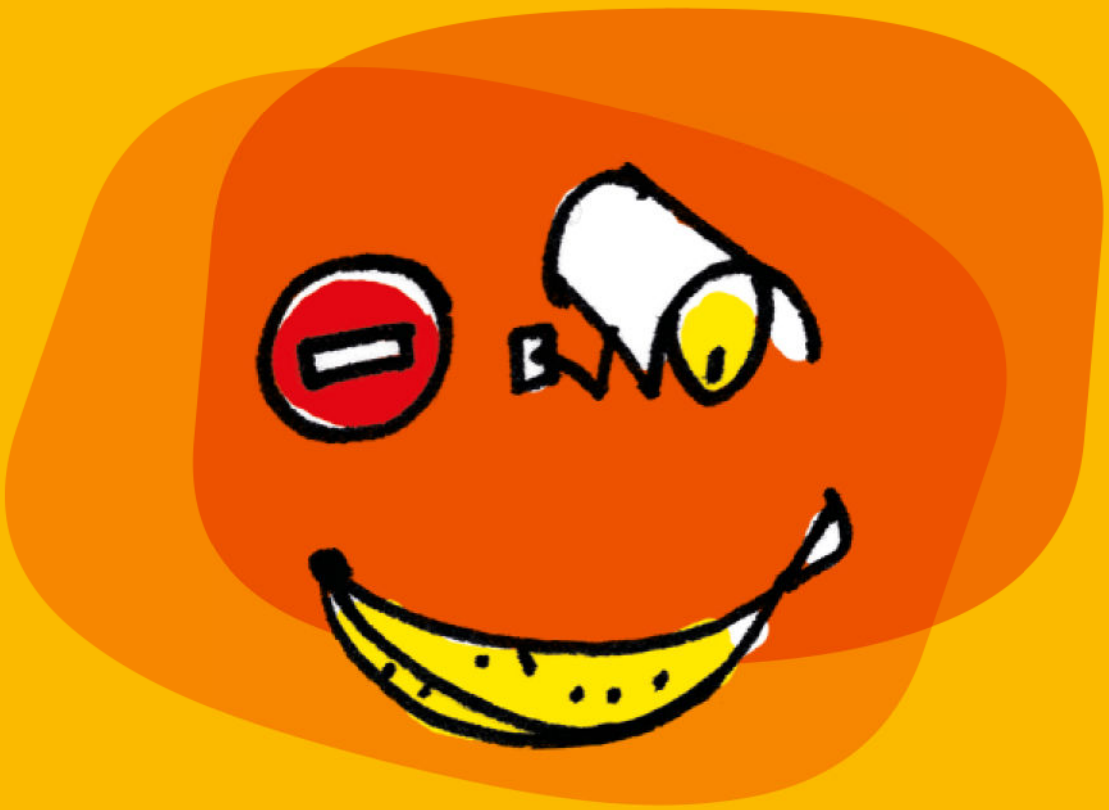
GUIDE MÉTHODOLOGIQUE

FOOD DEFENSE



Protection de la chaîne alimentaire contre les risques d'actions malveillantes, criminelles ou terroristes

Bonnes pratiques et retours d'expérience

GENERALI Solutions d'assurances

MFQ Mouvement Français pour la Qualité Aquitaine

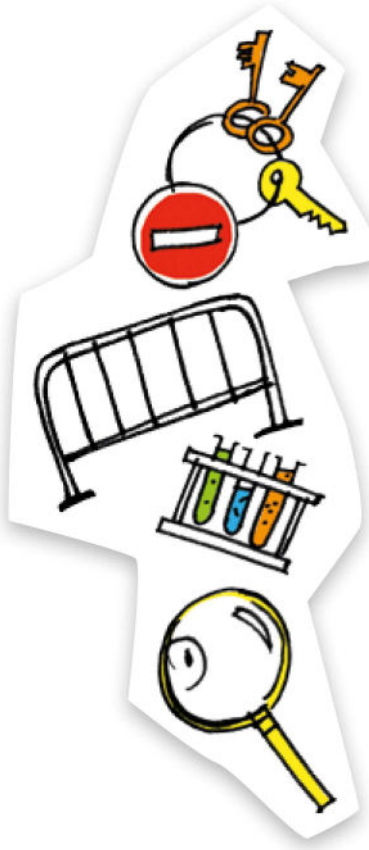
afnor GROUPE

Ont participé à l'élaboration collective de ce guide :

Emmanuelle ABDEL MAABOUD – EAM Conseil
Patrick BERCIS – GENERALI
Karine BRIANE – DOMAINES BARONS DE ROTHSCHILD (LAFITE)
Olivier BOUTOU – AFNOR
Estelle COMPIEGNE – SUCRE D'AQUITAINE
Stéphane DEMAY – SAVEURS & CREATIONS
Blanche DEMIAS – MARITEAM
Emilie DENTELLA – KIWI FRANCE
Éric DUFOUR – GENERALI
Emmanuel ESTEVE – ASA Conseil
Priscilla FORTIF – AQUITAINE SPECIALITES
Nona KERLAGUEN – ALLIANCE FB
Vanessa MARCET – CLE-P&S
Dominique MAUFRAND – DELPEYRAT
Luc MALBOS, MFR - VAYRES
Jeremy OMNES – VITI SOLUTIONS
Régine PASSUTO – GRM -SAS
Elodie PIET – SAVEURS & CREATIONS
Sylvie PONCET-VERDIER, AGROTEC
Sabine RAYMOND – AXAMILLESIMES
Leonardo SFERRAZZA – QSE IN FINE

AVANT-PROPOS

Si toutes les entreprises agro-alimentaires peuvent potentiellement être un jour la cible d'une action malveillante, criminelle, voire terroriste, il est vrai que l'émergence des exigences liées à la Food Defense dans les différents référentiels amène aujourd'hui les entreprises à s'interroger davantage sur leur vulnérabilité et à formaliser ou mettre en place des mesures de sûreté.



En 2003, l'Organisation mondiale de la santé (OMS) et son département Sécurité Alimentaire ont proposé un document d'orientation destiné aux gouvernements et aux industriels de l'agro-alimentaire.

Au niveau français, à la demande du Secrétariat Général de la Défense Nationale (SGDN), un travail de réflexion a été conduit à partir de 2003 sur les risques de contamination de la chaîne alimentaire. Une mission a été confiée à ce titre au Conseil général vétérinaire par la Direction Générale de l'Alimentation (DGAL). L'étude a porté sur les agents dangereux pour la santé publique et sur la vulnérabilité de la chaîne alimentaire. L'évaluation du risque pour la santé publique a été conduite par un groupe d'experts issus de l'Agence Française de Sécurité Sanitaire des Aliments (AFSSA), de l'Agence Française de Sécurité Sanitaire des Produits de Santé (AFSSAPS), de l'Institut de veille Sanitaire (INVS) et de l'Institut Pasteur.

Afin d'aider les industriels dans la mise en place volontaire de leurs mesures contre les actions terroristes, criminelles ou malveillantes, un guide pour les professionnels de l'agro-alimentaire a été élaboré au niveau interministériel.

Depuis les années 2000, la Food Defense est également un dispositif largement développé aux USA, où elle fait même l'objet de dispositions réglementaires. La FDA (Food Drug Administration), l'USDA (United States Département of Agriculture) et le FSIS (Food Safety and Inspection Service) proposent aux travers de leur site Internet de nombreuses ressources pour mettre en place des Plans de Food Defense (PFD) à destination de tous les acteurs de la chaîne alimentaire.

Si l'approche américaine de la Food Defense peut sembler excessive pour nos entreprises, elle s'est inscrite dans un contexte de risque terroriste avéré avec pour menace des attaques potentielles de type NRBC (risques nucléaires, radiologiques, bactériologiques, chimiques voire physiques).

De nombreuses interrogations sont soulevées par les opérateurs de la chaîne alimentaire. Elles concernent des points de repère sur les étapes nécessaires à l'établissement d'un plan de Food Defense (identification des prérequis, politique de sûreté, évaluation des zones sensibles, réponse aux situations d'urgence…) et la recherche d'outils simples et efficaces pour y répondre et pour convaincre l'ensemble des acteurs concernés du bien-fondé de la démarche.

Au niveau aquitain, un groupe d'une douzaine d'organismes s'est constitué en 2013 afin de réfléchir aux solutions qu'il pourrait mettre en place dans le cadre d'une démarche Food Defense, en s'attachant particulièrement aux exigences du référentiel IFS Food 6. Le présent guide est paru en 2015.

SOMMAIRE

1 INTRODUCTION

L'étude que notre groupe aquitain a réalisée lors de réunions de travail entre 2013 et 2014 permet de proposer un outil méthodologique pragmatique qui peut servir de guide aux entreprises agro-alimentaires pour conduire leur analyse de risques malveillance. Ce guide ne prend pas en compte les spécificités propres à chaque entreprise (produits, contexte, infrastructures, etc.) mais il propose une base de travail commune. N'importe quelle entreprise de la filière peut, à partir de ce socle, identifier et prendre en compte dans son analyse ses caractéristiques spécifiques.

Ce guide présente :

- **Des recommandations et des bonnes pratiques issues d'expériences d'approches Food Defense vécues dans des organismes de la chaîne alimentaire ;**
- **Des pièges à éviter ;**
- **Des méthodes et des outils (les exemples donnés en annexe, ne pouvant être considérés comme modèles).**

LES ÉTAPES RETENUES POUR LA DÉMARCHE FOOD DEFENSE SONT LES SUIVANTES :

Étapes préalables :

- Évaluation du contexte et engagement de la Direction dans la démarche ;
- Constitution d'une équipe chargée de la sûreté ;
- Réalisation d'un diagnostic sûreté ;
- Détermination des mesures de prévention préalables (MPP).

Étapes d'analyse :

- **Étape 1 :** l'évaluation des menaces / de la vulnérabilité ;
- **Étape 2 :** les mesures spécifiques et / ou supplémentaires de maîtrise ;
- **Étape 3 :** la gestion d'un acte malveillant (Gestion de crise et Retrait / Rappel) ;
- **Étape 4 :** le suivi, la mise à jour et l'amélioration de son Plan Food Defense.

DOMAINE D'APPLICATION

Les principes développés dans ce document s'appliquent à tout type d'organisme appartenant à la chaîne alimentaire quels que soient sa taille, sa nature et son domaine d'activité.

