*(Modèle - sera adapté à chaque application concrète)*

*Certains points sont à développer, à ajouter, à enlever, à préciser (en rouge)*

Manuel sécurité de l’information

1. Introduction

1.1 Présentation de notre organisation

1.2 Objet du manuel

2. Normes et définitions

3. Approche processus

3.1 Les processus dans l’organisation

3.2 Cartographie des processus

4. Contexte de l’organisation

4.1 Enjeux

4.2 Parties intéressées

4.3 Domaine d’application

4.4 Description du SMSI

5. Leadership

5.1 Engagement de la direction

5.2 Politique de sécurité de l’information

5.3 Rôles

6. Planification

6.1 Actions face aux risques et opportunités

6.2 Objectifs sécurité de l’information

7. Support

7.1 Ressources

7.2 Compétences

7.3 Sensibilisation

7.4 Communication

7.5 Informations documentées

8. Réalisation

8.1 Maîtrise opérationnelle

8.2 Appréciation des risques

8.3 Traitement des risques

9. Performances

9.1 Inspection, analyse et évaluation

9.2 Audit interne

9.3 Revue de direction

10. Amélioration

Historique des révisions du Manuel Sécurité de l’information

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Page | Modification | Révision | Auteur | Fonction | Approuvé | Fonction | Date |
| toutes | Création | 001 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Cette copie papier est un document contrôlé un jour après son impression.

**1. Introduction**

**1.1 Présentation de notre organisation**

**Informations générales**

|  |  |
| --- | --- |
| Nom | ….. |
| Forme juridique | ….. |
| Capital social | ….. |
| Siège social | ….. |
| Siret | ….. |
| Numéro TVA | ….. |
| NAF | ….. |
| Téléphone | ….. |
| Fax | ….. |
| Courriel | ….. |
| Site Internet | ….. |
| Directeur | ….. |
| Domaine d’activité | ….. |

**Organisation**

Notre organisation inclut les sites suivants : ……

Notre organisation inclut les départements (services) suivants : …..

**Mission (finalité)**

Garantir la confidentialité, l’intégrité, la disponibilité et la traçabilité de l’information

Réduire les risques liés à la sécurité de l’information

…

**Valeur**

La démarche préventive est la règle, l’action corrective étant l’exception

…

**Produits et prestations :**

Nos produits sont : …

Nos services sont : …

**Historique :**

L’historique de l’organisation est la suivante :…..

A présent l’organisation …..

**1.2 Objet du manuel**

Le présent manuel a pour objet de décrire les dispositions de notre système de management de la sécurité de l’information (SMSI) pour maintenir et améliorer :

* notre capacité à fournir des produits et prestations de service conformes
* les ressources nécessaires
* le respect des exigences légales et réglementaires applicables
* la satisfaction des clients et autres parties intéressées
* nos processus

Le manuel concerne l’ensemble des activités de notre organisation y compris le développement, la production, le marketing et les services d’assistance.

Le manuel est disponible en interne et en externe (sur demande, le responsable sécurité de l’information gère l’historique des distributions).

**2. Normes et définitions**

Notre système de management de la sécurité de l’information respecte les exigences des normes :

* **ISO 9001 (2015) : Systèmes de management de la qualité – Exigences**
* **ISO 27001 (2022) : Sécurité de l’information, cybersécurité et protection de la vie privée – Systèmes de management de la sécurité de l’information – Exigences**
* **ISO 31000 (2018) : Management du risque – Lignes directrices**

Pour les audits internes notre référence est la norme **ISO 19011 (2018) : Lignes directrices pour l'audit des systèmes de management**.

