Service Central de la Sécurité des Systèmes d'Information

GS - 001

Guide pour
l'élaboration d'une

Politique de Sécurité Interne

(PSI)

à l'usage du responsable
de la sécurité
du système d'information

15 septembre 1994

DISI/ SCSSI/DIS

P
S
I

VERSION 1.1

Avertissement au lecteur

1°) **Le présent guide est un support de réflexion.**

Élaboré par le SCSSI pour mettre son expérience au profit des différents départements ministériels, des administrations de l'État et des grands organismes publics, ce guide constitue une grille de travail.

Appliqué aux ministères, il est destiné aux fonctionnaires de sécurité des systèmes d'information (FSSI) afin de leur permettre de mettre en place une politique de sécurité, conformément à l'IGI 900.

Appliqué aux autres organismes, il offre une réponse possible pour l'application des actions préconisées par la Recommandation 901, relative aux informations sensibles ne relevant pas du secret de défense.

2°) **Le présent guide n'est pas un règlement : il n'a pas de portée obligatoire.**

Les références contenues dans ce guide ont uniquement pour objet de servir d'illustration et de souligner le sens qui peut être donné aux principes et aux règles de sécurité choisies par un organisme.

Tout particulièrement pour le domaine juridique, le lecteur est averti qu'il doit, dans tous les cas, vérifier la validité et la portée des textes législatifs auxquels il se réfère, dans le cadre des activités propres à son organisme.

Page laissée blanche

Sommaire

Page laissée blanche

Introduction générale et présentation du guide

POLITIQUE DE SÉCURITÉ INTERNE

Ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les biens, en particulier les informations sensibles, au sein de l'organisation.

Définition du Catalogue des critères d'évaluation de la sécurité des systèmes d'informatique, ITSEC, Commission européenne, juin 1991, chapitre 2, paragraphe 2.10.

Remarque importante :

Traduction du terme anglo-saxon "Corporate security policy", la Politique de sécurité interne (PSI) intéresse la sécurité relative à l'information et au système d'information. Cette politique doit être appliquée conjointement et en accord avec la sécurité générale de l'organisme couvrant la sécurité des personnes (sécurité du travail, sécurité incendie, assurances, etc.) ainsi que, en général, les consignes existantes pour les accès physiques aux bâtiments.

Introduction générale

Au cours de ces vingt dernières années, le développement rapide des technologies de l'information a entraîné une dépendance de plus en plus grande des organismes envers leur système d'information, devenu une composante stratégique au même titre que la recherche ou l'innovation.

Par ailleurs, l'utilisation croissante des systèmes d'information pour des applications de plus en plus diversifiées a fait prendre conscience à la communauté des utilisateurs qu'il ne suffisait pas de mettre en œuvre les moyens de communication les plus performants, mais que ces derniers devaient être fiables en terme de disponibilité, d'intégrité et de confidentialité.

> *La sécurité du système d'information est devenue un facteur essentiel du bon fonctionnement de l'organisme.*

Mais, le fait nouveau se situe également dans la mutation des qualifications requises pour assumer la fonction de responsable de la sécurité par rapport à une formation initiale technique, alors que la pluridisciplinarité de ce nouveau métier rend indispensable l'adoption d'une approche plus systémique. En effet, une parfaite intégration de la composante sécurité dans la gestion d'un organisme impose la prise en compte d'éléments aussi divers que les particularités de sa culture, les contraintes liées à sa mission ou à son métier, les orientations stratégiques qui représentent le devenir souhaité et, d'une façon générale, l'ensemble des règles touchant au personnel, à l'organisation et aux méthodes et techniques utilisées.

> *La pluridisciplinarité du domaine de la sécurité ouvre la voie à un véritable exercice de prospective au bénéfice de l'organisme tout entier : il en résulte une réflexion qui est l'essence même de la politique de sécurité interne.*

Présentation du guide

La première partie, intitulée "Les fondements de la politique de sécurité interne", situe la place d'une *politique de sécurité interne* dans l'organisme et précise les bases de légitimité sur lesquelles elle s'appuie.
La deuxième partie, intitulée "Principes et règles pour une politique de sécurité interne", expose les grands principes de sécurité qui peuvent être retenus ainsi que les règles qui en découlent.

Toutefois, ce guide n'est pas le document final, immédiatement appropriable par un responsable de la sécurité : il propose seulement les bases de légitimité essentielles ainsi qu'un corpus de principes et de règles dont certains peuvent apparaître indispensables et d'autres moins adaptés à la mission ou au métier d'un organisme.

> *Ce guide se présente sous l'aspect d'un catalogue permettant de déterminer les bases de légitimité correspondant aux missions de l'organisme et de choisir les principes et les règles les plus adaptés à ses activités.*

Étapes de l'élaboration d'une politique de sécurité interne

Au préalable, l'énoncé des bases de légitimité est produit à partir, d'une part, de l'analyse des objectifs stratégiques de l'organisme et, d'autre part, des lois et règlements existants ainsi que des arguments retenus parmi ceux énoncés dans la première partie du guide PSI. Les étapes suivantes sont :

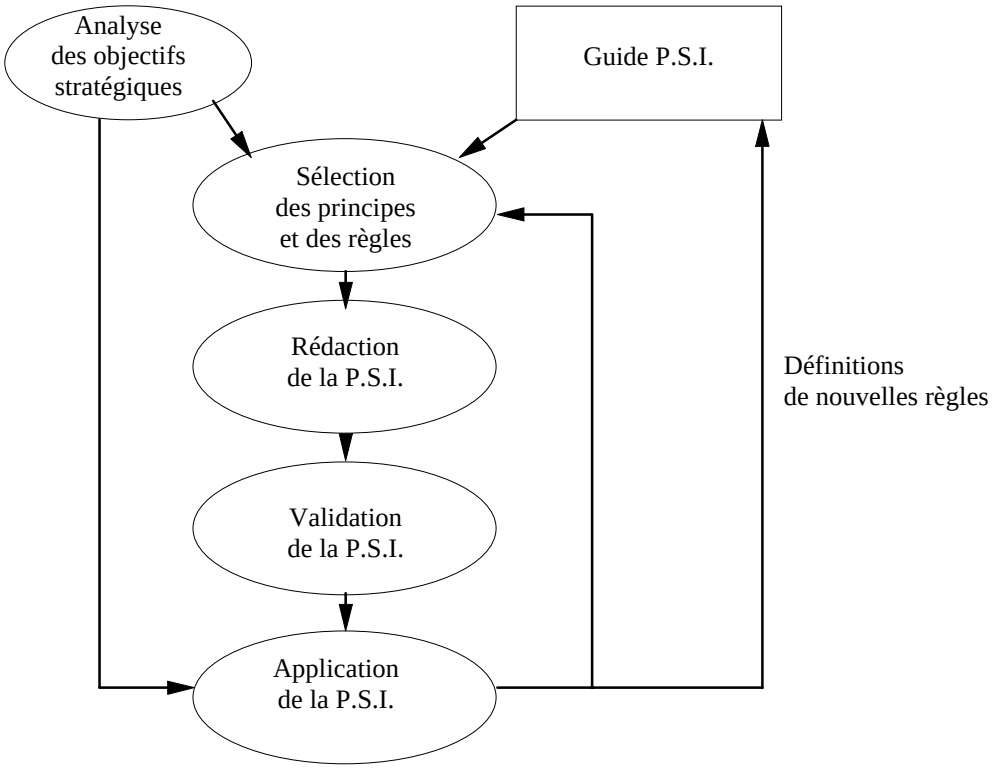
- la sélection des principes et des règles, qui découlent des bases de légitimité retenues, et qui peut s'inspirer de la liste structurée par thème dans la deuxième partie du guide PSI,

- la rédaction de la PSI, confiée à un comité de sécurité représentatif de toutes les activités de l'organisme, et selon un plan qui peut s'inspirer du guide PSI,

- La validation de la PSI, finalisée par la prise en compte du document par le responsable de la sécurité pour diffusion, sensibilisation et application,

- L'application de la PSI par les correspondants de sécurité de chaque site ou unité ce qui implique la rédaction d'un plan de sécurité - ou politique de sécurité du système (PSS)- énumérant les mesures et les consignes de sécurité adaptées à l'unité concernée et émanant des principes et des règles retenues dans la PSI.

Enfin, l'application de la PSI sur les sites ou unités doit permettre de modifier ou de définir de nouveaux principes ou règles ; l'observation, sur le terrain, des contraintes liées à leur application doit également être mise à profit pour effectuer une mise à jour du guide PSI.



Partie 1

Les fondements de la politique de sécurité interne

Page laissée blanche

Présentation de la première partie

La première partie de ce guide, intitulée "Les fondements de la politique de sécurité interne", ne s'intéresse qu'aux arguments propres à l'environnement national, international ou corporatif d'un organisme.

Un premier chapitre, intitulé "La politique de sécurité interne", se base sur des travaux ou des références universelles et plaide en faveur de l'adoption et de l'application d'une *politique de sécurité interne* dans un organisme.

Un second chapitre, intitulé "Les bases de légitimité de la politique de sécurité interne", expose des arguments déontologiques, législatifs et corporatifs ainsi que des recommandations diverses, issues de travaux et de réflexions d'instances nationales ou internationales, susceptibles d'être intégrés dans une *politique de sécurité interne.*

La recherche de toutes les références européennes et nationales qui intéresse le sécurité du système d'information d'un organisme, ainsi que l'éthique des métiers des technologies de l'information et leur utilisation, constitue les bases de légitimité d'une *politique de sécurité interne*[1].