Tous les acteurs au sein du domaine d'application retenu sont concernés par ce document et notamment :

- l'équipe dirigeante de l'organisme pour l'aider à déployer une approche Food Defense ;
- le responsable qualité et / ou sécurité / sûreté en leur proposant des éléments méthodologiques pour mettre en œuvre la Food Defense ;
- l'auditeur en sécurité des denrées alimentaires pour l'aider à évaluer l'efficacité et l'efficience du système de Food Defense et des éléments qui le composent.

RÉFÉRENCES BIBLIOGRAPHIQUES

- **Guide des recommandations pour la protection de la chaîne alimentaire contre les risques d'actions malveillantes, criminelles ou terroristes** – DGAL janvier 2014 ;
- **Lignes directrices sur la Food Defense dans l'IFS Food** version 6, janvier 2012 ;
- **PAS 96:2014** Guide to protecting and defending food and drink from deliberate attack – BSI ;
- **ISO/TS 22002-1 §18** – Prévention de l'introduction intentionnelle de dangers dans les denrées alimentaires, biovigilance et bioterrorisme.

TERMES ET DÉFINITIONS

Accessibilité (Guide DGAL) : Estimation de la facilité d'accès à la cible, et de la facilité à la quitter après une attaque.

Biosécurité (Dossier FAO) : Approche stratégique intégrée qui englobe le cadre des politiques et le cadre réglementaire (y compris les instruments et les activités) pour analyser et gérer les risques pesant sur la vie et la santé des personnes, des animaux et des plantes et les risques associés pour l'environnement.

Bioterrorisme (Dictionnaire) : Consiste en l'utilisation ou la menace d'utilisation de virus, de bactéries, de champignons, de toxines ou de micro-organismes dans le but de provoquer intentionnellement une maladie ou le décès d'êtres humains, d'animaux ou de plantes.

Carver / Shock (Guide DGAL) : Outil américain qui permet, dans une organisation, d'évaluer et hiérarchiser les risques et conséquences engendrés par un acte de malveillance, à partir des points les plus vulnérables, les plus attractifs et les plus accessibles pour une éventuelle attaque.

Criticité (Guide DGAL) : Estimation de la conséquence d'une attaque en termes de santé publique (nombre de décès possibles) et des impacts économiques.

Danger lié à la sécurité (Norme ISO 22000) : Agent biologique, chimique ou physique présent dans une denrée alimentaire ou état de cette denrée pouvant entraîner un effet néfaste sur la santé.

Diagramme de flux (Norme ISO 22000) : Présentation schématique et systématique de la séquence d'étapes et de leurs interactions.

Effet (Guide DGAL) : Estimation du montant de pertes directes résultant d'une attaque, mesuré par la perte de production.

Food Defense (Food & Drug Administration) : Ensemble des activités dans le domaine de la protection des approvisionnements alimentaires contre des actes de contaminations délibérées ou de manipulations frauduleuses.

Malveillance (Dictionnaire) : Intention de nuire ou animosité à l'égard d'autrui.

Menace (Dictionnaire) : Signe qui indique quelque chose que l'on doit craindre.

Mesures de maîtrise (Norme ISO 22000) : Action ou activité à laquelle il est possible d'avoir recours pour prévenir ou éliminer un danger lié à la sécurité des denrées alimentaires ou pour le ramener à un niveau acceptable.

Récupération (Guide DGAL) : Estimation de la capacité de récupération après une attaque.

Repérage (Guide DGAL) : Facilité d'identification de la cible.

Risque (Norme ISO 31000) : Effet de l'incertitude sur l'atteinte des objectifs.

VACCP (Guide DGAL) : Analyse de vulnérabilité et maîtrise des points critiques : méthode qui permet de développer un plan de protection interne à l'organisation après une analyse de vulnérabilité basée sur des principes semblables à ceux du système HACCP.

Vigilance (Dictionnaire) : Fait d'être attentif.

Vulnérabilité (Guide DGAL) : Estimation de la facilité à réaliser l'attaque.

2 ÉTAPES PRÉALABLES À L' ANALYSE FOOD DEFENSE

DÉTERMINATION DU CONTEXTE ET ENGAGEMENT DE LA DIRECTION

Détermination du contexte

De quoi parle-t-on ?

Il s'agit de définir le contexte interne de l'organisme (climat social, difficultés financières, rumeurs de délocalisation, représentation religieuse…) ainsi que le contexte externe (perception de ses activités par les parties prenantes, environnement géographique dans lequel l'organisme évolue, contexte sociétal, géopolitique et stratégique). Parmi les questions à se poser pour identifier son contexte :

- Le produit jouit-il d'une grande notoriété ?
- Le produit a-t-il une connotation particulière (religieuse, éthique, morale, etc.) ?
- Le produit peut-il être un ingrédient utilisé dans une grande variété d'autres produits ?
- L'origine des matières entrant dans la composition du produit peut-elle être controversée ?
- Le site est-il situé dans une région politiquement et socialement sensible ?
- L'entreprise est-elle impliquée dans un conflit ?
- Y a-t-il des personnalités célèbres à la tête de l'entreprise ?
- La marque est-elle susceptible d'attirer la convoitise des concurrents ou est-elle controversée ? …

Recommandations et bonnes pratiques

L'idée est d'**identifier clairement si l'organisme évolue dans un contexte** :

- Apaisé (menace imprécise) ;
- Agité (menace possible) ;
- Critique (menace certaine).

Plus la menace est certaine et plus l'organisme doit augmenter son niveau de vigilance.

Il convient que le contexte soit revu régulièrement et au moins une fois par an.

Engagement de la Direction

De quoi parle-t-on ?

L'engagement de la Direction est incontournable car :

- La Food Defense implique une vision stratégique qui s'inscrit sur le long terme ;
- Les conséquences possibles d'une réorganisation, d'un changement de stratégie, des risques sociaux, etc, seront à traiter par la Direction au plus haut niveau.

Recommandations et bonnes pratiques

Il convient que **la Direction établisse une politique Food Defense**. Cette politique pourra servir de cadre à la définition d'objectifs généraux.

Exemples :

- Diminuer la probabilité d'attaques malveillantes ;
- Limiter les impacts en cas de survenue ;
- Protéger la réputation de l'organisme ;
- Satisfaire les exigences des référentiels internationaux (IFS, BRC, ISO/TS 22002 series) ;
- Rassurer les clients, consommateurs, médias…

Pièges à éviter

- **Avoir un engagement de « façade » ;**
- **Sous-estimer la probabilité d'une attaque malveillante.**

CONSTITUTION D'UNE ÉQUIPE CHARGÉE DE LA SÛRETÉ

De quoi parle-t-on ?

Le maître mot dans la composition de l'équipe est la « confiance ». Les membres de l'équipe doivent être choisis en fonction de leur fiabilité, de leur implication directe dans le projet, de leurs compétences et connaissances. L'expérience est importante pour l'antériorité des évènements. Le leitmotiv de l'équipe chargée de la sûreté est la confidentialité, car elle va travailler sur les vulnérabilités de l'organisme.

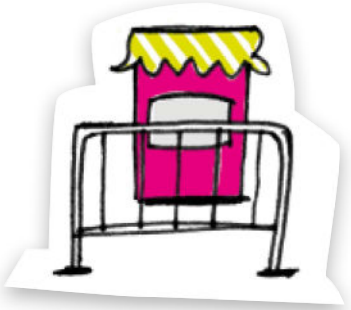
Recommandations et bonnes pratiques

La sélection des membres de l'équipe doit tenir compte de la capacité à communiquer judicieusement sur le thème de la sûreté (capacité également à ne pas communiquer sur ce thème; un comptable sera « secret » sur les comptes de la société, un vendeur sera communiquant…).

L'équipe s'organise autour de la mission qui lui est confiée, elle s'inscrit dans la durée (ce n'est pas une équipe projet).

L'équipe chargée de la sûreté peut être très différente de l'équipe pluridisciplinaire chargée de la sécurité des denrées alimentaires (équipe HACCP). Les membres peuvent être internes à l'organisme (directeurs, responsable sûreté / sécurité, responsable RH, responsable flux responsable production, responsable qualité, responsable des achats, responsable entretien & maintenance, services généraux, responsable logistique, responsable laboratoire…) mais aussi externes (assureurs, douanes, prestataires de services…).

Il convient toutefois de limiter le nombre de participants. Une fois l'équipe désignée, il y a lieu de bien définir les missions de chacun et de les faire former à la Food Defense par une personne compétente. Et comme pour l'HACCP, ne pas omettre de prendre en compte la suppléance, en cas d'absence.



RÉALISATION D'UN DIAGNOSTIC SÛRETÉ

De quoi parle-t-on ?

Le diagnostic doit permettre de mettre en évidence les forces et les faiblesses de l'organisme en matière de Food Defense. Ce diagnostic doit déboucher sur un plan d'action initial.

Il convient de préparer le diagnostic avec l'équipe sûreté. Celui-ci peut se baser sur des grilles préétablies reprenant les exigences du référentiel IFS. De nombreuses grilles sont disponibles en accès libre sur Internet. Ces grilles sont pour la plupart en anglais car proposées par les autorités américaines (FDA ou USDA par exemple).

Recommandations et bonnes pratiques

Le diagnostic réalisé par l'équipe sûreté peut être avantageusement complété par un test d'intrusion. Celui-ci, réalisé dans les conditions normales de fonctionnement impose certaines conditions :

- Choisir une personne inconnue des salariés ;
- Prévoir des scénarii de comportement hors norme (s'approcher des produits en hésitant, faire mine d'être observé, mal à l'aise, répondre en langue étrangère aux injonctions…) ;
- Mettre dans la confidence 1 ou 2 personnes sur la date retenue pour la réalisation du test ;
- Chronométrer la durée d'intrusion ;
- Faire un débriefing du test d'intrusion (lieu de pénétration, attitude des salariés envers l'intrus, facilité d'évolution dans les locaux…) ;
- Prévoir un plan d'actions suite à ce test.

L'annexe A1 « Exemple de grille d'identification des Mesures de Prévention Préalables (MPP) de leur mise en place et de leur effectivité » peut servir de trame à la réalisation d'un diagnostic sûreté.

DÉTERMINATION DES MESURES DE PRÉVENTION PRÉALABLES (MPP)

De quoi parle-t-on ?

Le guide des recommandations pour la protection de la chaîne alimentaire contre les risques d'actions malveillantes, criminelles ou terroristes de la DGAL (janvier 2014) pose la base des prérequis de sûreté pour la protection de la chaîne alimentaire, selon six grands domaines (Cf. Figure 1).

Recommandations et bonnes pratiques

Les mesures de prévention préalables (MPP) sont des éléments de base de la sûreté et sont donc en amont de l'analyse de risques Food Defense. Cette dernière sera menée en partant du principe que toutes les MPP sont appliquées de manière performante. C'est la clé d'une analyse de risques et d'une maîtrise efficace de la Food Defense.

