie du niveau de criticité** des scénarios de risques sûreté auxquels l'entreprise est exposée.

3. LE PLAN DE TRAITEMENT – *Comment se protéger ?*
Il s'agit du cœur opérationnel du plan. Une fois les risques identifiés, cette partie décrit les mesures concrètes mises en place pour les réduire, à savoir des **mesures de prévention** et de **protection** dans les domaines suivants :

- Humain : formation et sensibilisation du personnel et des prestataires, etc.
- Organisationnel : règlement intérieur, procédures d'accueil des visiteurs, consignes de sûreté, gestion des badges, gestion des incidents de sûreté, etc.
- Technique : protection mécanique, contrôles d'accès, détection d'intrusion, vidéosurveillance, etc.

4. L'AMÉLIORATION CONTINUE ET LE CONTRÔLE – *Est-ce que ça fonctionne ?*
Cette dernière partie impose un cycle de vérification régulier dont l'objectif est de corriger les failles découvertes et d'adapter le plan aux nouvelles menaces ou aux changements de l'organisation, au travers de quatre grands items :

- Auto-évaluation et indicateurs de performance
- Gestion des incidents et retour d'expérience (RETEX)
- Audits et tests de conformité : le plan prévoit la réalisation de tests (exercice sûreté, exercice de crise, audits sûreté interne et externe) pour vérifier la mise en œuvre des procédures écrites, leur pertinence et les éventuelles améliorations nécessaires
- Boucle d'amélioration : les résultats des audits, des exercices, des incidents, des indicateurs de sûreté et des changements de contexte permettent d'alimenter la revue de direction sûreté. Celle-ci débouche sur un plan d'actions correctives budgété et planifié dans le temps, fermant ainsi la boucle de l'amélioration continue.

ANNEXE 7 – TRAME DE LA REVUE DE DIRECTION SÛRETÉ

Si existant au sein de l'entreprise, un **marquage de classification de protection adaptée** doit lui être appliqué (restreint, confidentiel entreprise, etc.).

Date / Président de séance / Participants / Période couverte

1. **ORDRE DU JOUR ET OBJECTIFS**
   - Valider la pertinence, l'adéquation et l'efficacité du Système de Management de la Sûreté (SMS)
   - Décider des orientations stratégiques et des ressources pour la période à venir
   - S'assurer des liens avec la stratégie globale de l'entreprise.

2. **ANALYSE DU CONTEXTE ET DES ENJEUX (INTERNE & EXTERNE)**
   - Évolutions réglementaires : nouvelles lois, directives sectorielles, obligations légales (ex : RGPD, REC, régulations sectorielles spécifiques)
   - Contexte géopolitique et social : menaces émergentes (instabilité régionale, mouvements sociaux, terrorisme, espionnage économique, etc.)
   - Changements internes : restructurations, nouveaux sites, nouveaux produits, fusion/acquisition, changements technologiques majeurs.

3. **SUIVI DES DÉCISIONS DE LA REVUE PRÉCÉDENTE**
   - État d'avancement des actions décidées lors de la dernière revue (Réalisé, en cours, non initié)
   - Analyse des écarts concernant les actions non réalisées.

4. **RETOUR D'EXPERIENCE (RETEX) ET PERFORMANCE DE LA SÛRETÉ**
   - Suivi d'activité, indicateurs de performance, éventuellement ROI en sûreté
   - Synthèse des incidents et quasi-accidents :
     - Statistiques (vol, intrusion, cyberattaque, perte de données, etc.)
     - Analyse des causes des incidents majeurs
     - Efficacité des mesures correctives mises en place
   - Exercices sûreté, exercice de crise et tests :
     - Résultats des derniers exercices
     - Points forts et axes d'amélioration identifiés
   - Audits et inspections :
     - Synthèse des audits internes et externes (certification, audit client, audit initié par la direction, inspection réglementaire)
     - Etat des non-conformités majeures.