> *Ainsi, tous les arguments retenus qui s'inscrivent dans le cadre des fondements d'une politique de sécurité interne, serviront à la justification de tous les principes et les règles édictés par l'organisme.*

[1] voir également la note complémentaire n°1, annexe 1.

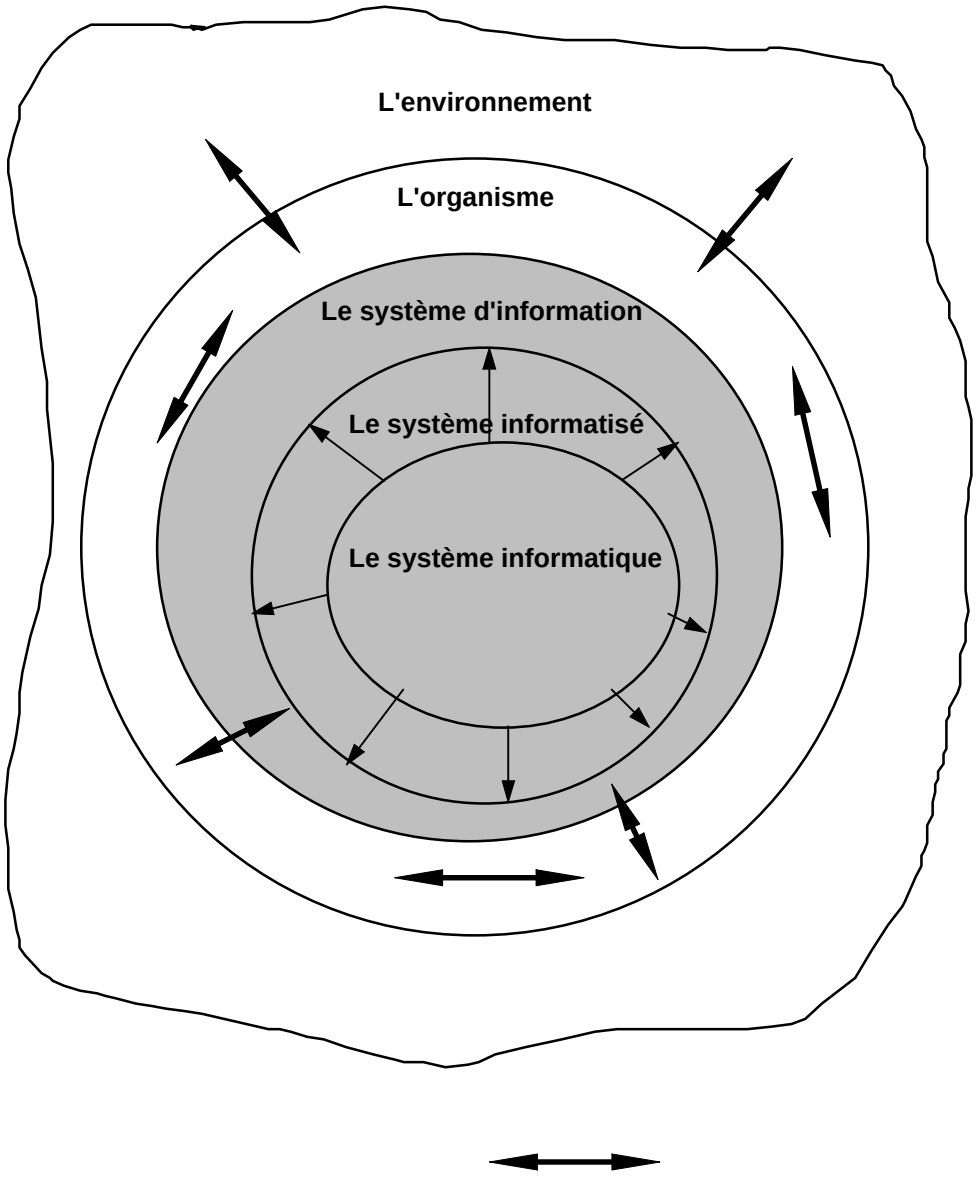
Page laissée blanche

Chapitre 1

La politique de sécurité interne

Ce chapitre propose, tout d'abord, une représentation d'un système d'information, puis il situe la place de la *politique de sécurité interne* dans la méthodologie préconisée dans le Catalogue des critères d'évaluation (ITSEC) ; il donne ensuite le lien avec le document intitulé "Lignes directrices régissant la sécurité des systèmes d'information"[2]. Il précise enfin la finalité, le champ d'application et les recommandations pour une mise en œuvre.

1.1. Représentation d'un système d'information et définitions



[2] Lignes directrices régissant la sécurité des systèmes d'informations, OCDE, Paris 1992

Flux d'informations

Les définitions suivantes concernent les termes les plus employés dans le guide PSI et qui pourraient recevoir, selon les domaines d'application, des sens différents.

Toutefois, pour tous les termes qui font l'objet d'une définition dans un texte juridique ou qui ont obtenu un large consensus au niveau des instances qualifiées, le lecteur est invité à consulter les divers glossaires qui s'y rapportent.

- **Organisme**

  Les organes qui ont pour tâche le fonctionnement d'un service, d'un parti, etc. (Dictionnaire Larousse)[3].

  Par convention de lecture pour ce guide, le terme "organisme" désigne tout établissement ministériel, public ou privé et comprend l'ensemble des biens, des personnes et des services attachés à la réalisation d'une mission ou d'un métier.

- **Système d'information**

"Le système d'information comprend les matériels informatiques et les équipements périphériques, les logiciels et les microprogrammes, les algorithmes et les spécifications internes aux programmes, la documentation, les moyens de transmission, les procédures, les données et les paramètres de contrôle de la sécurité, les données et les informations qui sont collectées, gardées, traitées, recherchées ou transmises par ces moyens ainsi que les ressources humaines qui les mettent en œuvre"[4].

En effet, le système d'information est caractérisé par l'organisation humaine qui donne une signification au recueil, au traitement, à la production des données contribuant au fonctionnement opérationnel.

Les systèmes d'information dont il est question dans ce guide concernent l'informatique de gestion, de services, scientifique ou industrielle.

- **Système informatisé**

  Le système informatisé, qui est un sous-ensemble d'un système d'information, fait référence à la dimension électrique pour le recueil, le traitement, la transmission et le stockage des données. Il fait abstraction de l'organisation humaine ainsi que de tous les traitements et les transferts d'informations manuels.

[3] Voir également la note complémentaire n°2, annexe 1
[4] Lignes directrices régissant la sécurité des systèmes d'informations, OCDE, Paris 1992, p.29.

- **Système informatique (ou système de traitement et d'analyse de données)**

Le système informatique, qui regroupe traditionnellement les centres informatiques de l'organisme, comprend les données, supports, logiciels, équipements, documentations. Il ne comprend pas l'aspect transmission, c'est-à-dire les équipements qui le supporte y compris les matériels d'extrémité (poste téléphonique, minitel, télécopie, etc.) ni les équipements électriques déconnectés ou isolés (micro-ordinateurs dédiés, portables, photocopieurs, etc.).

Les systèmes informatisés d'un organisme (système de production, de distribution, de gestion, etc.) sont "innervés" par le ou les systèmes informatiques qui composent le système d'information.

1.2. Lien entre la politique de sécurité interne et les Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC)

L'accomplissement de la mission ou du métier d'un organisme est soumis à un ensemble de règles et de pratiques qui régissent tous les aspects liés au fonctionnement (personnel, finances, recherche, production, communication, etc.). En conséquence, le système d'information qui contribue à assurer cette mission ou ce métier, doit tenir compte de toutes les contraintes d'environnement de l'organisme.

Par ailleurs, face aux menaces qui pèsent sur les systèmes d'information, l'utilisateur exige une protection convenable des informations et des services de traitement et de transport de l'information. La sécurité est donc devenue une des dimensions essentielles de la stratégie de l'organisme et elle doit être prise en compte dès la conception du système d'information.

En réponse à ces préoccupations, des travaux ont été entrepris au niveau européen ; ils ont abouti à l'élaboration des critères d'évaluation de la sécurité des systèmes informatiques (ITSEC) qui permettent de définir un cadre pour l'évaluation de produits ou de systèmes informatiques (voir annexe 2).

Ainsi, il a été établi que la sécurisation d'un système d'information nécessite la mise en place d'une *politique de sécurité interne* qui peut être vue comme l'ensemble des principes et des règles de sécurité pour la gestion et le fonctionnement du système d'information.

En France, une directive du Premier Ministre précise que les critères ITSEC sont les seuls critères à appliquer pour les évaluations de sécurité par les organismes officiels. Pour les départements ministériels ces critères doivent être utilisés à l'exclusion de tous autres, notamment pour la définition des

objectifs de sécurité des systèmes ou produits informatiques ainsi que pour l'élaboration des spécifications des marchés les concernant[5]
Pour les organismes publics et privés, ces critères ont valeur de recommandation.

La politique de sécurité interne constitue la première étape de la méthodologie de sécurisation d'un système d'information selon les Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC).

1.3. Lien entre la politique de sécurité interne et les Lignes directrices régissant la sécurité des systèmes d'information (document de l'OCDE)

Les neuf principes généraux exposés dans les Lignes directrices régissant la sécurité des systèmes d'information constituent une charte de sécurité applicable aux systèmes d'information d'un État ou d'un grand organisme.

La *politique de sécurité interne* d'un organisme, quant à elle, se situe à un niveau d'abstraction moins élevé : en effet, le système d'information auquel elle s'applique peut être décrit avec précision quant à ses constituants et sa frontière avec l'environnement.