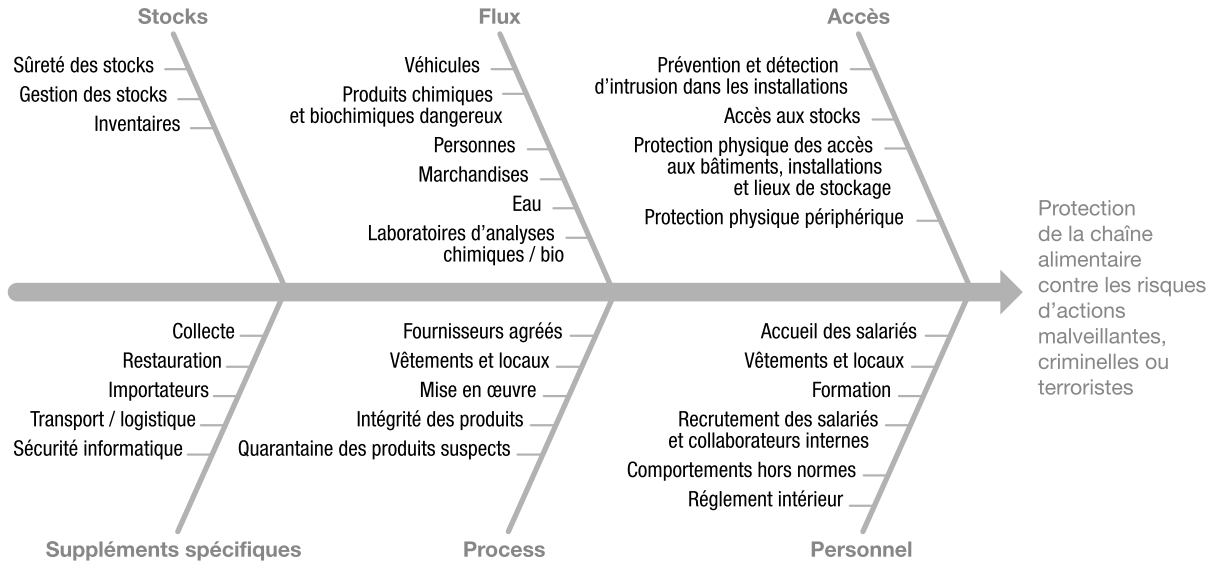
Une grande partie des éléments du guide de la DGAL sont des MPP à appliquer a priori pour tous types d'organismes agro-alimentaires sauf justifications particulières.

Pièges à éviter

• Lorsque certaines MPP ne sont pas en place et / ou vont nécessiter des investissements, une tendance à considérer qu'elles sont de fait « non applicables » peut se dessiner. Nous recommandons beaucoup de prudence afin de ne pas tomber dans cette solution de facilité. En effet, certains des prérequis du guide sont soit des exigences réglementaires de sécurité soit des exigences de l'IFS. Elles sont indiquées en couleur dans l'annexe A1.

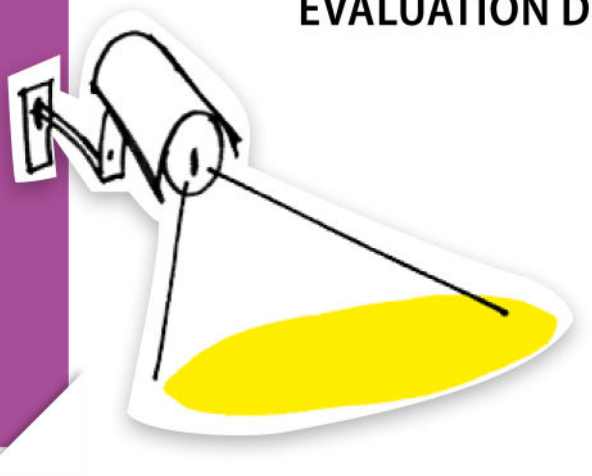
• En cas de MPP jugées « non applicables » par l'organisation au regard de ses spécificités, il est fondamental de l'argumenter et de formaliser la justification. Si la situation de votre organisation justifie pleinement la non application de certaines des MPP du guide de la DGAL, ceci est à décrire précisément (Cf. Annexes A1 Exemple de grille d'identification des MPP, de leur mise en place et de leur effectivité et A2 Exemple de procédure de sécurisation d'un site).

Figure 1. Domaines de prévention en matière de Food Defense



3 ÉTAPES DE L'ANALYSE FOOD DEFENSE

ÉVALUATION DES MENACES, DE LA VULNÉRABILITÉ



Identification des menaces possibles

De quoi parle-t-on ?

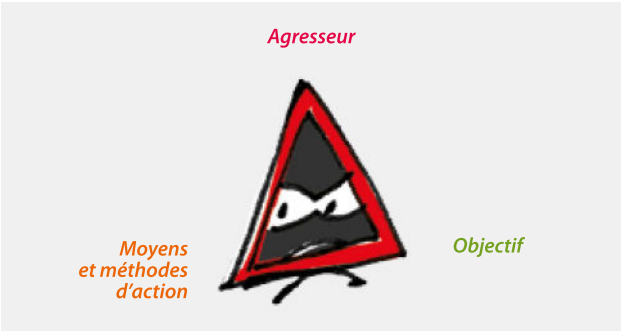
L'acte de malveillance peut être l'acte spontané ou planifié d'un individu ou d'un groupe.

Il peut s'agir d'une opération impulsive pas ou peu planifiée. Elle émane d'une personne pouvant avoir accès aux installations, aux matières premières, aux produits finis…

Il peut aussi s'agir d'une opération structurée et planifiée menée par des acteurs qualifiés avec une volonté de destruction matérielle ou humaine, qui visent une large cible. Ils peuvent faire appel à d'autres personnes (complices) pour arriver à leur fin.

Une menace humaine se traduit par les répercussions néfastes que pourrait avoir le comportement d'un individu ou d'un groupe d'individus sur l'organisme et ses produits / services. On parle de triangle de la menace (Cf. figure 2).

Figure 2. Le triangle de la menace



L'agresseur peut être interne ou externe à l'organisme (Cf. figure 3).

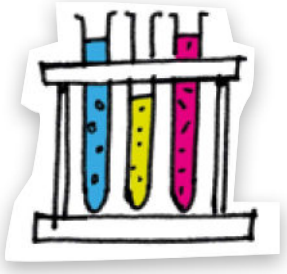
Figure 3. Tableau des agresseurs potentiels (liste non exhaustive)

En interne	En externe
• Employés mécontents	• Groupe activiste ou terroriste
• Equipes nettoyage, maintenance	• Prestataires transport, stockage
• Sous-traitants (à détailler)	• Anciens employés
• Employés temporaires, intérimaires	• Fournisseurs, concurrents
• Employés activistes	• Visiteurs, inspecteurs, auditeurs
• Stagiaires	• Riverains

Dans tous les cas, l'agresseur va agir sur le produit ou le procédé de fabrication afin de générer des dangers. Pour mémoire, un danger est « tout agent biologique, chimique ou physique présent dans un aliment ou état de cet aliment pouvant entraîner un effet néfaste sur la santé ».

Ils sont de 3 natures :

- Biologiques : virus, bactéries, parasites (ex : souches pathogènes « classiques », bacille du charbon, Anthrax…) ;
- Physiques : nuisibles, bris de verre, aiguilles, métal coupant, cailloux, mégots de cigarette…
- Chimiques : agents létaux (neurotoxiques, suffoquant, asphyxiants), allergènes, agents gazeux (sarin, chlore), agents solides (cyanure, arsenic, sels de mercure), pesticides, produits de nettoyage, de maintenance, de lutte contre les nuisibles…



Pièges à éviter

La première difficulté pour les organismes de la chaîne alimentaire réside dans le fait qu'ils ne sont que rarement confrontés à la malveillance de manière évidente.

Les pièges à éviter sont les suivants :

- **La paranoïa conduisant à être dans l'incapacité de prioriser les menaces potentielles ;**
- **Le refus total de considérer qu'il puisse y avoir des menaces potentielles.**

Il convient de maintenir distinctes les études HACCP (sécurité des aliments) et Food Defense (sûreté alimentaire), la première étant liée à une contamination accidentelle de l'aliment, quand l'autre concerne la contamination intentionnelle. Il vaut mieux ne pas inclure la Food Defense dans le HACCP. Néanmoins, il y a lieu d'utiliser le travail réalisé dans le cadre de l'HACCP (notamment les CP / PRPo et CCP) lorsqu'il permet d'enrichir la démarche Food Defense.

Identification des zones sensibles (cibles)

De quoi parle-t-on ?

Les zones sensibles sont importantes à identifier car ce sont à ces endroits précis que l'agresseur va pouvoir agir : l'identification de ces zones est un prérequis à l'analyse des risques, permettant de faciliter l'identification d'éventuelles mesures de MAÎTRISE spécifiques et / ou complémentaires aux MPP.

Pour identifier les zones, il convient de combiner l'approche géographique et les flux (Cf. figure 4).

Outre les accès classiques (portes, fenêtres, trappes de désenfumage…), d'autres accès doivent être pris en compte : ventilation, air comprimé, chauffage, gaz, eau (y compris forage, glace, vapeur), électricité, réfrigération, système de nettoyage en place, canalisations, cuves, stockages tampon, systèmes de traitement y compris à l'extérieur…

D'une manière générale, plus on se rapproche du procédé et donc du produit et plus la zone est sensible.

A l'issue de cette étape, l'équipe Food Defense dispose d'un ensemble de cibles vulnérables.