5. **ÉVALUATION DES RISQUES DE SÛRETÉ (MISE A JOUR)**
   - Revue de la cartographie des risques : les risques identifiés ont-ils changé (probabilité/gravité) ?
   - Nouveaux risques apparus
   - Efficacité du traitement des risques actuels.

6. SATISFACTION DES PARTIES INTÉRESSÉES

- Retours des clients (exigences de sûreté dans les contrats, etc.)
- Retours des employés (climat social, sentiment de sécurité, signalements, etc.)
- Relations avec les autorités (police/gendarmerie, DRSD, préfecture, etc.).

7. ADÉQUATION DES RESSOURCES

- Ressources humaines : effectifs de sûreté, compétences, formations réalisées vs planifiées, sensibilisation du personnel
- Dispositifs techniques : état des équipements (protection mécanique, contrôle d'accès, détection d'intrusion, vidéoprotection, SSI), obsolescence, besoins de maintenance ou de renouvellement
- Budget : coût global de la sûreté, analyse des écarts budgétaires (réalisé/budget), justification et prévision sur les années à venir.

8. OPPORTUNITÉS D'AMÉLIORATION CONTINUE

- Innovations technologiques pertinentes
- Parangonnage sectoriel
- Propositions d'amélioration des processus et procédures.

9. DÉCISIONS ET PLAN D'ACTION (LIVRABLE PRINCIPAL)

Décisions et actions stratégiques, avec désignation d'un responsable, d'une échéance, des ressources allouées avec un indicateur de succès.

10. CONCLUSION DE LA DIRECTION

- Appréciation globale sur la maturité du système de sûreté
- Confirmation de la politique générale de sûreté (maintien ou révision)
- Orientation de la direction pour engager les équipes
- Prochaine revue prévue le : [Date]

CONSEILS POUR RÉUSSIR CETTE REVUE :

- **Se baser sur des données** : ne pas venir avec des ressentis, mais avec des indicateurs chiffrés
- **Faire le lien avec le Business** : ne pas seulement montrer combien la sûreté « coûte », mais plutôt montrer que la sûreté :
    - Protège le chiffre d'affaires, la réputation et la continuité
    - Contribue à la performance globale de l'entreprise au travers de l'accès ou du maintien sur des marchés où la sûreté est un facteur discriminant
    - Renforce la confiance des clients et partenaires
- **Anticiper** : consacrer au moins un tiers du temps aux risques futurs et à la stratégie, pas seulement au bilan passé
- **Tracer** : le compte-rendu (PV) est une pièce justificative majeure en cas d'enquête ou d'audit pour prouver la diligence raisonnable de la direction.