Toutefois, la référence aux principes généraux du document de l'OCDE est donnée à maintes reprises pour justifier les principes et les règles énoncés dans les différents chapitres de ce guide.

La liste des principes généraux est donnée en annexe 3.

1.4. Finalités de la politique de sécurité interne

Les finalités de la *politique de sécurité interne* découlent de celles décrites dans les Lignes directrices de l'OCDE[6], à savoir :

- sensibiliser aux risques menaçant les systèmes d'information et aux moyens disponibles pour s'en prémunir,
- créer un cadre général pour aider les personnes chargées, dans les secteurs public et privé, d'élaborer et de mettre en œuvre des mesures, des consignes et des procédures cohérentes en vue d'assurer la sécurité des systèmes d'information,
- promouvoir la coopération entre les différents départements, services ou unités de l'organisme pour l'élaboration et la mise en œuvre de telles mesures, consignes et procédures,
- susciter la confiance dans le système d'information,

[5] Lettre n°106 SGDN/DISSI/26007 du 11 mars 1992
[6] Recommandation du Conseil et annexe, 26 novembre 1992, page 4 à 12

- faciliter la mise au point et l'usage du système d'information pour tous les utilisateurs autorisés du système d'information.

La *politique de sécurité interne* a pour but la garantie des services rendus ainsi que la protection des biens et des informations sensibles. De plus, elle constitue une référence par rapport à laquelle toute évolution du système d'information devra être justifiée, que ce soit pour l'intégration d'un élément nouveau du système ou pour la modification d'un élément existant.

L'élaboration de la *politique de sécurité interne* requiert une connaissance parfaite de l'organisme et de son environnement, tout autant que de son système d'information.

1.5. Champ d'application de la politique de sécurité interne

Le champ d'application de la *politique de sécurité interne* découle de celui décrit dans les Lignes directrices de l'OCDE, à savoir :

- la *politique de sécurité interne* s'adresse principalement aux administrations de l'État et aux organismes public,

- la *politique de sécurité interne* s'applique à tous les systèmes d'information,

- la *politique de sécurité interne* s'applique à un système existant ou à développer.

La *politique de sécurité interne* émane de la politique générale de l'organisme et elle est en accord avec le schéma directeur stratégique du système d'information[7].

Mais, le document qui en résulte ne doit pas être remis en cause par les seules évolutions technologiques ou celles résultant d'une modification de l'architecture du système d'information aussi longtemps que la mission de l'organisme reste inchangée ou, de façon plus ponctuelle, que les objectifs stratégiques ne sont pas modifiés (maintien du "cap stratégique"). Toutefois le caractère pérenne de la *politique de sécurité interne* n'exclut pas l'adaptation permanente des mesures de sécurité qui découlent de sa mise en œuvre.

Ainsi, étant donné les conséquences que pourraient entraîner une défaillance de la sécurité du système d'information sur la réalisation des objectifs stratégiques de l'organisme, la *politique de sécurité interne* doit être prise en compte au niveau de responsabilité le plus élevé.

[7] Voir également la note complémentaire n°4, annexe 1

La politique de sécurité interne est la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de son système d'information.

1.6. Les recommandations pour la mise en œuvre de la politique de sécurité interne

Les recommandations pour la mise en œuvre de la *politique de sécurité interne* découlent de celles décrites dans les Lignes directrices de l'OCDE, à savoir :

- établir des mesures, consignes et procédures qui traduisent les principes et les règles énoncés dans la *politique de sécurité interne*,
- faire en sorte que la mise en œuvre de la *politique de sécurité interne* s'accompagne de consultations, d'une coordination et coopération entre les différents acteurs du système d'information,
- convenir le plus rapidement possible d'initiatives spécifiques en vue de l'application de la *politique de sécurité interne*,
- donner une large diffusion aux principes et aux règles de la *politique de sécurité interne*,
- réexaminer la *politique de sécurité interne* en fonction des événements majeurs affectant la mission ou la vie de l'organisme ou, une fois au moins tous les cinq ans, pour vérifier l'adéquation des règles par rapport à l'évolution du système d'information de l'organisme.

La *politique de sécurité interne* est mise en œuvre au niveau de chaque site, division, service ou unité opérationnelle au moyen d'un plan de sécurité qui décline les principes et les règles de sécurité en mesures de sécurité techniques et non techniques adaptées aux moyens, à l'environnement et au fonctionnement du système d'information de l'échelon considéré[8].

Il appartient aux autorités qualifiées, responsables de chaque unité opérationnelle, de définir ces différentes mesures et de veiller à leur bonne application.

[8] Le plan de sécurité constitue la politique de sécurité du système (PSS) au sens ITSEC : voir schéma présenté à l'annexe 2

Chapitre 2

Les bases de légitimité pour une politique de sécurité interne

Les principes et les règles contenus dans une *politique de sécurité interne* puisent leurs bases de légitimité dans les lois, les réglementations, les normes et les recommandations émanant d'organismes internationaux, nationaux ou professionnels ; ils peuvent aussi trouver leur justification dans les composantes de la culture de l'organisme comme, par exemple, les traditions, les habitudes ou les règles internes.
Ces bases de légitimité sont déclinées selon leur portée et leur objectif en six rubriques :

- la déontologie,
- la lutte contre les accidents,
- la préservation des intérêts vitaux de l'État,
- l'arsenal juridique pour la lutte contre la malveillance,
- les contrôles technologiques,
- la préservation des intérêts particuliers de l'organisme.

> *Ces rubriques peuvent représenter les bases de légitimité pour une politique de sécurité interne ; elles devraient, de ce fait, être intégrées dans le champ des valeurs partagées par le personnel de l'organisme.*

Toutefois, ce chapitre ne peut prétendre à l'exhaustivité dans l'énumération des rubriques pouvant constituer des bases de légitimités ; les plus couramment citées sont données, à titre d'illustration, pour chacune des six rubriques énoncées précédemment.

Le lecteur trouvera une liste plus complète dans les annexes 4 à 7 de ce guide.

2.1. Les bases de légitimité reposant sur la déontologie

2.1.1. Les grands principes d'éthique

L'utilisation croissante de systèmes d'information par un public de plus en plus vaste et varié conduit à appliquer aux métiers des technologies de l'information des grands principes d'éthique tels que la garantie des droits de l'homme, la protection et le respect de la vie privée, la garantie des libertés individuelles ou publiques. Ces principes, appliqués au domaine des systèmes d'information, sont formulés :

Au niveau international,

par le **principe d'éthique et le principe de démocratie de l'OCDE** :

- le principe d'éthique stipule que la fourniture et l'utilisation des systèmes d'information ainsi que la mise en œuvre de leur sécurité doivent être telles que les intérêts légitimes des tiers soient respectés,

- le principe de démocratie stipule que la sécurité des systèmes d'information doit être compatible avec l'utilisation et la circulation légitimes des données et des informations dans une société démocratique.

et par **le principe de la garantie de l'anonymat**[9] dans l'usage de services fournis par des systèmes d'information (services téléphoniques, télématiques, de paiement électronique, etc.).

Au niveau de l'Union européenne,

par **le principe de protection des personnes**[10] à l'égard du traitement automatisé des données à caractère personnel.

Au niveau national,

par **la Loi "Informatique et Libertés"**[11] qui réglemente l'emploi et la constitution des fichiers nominatifs, c'est-à-dire, autorise les actions suivantes :

- la soumission, avant leur mise en œuvre, des traitements automatisés d'informations nominatives à des formalités administratives qui doivent être accomplies par les utilisateurs publics et privés,

[9] Conférence internationale des commissaires à la protection des données, Berlin, 30/08/89
[10] Convention 108 du Conseil de l'Europe du 28/01/81, approuvé par la loi 82.890 du 19/10/82
[11] Loi n°78-17 du 6 janvier 1978 sur l'informatique, les fichiers et les libertés

- la reconnaissance, pour toute personne figurant dans un fichier automatisé ou manuel, du droit d'accès aux informations qui la concernent,

- l'application de dispositions de protection s'appliquant à la collecte, l'enregistrement, le traitement et la conservation des informations nominatives des fichiers informatiques ou non informatiques,

- le contrôle de l'application de la loi par la Commission Nationale Informatique et Libertés.

Au niveau des organismes et des métiers qui s'y exercent,

par des **codes d'éthique** corporatifs (métiers juridiques, de la santé, de la recherche, de la banque, etc.) formulant des principes de base, des recommandations de politiques, des codes de conduites ou des règlements.

En particulier, et quel que soit le métier de l'organisme, celui-ci détient et traite des informations auxquelles il doit attribuer une mention spécifique, caractéristique de son domaine, comme la mention "confidentiel personnel" (domaine protégé par la Loi informatique et Libertés) ou "confidentiel professionnel, industriel, commercial", etc. (domaine protégé par le Code pénal).

Ainsi, parallèlement au code d'éthique propre au métier, l'organisme doit prendre en compte les spécificités concernant la protection d'informations d'ordre médical, juridique, etc., ainsi que le respect de l'anonymat des personnes ayant fourni des informations nominatives par le biais de questionnaires ou d'enquêtes.

2.1.2. Les codes d'éthique des métiers des technologies de l'information

Les codes d'éthique des métiers des technologies de l'information (annexe 4) font apparaître des règles de déontologie générale s'énonçant sous forme de devoirs et d'obligations à assumer :

- l'obligation de compétence et d'objectivité,

- les devoirs envers la clientèle, à savoir l'indépendance, le respect du client et de la mission confiée, le devoir de conseil et d'assistance,

- les devoirs envers les concurrents, à savoir le respect des principes de loyauté et de libre concurrence,

- le respect du secret de fabrique.