Recommandations et bonnes pratiques

Pour identifier les cibles potentielles, l'équipe en charge de la Food Defense peut avantageusement s'appuyer sur un certain nombre de documents comme par exemple :

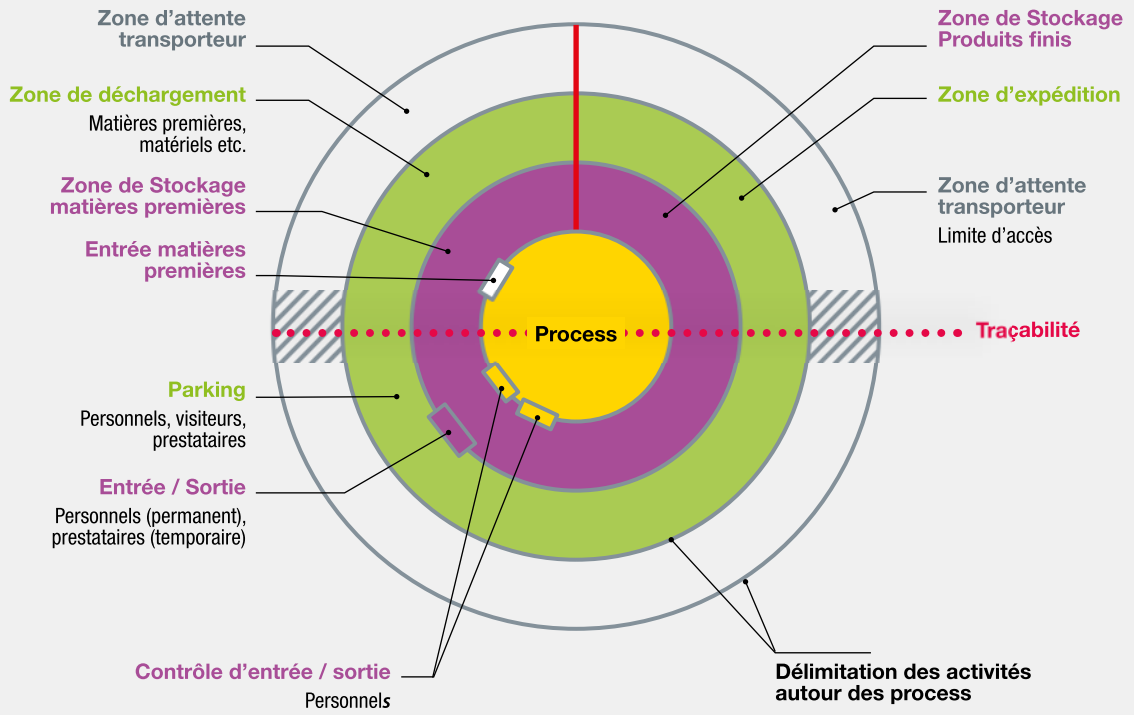
- Le plan de masse du site ;
- Le diagramme des flux (produits, personnel, visiteurs, déchets…) ;
- Le schéma d'implantation des équipements.

Pièges à éviter

Les zones à faibles risques et hauts risques définies dans l'HACCP peuvent servir de base de travail, mais la composante à intégrer en supplément concerne la possibilité pour une personne de commettre volontairement une contamination.

Figure 4. Approche combinée des zones géographiques et des flux

Protocoles 3 niveaux d'instructions



Évaluation de la vulnérabilité

L'annexe B présente un exemple de système d'évaluation de la vulnérabilité, élaboré à partir de 4 critères :

- Impact produit ;
- Gravité ;
- Accessibilité ;
- Facilité.

Des coefficients mais également des codes couleurs ont été attribués à chacun de ces critères. Ils permettent de définir un seuil critique pour l'évaluation brute de la vulnérabilité.

Lorsque le seuil critique est atteint, il y a lieu de mettre en place une mesure de sûreté supplémentaire pour réduire la vulnérabilité à un seuil plus acceptable.

Il convient donc de réaliser l'évaluation brute de la vulnérabilité (1re fois) puis de réaliser l'évaluation résiduelle de la vulnérabilité (après l'application des mesures de sûreté supplémentaires).

Le tableau présenté à l'annexe B a été construit de la façon suivante (colonnes) :

- Étapes du procédé de fabrication (Cf. annexe A3 Exemple de diagramme de fabrication) ;
- Cibles potentielles ;
- Agresseurs présumés ;
- Objectifs des agresseurs ;
- Moyens et méthodes d'action, type de danger ;
- Mesures de sûreté existantes spécifiques à l'étape concernée (hors MPP) ;
- Évaluation brute de la vulnérabilité : calcul selon la méthode expliquée précédemment.

En cas de dépassement du seuil critique :

- Mesures de sûreté supplémentaires (avec responsabilités et délais) ;
- Évaluation résiduelle de la vulnérabilité : calcul selon la méthode expliquée précédemment.

IDENTIFICATION DES MESURES SPÉCIFIQUES ET / OU SUPPLÉMENTAIRES DE MAÎTRISE

Compte tenu des résultats de l'évaluation de la vulnérabilité, il conviendra de définir des mesures de maîtrise spécifiques et / ou complémentaires aux MPP. Ces mesures devront faire l'objet d'une attention particulière car de leur bonne application dépendra la maîtrise effective de la malveillance.

Des exemples de mesures spécifiques et / ou supplémentaires sont mentionnés dans l'annexe C.

GESTION D'UN ACTE MALVEILLANT (GESTION DE CRISE ET RETRAIT / RAPPEL)

Il revient à la Direction générale et au responsable Food Defense de construire et de coordonner le dispositif de gestion de crise.

Sous cette réserve, des actions peuvent également être diligentées par la communication, les départements Sûreté et Sécurité de fonctionnement et les autres responsables opérationnels.

Le responsable Food Defense agit en collaboration avec d'autres acteurs pour la gestion effective de la crise. Les missions de coordinateur, secrétaire et porte-parole doivent être définies au préalable.

Dans le cadre de la gestion d'un acte malveillant, le responsable Food Defense a un rôle majeur à jouer :

- Veiller à ce que l'entreprise ait préparé ses modes de communication de crise, mettre en place des tests et des formations utiles ;
- Coordonner l'ensemble des actions et des initiatives ;
- Anticiper les menaces possibles par une étude de scenarii ;
- Inviter tous les acteurs à s'entraîner, à réagir dans un contexte inhabituel ;
- Maîtriser les notions clés de la gestion de crise ;
- Proposer les méthodologies et les procédures rendant opérationnel le dispositif de secours, de continuité et de retour à la normale ;
- Préparer et gérer l'après-crise (plan de continuité d'activité, pratique des retours d'expérience, actions correctives…).

La gestion d'un acte malveillant peut également déclencher un retrait / rappel des produits.

Dans ce cas précis :

- Évaluez précisément le risque pour la santé : si nécessaire, faites appel à un expert médical ou scientifique. Demandez des contre-analyses. Vérifiez la disponibilité du laboratoire ;
- Définissez précisément le produit à rappeler, les numéros de lots concernés, leur localisation, les quantités, DLC-DLUO, etc ;
- Enquêtez sur l'origine de la malveillance afin de vérifier si d'autres lots doivent être retirés ou rappelés. Si plusieurs n° de lot sont concernés, posez-vous la question du retrait de la totalité de la référence ;
- Évaluer le coût prévisionnel de l'opération envisagée ;
- Contactez l'assureur et prenez connaissance du montant de la garantie en cas de rappel de produit ;
- Constituez dès le début votre dossier de preuves (constat d'huissier, photos, originaux de résultats d'analyses…) ;
- Organisez le comptage des produits récupérés. Evaluez la quantité présente chez le consommateur. Conservez des échantillons ;
- Informez les distributeurs concernés et définissez avec eux les modalités du rappel : affichage en rayons ; retrait et isolement des produits ; récupération ou destruction ;
- Si l'administration n'est pas au courant, informez-la et présentez-lui votre plan d'action et de communication ainsi que le communiqué de presse ;
- Accordez-vous si possible avec les services administratifs concernés pour déterminer qui envoie le communiqué ;
- Vérifiez régulièrement à quel niveau de l'administration est traité votre dossier (départemental, régional ou cellule d'alerte nationale) ;
- Restez en contact permanent avec le(s) service(s) administratif(s) qui sui(ven)t votre dossier et référez-vous à la procédure de gestion des alertes et des crises de l'administration ;
- Débriefez le cas échéant avec votre maison mère, votre organisation professionnelle…

SUIVI, MISE À JOUR ET AMÉLIORATION DU PLAN FOOD DEFENSE

Il convient que l'organisme réalise le suivi des mesures de sûreté et procède à la vérification de l'efficacité de son système Food Defense.

Les méthodes et les tests sur lesquels l'organisme peut s'appuyer sont nombreux :

- Contrôles fréquents ;
- Audits internes ;
- Audits externes ;
- Simulations de situations (test d'intrusion par ex.) ;
- Inspections des parties prenantes (services des fraudes par exemple) ;
- Résultats liés aux objectifs Food Defense ;
- Enregistrement des dérives ou actes malveillants identifiés ;
- Benchmark et veille.

La révision du plan Food Defense se fera :

- De façon systématique (au moins annuelle) en fonction des résultats des vérifications de l'application et de l'efficacité des mesures de sûreté mises en place ;
- En cas de modification du contexte (interne et externe) ;
- Suite aux tests d'intrusion, si nécessaire ;
- Le cas échéant, suite à un véritable acte de malveillance ;
- Les résultats de l'efficacité du Plan Food Defense pourront être intégrés dans la revue de direction.

CONCLUSION / BILAN

La rédaction de ce document a suscité beaucoup d'intérêt, d'enthousiasme, d'échanges d'expérience vifs et animés et d'engagement bénévole. Que l'ensemble des contributeurs à ce groupe de travail et leurs organisations en soient sincèrement remerciés.

Les contributeurs espèrent que ce document vous permettra de maîtriser au mieux les risques réels auxquels vous êtes régulièrement confrontés.