Nous utilisons autant que faire se peut les définitions des normes suivantes :

* **ISO 9000 (2015) : Systèmes de management de la qualité — Principes essentiels et vocabulaire**
* **ISO 27000 (2018) : Technologies de l’information – Techniques de sécurité – Systèmes de management de la sécurité de l’information – Vue d’ensemble et vocabulaire**

Certains termes que nous utilisons :

**Actif**: *tout élément ayant de la valeur pour l’organisation*

**Action corrective** : *action pour éliminer les causes d’une non-conformité ou tout autre événement indésirable et empêcher leur réapparition*

**Appréciation du risque**: *processus d’analyse et d’évaluation du risque*

**Client** : *celui qui reçoit un produit*

**Compétence** : *aptitudes, connaissances et expériences personnelles*

**Confidentialité**: *propriété d’une information d’être accessible à seulement une entité*

**Conformité** : *satisfaction d’une exigence spécifiée*

**Déclaration d’applicabilité (DdA)**: *document décrivant les objectifs et les mesures de sécurité*

**Direction** : *groupe ou personnes chargées de la gestion au plus haut niveau de l’organisation*

**Disponibilité**: *propriété d’une information d’être utilisable par une entité*

**Efficacité** : *capacité de réalisation des activités planifiées avec le minimum d’efforts*

**Efficience** : *rapport financier entre le résultat obtenu et les ressources utilisées*

**Exigence** : *besoin ou attente implicite ou explicite*

**Indicateur** : *valeur d’un paramètre, associé à un objectif, permettant de façon objective d’en mesurer l’efficacité*

**Information documentée** : *tout support permettant le traitement d’une information*

**Intégrité**: *propriété d’une information d’être non altérée*

**Non-conformité** : *non-satisfaction d’une exigence spécifiée*

**Objectif** : *but mesurable à atteindre*

**Organisation (entreprise)** : *structure qui satisfait un besoin*

**Partie intéressée** : *personne, groupe ou organisation pouvant affecter ou être affecté par une organisation*

**Prestataire externe (fournisseur)** : *celui qui procure un produit*

**Processus** : *activités qui transforment des éléments d’entrée en éléments de sortie*

**Produit** **(ou service)** : *tout résultat d’un processus ou d’une activité*

**Qualité** : *aptitude à satisfaire aux exigences*

**Risque résiduel**: *risque accepté*

**Risque** : *vraisemblance d’apparition d’une menace ou d’une opportunité*

**Sauvegarde**: *copie de données afin d’archiver et de protéger*

**Sécurité de l’information**: *mesures permettant de protéger la confidentialité, l’intégrité et la disponibilité de l’information*

**SMSI**: *système de management de la sécurité de l’information*

**Système de management** : *ensemble de processus permettant d’atteindre les objectifs*

**Traitement du risque**: *activités de modification du risque*

**Vulnérabilité**: *faiblesse d’un actif pouvant conduire à un accès non autorisé*

**3. Approche processus**

**3.1 Les processus dans notre organisation**

La direction fournit, maintient et améliore les ressources et le personnel nécessaires. Plus de détails dans le processus « Gérer la documentation » et dans le document « Processus ». Les processus sont classés en 3 types (management, réalisation et support).

Les processus de management dans notre organisation sont les suivants :

* élaborer la stratégie
* piloter les processus
* développer la politique
* planifier le SMSI
* déployer les objectifs
* communiquer
* réaliser la revue de direction
* auditer
* améliorer
* apprécier les risques
* traiter les risques

Les processus de réalisation sont :