ANNEXE 8 – DÉTAIL DE CERTAINES PROCÉDURES DE SÛRETÉ

- Procédure **d'ouverture et de fermeture des locaux**, précisant par exemple le verrouillage ou la fermeture des fenêtres le soir, la sécurisation des documents sensibles avant de quitter le bureau, le nettoyage des tableaux blancs et autres *paperboards*, la destruction des documents papiers sensibles laissés dans la poubelle, le cas échéant, le verrouillage systématique des accès avant de quitter le local/bureau/bâtiment, la mise sous alarme des locaux par le dernier personnel, etc.
- Procédure de **remontée interne/externe et de traitement des incidents de sûreté**. Ces derniers devront systématiquement faire l'objet d'un compte-rendu via un rapport d'étonnement et d'une exploitation à des fins d'évolution des mesures de sûreté. La remontée d'un incident prendra différentes formes en fonction de sa gravité. Le cas échéant, les incidents devront être remontés vers la DRSD, voire les clients et/ou la DGA
- **Fiches réflexes à l'attention des collaborateurs** pour des faits de sûreté : intrusion, individu suspect, véhicule suspect, alerte à la bombe, survol de drone, etc.
- **Procédure d'accueil des visiteurs**, notamment par les mesures suivantes :
    - Formaliser l'annonce préalable des visiteurs selon des modalités définies (délai, changement accepté, biodata, etc.)
    - Solliciter la présentation d'une pièce d'identité à l'agent d'accueil afin qu'il puisse vérifier que le porteur de la pièce d'identité est bien le bon visiteur autorisé
    - Remettre un badge « visiteur », ou tout autre dispositif visuel d'identification, à porter de manière visible et permanente (y compris pour les sous-traitants)
    - Sécuriser le registre « visiteur » et le renseigner uniquement par le personnel de l'établissement
    - Accompagner systématiquement les visiteurs lors des déplacements à l'intérieur du site
- **Consignes de discrétion** précisant notamment la discrétion accrue en présence de personnes extérieures à proximité, dans les lieux publics dont les restaurants ou les transports publics, la remontée vers le responsable sûreté de toute question trop intrusive sur les dispositifs de sûreté ou l'activité de l'établissement, des mesures de vigilance concernant l'utilisation des réseaux sociaux et des logiciels d'intelligence artificielle générative
- Procédure de **sûreté liée à la mobilité à l'international** : procédure de validation des déplacements, sensibilisation associée, mesures de protection ; en fonction des pays : utilisation d'ordinateurs et téléphones portables blanchis, interdiction d'utiliser son téléphone personnel, inscription sur Le fil d'Ariane du ministère de l'Europe et des Affaires étrangères, etc.
- Procédure de **gestion des prestataires** précisant entre autres l'obligation d'une sensibilisation en matière de sûreté, l'accompagnement permanent dans certains locaux sensibles, la discrétion accrue du personnel en présence de prestataires, l'identification du statut externe dans l'adresse de messagerie, etc.

- Procédure **de gestion des intérimaires** précisant notamment l'obligation d'une sensibilisation en matière de sûreté, la discrétion accrue du personnel en leur présence, l'identification du statut temporaire dans l'adresse de messagerie le cas échéant
- Procédure de **gestion de stagiaires et alternants** précisant entre autres l'identification d'un tuteur, la relecture des rapports de stage, l'obligation d'intégration d'une clause de confidentialité dans les conventions, l'accès restreint à certaines données voire à certains locaux, la discrétion accrue du personnel en présence des stagiaires, le port d'un tour de cou apparent obligatoire d'une couleur spécifique, l'identification du statut temporaire dans l'adresse de messagerie, etc.
- Procédure de **gestion de badges, clés et codes** comprenant les mesures suivantes :
    - **Pour les badges**, si le dispositif actuel le permet pour certaines mesures :
        - Procédure d'attribution des badges (identification, création, distribution, restitution, etc.)
        - Vérification annuelle de tous les badges en circulation
        - Identification d'une période d'activation (1 an pour les prestataires et 3 ans pour les collaborateurs par exemple)
        - Identification d'une plage horaire d'utilisation pour l'ensemble des badges et surtout pour les prestataires
        - Interdiction de prêter le badge
        - Vérification périodique du journal d'activités des badges pour détecter tout événement inhabituel (création de badges non sollicitée et tentative d'utilisation de badge à des heures indues ou pour accéder à de futurs locaux non autorisés par exemple)
        - Formalisation d'une procédure de perte et de vol des badges
        - Sensibilisation à l'arrivée d'un nouveau personnel sur l'importance du respect des consignes
    - **Pour les clés** :
        - Établissement d'un organigramme de l'ensemble des clés en circulation
        - Ouverture du registre de perception des clés pour le personnel
        - Formalisation de la procédure de perte et de vol des clés
        - Sécurisation des clés communes dans un ou plusieurs coffres
        - Inventaire périodique de toutes les clés en circulation
        - Vérification périodique de l'application des mesures et la responsabilisation du personnel sur la sensibilité de celles-ci
    - **Pour les codes** :
        - Recensement de tous les dispositifs physiques et électroniques de sûreté fonctionnant à code
        - Individualisation des codes dans la mesure du possible et changement systématique de celui-ci après le départ d'un collaborateur en ayant eu connaissance
        - Changement périodique des codes communs (au moins une fois par an).