Vos retours d'expérience permettront d'optimiser cet outil et notre groupe compte sur vous pour nous faire part de vos remarques et voies d'amélioration à :

dj.maufrand@gmail.com
olivier.boutou@afnor.org

4 ANNEXES

ANNEXE A1

EXEMPLE DE GRILLE D'IDENTIFICATION DES MESURES DE PRÉVENTION PRÉALABLES (MPP) DE LEUR MISE EN PLACE ET DE LEUR EFFECTIVITÉ

Base : Guide des recommandations pour la protection de la chaîne alimentaire contre les risques d'actions malveillantes, criminelles ou terroristes. Edition janvier 2014 (Ministères français)			**Eléments mis en place**	**Commentaires: Attention lorsque la MPP n'est pas retenue il faut l'argumenter**	**À mettre en place**	
N°	**Objectifs**	**Recommandations de moyens** (extraits Guide 2014)			**oui**	**non**
1-1 Protection physique périphérique	Empêcher l'accès de personnes non autorisées et non identifiées vers les locaux de production (stockage compris).	Mettre en place des clôtures suffisament hautes, avec signalétique d'interdiction lisible.	Clôture d'environ 2m sur toute la périphérie du site mais sans signalétique	Pose d'une signalétique d'interdiction d'entrer	oui	
		Organiser un poste de contrôle d'accès au site, soit unique, soit si possible en différenciant l'accès du personnel de l'accès d'intervenants extérieurs (livreurs, visiteurs, prestataires, clients).	Pas de poste de contrôle d'accès	Non réalisable vu la situation du site		non
		Mettre en place des dispositifs de surveillance : éclairage de nuit, gardiennage, vidéo.	Éclairage de nuit	Possibilité de mettre en place une surveillance vidéo	oui	
		Installer des dispositifs de détection d'effraction ou de franchissement.	Pas de dispositif	Non justifié		non
1-2 Protection physique des accès aux bâtiments et lieux de stockage	Empêcher l'accès de personnesnon autorisées et non identifiées à l'intérieur des locaux de production (stockage compris).	Maintenir les portes piétonnières du rez-de-chaussée sous surveillance (humaine ou autre) pendant les heures de travail et fermées par des serrures de sûreté hors des heures de travail.	Réalisé			non
		Maintenir les issues de secours fermées par des serrures de sûreté en dehors des heures de travail et s'assurer qu'elles ne permettent pas d'entrer par l'extérieur en toute période.	Réalisé			non
		Maintenir l'accès aux quais ou sas de chargement et de déchargement fermé en dehors des livraisons ou expéditions.	Réalisé			non
		Munir si possible les fenêtres du rez-de-chaussée de grilles ou barreaux et les maintenir fermées hors de la présence de personnel dans le local concerné.	Fait pour la production mais pas pour les fenêtres des bureaux		oui	
		Renforcer la solidité des ouvertures de toit (vasistas, exutoires de fumées).	Pas de protection particulière	Installer des croisillons	oui	
		Surveiller l'accès aux toitures, systèmes de ventilation et de climatisation.	Fait dans le cadre de la surveillance des locaux			non

Base : Guide des recommandations pour la protection de la chaîne alimentaire contre les risques d'actions malveillantes, criminelles ou terroristes. Edition janvier 2014 (Ministères français)			Eléments mis en place	Commentaires: Attention lorsque la MPP n'est pas retenue il faut l'argumenter	À mettre en place	
N°	**Objectifs**	**Recommandations de moyens** (extraits Guide 2014)			**oui**	**non**
1-3 Prévention et détection d'intrusions dans les installations	Mettre en place une organisation de la gestion des accès (ex : gestion des clés et ou des codes) et un système de surveillance du ou des sites ou des bâtiments adaptés et efficaces pendant et en dehors des heures de travail.	Mettre en place des systèmes d'alarme pour détecter les intrusions par les accès du rez-de-chaussée, et pour détecter une présence anormale dans les locaux « sensibles » ou dans les couloirs de circulation qui y mènent en dehors des heures de travail.	Mis en place dans les bureaux mais pas dans les locaux de production.	Non envisagé.		non
		Mettre en place une centrale d'alarmes avec des procédures adaptées.	Pas d'alarme.	Non envisagé.		non
		Installer, dans les zones les plus sensibles, des systèmes de vidéo-surveillance : • Réseau de caméras • Enregistrement selon la législation en vigueur vis-à-vis de la vidéo-surveillance et traitement des données en conséquence.	Vidéo surveillance en place en dehors des heures de travail.	Peut être étendue 24h / 24.		non
		Mettre en place, si possible, des systèmes d'identification et de circulation par badges : • Avec badges différenciés ou systèmes de puces d'identification selon les catégories de personnes et les zones d'habilitation • Avec procédures de mode d'établissement et mode de gestion de ces systèmes • Garder une traçabilité, un historique.	Badge pour accéder aux locaux + maintenance stockage produits nettoyage et autres produits chimiques (y compris le laboratoire) fermé à clé historique centralisé ?	Pas de zone d'habilitation hors maintenance.		non
		Vérifier en cas de recours à des prestataires de sûreté extérieurs (gardiennage …).	Pas de gardiennage.			non
		Organiser la gestion des clés et codes d'accès : • Affectation personnalisée des clés et / ou des codes d'accès • Passe-partout hiérarchisés • Stockage sécurisé des clefs essentielles « sensibles • Garder une traçabilité des affectations successives.	Suivi personnalisé des clés mais pas de procédure.	Création d'un document.	oui	
1-4 Les accès aux stocks	Avoir un accès au stock maîtrisé. NB: PRP Hygiène en rouge imposé par le Paquet Hygiène et l'IF.	Veiller au respect du stockage séparé, ceci particulièrement pour les matières premières alimentaires, les produits finis, les conditionnements et emballages, les produits potentiellement dangereux (intrants biochimiques, chimiques, produits de nettoyage, de maintenance).	Réalisé.			non
		Installer des systèmes de fermeture des locaux de stockage, à utiliser en période de non production.	Portes de chambres froides et locaux produits chimiques fermés à clé. Stock de boîtes vides non sécurisé.			non
		N'autoriser l'accès aux stocks qu'à des personnes habilitées.	Accès limité pour une partie du stock (ingrédients, chambre négative).			non
		Fermer systématiquement à clé les accès aux locaux et armoires de stockage de produits dangereux, en dehors de la présence du personnel concerné.	Réalisé.			non
		Veiller à la sécurisation des fenêtres, trappes, grilles et ouvertures de plafond pouvant permettre l'accès aux locaux de stockage.	Pas de sécurisation particulière.	Installation de croisillons.	oui	
		Proscrire au maximum les stockages en plein air : Sécuriser ceux qui le sont (ex cuves à lait) par des systèmes de verrouillage efficaces.	Stockage externe de sulfite protégé, stockage de palettes de sel non sécurisé.	Création d'un local spécifique ou emplacement dédié dans l'usine.	oui	
		Réduire au maximum toutes zones où pourraient être cachés des produits (niches, faux-plafonds,…) et y réaliser des contrôles réguliers.	Inspections réalisées.			non
2-1 Flux de véhicules	Maîtriser les flux des véhicules sur le site NB: Les élements en rouge sont des exigences de sécurité.	Mettre en place un plan de circulation et de stationnement affiché à l'entrée du site.	Plan de circulation mis en place.	À formaliser et à afficher.	oui	
		Déterminer des zones de parking spécifiques pour les différents intervenants : véhicules professionnels de l'entreprise, véhicules de prestataires, du personnel, de visiteurs.	En place.			non
		Situer les aires de stationnement des visiteurs et des personnels, autant que possible à distance, voire avec séparation physique, des installations.	Non réalisé.		oui	
		Signaliser les emplacements réservés, autorisés et interdits.	Réalisé.			non
		Surveiller la présence anormale de véhicules stationnant en dehors de horaires de fonctionnement de l'établissement.	Formation du personnel sur ce thème + surveillance du concierge.			non
		Organiser un contrôle des véhicules entrant ou sortant du site et si possible une traçabilité.	Non réalisé.	Non réalisable (pas de poste de contrôle).		non

Base : Guide des recommandations pour la protection de la chaîne alimentaire contre les risques d'actions malveillantes, criminelles ou terroristes. Edition janvier 2014 (Ministères français)			Eléments mis en place	Commentaires: Attention lorsque la MPP n'est pas retenue il faut l'argumenter	À mettre en place	
N°	Objectifs	Recommandations de moyens (extraits Guide 2014)			oui	non
2-2 Flux de personnes (sauf grand public)	ATTENTION ZONE SENSIBLE A DEFINIR AVANT L'ANALYSE ET A VALIDER PAR L'ANALYSE. Qu'est ce qu'une zone sensible et méthodologie à déterminer ? Déterminer les zones sensibles et maîtriser le flux des personnes en adéquation avec la sensibilité définie.	Analyser le process interne pour déterminer les zones les plus sensibles : les identifier et y limiter l'accès.	Les zones sensibles sont déterminées, le personnel est formé.			non
		Gérer les accès des personnes (membres du personnel ou non) aux différentes zones, en fonction de la sensibilité recensée (badges, digicodes, tenues…).	Uniquement maintenance et stockage des produits chimiques.			non
		Tenir un registre des personnes entrant ou sortant des installations et le conserver.	Réalisé.			non
		Préétablir une liste permettant de connaître : • le personnel qui est normalement prévu sur le site • les personnes extérieures attendues et les membres du personnel qui ont la responsabilité de leur prise en charge.	Réalisé pour le personnel qui pointe (intégré à un planning de production) mais pas réalisé pour l'encadrement.	À mettre en place pour toute personne présente sur le site	oui	
		Traiter tout écart selon une procédure définie, et l'enregistrer.	Non réalisé.	Non justifié		non
		Doter le personnel de tenues différentes selon les secteurs d'activité de l'établissement.	Réalisé.			non
		Doter de même tous les intervenants extérieurs et visiteurs de badges et de tenues spécifiques.	Tenues spécifiques.			non
		Installer, lorsque cela est possible, des systèmes d'accès identifiant les individus et gérant les entrées et sorties des zones différenciées.	Gestion des entrées mais pas d'identification des individus.	Non justifié		non
		A défaut, sensibiliser les collaborateurs à la reconnaissance de présence anormale.	Réalisé (sensibilisation du personnel et formation de l'encadrement).			non
		Encadrer toutes les visites (écoles de tous niveaux, clubs des anciens, agriculteurs livreurs, clients actuels ou potentiels…) par un membre du personnel, en interdisant tout accès aux zones sensibles.	Réalisé.			non
		Prohiber ces visites d'écoles (…) en cas d'alerte grave.	Réalisé.			non
		Mettre en place un dispositif de contrôle de tous les accédants aux chantiers de moyenne ou longue durée.	Réalisé par signature du procès verbal.			non
		Limiter physiquement les passages entre le chantier et les installations.	Installation de protections dans la mesure du possible.			non
2-3 Flux de marchandises	Avoir une procédure de réception et de contrôle à réception adaptés (y comprisla gestion des échantillons et des retours de marchandise). Attention aux exigences IFS et Paquet Hygiène à mettre en rouge.	Contrôler la conformité de la livraison réelle par rapport à la livraison commandée attendue.	Réalisé.			non
		Appliquer les procédures de réception habituelles (dont Qualité) et, en cas de doute sur un produit identifié, intégrer les contrôles spécifiques sur ce produit	Réalisé.			non
		Vérifier les documents (nature et origine des marchandises, volumes, date et heure de départ en particulier), l'identité du transporteur livreur et son appartenance à la société prestataire notamment pour un livreur inhabituel	Réalisé.			non
		Vérifier l'intégrité des citernes en cas de vrac et des emballages en cas de sacs, big-bags ou autres, procéder éventuellement à un échantillonnage	Réalisé à réception ou à l'utilisation en fonction des produits.			non
		Contrôler les procédures de nettoyage des moyens de transports	Réalisé.			non
		Ne pas accepter de réception en dehors de la présence des responsables et hors des heures prévues. Eviter les livraisons en sas sans surveillance, en particulier la nuit	Réalisé.			non
		Etablir des procédures internes de détection de toute anomalie concernant les modalités de la livraison, la conformité à la commande, les conditionnements et emballages, les produits. Noter, signaler et traiter toute anomalie détectée	Réalisé.			non
		Établir une procédure claire pour les cas particuliers des retours de marchandises et échantillons arrivant par transporteur ou par poste	Réalisé.			non
		Respecter et sécuriser les zones de stockage affectées à chaque type de marchandise, alimentaire ou autre (conditionnements, emballages, produits dangereux, gaz)	Réalisé.			non
		Vérifier l'intégrité des emballages et conditionnements au déstockage des marchandises	Réalisé.			non
		Établir des procédures de reconditionnement des produits	Non justifié dans ce cas.			non
		Prohiber la réutilisation d'emballages sauf cas prévus et cadrés par une procédure	Procédure de réutilisation dans certains cas définis.			non
		Vérifier l'intégrité des conditionnements et des étiquetages lors de l'utilisation des marchandises	Réalisé pour les conditionnements.			non
		Matérialiser la zone d'expédition et si possible la fermer	Réalisé.			non

