Partie I
Sécurité et information

Cette partie de l'ouvrage nous permettra de positionner les principaux concepts relatifs à l'information et à la sécurité.

Ensuite, nous détaillerons les exigences contenues dans l'ensemble des normes ISO qui traitent de ce sujet, notamment la série des ISO/CEI 27000.

Enfin, nous dresserons l'inventaire des composantes du système de management de la sécurité de l'information (SMSI) que tout organisme candidat à la certification doit définir, mettre en œuvre et améliorer en permanence.

Clé n° 1
La sécurité, qu'est-ce que c'est ?

Cette première clé ouvre la porte des concepts de la sécurité.

Le terme « sécurité » est employé pour s'appliquer à de nombreux domaines : civil, industriel, financier, transport, militaire, sanitaire, professionnel, juridique… et informatique.

La sécurité correspond à une situation qui présente un minimum de risques. Elle suscite donc un sentiment de confiance.

1.1 La définition de la sécurité

Ce mot vient du terme latin *securitas* et signifie « sûr ». Le dictionnaire *Le Robert* en donne la définition suivante : « État d'esprit confiant et tranquille d'une personne qui se croit à l'abri du danger. Situation tranquille qui résulte de l'absence réelle de danger (absence d'accident). »

Un danger est une menace qui pèse sur l'existence de quelqu'un ou de quelque chose. Les conséquences de cette menace pourront avoir des impacts plus ou moins importants. En cas extrême, ces conséquences peuvent entraîner des dommages irrémédiables pouvant aller jusqu'à la mort.

Le fascicule de documentation FD X 50-252:2006[5] définit ainsi le danger :

> **Danger :** c'est une substance, un objet, une situation ou un phénomène pouvant être à l'origine d'un dommage ou d'un préjudice.

Exemples de dangers : produit toxique, virus, inondation, incendie, etc.

Dans toute activité humaine, personnelle ou professionnelle, il existe une multitude de dangers qui planent sur le cours du temps. Ces dangers représentent une ou des menace(s) qui risquent d'attaquer notre sécurité et de l'altérer.

La norme ISO/CEI 27000:2016[6] définit ainsi l'attaque et la menace :

> **Attaque (§ 2.3) :** tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'utiliser sans autorisation un actif, ou de faire un usage non autorisé de celui-ci.

> **Menace (§ 2.83) :** cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

Afin de combattre le sentiment d'insécurité qui va résulter des menaces et des attaques, il nous appartient de prendre conscience de ces dangers, d'en identifier les faits générateurs et de trouver des remèdes efficaces pour les contrer afin de réduire ou de faire disparaître les conséquences néfastes.

Les solutions de type « parades » (ou mesures de sécurité) doivent nous permettre de réduire les effets de ces dangers, voire d'en éliminer les causes.

> **Mesure de sécurité (§ 2.16) :** mesure qui modifie un risque.

Les mesures de sécurité comprennent tous les processus, politiques, dispositifs, pratiques ou autres actions qui modifient un risque.

Nous pouvons remarquer qu'en matière de sécurité, de nombreux rapprochements peuvent être faits avec le domaine de la qualité. Les problématiques sont complexes.

Les solutions à mettre en œuvre sont souvent de nature transverse. Il est aussi possible de faire une distinction entre la qualité/sécurité réelle et la qualité/sécurité perçue.

5 *Management du risque – Lignes directrices pour l'estimation des risques.*

6 *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Vue d'ensemble et vocabulaire.*

1.2 Les composantes de la sécurité

Pour décrire la sécurité, deux aspects sont souvent utilisés :

- La sécurité passive : cette notion fait appel au domaine de la prévention (actions préventives). Son rôle consiste à réduire les facteurs de survenance ou de déclenchement de l'accident.
- La sécurité active : cette notion fait appel au domaine de la résolution (actions correctives). Son rôle consiste à déployer des mesures de protection à l'encontre des conséquences dommageables lorsque l'accident survient.

1.3 Les acteurs de la sécurité

La sécurité se situe dans un environnement qui correspond à un échange entre deux ou plusieurs acteurs.

1.3.1 L'organisation (l'organisme)

La norme ISO/CEI 27000:2016 définit ainsi l'organisation :

> **Organisation (§ 2.57) :** personne ou groupe de personnes qui exerce ses propres fonctions associées aux responsabilités, pouvoirs et relations nécessaires pour atteindre ses objectifs.

Une organisation (ou un organisme) peut être publique ou privée. À titre d'exemples, nous pouvons citer :

- une compagnie ;
- une société ;
- une firme ;
- une entreprise ;
- une institution ;
- une œuvre de bienfaisance ;
- un travailleur indépendant ;
- une association ;
- des parties ou des combinaisons de ces entités.

1.3.2 Les parties prenantes

La norme ISO/CEI 27000:2016 définit ainsi la partie prenante :

> **Partie prenante (§ 2.82) :** personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité.

À titre d'exemples, nous pouvons citer :

- ► les clients ;
- ► les propriétaires ;
- ► les collaborateurs d'un organisme ;
- ► les fournisseurs ;
- ► les banques ;
- ► les syndicats ;
- ► des partenaires ;
- ► d'autres sociétés.

1.3.3 La direction

La norme ISO/CEI 27000:2016 définit ainsi la direction :

> **Direction (§ 2.84) :** personne ou groupe de personnes qui dirige et contrôle un organisme au plus haut niveau.

La direction a le pouvoir de déléguer l'autorité et de fournir des ressources au sein de l'organisation. Dans un certain nombre de cas, le périmètre concerné peut englober seulement une partie de l'organisation (par exemple, la Direction du système d'information[7]). Dans ce cas, la direction impliquée est limitée à la direction qui contrôle cette partie de l'organisation.