2.2. Les bases de légitimité reposant sur la lutte contre les accidents

Les accidents pouvant survenir à l'intérieur d'un organisme ou provoqués à l'extérieur de celui-ci par ses activités peuvent entraîner des pertes humaines ou des atteintes à l'environnement ou bien encore au patrimoine national ou privé. Aussi, est-il fait obligation légale à tous les responsables d'organismes de lutter, avec les moyens appropriés, contre les accidents divers[12].

Si cette préoccupation est généralement prise en compte au niveau de la sécurité générale (et, tout particulièrement celle touchant au personnel), elle est rappelée dans ce chapitre pour souligner que dans de nombreux cas les accidents de toute nature peuvent avoir pour cause des erreurs ou malveillances commises dans l'utilisation du système d'information (par exemple, dans le domaine du nucléaire, de la gestion du trafic fluvial, ferroviaire, aérien, des agences de bassin, etc.).

C'est ainsi que, indépendamment de l'obligation faite par la loi dans tous les pays développés, il est un devoir prioritaire pour les responsables d'organismes de renforcer les contrôles de sécurité et de les inscrire comme base de légitimité partout où il existe un risque, aussi minime soit-il, d'accident lié à l'utilisation du système d'information.

2.3. Les bases de légitimité reposant sur la préservation des intérêts vitaux de l'État

Les organismes gouvernementaux et ceux qui collaborent avec eux, sont soumis au respect des lois nationales et aux instructions interministérielles.

Lorsqu'un organisme, y compris en dehors de sa mission propre, est amené contractuellement ou non à utiliser ou traiter des informations classifiées relevant du secret de défense ou des informations sensibles comme, par exemple, celles relevant du patrimoine national, il doit appliquer les lois et les textes réglementaires qui s'y rapportent.

La liste des principaux textes est donnée dans les annexes 5 et 6.

[12] Décret n°92-158 du 20 février 1992. Voir également la note complémentaire n°3, annexe 1

2.3.1. Les informations relevant du secret de défense

pour les informations relevant du secret de défense, les obligations réglementaires de protection portent sur :

2.3.1.1. La protection du secret et des informations concernant la défense nationale et la sûreté de l'État

Une instruction[13], qui s'adresse à tous les départements ministériels et à tous les organismes publics ou privés où sont émises, reçues, mises en circulation ou conservées des informations intéressant la défense nationale et la sûreté de l'État, aborde les thèmes suivants :

- l'organisation et le fonctionnement des services de sécurité de défense,
- la protection des personnes,
- la protection des informations classifiées,
- la protection du patrimoine national et des informations qui doivent rester diffusion restreinte,
- la sensibilisation aux risques de compromission d'informations classifiées,
- les contrôles et inspections.

2.3.1.2. La sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées

Une instruction[14] qui s'adresse à toutes les administrations et services extérieurs de l'État, notamment aux établissements publics nationaux ou organismes placés sous l'autorité d'un ministre, précise les règles à respecter pour protéger les secrets de la défense nationale dans les systèmes d'information et aborde les thèmes suivants :

- les informations nécessitant une protection,
- les moyens de protection,
- les principes généraux de sécurité des systèmes d'information,
- les rôles respectifs, l'organisation et les missions des divers intervenants,
- les contrôles et inspections.

[13] Instruction générale interministérielle n°1300/SGDN/SSD
[14] Instruction générale interministérielle n°900/SGDN/SSD/DR et n°900/DISSI/SCSSI/DR

2.3.1.3. La protection du secret dans les rapports entre la France et les états étrangers

Une instruction[15] précise les dispositions générales et les protocoles de sécurité à établir dans le cadre d'études et de rapport entre la France et les pays étrangers.

Une autre instruction[16] porte sur la protection du patrimoine scientifique et technique français dans les échanges internationaux.

2.3.1.4. La protection du secret et des informations pour les marchés et autres contrats

Une instruction[17] précise les dispositions à prendre pour la protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les marchés ainsi que dans tous les autres contrats administratifs qui entraînent la mise en œuvre de systèmes d'information faisant l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées. Elle traite en particulier des dispositions à prendre vis-à-vis des personnes, des documents et des matériels.

2.3.1.5. Les instructions techniques particulières pour la lutte contre les signaux parasites compromettants

On entend par signal parasite compromettant tout signal électromagnétique émis par un équipement du système d'information pouvant être capté à l'extérieur du local de l'équipement, ou inversement, tout signal qui, émis depuis l'extérieur du local de l'équipement, pourrait perturber des traitements informatiques ou leurs données, ou même détériorer des matériels.

2.3.2. Les informations ne relevant pas du secret de défense

Une instruction[18] sur la sécurité des systèmes d'information traitant des informations sensibles non classifiées de défense reprend certains grands principes de l'IGI n900 et se présente suivant la même articulation. Elle s'applique à toutes les administrations et tous les services déconcentrés de l'État ainsi qu'aux établissements placés sous l'autorité d'un ministre. Cette instruction est également une référence pour les entreprises privées qui désirent assurer une protection de leurs propres secrets scientifiques, technologiques, industriels, commerciaux ou financiers ou qui désirent garantir leurs intérêts et leur patrimoine.

[15] Instruction interministérielle n°50/SGDN/SSD
[16] Instruction interministérielle n°486/SGDN/SSD
[17] Instruction interministérielle n°2000/SGDN/SSD
[18] Instruction générale interministérielle n°901/DISSI/SCSSI/DR

Elle recommande une harmonisation entre les mesures prises au titre de la protection du secret de défense et celles concernant la protection des informations sensibles ; c'est ainsi qu'une organisation fonctionnelle unique est conseillée.

Une autre instruction[19] édicte des recommandations relatives aux informations, aux systèmes ou aux applications ne relevant pas du secret de défense, mais dont la destruction, le détournement ou l'utilisation frauduleuse pourraient porter atteinte aux intérêts nationaux, au patrimoine scientifique et technique ou à la vie privée ou professionnelle des individus. Ces recommandations concernent plus particulièrement la sécurité des postes de travail autonomes ou connectés à un réseau.

2.4. Les bases de légitimité reposant sur l'arsenal juridique pour la lutte contre la malveillance

Au niveau de *l'Union européenne*, une recommandation[20] du Conseil de l'Europe sur la criminalité en relation avec l'ordinateur et une directive[21] sur la protection juridique des programmes d'ordinateur réglementent **la protection du logiciel**.

Au *niveau national*, les logiciels sont considérés comme des œuvres de l'esprit protégées par **le code de la propriété intellectuelle** et des lois réglementent les peines associées aux infractions telles que :

- la copie ou l'utilisation illicite de logiciel,
- la divulgation non autorisée de documents techniques ou commerciaux, même après une rupture de contrat,
- le délit ou la tentative de délit, avec ou sans entente concertée, correspondant aux infractions comme l'accès ou le maintien frauduleux dans tout ou partie d'un système, l'entrave au fonctionnement, la modification de données,
- l'interception de télécommunications.

Mais il appartient à l'organisme de prendre les mesures qu'il juge nécessaire à la protection de son système d'information (mesures de prévention, de détection et de réparation), afin de se protéger contre les menaces redoutées, qu'elles soient accidentelles ou intentionnelles comme, par exemple, l'interception, le détournement, l'utilisation ou la divulgation non autorisée d'éléments du système d'information.

On trouvera, à l'annexe 7, la liste de ces lois et recommandations.

[19] Recommandation n°600/SGDN/DISSI/SCSSI
[20] Recommandation R(89) du Conseil de l'Europe du 19 septembre 1989
[21] Directive n°91/250/CEE du 14 mai 1991

2.5. Les bases de légitimité reposant sur les contrôles technologiques

2.5.1. Le contrôle étatique dans le domaine de la cryptologie

"On entend par prestation de cryptologie toute prestation visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou visant à réaliser l'opération inverse, grâce à des moyens matériels ou logiciels conçus à cet effet"[22].

La réglementation française (annexes 5 et 7) s'appuie sur des lois et instructions interministérielles dont le but est de préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État.

La réglementation sur la cryptologie s'applique à tous les moyens cryptologiques, utilisés dans le secteur privé ou public : elle concerne la fourniture, l'exportation, l'utilisation de moyens ou de prestations cryptologiques.

2.5.2. Le contrôle consumériste

Les utilisateurs de systèmes d'information sont soumis d'une part à l'offre des constructeurs, chacun ayant ses systèmes spécifiques et, d'autre part, à la nécessité d'utiliser et de faire communiquer ces systèmes entre eux.

2.5.2.1.La normalisation

L'utilisation de produits normalisés est nécessaire pour assurer l'interopérabilité des systèmes.

La définition en est donnée par une directive de l'Union européenne portant sur l'élaboration des normes nationales[23]. Elle est reprise par un décret national fixant le statut de la normalisation[24] : "la normalisation a pour objet de fournir des documents de référence comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux".

[22] Loi 90-1170 du 29 décembre 1990 modifiée, article 28
[23] Directive 83.189/CEE du 28 mars 1983
[24] Décret n°84-74 du 28 janvier 1984, modifié par le décret n°90-853 du 18 juillet 1990

Le choix de produits normalisés ayant valeur de recommandation, il peut prendre un caractère obligatoire en raison de la publication :

- d'une directive communautaire particulière,
- d'un arrêté du Ministère de l'Industrie,
- de réglementations spécifiques comme, par exemple, les codes des marchés publics,
- de contrats particuliers protégés par le code civil.