Base : Guide des recommandations pour la protection de la chaîne alimentaire contre les risques d'actions malveillantes, criminelles ou terroristes. Edition janvier 2014 (Ministères français)			Eléments mis en place	Commentaires: Attention lorsque la MPP n'est pas retenue il faut l'argumenter	À mettre en place	
N°	Objectifs	Recommandations de moyens (extraits Guide 2014)			oui	non
2-3 Flux de marchandises	Avoir une procédure d'expédition et de contrôle adaptés. Attention aux exigences IFS et Paquet Hygiène et règlementation du transport à mettre en rouge.	Vérifier la conformité des expéditions par rapport à la commande (date, nature, quantité).	réalisé			non
		S'assurer que les emballages sont hermétiques : « filmer » les palettes.	réalisé			non
		Vérifier que le bon de livraison porte bien les informations utiles pour le contrôle à réception du destinataire, y compris le numéro du camion, et éventuellement la nature des emballages.	réalisé			non
		Respecter les plannings et horaires d'expédition.	réalisé			non
		Surveiller les chargements en particulier en cas de groupage.	réalisé			non
		Établir une procédure d'enregistrement des expéditions suffisamment documentée pour servir en cas d'incident constaté ultérieurement.	flashage des expéditions et suivi ERP pour la traçabilité			non
2-4 Divers flux	Gérer les produits chimiques selon la règlementation en vigueur. Maîtriser la qualité de l'eau à la réception et dans les flux internes de l'entreprise (rouge réglementaire). Gérer les flux et accès pour les laboratoires (selon exigence 4,8,4 de l'IFS).	Produits chimiques et biochimiques dangereux : Mettre en place un système de stockage d'étiquetage de gestion et de circulation des produits chimiques dangereux : stockage spécifique fermé hermétiquement, accessibilité réservée aux personnels désignés, et gestion des stocks précise. Disposer des fiches de toxicité et de données de sécurité complètes et à jour. NB: penser aussi aux pièges à rongeurs.	réalisé			non
		Eau : vérifier et contrôler régulièrement les captages et leur sécurisation selon la législation en vigueur.	Eau de réseau uniquement.			non
		Eau : vérifier et contrôler les circuits d'arrivée et de circulation interne des eaux.	Réalisé suivant un planning défini.			non
		Eau : vérifier et contrôler les citernes de stockage internes.	Réalisé.			non
		Eau : vérifier et contrôler les installations internes de recyclage.	Réalisé.			non
		Eau : vérifier et contrôler les adoucisseurs d'eau.	Pas d'adoucisseur.			non
		Eau : prévoir, si possible, un circuit alternatif temporaire en cas d'alerte.	Non réalisé.			non
		Laboratoire interne : isoler physiquement les laboratoires d'analyses (qui peuvent détenir des produits chimiques ou des souches de microorganismes) des autres installations. NB: Penser aussi à la verrerie.	Réalisé.			non
		Laboratoire interne : gérer strictement les accès et les liens avec les sites de production. Fermer les lieux de stockage des produits. Gérer les stocks de produits.	Réalisé.			non
3.1 Recrutement des salariés et collaborateurs internes	Gérer le recrutement et l'accueil des salariés (exigences réglementaires et IFS).	Mener, dans le respect des textes réglementaires en vigueur, les actions d'information nécessaires avant tout recrutement, quelle que soit la catégorie du salarié (permanent, CDD, intérimaire…).	Réalisé.			non
		Des dispositions (contrats) du même type seront en place avec les agences d'intérim, les sociétés de nettoyage et de gardiennage.	Réalisé.			non
		Former et suivre l'intégration des nouveaux employés au cours des premières semaines de présence.	Réalisé (tuteur au poste + formation par le Service qualité).			non
3.2 Vêtements et locaux du personnel	Assurer la gestion des tenues et des locaux (exigences réglementaires et IFS).	Prévoir des recommandations sur la gestion des vêtements de travail et les locaux du personnel.	Réalisé dans le livret d'accueil avec vérifications dans le cadre des audits hygiènes + contrôle des tenues.			non
3.3 Règlement intérieur et comportement	Gérer les comportements anormaux : règlement intérieur et sensibilitation (en rouge : règlementation)	Un règlement intérieur rappellera, par établissement, les dispositions générales et précisera les dispositions particulières liées à la sûreté. Le personnel en sera informé dès son embauche et régulièrement. Toute modification sera clairement portée à la connaissance du personnel.	Réalisé dans le livret d'accueil + rappel lors des réunions annuelles d''expression des salariés.			non
		Détecter les comportements hors normes.	Personnel sensibilisé par le biais des formations et des réunions de service.			non
3.4 Formation du personnel	Adapter le plan de formation en y intégrant les éléments de sureté	Mettre en place un programme de formation aux mesures de sûreté : • formations initiales, formations régulières • formation / information en situation d'alerte, d'urgence et de crise.	OK sur formations intiiales et en cours sur les formations suivantes.			non
3.5 Dispositions après le départ des collaborateurs	Gérer le recrutement et l'accueil des salariés (exigences IFS)	Instaurer, en fonction des causes de départ, les dispositions de sûreté à mettre en place vis-à-vis des différentes catégories de personnel ayant quitté l'entreprise.	Réalisé et formalisé dans la procédure RH.			non

Base : Guide des recommandations pour la protection de la chaîne alimentaire contre les risques d'actions malveillantes, criminelles ou terroristes. Edition janvier 2014 (Ministères français)			Eléments mis en place	Commentaires: Attention lorsque la MPP n'est pas retenue il faut l'argumenter	À mettre en place	
N°	**Objectifs**	**Recommandations de moyens** (extraits Guide 2014)			**oui**	**non**
4 Gestion des stocks	Procédure de contrôle des stocks (matières premières, produits en cours, produits finis) et bilans intermédiaires.	Analyser les marchandises sensibles et déterminer les fréquences des contrôles de stocks en fonction de la dangerosité des marchandises.	Non réalisé.		oui	
		Vérifier l'intégrité des contenants à chaque stockage / déstockage de marchandises.	Réalisé.			non
		Faire des rapprochements entre les stocks théoriques (dont stocks donnés par les systèmes informatiques) et les stocks physiques en fonction de l'analyse ci-dessus, et détecter d'éventuelles anomalies.	Réalisé.	Possibilité d'augmenter la fréquence des rapprochements de stock.	oui	
		Mettre en place les procédures de gestion des stocks et de traitement des anomalies et des écarts de stocks	Réalisé.			non
5 Process	Tableau d'analyse des dangers et d'évaluation des risques sur les zones (vu en 2.2) et sur les procédés.	Analyser les points de vulnérabilité du process pour les réduire et augmenter la surveillance.	Réalisé.			non
		S'assurer que le déroulement des étapes du process a respecté les règles prévues.	Réalisé.			non
	Maîtrise des fournisseurs (exigence réglementaire et IFS).	S'assurer que les marchandises utilisées proviennent de fournisseurs agréés et que les fournisseurs ont eux-mêmes mis en place des procédures de sûreté adaptées.	Réalisé (procédure d'achats + audit du processus achats).			non
		S'assurer que les produits fabriqués (rôle du fabricant) ou livrés (rôle du réceptionnaire) disposent d'un conditionnement et d'un emballage dont l'intégrité peut être aisément et efficacement contrôlée jusqu'au moment de leur utilisation, que ce soit par un transformateur ou par un distributeur (ex palettes filmées) ou par le consommateur final (ex bouchons de bouteilles et couvercles des pots — notamment pots bébé— protégés individuellement par film ou sertissage à briser).	Non réalisé.		oui	
		S'assurer que les procédures de qualification des marchandises ont été respectées.	Réalisé.			non
	Procédure de contrôle à réception et à expédition (exigence réglementaire et IFS).	S'assurer de l'intégrité des emballages et conditionnements à la livraison et lors de l'utilisation.	Réalisé.			non
		S'assurer de l'intégrité et de la conformité des produits mis en œuvre.	Réalisé.			non
		Banaliser au maximum les emballages pour éviter une identification rapide des produits lors du transport ou en entrepôt.	Réalisé.			
	Procédure de traitement d es produits non-conformes. (exigence réglementaire et IFS	Mettre en quarantaine tout produit suspect (couleur, odeur, hétérogénéité anormale, granulométrie, emballage endommagé, comportement du produit inhabituel, etc.).	Réalisé (procédure de gestion des non-conformités).			non
		Traiter les anomalies détectées et les enregistrer.	Réalisé.			non
6 Sûreté informatique	Processus support informatique : • codes d'accès, • systèmes de protection (anti virus, …) centralisés ou par poste, • systèmes de sauvegarde.	Analyser les points de vulnérabilité	réalisé par le service informatique			non
		Appliquer les 40 recommandations simples pour sécuriser le SI avezc le guide d'hygiène informatique édité par l'ANSSI	Réalisé.			non
		Sensibiliser le service informatique au problème de sûreté : établir les procédures de suivi d'utilisation, **cartographie des SI, séparation des flux d'administration et d'utilisateurs, gestion des sauvegardes**	Réalisé (gestion des accès).			non
		Mettre en place des systèmes de protection physique des installations (locaux spécifiques pour les centres de commande, locaux techniques SI et gestion des accès en fonction d'une évaluation des zones à protéger)	Non réalisé.		oui	
		Mettre en place un système contre l'intrusion et la prise de contrôle des systèmes directement par des opérateurs extérieurs (ex: télémaintenance) ou matériels connectés à internet. Voir les recommandations de l'ANSSI sur la cybersécurité des systèmes industriels.	Non réalisé.		oui	
		Se rapprocher des autorités pour toute intrusion suspecte.	Prévu.			non

ANNEXE A2

EXEMPLE DE PROCÉDURE DE SÉCURISATION D'UN SITE

La procédure de sécurisation du site couvre les domaines d'activité suivants :

- La surveillance générale du site ;
- La gestion des accès physiques au site ;
- La gestion des accès physiques aux bâtiments sur le site ;
- La gestion de la circulation des véhicules et des emplacements de parkings sur le site ;
- La gestion des responsabilités concernant l'ouverture / fermeture du site.