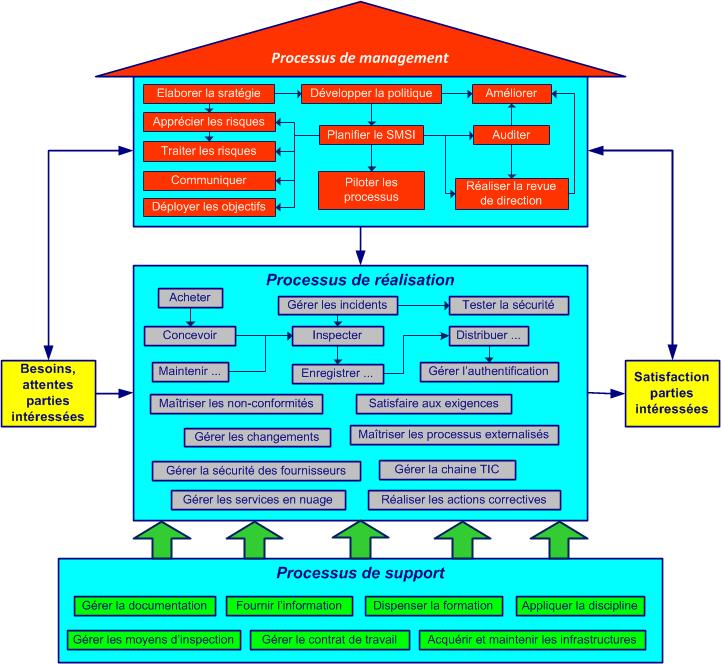
* gérer les actifs
* gérer les identités
* gérer l’authentification
* distribuer les accès
* maîtriser les processus externalisés
* gérer la sécurité des fournisseurs
* satisfaire aux exigences de sécurité
* gérer la chaîne TIC
* gérer les services en nuage
* gérer les incidents
* gérer les vulnérabilités
* gérer les configurations
* supprimer l’information
* utiliser la cryptographie
* coder
* tester la sécurité
* gérer la continuité d’activité
* passer en revue la sécurité
* gérer les changements
* inspecter
* enregistrer et désinscrire
* développer et soutenir la sécurité
* appliquer la sécurité
* concevoir et développer
* acheter
* maintenir les équipements
* administrer les réseaux
* maîtriser les non-conformités
* réaliser les actions correctives

Les processus de support sont :

* gérer le contrat de travail
* appliquer la discipline
* tenir à jour la veille réglementaire
* acquérir et maintenir les infrastructures
* gérer les moyens d'inspection
* dispenser la formation
* fournir l'information
* gérer la documentation

**3.2 Cartographie des processus**

La cartographie des processus est représentée ci-dessous :



Une revue de processus (pour les processus clés) est conduite périodiquement par le pilote du processus. Plus de détails dans le processus « Piloter les processus ».

**4. Contexte de l’organisation**

**4.1 Enjeux**

Notre direction a réalisé un état des lieux du contexte dans lequel notre organisation se trouve et prend en compte les enjeux externes et internes pertinents par rapport à notre orientation stratégique et notre capacité à atteindre les objectifs du SMSI (cf. les documents Domaine d’application du SMSI et Veille réglementaire.

Nous surveillons et passons en revue régulièrement toute information en lien avec les enjeux et les facteurs pouvant influencer sur l’atteinte de nos objectifs.

**4.2 Parties intéressées**

Notre direction a déterminé les parties intéressées pertinentes pour notre organisation et notre SMSI (cf. le document « Liste des parties intéressées ») et leurs exigences qui concernent notre organisation. Ces exigences sont par rapport à la sécurité de l’information et aux lois et règlements applicables.

**4.3 Domaine d’application**

Ce manuel du système de management de la sécurité de l’information s'applique à tous les :

* secteurs d'activités de notre organisation y compris les relations avec les fournisseurs et sous-traitants
* actifs (information, équipements, personnel)

Plus de détails dans le document « Domaine d’application du SMSI ».

Le domaine d’application de l’organisation est : …..

Les sites concernés sont : …..

Les exigences de la norme ISO 27001 suivantes ….. ne sont pas applicables (§ xx). Ces exigences n’ont aucune incidence sur notre aptitude ou responsabilité à assurer la sécurité de l’information et améliorer la satisfaction de nos clients.

La justification est : …..

**4.4 Description du SMSI**

Le présent manuel sécurité de l’information décrit les processus, politiques et les informations documentée à tenir à jour (procédures) et à conserver (enregistrements) nécessaires pour établir, mettre en place, maintenir et améliorer en continu notre SMSI conformément à l’ISO 27001. L’objet du manuel est décrit dans le § 1.2.

**5. Leadership**

**5.1 Engagement de la direction**

La direction définit la politique de sécurité de l’information par une déclaration écrite. Cette déclaration est affichée à quelques endroits clés, visibles par le personnel et les clients. La politique de sécurité de l’information soutient notre orientation stratégique et est définie par un engagement de la direction.