ANNEXE 9 – GLOSSAIRE

ACTIF : tout élément ayant de la valeur pour un organisme.

ALÉA : manifestation d'un phénomène naturel ou anthropique. Il exclut toute intention malveillante.

ANALYSE DE RISQUES : processus mis en œuvre pour comprendre la nature des risques et pour déterminer le niveau de risque. L'analyse de risque fournit la base de l'évaluation des risques et les décisions relatives au traitement des risques.

CYBERSÉCURITÉ : protection de la confidentialité, de l'intégrité et de la disponibilité des systèmes numériques.

CRISE : situation globalement imprévisible où les faits recueillis permettent de constater que les processus et l'organisation habituelle mis en place ne permettent plus d'absorber la totalité des impacts rencontrés et la multiplicité des parties prenantes concernées, impliquées ou à informer.

DÉFENSE EN PROFONDEUR : s'appuie sur des barrières successives allant de la périphérie, la périmétrie à la volumétrie. Les mesures associées, d'ordres humaines, organisationnelles et techniques doivent être homogènes, redondantes et complémentaires.

DÉTECTABILITÉ : capacité d'un organisme à détecter tout signe avant-coureur, ou signe d'alerte précoce, et d'y réagir.

ÉVÈNEMENT : occurrence ou changement d'un ensemble particulier de circonstances. Il peut avoir plusieurs causes et plusieurs conséquences, il peut être quelque chose qui est attendu, mais qui ne se produit pas, ou quelque chose auquel on ne s'attend pas, mais qui se produit.

GOUVERNANCE : système permettant de diriger et de contrôler.

GRAVITÉ : conséquences de l'événement (qu'il soit issu d'une menace ou d'un aléa) sur l'organisme.

IMPACT : résultat d'une perturbation affectant les objectifs pouvant être d'ordre humain, matériel, financier, juridique, organisationnel, réputationnel, etc.

INCIDENT : événement qui peut être, ou conduire à, une situation indésirable.

INDICATEUR CLÉ DE PERFORMANCE (KPI, pour *Key Performance Indicator*) : mesurage quantifiable en termes de qualité utilisé par un organisme pour estimer ou comparer ses performances par rapport à la réalisation des objectifs stratégiques et opérationnels.

INDICATEUR DE SUIVI D'ACTIVITÉ : mesurage quantifiable en termes de quantité utilisé par un organisme pour estimer ou comparer son activité et ses moyens.

INDICATEUR DE RETOUR SUR INVESTISSEMENT (ROI, pour *Return On Investment*) : mesurage financier utilisé par un organisme pour estimer la rentabilité globale d'un investissement. Il compare le gain (ou la perte) généré par rapport au coût initial de l'investissement.

MALVEILLANCE : risque d'origine humaine et intentionnel, que cela soit par une action ou une inaction, envers une personne, le patrimoine matériel ou immatériel d'un organisme.

MANAGEMENT DU RISQUE : activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque.

MENACE : cause potentielle d'un incident indésirable susceptible de porter préjudice.

MESURES DE DÉTECTION : dispositifs ou actions propres à augmenter la capacité de détection d'un incident, pouvant être source de risque, au moyen de solutions organisationnelles, techniques et humaines.

MESURES DE PRÉVENTION : dispositifs ou actions propres à diminuer la probabilité d'occurrence d'un risque, au moyen de solutions organisationnelles, techniques et humaines.

MESURES DE PROTECTION : dispositifs ou actions propres à diminuer, réduire ou contenir les effets d'un risque après sa survenue. Les moyens de protection agissent sur la diminution des conséquences du risque, au moyen de solutions organisationnelles, techniques et humaines.

NIVEAU DE CRITICITÉ DU RISQUE : Degré d'importance d'un risque, exprimé en termes de combinaison de la probabilité et de la gravité d'un scénario, et cartographié sur une matrice des risques.

OBJECTIF : résultat à atteindre pouvant être de différent niveau (stratégique, tactique ou opérationnel) et se rapporter à différents domaines (finance, production, sécurité, etc.)