Les informations relatives à la procédure de sécurisation du site sont communiquées :

- Au personnel par le biais de la procédure « sécurisation du site » ;
- Aux prestataires de service, transporteurs (y compris les intérimaires et les étudiants) par le biais du contrat de prestations ;
- Aux visiteurs par le biais du registre d'accueil.

1. La surveillance générale du site

La surveillance générale du site est assurée par l'utilisation d'un système de vidéosurveillance en conformité avec la réglementation en vigueur.

Les personnes ayant accès au site Internet d'enregistrement de cette surveillance sont à ce jour :

- M. XXX – Fonction : xxxxxx
- M. YYY – Fonction : xxxxxx

Une procédure en cas de déclenchement d'alarme est disponible sur site, dans laquelle on retrouve les personnes concernées et leurs coordonnées ainsi que les consignes données au télésurveilleur.

2. La gestion des accès physiques au site et dans les bâtiments

2.1 ZONES SUR LE SITE

Le site est divisé zones. Une première constituée de l'espace interne aux clôtures et portails et une seconde constituée de l'espace intérieur aux bâtiments.

Certains bâtiments peuvent renfermer des locaux sensibles spécialement protégés. Des zones définies comme critiques sont également identifiées à l'intérieur des bâtiments, mais également aux abords de l'usine (se référer au plan de votre usine).

De manière générale, seules les personnes dûment autorisées peuvent avoir accès au site ou aux différentes zones dans les bâtiments.

2.2 AUTORISATION D'ACCÈS

Pour toute personne ne faisant pas parti du personnel de l'entreprise, un enregistrement de leur passage doit être fait au niveau de l'accueil (enregistrement sur un registre d'entrée des visiteurs et prestataires de service).

Dans le cadre des sociétés extérieures, l'attribution des accès au site se fait en accord avec les responsables de SOCIÉTÉ XXX. Cette information doit se retrouver sur le plan de prévention du prestataire, annexé à la procédure.

2.3 ACCÈS AU SITE

L'accès au site peut se faire à plusieurs endroits d'accès situés en périphérie du site.

Le personnel SOCIÉTÉ XXX peut accéder au site du lundi au vendredi et 24h / 24h.

Les personnes ne faisant pas parti de la SOCIÉTÉ XXX peuvent accéder au site selon un calendrier et un horaire fixe.

Les possibilités sont les suivantes :

- Du lundi au vendredi les jours ouvrables
- Horaires :
  > De 8h30 à 12h00
  > De 13h30 à 17h00

Toute personne extérieure doit se présenter à l'accueil de l'entreprise afin de s'identifier auprès de la personne en charge de la réception et doit y attendre son interlocuteur privilégié.

Accès piétons

Les accès piétons sont autorisés depuis le parking du personnel, ainsi que depuis le parking des visiteurs.

Accès véhicule

Les accès en véhicule se font par plusieurs endroits d'accès situés en périphérie du site.

2.4 ACCÈS AUX BÂTIMENTS

L'accès aux bâtiments peut se faire :

- Par l'accueil pour accéder aux bureaux ;
- Par les vestiaires pour accéder à la zone de production. L'accès aux zones de production n'est autorisé qu'au personnel ou aux prestataires de service et aux visiteurs s'ils sont accompagnés d'un interlocuteur de la SOCIÉTÉ XXX.

3. Sécurisation des locaux et des biens

Afin de limiter les possibilités d'intrusion dans les bâtiments et les locaux, une attention particulière doit être apportée :

- À la fermeture des portes d'accès aux bâtiments ;
- À la fermeture des portes et fenêtres en quittant un local.

Une instruction concernant la fermeture/ouverture du site est disponible sur site. Il reprend l'ensemble des portes et portails à fermer, ainsi que les responsabilités et suppléance en cas d'absence.

Par ailleurs, les équipements et outils pouvant faciliter une effraction sont à ranger dans des locaux fermant à clef. Il en est spécialement ainsi pour les échelles.

L'utilisation des sorties de secours est strictement interdite en dehors des situations d'urgence qui nécessitent leur utilisation.

Cependant, seront fermés à clef en dehors des heures de présence du personnel y travaillant, les locaux refermant des valeurs scientifiques ou financières, sensibles ou importantes, du matériel et équipements de valeur facilement transportables qui ne peuvent être rangés dans des armoires fermant à clef.

Pour des raisons de sécurité et pour permettre des interventions urgentes en dehors des heures de présence normales dans le local, le service technique des bâtiments doit être en possession d'un système d'accès à tous ces locaux.

Chaque membre du personnel doit veiller également à prendre un certain nombre de mesures préventives :

- Ne pas laisser dans les vestiaires et/ou en évidence des objets de valeur (téléphone portable, argent, lecteurs audio, montres, etc.) ;
- Fermer les tiroirs et armoires à clef, même en cas de courte absence (pause, réunion…) ;
- Sécuriser systématiquement son PC dès que l'on quitte son poste (mise en veille forcée avec reprise par mot de passe).

Tout préjudice (vol, vandalisme, intrusion, effraction…) doit être immédiatement signalé :

- À un membre de l'équipe de Direction ;
- À un membre de l'équipe « Food Defense ».

4. Confidentialité

Il est interdit de photographier ou faire des vidéos sur le site, tant à l'extérieur qu'à l'intérieur des bâtiments, sauf autorisation donnée explicitement par la Direction du site.

Les données, sur quelques supports que ce soit, constituent un élément primordial du patrimoine de la SOCIÉTÉ XXX. Leur confidentialité doit donc être respectée.

Chaque membre du personnel doit veiller en permanence à ne pas permettre à des personnes non autorisées de pouvoir accéder à des données propres à l'entreprise, qu'il s'agisse de données sous format papier et/ou numérique.

Quelques lignes de conduite à respecter :

- Sécuriser son ordinateur en permanence : mot de passe pour reprise de veille forcée, veille automatique après 20 minutes de non utilisation ;
- Appliquer une politique « sûrete des données » : rangement de son environnement de travail, y compris la sécurisation des supports de données (CD, disques durs externes, papier…) ;
- Effacer les informations reprises sur les tableaux blancs dans les salles de réunion ;
- Utiliser des destructeurs de documents pour la destruction des données confidentielles.

5. Procédures relatives à la procédure de sécurisation du site

La rédaction et la modification des procédures en matière de sécurisation du site sont du ressort de la Direction.

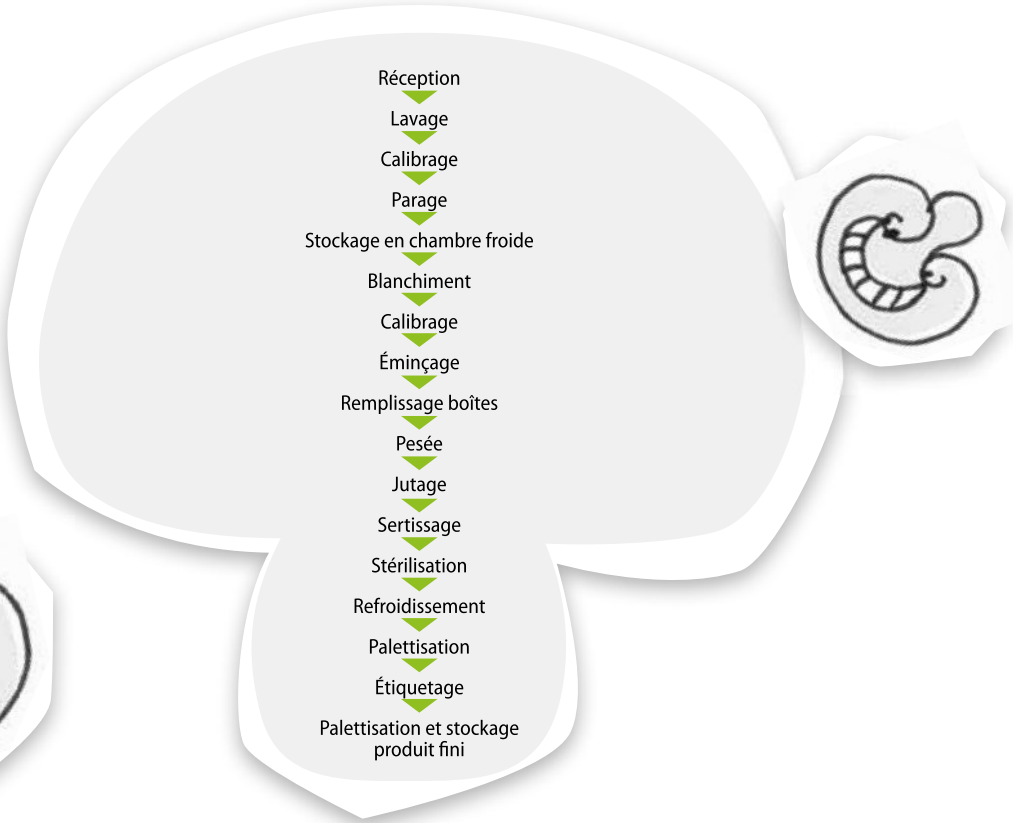
En cas de nécessité, la Direction du site se réserve le droit de prendre toute mesure permettant d'assurer la sécurisation du site.