Déclaration de la direction

L’engagement personnel du directeur pour améliorer l’efficacité du SMSI s’exprime par :

* notre réussite passe impérativement par la satisfaction des exigences de toutes les parties intéressées qui attendent de nous une performance sans faille de :
  + notre sécurité de l’information
  + nos délais et
  + nos coûts
* nos efforts pour faire preuve de justesse et de compétence dans l'écoute, la compréhension, l'anticipation et la réalisation de souhaits des clients
* l’amélioration continue de nos performances
* l'application correcte, la maintenance et l'amélioration continue de notre système de management de la sécurité de l’information (SMSI)
* la poursuite de la conquête du marché
* le respect de l’esprit et les dispositions des :
  + lois et règlements applicables
  + codes de bonnes pratiques
* l’identification, l’évaluation et la réduction des risques liés à nos activités
* la fourniture des ressources nécessaires qui nous aideront à maintenir et à élargir notre position concurrentielle sur le marché
* la sensibilisation du personnel à notre politique de sécurité de l’information
* l’intégration des exigences du SMSI dans les processus métier
* la définition et l’atteinte des objectifs fixés
* la communication de nos résultats en matière de sécurité de l'information en interne et en externe

Je confie à Martin, notre responsable sécurité de l’information, toute autorité pour mettre en œuvre notre politique et mener les actions nécessaires appropriées. Cette politique s'appuie sur une amélioration permanente de notre organisation, de nos équipements, de nos connaissances grâce à la participation et la sensibilisation de l'ensemble du personnel. Notre manuel sécurité de l’information est le moteur de ce progrès permanent et le reflet du management au quotidien de l'organisation.

Le directeur Dupond, date

**5.2 Politique de sécurité de l’information**

Les exigences de nos clients et parties intéressées sont déterminées et respectées par :

* la mise en place de moyens d’écoute dynamiques
* leur transformation en exigences internes
* la mesure de la satisfaction des parties intéressées

Les outils utilisés sont :

* revues des exigences
* sondages
* enquêtes ponctuelles
* visites fréquentes

La politique de sécurité de l’information est définie par la déclaration de la direction. La politique concerne :

* les informations de l’organisation :
  + des ordinateurs
  + des réseaux
  + des logiciels
* les informations des clients
* le personnel, les fournisseurs et les sous-traitants

La politique est disponible, sur simple demande, à toute partie intéressée. Plus de détails dans la politique « Sécurité de l’information ».

Le plan stratégique à court terme et à moyen terme est défini et mis à jour annuellement par la direction.

Le système de management de la sécurité de l’information est l’outil de notre politique de sécurité de l’information.

La direction s'assure régulièrement que cette politique est bien comprise, mise en œuvre et tenue à jour pour atteindre les objectifs visés par :

* des réunions mensuelles de la direction avec les responsables de tous les départements
* des réunions hebdomadaires des pilotes de processus
* le suivi d'indicateurs de défauts, d'efficience, de coûts d'obtention de la qualité
* des audits internes
* l'affichage
* l'intranet

Les politiques détaillées sur des aspects spécifiques de la sécurité de l'information concernent surtout les activités suivantes :

* la sécurité de l'information
* l’utilisation correcte de l’information
* la classification de l’information
* le transfert de l’information
* le contrôle d’accès
* les droits d’accès
* les relations avec les fournisseurs
* l’utilisation des services en nuage
* les droits de propriété intellectuelle
* la protection des enregistrements
* la protection de la vie privée
* la conformité aux règles et normes
* le contrat de travail
* la sensibilisation et la formation
* le travail à distance
* le bureau propre et l’écran vide
* les supports de stockage
* les terminaux utilisateurs
* l’authentification sécurisée
* les vulnérabilités techniques
* la sauvegarde de l’information
* la journalisation
* l’utilisation de la cryptographie

**5.3 Rôles**

Le représentant de la direction M. Martin, responsable sécurité de l’information, a l’autorité pour s’assurer que le système de management de la sécurité de l’information est défini, mis en œuvre et entretenu conformément aux exigences de la norme ISO 27001.