ORGANISME : personne morale de droit public ou privé pouvant comprendre plusieurs établissements.

PÉRIMETRIE : zone située entre la limite de propriété jusqu'à l'enveloppe des bâtiments.

PÉRIPHERIE : espace extérieur de l'emprise à protéger, souvent matérialisée par la limite de propriété.

PLAN DE SÛRETÉ : ensemble documenté de dispositions planifiées permettant de s'assurer que la sécurité est gérée de façon satisfaisante.

POLITIQUE : intentions et orientations d'un organisme, telles qu'elles sont officiellement formulées par sa direction.

PROBABILITÉ : possibilité qu'un scénario se produise.

PROCESSUS : ensemble d'activités, corrélées ou en interaction, réalisées dans un ordre déterminé permettant de transformer des éléments d'entrée en éléments de sortie et ainsi obtenir un résultat souhaité.

RESPONSABLE SÛRETÉ : personnel de l'organisme ayant été désigné par sa direction pour assurer la responsabilité de la gestion de la sûreté au sein de l'organisme.

RETOUR D'EXPERIENCE (RETEX ou REX) : démarche a posteriori d'analyse, de bilan, de mise en lumière des forces et des faiblesses d'un événement et de sa gestion. Il permet de faire ressortir des axes d'amélioration et mettre à jour les dispositifs humains, organisationnels et/ou techniques.

REVUE DE DIRECTION : évaluation formalisée effectuée par la direction pour déterminer la pertinence, l'adéquation et l'efficacité du système de management de la sûreté par rapport à la politique générale de sûreté.

RISQUE : correspond à la probabilité de survenance d'un événement dommageable pouvant porter préjudice à la réalisation des objectifs d'une organisation. Il résulte de l'appréciation de deux composantes : la probabilité de l'événement et la gravité (ou effets de l'événement).

RISQUE BRUT : risque identifié pour l'organisation dont l'évaluation de la criticité se fait avant la prise en compte des moyens de maîtrise. Un risque brut peut être significatif ou non significatif.

RISQUE NET : risque identifié pour l'organisation dont l'évaluation de la criticité se fait après la prise en compte des moyens de maîtrise. Un risque net peut être un risque significatif confirmé (non maîtrisé) ou un risque significatif maîtrisé.

RISQUE NON SIGNIFICATIF : risque dont l'évaluation initiale (risque brut) est inférieure au seuil d'acceptabilité défini par le propriétaire du risque.

RISQUE RÉSIDUEL : risque subsistant après le traitement du risque. Un risque résiduel peut également être appelé « risque pris ».

RISQUE SIGNIFICATIF : risque dont l'évaluation initiale (risque brut) est supérieure au seuil d'acceptabilité défini par le propriétaire du risque.

RISQUE SIGNIFICATIF CONFIRMÉ : risque net dont le niveau de criticité net est supérieur au seuil d'acceptabilité défini par le propriétaire du risque. Un risque significatif confirmé correspond à un risque significatif non maîtrisé.

RISQUE SIGNIFICATIF MAÎTRISÉ : risque net dont le niveau de criticité net est inférieur au seuil d'acceptabilité défini par le propriétaire du risque.

SCÉNARIO : situation fictive, envisagée et plausible, dans laquelle une menace ou un aléa affecte le personnel, les installations, les informations, les moyens et/ou les activités de l'organisme.

SÉCURITÉ : prévention et lutte contre les risques accidentels, naturels et technologiques, c'est-à-dire contre les risques d'origine non intentionnelle (par opposition au risque malveillant qui relève de la sûreté).

SÉCURITÉ DE L'INFORMATION : protection de la sécurité et préservation de la confidentialité, de l'intégrité et de la disponibilité de tous les actifs informationnels.

SEUIL D'ACCEPTATION DU RISQUE : limite en dessous de laquelle les risques identifiés sont considérés comme maîtrisés par le propriétaire du risque, et au-dessus de laquelle ils nécessitent des moyens de maîtrise intégrés à un plan de traitement.