2.5.2.2. La certification

La situation juridique communautaire s'appuie sur une résolution[25] portant sur l'approche globale en matière d'évaluation de la conformité. En ce qui concerne la certification de produits ou de systèmes informatiques, quatre pays européens (Allemagne, France, Grande-Bretagne et Pays-Bas) ont développé les critères d'évaluation de la sécurité des systèmes informatiques (ITSEC) qui ont vocation de devenir une recommandation.

La définition de la certification qui y est donnée est la suivante : "la certification atteste formellement des résultats de l'évaluation et le fait que les ITSEC ont été correctement appliqués"[26]. Ces critères doivent être utilisés par les administrations de l'État pour la définition des objectifs de sécurité des systèmes ou produits informatiques ainsi que pour l'élaboration des spécifications des marchés les concernant.

En France, une évaluation réussie suivant les critères harmonisés européens peut donner lieu à la délivrance d'un certificat par le Service central de la sécurité des systèmes d'information (S.C.S.S.I).

2.6. Les bases de légitimité reposant sur la préservation des intérêts particuliers de l'organisme

L'organisme peut se définir par :

- sa mission (pour un organisme étatique) ou son métier (pour un organisme privé),
- sa culture,
- ses orientations stratégiques et sa structure,
- ses relations avec l'environnement,
- ses ressources,

[25] Résolution du conseil 90/C/10.01 du 21 décembre 1989
[26] ITSEC, page 111, paragraphe 6-7

Lorsque l'organisme considère qu'un de ces thèmes a un impact majeur sur sa sécurité, il l'élève au rang de base de légitimité pour justifier les principes décrits dans sa *politique de sécurité interne*.

C'est ainsi que les principes et les règles qui sont suggérés dans la deuxième partie de ce guide doivent être en accord, comme le recommande l'OCDE (principes généraux d'intégration et de pluridisciplinarité), avec les décisions et les actions touchant aux bases de légitimité décrites dans ce chapitre[27].

2.6.1. La mission ou le métier de l'organisme

Toutes les potentialités et les ressources dont dispose un organisme n'ont pour finalité que l'accomplissement de sa mission ou de son métier.

Il en découle des objectifs qui devraient être clairement exprimés et portés à la connaissance des acteurs concernés, à l'intérieur comme à l'extérieur de l'organisme, pour assurer la cohésion des missions dévolues à chacune des unités fonctionnelles.

2.6.2. La culture de l'organisme

La culture de l'organisme se définit par le partage d'un ensemble de valeurs, de savoir-faire, d'habitudes de vie collective et par le sentiment d'une identité commune.

Elle s'exprime au niveau de chaque individu par :

- le respect de la mission et l'adhésion au projet de l'organisme ; par exemple, pour des entreprises utilisant des informations relevant du secret de défense, intégration de la sécurité dans le cadre quotidien du travail ; pour une organisation dont la mission est la distribution, livraison de la commande dans les délais les plus brefs ; pour un constructeur de matériels haut de gamme, mobilisation permanente pour la qualité,
- le respect de la mémoire collective,
- la conservation du patrimoine de l'organisme,
- le respect du règlement,
- etc.

Toute action visant à modifier un de ces éléments a un impact d'autant plus important que l'élément modifié est profondément inscrit dans la culture de l'organisme et accepté par l'ensemble du personnel.

[27] Voir également la note complémentaire n°5, annexe 1

2.6.3. Les orientations stratégiques et la structure de l'organisme

Les choix fondamentaux et les objectifs que se fixe l'organisme découlent de sa propre stratégie ; le responsable de la sécurité doit alors veiller à ce que les projets qui s'inscrivent dans ce cadre et qui touchent à la structure même de l'organisme, restent en cohérence avec les objectifs assignés à la sécurité du système d'information.
En effet, la structure de l'organisme est une adaptation permanente des orientations stratégiques choisies pour mieux gérer les différentes fonctions de l'organisme et leur évolution. Tout changement affectant la structure de l'organisme modifie, en conséquence, ses flux d'informations.

L'aspect formel de la structure est représenté par un organigramme[28] qui rend compte de l'organisation des différentes entités constitutives de l'organisme (directions, départements, services, unités, etc.).

L'aspect informel peut être représenté par un sociogramme qui met en lumière les facteurs d'influence pour les personnes ou les postes stratégiques et qui pèsent sur les orientations et les décisions de l'organisme. C'est, par exemple, l'influence sur la direction et sur les informaticiens de la nomination d'un responsable non technicien au poste de responsable de la sécurité des systèmes d'information. Ces difficultés relationnelles qui sont souvent difficiles à évaluer, exigent pour être mises en lumière l'observation des jeux de pouvoir au sein de l'organisme. En particulier, les flux de communication transverses par rapport à la structure hiérarchique, bien que répondant souvent à un réel besoin opérationnel, peuvent être la conséquence d'une rétention de l'information ; il se crée alors au sein de l'organisme des flux qui échappent aux contrôles de la sécurité.

2.6.4. Les relations de l'organisme avec son environnement : les contrats passés avec des tiers

Les engagements pris avec d'autres organismes font l'objet de contrats où peuvent figurer en particulier des clauses spécifiques concernant la sécurité des systèmes d'information[29]. Elles sont d'autant plus importantes que la nature des engagements concerne une composante stratégique ou est susceptible d'influer sur la culture de l'organisme. Toutes relations nouvelles avec l'environnement de l'organisme nécessite un effort préalable de communication à l'intérieur de l'organisme.

[28] Voir également note complémentaire n°6, annexe 1
[29] Article 1134 du code civil : "Les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites".

A titre d'exemple, dans le cas d'un contrat de gestion de l'exploitation (traduction du terme anglo-saxon "facility management"), il existe des clauses spécifiques pour le transfert du savoir-faire et, en interne, le personnel doit avoir les éléments lui permettant de comprendre pourquoi et comment ce nouveau choix s'intègre dans la stratégie de l'organisme et quelles en sont les implications sur les consignes de sécurité.

Un autre exemple est celui des contrats de sous-traitance, pour lesquels il existe souvent des clauses spécifiques relatives à la fourniture de programmes-sources et à leur usage[30].

Dans le cadre de coopération internationale, les engagements contractuels garantissent les parties et doivent être en accord avec la réglementation des pays concernés.
Plus généralement, dans le cadre des relations avec l'environnement, l'organisme demandeur doit faire valoir les exigences suivantes :

- vis-à-vis des fournisseurs : le devoir de conseil, de qualité et de maintenabilité,
- vis-à-vis des prestataires de services : le devoir de conseil, l'obligation de moyens et de résultats,
- vis-à-vis de la sous-traitance : les clauses spécifiques garantissant la non concurrence,
- vis-à-vis des autres organismes : les clauses spécifiques pour la coopération et l'interopérabilité des systèmes d'information.

2.6.5. Les ressources de l'organisme

L'organisme est une unité économique de production de biens ou de services, composée de ressources humaines, juridiques, techniques et financières.

Les unités de l'organisme ont, assez souvent, des missions et des objectifs différents qui peuvent apparaître comme des contraintes que la sécurité doit prendre en compte, par exemple :

- pour les ressources humaines : nécessité de la confidentialité des critères d'embauche,
- pour les ressources juridiques : nécessité de la confidentialité des contrats,
- pour le savoir-faire et les ressources techniques : nécessité de la protection des idées nouvelles,
- pour les ressources financières : nécessité de la confidentialité des comptes avant leur publication.

[30] En particulier, la loi 94-361 du 10 mai 1994, qui est devenue conforme au standard européen en matière de protection des logiciels, modifie les droits de l'auteur et de l'utilisateur et a pour conséquence la modification de l'ensemble des contrats de concession et de licence.

Partie 2
Les principes et les règles pour une politique de sécurité interne

La liste récapitulative des règles, dans l'ordre des index, est donnée à l'annexe 9.

Présentation de la deuxième partie

La deuxième partie de ce guide, intitulée "Les principes et les règles pour une politique de sécurité interne", propose au responsable de l'élaboration d'une politique de sécurité interne le choix parmi 21 principes, déclinés en 74 règles. Elle est articulée autour de six chapitres qui répondent aux questions suivantes :

- *qui prend en charge la politique de sécurité interne au sein de l'organisme ?*

  le premier chapitre porte sur le principe général des **responsabilités** à définir pour doter un organisme d'une politique de sécurité interne,

- *quels sont les biens de l'organisme qu'il convient de protéger ?*
  les deuxième et troisième chapitres traitent respectivement de **l'information** et des **biens physiques** de l'organisme,

- *comment mettre en place la sécurité ?*
  les quatrième et cinquième chapitres portent respectivement sur l'**organisation** et sur le **personnel** à mettre en place,

- *quels sont les états du système d'information qui nécessitent la mise en place de mesures de sécurité* ?
  le sixième chapitre traite des principes de sécurité liés au cycle de vie du système d'information.

Il peut paraître surprenant au responsable de l'élaboration d'une politique de sécurité qu'aucun chapitre n'ait été dédié à la question suivante : *contre quels risques doit-on se protéger* ?

En fait, la réponse à cette question a rang de principe dans le chapitre 6 intitulé "Principe de spécifications pour le développement du système d'information sécurisé". En effet, et tout au moins sur le plan théorique, l'analyse des risques nécessite une étude complète du système d'information. Or, une telle étude ne peut raisonnablement avoir lieu qu'une fois atteint un degré de connaissance suffisant des éléments composant le système comme, par exemple, le recensement et l'attribution d'une valeur aux informations et aux biens de l'organisme. De plus, tant que l'organisme ne connaît pas de restructuration ou de diversification de ses activités, la pérennité des principes énoncés dans la politique de sécurité interne s'oppose à l'instabilité des événements conjoncturels et humains qui génère une évolution permanente des risques. Aussi, répondre prématurément à la question posée peut conduire à une identification très incomplète des risques pesant sur le système d'information. Ainsi, le présent guide préconise de situer les principes retenus pour une politique de sécurité interne en amont de l'analyse de risques du système d'information.