Les descriptions de fonction de tous les postes de l’ensemble du personnel se trouvent dans les fiches attachées à la procédure « Formation et sensibilisation ».

Le personnel est tenu de respecter les politiques en vigueur, y compris l’usage raisonnable des moyens informatiques.

Tout manquement peut être sanctionné selon le processus « Appliquer la discipline ».

**6. Planification**

**6.1 Actions face aux risques et opportunités**

Pour faire face aux risques et saisir les opportunités d’améliorations nous prenons en compte l’orientation stratégique et les enjeux identifiés. Les enjeux les plus importants concernent les exigences légales applicables et l’environnement de travail. Cela nous permet d’atteindre les résultats escomptés du SMSI, d’éliminer ou de réduire les effets indésirables et d’accroître les effets souhaitables.

La planification des actions à mener pour faire face aux risques et opportunités nous permet d’intégrer ces actions dans le SMSI et d’évaluer leur efficacité. Plus de détails dans les processus « Apprécier les risques » et « Traiter les risques ».

La « Déclaration d'applicabilité » de l’annexe A de l’ISO 27001 inclut le statut des toutes les mesures que nous utilisons pour diminuer les risques de sécurité de l’information.

**6.2 Objectifs sécurité de l’information**

La politique de sécurité de l’information fournit le cadre pour définir les objectifs sécurité de l’information.

Quelques objectifs utilisés :

* améliorer la sécurité du périmètre physique de l’organisation
* développer la créativité et la prise d’initiative
* intégrer la sécurité de l’information dans les processus métier
* mieux prendre en compte la confidentialité dans les processus opérationnels
* poursuivre la sensibilisation du personnel
* tirer les leçons des :
  + retours d’information
  + incidents de sécurité
  + vulnérabilités identifiées
* communiquer en continu sur le niveau des indicateurs

Les objectifs sont déployés dans chaque département (et processus concerné) et suivis quotidiennement au moyen d’indicateurs. Plus de détails dans le document « Plan d’atteinte des objectifs ».

Les objectifs prennent en compte :

* les retours d’information des clients
* les incidents de sécurité
* les vulnérabilités techniques

**7. Support**

**7.1 Ressources**

Les ressources nécessaires sont planifiées et assurées par la direction pour :

* mettre en œuvre le système de management de la sécurité de l’information
* améliorer l’efficacité du système de management de la sécurité de l’information
* accroître la protection des informations opérationnelles

Les ressources sont :

* le personnel qui :
  + a des compétences spécifiques
  + est formé selon les besoins identifiés (programme de formation)
* les infrastructures appropriées :
  + bâtiments
  + équipements
  + services de support (système informatique, logistique, métrologie, transport)
* les ressources technologiques
* les ressources financières
* l'environnement du travail :
  + facteurs humains :
    - éthique
    - morale
    - prévention des risques
  + physiques :
    - air
    - propreté
    - lumière
    - température
    - humidité
    - ESD (décharges électrostatiques)

L’accès aux zones sécurisées est protégé par un lecteur de badge pour les personnes habilitées.

Les équipements informatiques sont installés conformément aux règles de l’art (alimentation électrique, climatisation, câblage, détection d’incendie, etc.).

**7.2 Compétences**

Pour chaque poste ayant une incidence sur la sécurité de l’information les compétences nécessaires sont définies et les besoins en formation identifiés et établis. L’ensemble des opérateurs est suivi par une matrice de compétence, mise à jour au moins une fois par mois.

La procédure « Formation et sensibilisation » montre comment :

* identifier les besoins en formation
* atteindre les compétences requises
* appliquer une motivation pour :
  + atteindre les objectifs sécurité de l’information
  + réaliser une amélioration continue
  + créer un environnement propice à l'innovation

Une formation est faite sur le poste de travail à chaque nouveauté ou modification y compris pour le personnel temporaire ou intérimaire.