Liste des documents associés à la procédure :

Documents consultés	Référence	
Analyse Food Defense	Étude Food Defense	XX1
	Démarche Food Defense	XX2
Documents de référence	Plan de sécurité et sûreté	XX3
	Engagement de la direction	XX4
	Fiche de définition d'emploi Responsable Food Defense (Directeur Usine) + Suppléance (RQ)	XX5
	Clause de confidentialité Equipe Food Defense	XX6
	Procédure de sécurité et de sûreté (Food Defense)	XX7
	Check-list de fermeture du site	XX8
	Formulaire d'introduction d'objets non autorisés	XX9
	Procédure de gestion de crise (crise retrait / rappel dont acte de malveillance)	XX10
	Charte sûreté	XX11
	Check-list gardiennage	XX12
	Processus d'accueil et de formation des nouveaux arrivants	XX13
	Affichage des règles d'hygiène, sécurité, santé et sûreté	XX14
	Liste N° de téléphone à faire pour un visiteur à l'accueil : à mettre à jour	XX15
	Livret d'accueil intérimaire	XX16
	Livret d'accueil titulaire	XX17
	Procédure de gestion des outils informatiques	XX18
	Support de formation SURETE	XX19
	Questionnaire d'évaluation SURETE à chaud	XX20
	Questionnaire d'évaluation SURETE à froid	XX21
	Règlement intérieur	XX22
	Registre des clés et des badges	XX23
	Processus recrutement	XX24
	Formulaire recrutement (avec contrôle auprès des anciens employeurs)	XX25
	Formulaire de suivi arrivée / départ d'un nouveau salarié	XX26
	Registre visiteurs	XX27
	Plan de prévention prestataire de services	XX28
	Protocole de sécurité transporteurs simplifié (affichage chauffeurs multilingue)	XX29
	Protocole de sécurité transporteurs	XX30

ANNEXE A3

EXEMPLE SIMPLIFIÉ D'UN DIAGRAMME DE FABRICATION DE CHAMPIGNONS DE PARIS APPERTISÉS



ANNEXE B

EXEMPLE DE GRILLE D'ÉVALUATION DE LA VULNÉRABILITÉ

IMPACT PRODUIT : (on estime la quantité de produit impacté) : lien avec la quantité de produit, taille du lot… La quantité concernée a une conséquence sur le nombre de personnes touchées..

- **1 = impact très faible** = touche quelques unités de vente consommateur.
- **2 = impact faible** = touche 1 journée de production ou 1 lot de production.
- **3 = impact fort** = touche plus d'1 journée de production ou plusieurs lots ou plusieurs jours de production.
- **4 = impact très fort** = touche toutes les productions en cours.

GRAVITÉ : (on estime la gravité des effets sur la santé).

- **1 =** Lésions ou atteintes réversibles sans acte médical – **Malaises, gênes.**
- **3 =** Lésions ou atteintes réversibles avec un traitement médical – **Handicap temporaire.**
- **6 =** Lésions ou atteintes irréversibles – **Handicap permanent.**
- **9 =** Lésions ou atteintes mortellement graves – **Décès.**

ACCESSIBILITÉ : (on estime la facilité d'accès "géographique" et physique à la cible et la facilité à la quitter après une attaque). La cible, c'est ce qui va être attaqué (produit, machine, camion, zone de stockage…).

- **1 = zone et / ou produit très difficile d'accès** = zone dont l'accès est limité aux personnes habilitées (par ex un local technique) et / ou produit en conditionnement fermé garanti (citerne scellée, sachets cousus, etc.).
- **2 = zone et ou produit difficile d'accès** = zone dont l'accès est limité au personnel de production (par ex accessible au personnel de maintenance, personnel de la qualité…) et / ou produit en conditonnement fermé sans dispositif de garantie.
- **3 = zone et ou produit facile d'accès** = zone accessible aux internes (personnel permanent, saisonnier et temporaire) et non accessible aux externes (transporteur…) et / ou produit facilement accessible.
- **4 = zone très facile d'accès** = zone ouverte, accessible à tout le monde (internes et externes) et / ou produit nu.

FACILITÉ : (on estime la facilité à réaliser l'attaque) : il faut avoir les moyens, les compétences, les méthodes : « MCM » et le motif).

- **1 = l'attaque est très difficile** (on n'a pas les moyens, il faut de grandes compétences, les méthodes sont complexes pour réaliser l'attaque).
- **2 = l'attaque est relativement difficile mais pas impossible** (il manque plusieurs éléments clés pour réaliser l'attaque).
- **3 = l'attaque est relativement facile** (il manque un élément clé pour réaliser l'attaque), motif sérieux.
- **4 = l'attaque est très facile** (les 4 éléments clés sont présents : ex : eau de javel sur place, produit ouvert sur la ligne, pas besoin de connaissance particulière, motif sérieux).

RÈGLES D'ÉVALUATION BRUTE DE LA VULNÉRABILITÉ

Si impact produit x gravité x accessibilité x facilité est **supérieur ou égal à 54**
ou
si 3 facteurs sur 4 sont en rouge (voir ci-dessus)

→ **des mesures préventives complémentaires doivent être prises et une nouvelle évaluation réalisée**

ANNEXE C

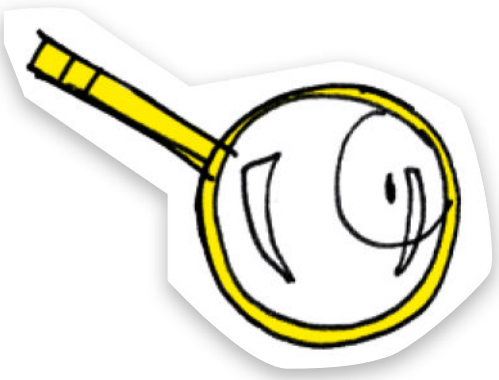
EXEMPLE DE TABLEAU D'ANALYSE DE RISQUES

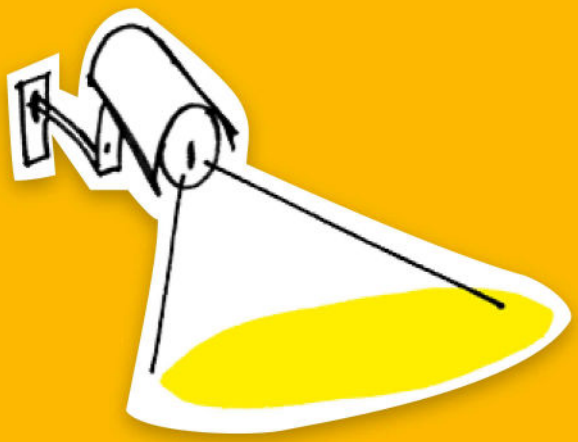
	Étapes du process	Réception	Réception	Réception	Réception	Réception	Réception	Réception	Réception	Réception
	Cible	Champignon frais	Champignon frais	Champignon frais	Ingrédients	Ingrédients	Ingrédients	Emballages primaires	Emballages primaires	Emballages primaires
	Agresseur	Salarié, Chauffeur, Producteur	Salarié, Chauffeur, Producteur	Salarié, Chauffeur, Producteur	Salarié, Chauffeur,	Salarié, Chauffeur,	Salarié, Chauffeur,	Salarié, Chauffeur,	Salarié, Chauffeur,	Salarié, Chauffeur,
	Objectif : Préciser la nature de la menace: chimique, physique, biologique, CE, autre	contaminer le champignon : **physique**	contaminer le champignon : **micro-biologique**	contaminer le champignon : **allergène**	contaminer les ingrédients : **chimique**	contaminer les ingrédients : physique	contaminer les ingrédients **micro-biologiques**	contaminer le contenant : **physique**	contaminer le contenant : **chimique**	contaminer le contenant: **micro-biologique**
	Moyens et méthodes d'action	Introduction sur le produit	Introduction sur le produit	Introduction sur le produit	Introduction sur le produit	Introduction sur le produit	Introduction sur le produit	Introduction dans / sur le contenant:	Introduction dans / sur le contenan	
	Mesures de surêté existantes et spécifiques à la zone étudiée (hors MPP)	Les étapes ultérieures du process permettent de réduire la gravité	Les étapes ultérieures du process permettent de réduire la gravité et l'impact produit	/	/	Filtre juteuse permet d'éliminer les corps étrangers	Les étapes ultérieures du process permettent de réduire la gravité et l'impact produit	Chantourneur, soufflage ou lavage avant utilisation des emballages	Chantourneur, soufflage ou lavage avant utilisation des emballages	
Evaluation brute de la vulnérabilité	Impact produit	1	1	2	3	1	2	1	1	
	Gravité	3	9	3	9	3	9	3	9	
	Accessibilité	2	2	2	1	1	1	2	2	
	Facilité (M C M)	1	1	3	2	2	1	2	2	
	IxGxAxF	18	18	36	54	6	18	12	36	
Mesures de sûretés supplémentaires Evaluation résiduelle de la vulnérabilité	Descriptions				Refus systématique de tout emballage non intègre					
	Responsables									
	Délais									
Evaluation résiduelle de la vulnérabilité	Impact produit									
	Gravité									
	Accessibilité									
	Facilité									
	I x G x A X F									

ANNEXE D

EXEMPLE DE SOMMAIRE DE PLAN FOOD DEFENSE

1. Page de garde / sommaire
2. Objectifs du plan
3. Les principes clés
4. Rôles et composition de l'équipe Food Defense
5. Politique Food Defense
6. Mesures de prévention Food Defense
   - a. Accès
   - b. Flux
   - c. Stocks
   - d. Personnel
   - e. Process
   - f. Spécifiques
7. Évaluation de la vulnérabilité / niveau de vigilance
8. Mesures spécifiques de prévention
9. Préparation et gestion d'un acte malveillant (gestion de crise)
   - a. **Rôles et composition de la cellule de crise**
     - I Président de la cellule de crise
     - II Coordinateur de la cellule de crise (site, filiale)
     - III Chargé de communication / porte-parole
     - IV Assistant de la cellule de crise
   - b. **Aides mémoire**
     - I Fiche d'aide à l'évaluation d'une crise
     - II Premières actions : coordinateur crise
     - III Aide-mémoire : assistante de la cellule de crise
     - IV Aide-mémoire : animation de la cellule de crise
     - V Ordre du jour de la cellule de crise
   - c. **Fiches outils prêtes à l'emploi**
     - I Livre de bord, CR de réunion de la cellule, fiche de recueil d'appels,
   - d. **Communication : aides mémoire**
     - I Préparation de la communication,
     - II Le communiqué de presse,
     - III Les questions – réponses,
     - IV Brief pour le filtrage des appels,
   - e. **Communication : Fiches outils prêtes à l'emploi**
     - I Fiche de recueil d'appel de journalistes
     - II Modèle de communiqué de presse d'attente
   - f. **Annexes**
     - I Liste des membres de la cellule de crise
     - II Liste des contacts crise
     - III Liste des experts externes
     - IV Liste des organismes officiels
     - V fiche de REX d'une crise
10. Suivi, mise à jour et amélioration du plan Food Defense





Contact :
www.afnor.org

Communication Groupe AFNOR – S1502120 – 04/2015 – Conception graphique et illustrations : GAYA

afnor GROUPE

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis cedex - France
Tél. : +33 (0)1 41 62 80 00 - Fax. : +33 (0)1 49 17 90 00