Symboles utilisés

- Une règle précédée du symbole "✔" signifie qu'elle est une règle de base et, qu'à ce titre, les organismes qui sont candidats pour l'adoption d'un profil minimum de sécurité devraient l'adopter ; c'est ainsi que la pratique peut rendre, de facto, certaines règles obligatoires comme, par exemple, la règle relative au plan de reprise d'activité.

- Une règle précédée du symbole "▲" souligne le caractère majeur pour les organismes sensibles : précisons que le caractère obligatoire de certaines règles, au sens de la réglementation, se situe au niveau de leur mise en œuvre et non de leur déclaration dans une politique de sécurité. A titre d'exemple, citons les règles relatives à l'évaluation pour les administrations de l'État.

- En revanche, les règles non précédées d'un symbole recèlent un caractère spécifique qui est lié à l'identité de l'organisme et, en dehors de contextes très particuliers, elles peuvent s'avérer inapplicables ; ainsi, la règle qui prévoit la rotation des personnes aux postes sensibles ne peut pas être toujours appliquée, dès lors que la ressource en personnel qualifié est insuffisante.

Trigrammes de chapitre

Pour faciliter le repérage d'une règle, celle-ci est précédée d'un trigramme désignant le chapitre et d'un numéro d'identification à l'intérieur du chapitre :

- **PSI** pour le 1er chapitre, se rapportant au principe général pour une PSI,
- **INF** pour le 2ème chapitre, se rapportant à l'information,
- **BPH** pour le 3ème chapitre, se rapportant aux biens physiques,
- **OGS** pour le 4ème chapitre, se rapportant à l'organisation de la sécurité,
- **PER** pour le 5ème chapitre, se rapportant au personnel,
- **CVE** pour le 6ème chapitre, relatif au cycle de vie du système d'information.

Énoncés de règle

Le formalisme utilisé pour l'écriture des règles, "Une règle prévoit...", ne signifie pas que l'énoncé de la règle est en lui-même suffisant pour être applicable en tant que consigne ou mesure opérationnelle : il ne fait que traduire l'expression de la volonté de la hiérarchie de voir inscrire dans les habitudes de travail tel ou tel aspect de la sécurité et il signifie ce à quoi il est nécessaire de veiller.

Commentaires de règle

Les commentaires de règle ne sont que des illustrations permettant de comprendre le sens des mots ou concepts utilisés, ainsi que les incidences, pour le système d'information, de l'absence de la règle proposée et, dans certains cas, de suggérer quelques procédures ou consignes qu'il conviendrait d'adopter.

Polices de caractères utilisées

Des polices de caractères différentes ont été utilisées pour les règles de sécurité et leurs commentaires : les règles sont écrites en caractère **gras** et les commentaires en caractères *italiques*.

Chapitre 1

Principe général pour une politique de sécurité interne

Rappel : "✓" : règle de base - "▲" : règle à caractère majeur pour les organismes sensibles

✓▲ **PSI-001** **Une règle prévoit la responsabilité générale pour la sécurité du système d'information de l'organisme**

La nomination d'un responsable de la sécurité permet de veiller au respect d'une politique de sécurité interne à tous les échelons et domaines de l'organisme.

Ce responsable, rattaché à la direction de l'organisme doit pouvoir faire prévaloir l'aspect sécuritaire sur les intérêts particuliers et intégrer la sécurité dans tous les projets touchant les systèmes d'information.

La mise en place de cette fonction révèle l'importance donnée par l'organisme à sa politique de sécurité.

▲ **PSI-002** **Une règle prévoit les responsabilités pour l'élaboration et la mise en œuvre d'une politique de sécurité interne**

La politique de sécurité interne concerne toutes les fonctions vitales d'un organisme ; en effet, celui-ci ne pourrait généralement pas supporter une défaillance prolongée de son système d'information.

De ce fait, la politique de sécurité interne revêt un intérêt stratégique : une règle peut définir les responsabilités pour son élaboration au sein, par exemple, d'un comité de pilotage.

De plus, dans la phase de mise en œuvre de la politique de sécurité, la règle établit les responsabilités des autorités qualifiées dans la mise en place et le contrôle des consignes de sécurité pour l'installation et l'exploitation des moyens composant le système d'information.

Elle met tout particulièrement en évidence, la nécessité d'une intégration de la sécurité dès la conception et le développement de nouveaux projets intéressant le système d'information.

Page laissée blanche

Chapitre 2

Principes de sécurité liés à l'information

Rappel : "✓" : règle de base - "▲" : règle à caractère majeur pour les organismes sensibles

L'information, sous réserve qu'elle soit pertinente - donc utile -, est devenue au même titre que tout autre matière première une nécessité vitale pour l'accomplissement des activités d'un organisme.

Aussi, parmi toutes les définitions du concept d'information, nous suggérons de présenter celle, plus délimitée mais plus en rapport avec le titre de ce chapitre, "d'information utile" : "L'information utile est celle dont ont besoin les différents niveaux de décision de l'entreprise ou de la collectivité concernés pour élaborer et mettre en œuvre de façon cohérente la stratégie et les tactiques nécessaires à l'atteinte des objectifs définis (innovation technologique, produits, parts de marchés, performances, etc.). Les actions qui en découlent s'ordonnent au sein de l'entreprise en un cycle ininterrompu, générateur d'une vision partagée des objectifs à atteindre"[31] .

2.1. Principe de protection juridique des informations

Les règles de sécurité énoncées dans ce paragraphe sont l'application des textes législatifs et des recommandations en vigueur (voir les annexes 5 à 7) portant sur le principe de la protection juridique des informations comme, par exemple, le Code de la propriété intellectuelle.

✓ ▲ **INF-001** **Une règle prévoit les directives d'application pour la protection juridique des informations de l'organisme**

Cette règle vise à sensibiliser le personnel sur le devoir de protection juridique des informations qu'il utilise ou qui lui sont confiées afin de diminuer le risque de détournement ou d'appropriation par des tierces personnes.

Les directives d'application se réfèrent, en partie, au principe de responsabilité du personnel et, plus particulièrement, à la règle relative à la notion de responsable-détenteur (PER-007).

[31] D'après l'article de J. PICHOT-DUCLOS paru dans la revue Défense nationale, intitulé "L'intelligence économique, arme de l'après-guerre froide", décembre 1993, pages 83 à 104

✓ ▲ **INF-002** **Une règle prévoit la protection des informations confiées à l'organisme**

Cette règle permet de s'assurer du bon respect de la loi et de la réglementation existante.

Les informations détenues provisoirement par l'organisme et qui comportent, du fait de leur propriétaire, une classification ou une mention particulière de protection doivent être protégées rigoureusement selon les mêmes mesures qui sont appliquées par l'organisme d'origine. Ces mesures peuvent découler d'instructions interministérielles comme, par exemple, celle traitant du respect de la classification des informations liées au secret de défense (IGI n°900), de la protection des informations concernant le patrimoine national (II n°486) ou de l'établissement d'un marché de défense (II n°2000) ; dans le cadre d'un contrat particulier liant plusieurs organismes, les mesures de protection relèvent de l'application du Code civil.

2.2. Principe de typologie des informations nécessitant une protection

L'adoption d'une typologie a pour but l'identification des informations nécessitant une protection en vue de leur regroupement en classes de même niveau d'exigence de sécurité.
La réglementation en vigueur distingue deux types d'informations :

- **les informations relevant du secret de défense** définies dans l'IGI n°900 et pour lesquelles le niveau d'exigence de sécurité n'est pas négociable ; la typologie retenue dans l'article 5 décrit **les informations traitées**, principalement sous l'angle de la confidentialité et de l'intégrité et **les informations traitantes** dites **vitales** pour le fonctionnement du système, principalement sous l'angle de la disponibilité et de l'intégrité,

- **les informations** dites **sensibles ne relevant pas du secret de défense** au sens de la Recommandation n°901 et pour lesquelles le niveau d'exigence de sécurité est négociable en fonction des considérations environnementales propres à l'organisme.

Toutefois une autre typologie, couramment retenue en milieu non gouvernemental, distingue :

- **les informations sensibles**, qu'elles relèvent ou non du secret de défense,

- **les informations vitales** pour l'exercice de la mission ou du métier de l'organisme,

les informations nominatives au sens de la Loi informatique et libertés.

De plus, certains experts élargissent cette typologie aux notions :

- **d'informations stratégiques** qui sont des informations non nécessairement sensibles ou vitales mais dont l'acquisition est nécessaire pour atteindre les objectifs correspondant aux orientations stratégiques de l'organisme,
- **d'informations coûteuses** qui sont des informations dont la collecte, le traitement, le stockage ou la transmission nécessitent un délai important ou un coût d'acquisition élevé.

Cette deuxième typologie offre l'avantage d'élargir la notion d'information ne relevant pas du secret de défense à celles qui puisent leur légitimité sur la préservation des intérêts particuliers de l'organisme. Elle ne minimise pas pour autant l'importance qui doit être accordée à l'identification et à la protection de l'information relevant du secret de défense selon la réglementation en vigueur.