**7.3 Sensibilisation**

Le personnel a conscience :

* de sa contribution à l'atteinte des objectifs
* de l'importance du respect de la politique de sécurité de l’information
* de la responsabilité de tous pour la prévention et l’amélioration continue
* des conséquences des dysfonctionnements potentiels

**7.4 Communication**

Les activités de communication en interne et en externe sont planifiées et documentées (cf. processus « Communiquer »). La direction met en œuvre des dispositions de communication transparente avec les clients, le personnel et les autres parties intéressées à propos :

* des informations sur le produit (spécifications techniques, conditions d'utilisation et autres)
* des consultations, des cotations, des contrats et des commandes
* d'informations des clients, surtout des réclamations et actions mises en place
* de l'importance pour tous de respecter les exigences des clients, légales et réglementaires
* de la prévention et du traitement des risques

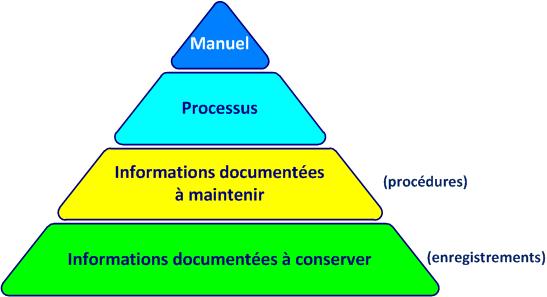
Nous classons les informations de nos actifs en quatre niveaux :

* secrètes
* confidentielles
* internes
* publiques

**7.5 Informations documentées**

Nous utilisons le terme procédure qui correspond à information documentée à tenir à jour. La même chose pour le terme enregistrement qui correspond à information documentée à conserver.

Notre organisation a basé son système de management de la sécurité de l’information sur une documentation à 4 niveaux, symbolisée par la pyramide de documentation :



Le présent manuel sécurité de l’information décrit les dispositions générales liées aux exigences du système de management de la sécurité de l’information :

* il fait référence et s'appuie sur les processus, procédures et enregistrements
* les procédures font elles-mêmes référence et s'appuient sur des instructions et enregistrements

Le présent manuel est rédigé par le responsable sécurité de l’information (RSI) et a été approuvé par la direction.

Tout client ou prestataire externe peut obtenir après accord de la direction ou du RSI un exemplaire du manuel sécurité de l’information. Les exemplaires papiers distribués sont en diffusion contrôlée pendant un jour après leur impression. Le responsable sécurité de l’information tient à jour une liste des exemplaires distribués, les destinataires, la version et la date.

Le responsable sécurité de l’information met à jour le manuel après chaque modification du système de management de la sécurité de l’information (SMSI).

Les réponses point par point à toutes les exigences des articles 4 à 10 de la norme ISO 27001 y compris l’annexe A sont présentes dans notre système documentaire.

Le processus « Gérer la documentation » définit comment identifier, mettre en place et tenir à jour la maîtrise des documents et enregistrements. Sont inclus les documents d’origine externe (des fournisseurs, des clients, des normes, des parties intéressées). Pour tout document et enregistrement du SMSI la procédure permet de gérer :

* la localisation
* la vérification
* l’approbation
* la mise à jour
* l’accès
* l’utilisation
* la version pertinente en vigueur
* la disponibilité
* la maîtrise des documents d’origine externe
* l'empêchement d’utilisation de documents périmés (obsolètes)
* la conservation
* la protection
* l’élimination
* l'archivage

Dans la « Liste d’informations documentées » est montrée la correspondance des procédures et enregistrements de notre SMSI avec les paragraphes de la norme ISO 27001 et de l’annexe A.