SÛRETÉ : prévention et lutte contre la malveillance.

SYSTÈME DE MANAGEMENT : ensemble d'éléments corrélés ou en interaction d'un organisme utilisés pour établir des politiques, des objectifs et des processus de façon à atteindre lesdits objectifs.

TRAITEMENT DU RISQUE : processus générique destiné à modifier un risque et pouvant inclure :

- Un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque
- La prise ou l'augmentation d'un risque afin de saisir une opportunité
- L'élimination de la source d'une menace ou d'un aléa
- Une modification de la probabilité
- Une modification des conséquences
- Un partage du risque avec une ou plusieurs autres parties incluant des contrats et un financement du risque
- Un maintien du risque fondé sur une décision argumentée.

SURVEILLANCE : vérification, supervision, observation critique ou détermination de l'état des menaces et des aléas afin d'identifier continûment des changements par rapport au niveau de performance exigé ou attendu.

URGENCE : situation globalement imprévisible où les faits recueillis permettent de constater que les processus et l'organisation habituelle mis en place permettent d'absorber la totalité des impacts rencontrés et la multiplicité des parties prenantes concernées, impliquées ou à informer.

VALEUR : bien, personne, information matérielle ou immatérielle, savoir-faire que détient un organisme et qui revêt un caractère précieux, voire indispensable (pour son activité, son fonctionnement, sa pérennité) et vulnérable du fait de son prix, de son attrait commercial, de son coût, de son délai de remplacement ou de son caractère unique.

VOLUMÉTRIE : regroupe l'ensemble des volumes intérieurs d'un bâtiment.

VULNÉRABILITÉ : faiblesse d'une organisation ou d'un système susceptible d'être exploitée par des menaces ou d'augmenter l'exposition aux risques, d'être donc une source de risque.

ANNEXE 10 – BIBLIOGRAPHIE

- Norme NF ISO 22300 : Sécurité et résilience – vocabulaire
- Norme NF ISO 22340 : 2024 Sécurité et résilience – sûreté préventive – les lignes directrices pour une architecture et un cadre de sûreté préventive de l'entreprise
- Norme NF ISO 22342 : 2023, Sécurité et résilience – sûreté préventive – les lignes directrices pour l'élaboration d'un plan de sûreté destiné à un organisme
- Norme NF ISO 31000 : 2018 Management du risque – lignes directrices
- Norme AFNOR SPEC 2404 : 2025, Plan de sûreté – exigences opérationnelles
- Traité pratique de sûreté malveillance, CNPP
- Référentiel 1302, système de management de la sûreté, lutte contre la malveillance et prévention des menaces, CNPP
- Référentiel APSAD D83, documentation technique pour la conception et l'installation d'un contrôle d'accès, CNPP
- Référentiel APSAD R31, règles et prescriptions de télésurveillance, CNPP
- Référentiel APSAD R81, règles d'installation de la détection d'intrusion, CNPP
- Référentiel APSAD R82, règles d'installation de la vidéosurveillance, CNPP
- 29 fiches pratiques de la sécurité économique, 2021, SISSE
- Jeu des 8 familles d'atteintes à la sécurité économique, 2020, IHEMI
- Guide de la cybersécurité pour les TPE/PME en 13 questions, 2024, ANSSI
- Guide pratique d'analyse de risques, 2023, DRSD et DPID
- Guide de survie face à la crise à l'usage des entreprises de la BITD, 2024, DRSD
- Outil-guide d'élaboration et de mise en œuvre des PCA pour les PME et TPE de la BITD, 2025, DRSD
- Fiche gestion d'un document Diffusion Restreinte, 2025, DRSD
- Fiche parcours de notoriété, 2025, DRSD
- Fiche memo salons, 2024, DRSD
- Affiche de sensibilisation à la sûreté des employés, 2024, DRSD
- Affiches de sensibilisation à message spécifique de sûreté, 2025, DRSD.