1.3.4 Les instances dirigeantes

La norme ISO/CEI 27000:2016 définit ainsi les instances dirigeantes :

> **Instances dirigeantes (§ 2.29) :** personne ou groupe de personnes ayant la responsabilité des performances et de la conformité de l'organisme.

La direction a le pouvoir de déléguer l'autorité et de fournir des ressources aux instances dirigeantes.

7 DSI.

1.3.5 Entité de communication des informations sécurisées

La norme ISO/CEI 27000:2016 définit ainsi l'entité de communication des informations sécurisées :

> **Entité de communication des informations sécurisées (§ 2.85) :** organisme indépendant qui prend en charge l'échange d'informations dans une communauté de partage d'informations.

Cette partie prenante spécialisée va jouer un rôle spécifique dans l'organisation de la sécurité.

1.4 Monsieur Sécurité

Pour définir, mettre en œuvre et suivre la démarche sécurité au sein de l'organisme, il importe de désigner un « Monsieur Sécurité[8] ». Un peu comme le « Monsieur Qualité », représentant de la direction et exigé par la version 2008 de la norme ISO 9001[9], ce Monsieur Sécurité est investi par la direction de la responsabilité de la gestion de la sécurité de l'information.

Les objectifs de Monsieur Sécurité sont à la fois stratégiques et opérationnels. Il doit notamment :

- ► participer à la définition de la politique et des objectifs de sécurité ;
- ► établir un plan de gestion des risques ;
- ► obtenir de la direction les ressources nécessaires ;
- ► établir le système de management de la sécurité de l'information ;
- ► développer les outils permettant de suivre et de tracer l'activité ;
- ► entretenir un esprit de gestion des risques ;
- ► mettre en place un suivi.

Comme Monsieur Qualité, Monsieur Sécurité doit être rattaché hiérarchiquement à la direction générale qui lui donne autorité et à laquelle il doit rendre compte de sa mission.

8 En anglais, cette fonction est appelée *risk manager*. Une description sommaire de la fonction est donnée dans la fiche technique n° 28.

9 *Systèmes de management de la qualité – Exigences*. Remplacée par l'ISO 9001:2015, *Systèmes de management de la qualité – Exigences*.

Pour réussir, Monsieur Sécurité devra faire preuve de sérieuses capacités de communication. D'abord en interne pour faire prospérer la notion de sécurité, ensuite à l'extérieur avec les fournisseurs pour leur faire adopter le même état d'esprit.

Il devra aussi gérer tous les processus :

- ► d'évaluation et de gestion des risques ;
- ► de gestion de surveillance et de contrôle du SMSI ;
- ► de réponse aux incidents de sécurité.

Il devra être capable d'anticiper et de fournir des recommandations adaptées.

Concevoir, déployer, gérer, maîtriser, dialoguer, anticiper, évoluer, former, communiquer, etc. : telles sont les qualités requises pour réussir la mission d'un Monsieur Sécurité.

Clé n° 2
L'information, qu'est-ce que c'est ?

Cette deuxième clé ouvre la porte des concepts de l'information.

Il est souhaitable de faire une distinction sémantique entre les deux mots « information » et « donnée ».

En effet, ces deux mots ne recouvrent pas les mêmes concepts.

2.1 La définition de l'information

Le terme « information » vient du latin *informare* qui signifie mettre en forme. En fait, le même mot désigne à la fois le message (communication, média) et les symboles codés (signes, alphabet) qui sont contenus dans le message.

La notion d'information est étroitement liée à la relation des individus que nous sommes avec notre environnement. Ces messages, échangés sous la forme de signaux, sont véhiculés à notre niveau par nos cinq sens (vision, toucher, ouïe, goût, odorat). Dans notre civilisation technologique, les moyens de communication biologiques sont prolongés par des outils qui en accélèrent la vitesse de transmission et réduisent les limites espace/temps. Il en résulte que toute perturbation (distorsion, déformation, insuffisance, perte) de la qualité et de la sécurité de cette information peut avoir de lourdes conséquences sur nos relations, donc sur notre vie.

Au regard de la sécurité, il importera donc de prendre en compte ces deux aspects de l'information et d'intervenir à la fois :

- ► sur le message et sa transmission ;
- ► sur le contenu du message.

2.2 La définition de la donnée

Le terme « donnée » correspond à une représentation de l'information selon des règles codées, généralement pour procéder à son traitement.

La norme ISO/CEI 2382-1:1993[10] définissait ainsi la donnée :

> Représentation réinterprétable d'une information sous une forme conventionnelle convenant à la communication, à l'interprétation ou au traitement.

La norme ISO/CEI 27000:2016 définit ainsi les données :

> **Données (§ 2.20) :** c'est un ensemble de valeurs attribuées aux mesures élémentaires (définies en fonction d'un attribut et de la méthode de mesurage spécifiée pour l'identifier), aux mesures dérivées (définies en fonction d'au moins deux mesures élémentaires) et/ou aux indicateurs (mesure qui fournit une estimation ou une évaluation d'attributs spécifiés à partir d'un modèle analytique concernant des besoins d'information définis).

Les données sont conservées sur différents types de supports (papier, magnétique, numérique).

Pour transmettre un message, il faut le coder. Le code utilisé est dépendant de la nature du canal de transmission. Par exemple :

- ► l'écriture ;
- ► la parole ;
- ► le code morse ;
- ► le code binaire ;
- ► etc.

Dans le domaine des systèmes de traitement de l'information, les données sont gérées séparément des traitements.

10 *Technologies de l'information – Vocabulaire – Partie 1 : termes fondamentaux*. Remplacée par l'ISO/CEI 2382:2015, *Technologies de l'information – Vocabulaire*.