Remarque : Dans le secteur non gouvernemental, il est également courant d'utiliser cette typologie pour définir une échelle de valeurs des informations permettant ainsi d'apprécier le risque qui peut leur être attaché, (à savoir, niveau stratégique, critique, sensible et de faible risque)

✓ ▲ INF-003 Une règle prévoit l'adoption d'une classification des informations sensibles

Les informations sensibles sont celles dont la divulgation ou l'altération peuvent porter atteinte aux intérêts de l'État, tout comme à ceux de l'organisme pour lequel un préjudice financier, par exemple, peut le conduire à la faillite. Il faut par conséquent, assurer principalement leur confidentialité et, assez souvent, répondre à un besoin important d'intégrité.

Les informations classées dans cette catégorie sont :

- *d'une part, les informations relevant du secret de défense au sens de l'article 5 de l'IGI n°900 ; l'organisme est alors tenu de respecter les règles de classification spécifiées dans la réglementation,*

- *d'autre part, les informations sensibles non classifiées de défense au sens de l'article 4 de la recommandation n°901, c'est-à-dire, celles liées à la mission ou au métier de l'organisme (par exemple, au savoir-faire technologique), celles relatives aux propositions commerciales ou bien encore aux renseignements sur l'état de la sécurité (par exemple, les résultats d'audits internes).*

La classification retenue vise à faciliter le contrôle et, par conséquent, à améliorer la protection des informations sensibles. Pour celles qui ne ressortissent pas de l'IGI 900, la classification choisie doit être approuvée par l'organisme.

▲ INF-004 Une règle prévoit l'adoption d'une classification des informations vitales

Les informations vitales sont celles dont l'existence est nécessaire au bon fonctionnement de l'organisme. Il faut principalement assurer leur disponibilité et, assez souvent, répondre à un besoin important d'intégrité.

Les informations que l'on peut identifier comme vitales sont:

- *d'une part, les informations traitantes relevant du secret de défense au sens de l'article 6 de l'IGI n°900,*

- *d'autre part, les informations traitantes ne relevant pas du secret de défense au sens de l'article 5 de la Recommandation n901 mais nécessaires pour le fonctionnement du système, ainsi que des informations traitées (sortant du champ de l'article 5) comme, par exemple, les nomenclatures d'articles pour une unité de production.*

  La classification retenue vise à faciliter le contrôle et, par conséquent, à améliorer la protection des informations vitales. Pour celles qui ne ressortissent pas de l'IGI 900, la classification choisie doit être approuvée par l'organisme. En particulier, il peut être prévu la spécification d'un seuil minimum de disponibilité des informations vitales (traitées ou traitantes) en dessous duquel le système d'information est déclaré inopérant.

INF-005 Une règle prévoit l'adoption d'une classification des informations nominatives.

Cette règle est une application de la loi "Informatique et Libertés" dont l'article 4 définit la notion d'information nominative : "les informations nominatives sont celles qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale".

La classification retenue vise à faciliter le contrôle et, par conséquent, à améliorer la protection des informations nominatives conformément à la loi ; elle peut s'appuyer sur des critères propres à l'organisme comme, par exemple, un domaine particulier (médical, recrutement, etc.), le type de sondage ou d'enquête, le lieu de traitement ou de stockage.

▲ **INF-006** **Une règle prévoit l'adoption d'une classification des informations stratégiques**

Les informations stratégiques sont des informations non nécessairement sensibles ou vitales mais dont la connaissance est nécessaire pour atteindre les objectifs correspondant aux orientations stratégiques de l'organisme. Elles peuvent être protégées par des textes législatifs cités en annexe 7.1., mais peuvent aussi faire l'objet de contrats, de conventions ou de protocoles d'accord protégés par le Code civil.

La classification retenue vise à faciliter le contrôle et, par conséquent, à améliorer la protection des informations stratégiques ; elle peut s'appuyer sur des critères propres à l'organisme comme, par exemple, un secteur particulier (études, innovations, marchés, etc.), le niveau de valeur accordé et la durée de validité.

INF-007 **Une règle prévoit l'adoption d'une classification des informations coûteuses**

Les informations coûteuses sont des informations qui font partie du patrimoine de l'organisme et dont la collecte, le traitement, le stockage ou la transmission nécessitent un délai important ou un coût d'acquisition élevé. Les dispositions législatives énumérées dans la règle précédente peuvent être appliquées à cette catégorie.

La classification retenue vise à faciliter le contrôle et, par conséquent, à améliorer la protection des informations coûteuses ; elle peut s'appuyer sur des critères propres à l'organisme comme, par exemple, un secteur particulier (études, innovations, etc.), la provenance et le niveau de coût.

2.3. Principe de continuité dans la protection des informations

Le principe de continuité dans la protection des informations s'inscrit dans les phases de recueil, de diffusion interne ou externe à l'organisme et de stockage ; pour ce faire, il est essentiel de disposer de critères, approuvés par l'organisme, permettant de trier, de diffuser et de stocker les informations autres que celles relevant du secret de défense et pour lesquelles s'applique la réglementation.

La protection requise pour le traitement des données en phase d'exploitation du système d'information est un aspect important qui est traité au chapitre 5, intitulé "Principes de sécurité liés au cycle de vie du système d'information".

INF-008 Une règle prévoit les critères d'appréciation de la nature et de la valeur des informations recueillies

En dehors des informations relevant du secret de défense et des informations nominatives pour lesquelles les textes législatifs en vigueur doivent être appliqués, il est utile de disposer de critères propres à l'organisme, et liés à ses orientations stratégiques, pour apprécier la nature et la valeur des informations recueillies.

Ces critères portent principalement sur le contrôle de l'origine des informations, sur l'appréciation de leur intérêt et de leur validité par rapport à leur cycle de vie dans le processus opérationnel de production :

- *le contrôle de l'origine des informations (provenance étrangère, domaine public, client, fournisseur, etc.) revêt un caractère majeur pour la sécurité ; des critères plus spécifiques peuvent alors être prévus en fonction de la provenance pour juger d'une éventuelle compromission avant leur collecte, de leur exactitude, de leur validité et de leur correcte présentation pour le système,*

- *l'appréciation de l'intérêt et de la validité de l'information recueillie se fait par application de critères clairement définis par la direction de l'organisme et qui peuvent porter sur un domaine particulier (R&D, cercles de qualité, veille technologique, etc.).*

A ces contrôles, il est souvent associé celui de l'intégrité des supports de l'information, lorsque celle-ci est déjà codifiée sous forme de données exploitables par le système d'information.

▲ INF-009 Une règle prévoit les critères de diffusion interne des informations

Afin d'éviter les indiscrétions et les fuites, les informations et généralement les supports associés, ne doivent pouvoir être utilisés que dans un environnement répondant aux exigences de sécurité définies par l'organisme.

Le contrôle de la diffusion interne a pour but de s'assurer que les informations sont rendues disponibles exclusivement aux personnes ayant le besoin de les connaître dans le cadre de leur travail. Un contrôle permet également de vérifier que la recopie d'informations est conforme aux prérogatives prévues par la loi (droit d'auteur, copyright) et à la réglementation (secret de défense).

✓ ▲ INF-010 Une règle prévoit les critères de diffusion externe des informations

La mise à disposition non contrôlée d'informations nécessitant une protection peut porter préjudice à l'organisme (par exemple, perte de crédibilité ou d'image de marque, récupération de savoir-faire, etc.).

La mise en place de critères permet de s'assurer que les informations transmises à l'extérieur d'un organisme, si elles sont de nature confidentielle, impose un contrôle préalable d'habilitation du récepteur ou une clause contractuelle liant les organismes concernés ; dans le cas d'informations nominatives, la communication doit être en accord avec la loi.

Par ailleurs, dans le cadre de cette règle, il peut être envisagé que la diffusion externe des informations soit effectuée par du personnel habilité et selon une procédure d'autorisation préalable.

✓ ▲ INF-011 Une règle prévoit les normes de conservation et de destruction des informations nécessitant une protection

Les catégories d'informations précédemment décrites nécessitent des conditions de stockage et de destruction adaptées. En ce qui concerne les informations relevant du secret de défense, la réglementation précise les mesures à prendre suivant leur niveau de classification. Pour les autres catégories, les mesures sont adaptées à l'environnement propre à l'organisme et doivent demeurer cohérentes entre elles.

En particulier, le contrôle préalable des bonnes conditions de stockage revêt un aspect fondamental dès lors que l'information est confiée contractuellement à un organisme. La destruction d'urgence peut, pour certains organismes, revêtir un aspect majeur en situations exceptionnelles (émeutes, guerre civiles, etc.) mais, plus couramment, des normes précises peuvent être adoptées pour l'élimination de l'information périmée qui conserve un caractère résiduel de confidentialité.

Page laissée blanche

Chapitre 3

Principes de sécurité liés aux biens physiques

Rappel : "✓" : règle de base - "▲" : règle à caractère majeur pour les organismes sensibles

Les principes de sécurité présentés dans ce chapitre s'appliquent aux biens physiques constitués par :

- **l'infrastructure** au sein de laquelle fonctionne le système d'information à savoir, les sites d'installation, les bâtiments et les locaux abritant le système d'information,

- **les matériels** composant le système d'information à savoir, les diverses unités utilisées pour la collecte, le traitement, la transmission, l'enregistrement et la conservation des informations,

- **les équipements de soutien** assurant les services nécessaires au fonctionnement des matériels composant le système d'information comme, par exemple, la fourniture d'énergie et de climatisation ; on range également dans cette catégorie la documentation, les matériels consommables lorsqu'ils représentent des ressources sensibles pour la mission ou le métier de l'organisme comme, par exemple, un stock de cartes à puce prépersonnalisées destiné à une application sensible,

- **les moyens de protection**, au sens du chapitre 2 de l'IGI 900, comprenant les équipements et mécanismes (matériels et logiciels) qui sont incorporés dans le système d'information pour assurer la disponibilité, l'intégrité et la confidentialité des informations.