**8. Réalisation**

**8.1 Maîtrise opérationnelle**

Pour tout risque identifié dans l'un des processus une procédure est mise en place pour diminuer ce risque. Le périmètre d'application de cette maîtrise opérationnelle englobe toutes les activités associées à chaque risque identifié comme :

* les postes de travail
* les équipements
* les machines
* les matériels
* le personnel
* les fournisseurs
* la maintenance
* les achats :
  + d'infrastructures :
    - bâtiments
    - équipements
    - services
  + de produits
* la conception :
  + des postes de travail
  + des équipements
  + des machines
  + des processus d'organisation du travail

Les exigences de certaines procédures opérationnelles sont divulguées aux fournisseurs et aux sous-traitants.

Nous conservons les informations documentées dans la mesure nécessaire pour avoir la certitude que les processus ont été menés à bien comme prévu. Nous gérons tout changement prévu et examinons les conséquences des changements imprévus, en prenant des mesures pour atténuer tout effet négatif.

Les documents les plus utilisés sont :

* plan de prévention
* protocole de sécurité
* plan d'urgence
* dispositif de protection
* fiche de poste
* fiche incident/accident

Le but étant de respecter la politique de sécurité de l’information et d’atteindre les objectifs et indicateurs. Cela permet :

* de maîtriser par la prévention des écarts potentiels envers la politique de sécurité de l’information
* d'établir les rôles et les responsabilités de chacun
* de communiquer les exigences à tous les niveaux

**8.2 Appréciation des risques**

Les risques sont analysés et évalués régulièrement en tenant compte des changements du contexte et des lois et réglementations en vigueur. Les risques sont classés en acceptables et non-acceptables.

**8.3 Traitement des risques**

Le plan de traitement des risques est mis à jour deux fois par an. Les options utilisées :

* éviter le risque
* accepter le risque
* éliminer la source du risque
* modifier la probabilité d’apparition du risque
* partager le risque
* accepter le risque résiduel

**9. Performances**

**9.1 Inspection, analyse et évaluation**

Nous effectuons une analyse et une évaluation des informations des inspections. Nous appliquons des dispositions (y compris les techniques statistiques) pour mesurer la performance aux moyens d’indicateurs :

* du système de management de la sécurité de l’information
* de la maîtrise des processus
* des fournisseurs
* des actions menées face aux risques
* de l'amélioration continue grâce aux opportunités saisies

**9.2 Audit interne**

L’audit interne nous permet d’évaluer la conformité et l’efficacité du système de management de la sécurité de l’information (cf. processus « Auditer »). Les audits internes permettent de vérifier si le système de management de la sécurité de l’information est correctement mis en place, si des écarts existent et si le SMSI reste opérationnel. La conformité est déterminée par rapport :

* aux dispositions planifiées et convenues
* au système de management de la sécurité de l’information
* aux lois et réglementations

Le processus auditer est basé sur la norme ISO 19011 (2018).

**9.3 Revue de direction**

La revue de direction est planifiée et ses enregistrements conservés selon le processus « Réaliser la revue de direction ». Son objectif est de revoir si le système de management de la sécurité de l’information est pertinent, adéquat et efficace.

**10. Amélioration**

Les non-conformités découvertes lors des audits, les incidents apparus et les actions correctives entreprises suivis et traités selon la procédure « Gestion des incidents ».

Les activités suivantes sont réalisées pour :

* procéder à la revue des non-conformités
* traiter les non-conformités
* déterminer et éliminer les causes
* évaluer les risques
* évaluer le besoin d’actions correctives pour empêcher la réapparition de non-conformités
* mettre en œuvre des actions curatives et correctives
* enregistrer les résultats des actions correctives et leur suivi

Toute action corrective est menée pour trouver et éliminer la cause de l’apparition des non-conformités.

Le processus d’amélioration continue « Améliorer » repose sur :

* des processus stables
* les résultats des audits
* l’analyse des données
* l’établissement de nouveaux objectifs d'amélioration
* la recherche et l’évaluation de solutions
* la mise en œuvre des solutions et la mesure des résultats
* la formalisation des changements quand les objectifs sont atteints

La méthode Kaizen d'amélioration continue par petits pas est largement utilisée dans tous les départements. C'est un outil redoutable de lutte contre le gaspillage sous toutes ses formes.