Ce chapitre décrit les principes appliqués aux biens physiques du système d'information, à savoir :

- **le principe de protection**, qui a pour objet la réduction des risques identifiés ou redoutés,

- **le principe de gestion**, qui a pour objet la prise en compte et le suivi des biens physiques.

Les principes et les règles concernant la détention des biens physiques sont traités au chapitre 5, relatif au personnel ; ceux concernant l'utilisation sont traités au chapitre 6, relatif au cycle de vie du système d'information.

3.1. Principe de protection des biens physiques

Tout organisme, quel que soit son type d'activité et son niveau de vulnérabilité, est soumis à des menaces potentielles qui peuvent être accidentelles ou intentionnelles et entraîner la mise hors service, temporaire ou définitive, de tout ou partie du système d'information.

Les quatre éléments de l'environnement naturel (l'eau, l'air, la terre et le feu) engendrent des phénomènes qui font peser sur le système d'information les menaces accidentelles suivantes :

- celles résultant des phénomènes naturels provoqués par l'élément liquide comme, par exemple, l'inondation ou le gel,
- celles résultant de la transformation d'un élément gazeux comme, par exemple, la vapeur acide ou l'explosion,
- celles résultant des phénomènes générant des ondes de chocs comme, par exemple, les séismes,
- celles résultant de la transformation d'un champ d'énergie comme, par exemple, la chaleur ou la foudre.

A ces phénomènes naturels s'ajoutent les perturbations des matériels électroniques dus aux rayonnements électromagnétiques ou nucléaires (radars, antennes, lignes très haute tension, etc.) ; ces dysfonctionnements sont aussi le fait de défaillances matérielles ou humaines comme, par exemple, la panne d'un composant, une coupure d'électricité ou une erreur d'exploitation.

Quant aux menaces intentionnelles, elles correspondent à des actions qui visent principalement à nuire (vol, sabotage, destruction, etc.).

✓ ▲ **BPH-001** **Une règle prévoit la prise en compte des contraintes opérationnelles de l'organisme dans la mise en place des moyens et procédures de sécurité physique**

Cette règle est une application du principe général de pluridisciplinarité de l'OCDE, à savoir :

"Les mesures, pratiques et procédures de sécurité des systèmes d'information doivent prendre en compte toutes les considérations pertinentes qu'elles soient d'ordre technique ou administratif et concernant l'organisation, l'exploitation, le commerce, l'éducation ou le droit".

La mise en place de moyens et procédures de sécurité physique qui ne prend pas en compte les contraintes de l'organisme peut constituer

une entrave au bon fonctionnement des tâches opérationnelles et engendrer un rejet de la part du personnel vis-à-vis de la sécurité.

▲ BPH-002 Une règle prévoit la gradation des mesures de protection physique

Cette règle est une application du principe général de proportionnalité de l'OCDE, à savoir : "Les niveaux, coûts, mesures, pratiques et procédures de sécurité doivent être appropriés et proportionnés à la valeur et au degré de dépendance envers les systèmes d'information, ainsi qu'à la gravité, la probabilité et l'ampleur des éventuels préjudices".

***Les mesures de protection** des biens physiques ont pour objectif de réduire l'ampleur des atteintes, principalement dans le domaine de la disponibilité et de l'intégrité.*

L'absence de solutions universelles capables de répondre à toutes les formes de menaces oblige l'organisme à mettre en œuvre un ensemble de mesures susceptibles de contrecarrer le cheminement d'une attaque et de réparer les dommages causés : ce sont les mesures de prévention, de détection, de réaction et de recouvrement.

***Les mesures de prévention** visent à diminuer la probabilité d'apparition d'un sinistre. Elles consistent, par exemple, à porter attention à la localisation de certains locaux (comme les bandothèques, les salles d'archives, les canalisations, les salles de rangement de produits dangereux) face aux risques d'incendie ou d'inondation ou à surveiller la conformité de l'utilisation des matériels.*

***Les mesures de détection** visent à donner l'alerte lors d'une tentative d'intrusion ou du déclenchement d'un sinistre dans le périmètre du système d'information. Elles doivent également permettre de localiser cette alerte. Ces mesures se traduisent par la mise en place aux endroits critiques de moyens de détection et d'alerte comme, par exemple, des capteurs de chaleur ou des caméras de surveillance.*

***Les mesures de réaction** visent à lutter contre un sinistre déclaré en vue de réduire son impact. Ces mesures se traduisent par le déclenchement de moyens d'interventions prévus par l'organisme comme, par exemple, un service de lutte contre l'incendie.*

***Les mesures de recouvrement** visent à limiter les conséquences d'un sinistre et à faciliter le retour au fonctionnement normal du système d'information. Elles peuvent se traduire par l'activation de moyens de secours ou par la désactivation de fonctions de sécurité comme, par exemple, la suppression temporaire du contrôle d'accès*

physique dans le cadre d'un fonctionnement de la sécurité en mode dégradé.

Pour l'ensemble des sinistres redoutés par l'organisme, les mesures choisies devraient être graduelles, afin d'offrir un niveau de résistance suffisant pour contrecarrer ou atténuer l'attaque.

▲ **BPH-003 Une règle prévoit l'adéquation des mesures de protection aux catégories de biens physiques**

Cette règle peut être rattachée au principe général d'intégration de l'OCDE, à savoir :
"Les mesures, pratiques et procédures de sécurité des systèmes d'information doivent être coordonnées et harmonisées entre elles et les autres mesures, pratiques et procédures de l'organisme afin de réaliser un dispositif de sécurité cohérent".

Cette règle indique que les mesures dont il est fait mention à la règle précédente peuvent être déclinées selon les trois catégories de biens physiques à savoir, l'infrastructure, les matériels et les équipements de soutien.

▲ **BPH-004 Une règle prévoit le contrôle permanent de l'intégrité des moyens de protection**

Le contrôle de l'intégrité des moyens de protection est un aspect fondamental de la sécurité. Cette règle concerne les dispositifs de sécurité auxquels il est fait confiance pour assurer la protection des informations traitées : il s'agit des équipements, des mécanismes (matériels et logiciels) et de la documentation qui leur est associée, nommés dans l'article 10 de l'IGI 900, "Articles Contrôlés de Sécurité des Systèmes d'Information" (ACSSI).

Le maintien de cette confiance justifie un contrôle de l'intégrité de ces moyens qui ont un cycle de vie : ils sont conçus, réalisés, utilisés, réparés puis réformés ou détruits. Leur intégrité, condition fondamentale de l'efficacité de la sécurité, est garantie par la mise en œuvre de mesures de gestion spécifiques.

3.2. Principe de gestion des biens physiques

La base essentielle d'une politique de sécurité repose sur la connaissance des biens physiques qui composent le système d'information. La mise en œuvre d'une gestion de ces biens en permet un suivi rigoureux.

Le principe de cette gestion regroupe les règles portant sur le découpage de l'infrastructure en zone de sécurité, la continuité dans la gestion ainsi que la gestion spécifique des biens physiques nécessitant une protection.

▲ **BPH-005 Une règle prévoit le découpage de l'infrastructure en zones de sécurité**

Les sites, les bâtiments et les locaux contenant des biens matériels ou immatériels (les informations et leurs supports associés, les matériels constitutifs du système d'information) ou abritant des activités critiques au regard de la sécurité, doivent être contrôlés tout particulièrement au niveau de leurs accès.

Une zone de sécurité est une zone dans laquelle des dispositions permanentes sont prises pour contrôler les mouvements du personnel et des matériels, ainsi que pour détecter et empêcher toute écoute.

Un découpage de l'infrastructure en zones de sécurité facilite la mise en place de dispositifs adaptés, tout particulièrement pour le contrôle de la circulation du personnel par attribution de droits d'accès spécifiques aux zones. Ces droits peuvent être liés aux postes de travail et aux niveaux de responsabilité.

BPH-006 Une règle prévoit la continuité dans la gestion des biens physiques

La gestion des biens physiques est assurée tout au long de leur cycle de vie : phases d'affectation, d'installation, de fonctionnement, d'entretien, de mise au rebut et de destruction. Ces biens peuvent également être amenés à changer de propriétaire ou de responsable, d'environnement ou d'usage (prêt de matériels pour une exposition, réaffectation d'un matériel dans le cadre d'un projet nouveau).

La règle prévoit que les mesures choisies offrent une protection continue quelles que soient les évolutions ou les changements d'utilisation des biens physiques.

Cette continuité de gestion repose sur l'adoption d'une classification (incluant, le cas échéant, la classification de défense au sens de l'IGI 900), sur le suivi des biens physiques depuis leur mise en service, leur évolution jusqu'à leur remplacement. Les principales mesures qui découlent de cette règle intéressent le recensement, le marquage des biens et les mesures spécifiques de protection physique correspondant à leur état (prêt, maintenance, etc.) ou à leur classification :

- *le recensement des biens physiques permet d'identifier ceux nécessitant une protection,*
- *l'opération de marquage est la matérialisation concrète de la reconnaissance qu'un élément appartient à une classe donnée,*
- *les mesures spécifiques de protection physique désignent les actions à entreprendre suivant la classification choisie. Par exemple, un calculateur marqué "Confidentiel XX" devra se situer dans un environnement physique adapté à ce niveau de protection, comme celui d'une "zone réservée".*

▲ BPH-007 Une règle prévoit la gestion spécifique des biens physiques nécessitant une protection

La gestion des biens physiques nécessitant une protection comprend l'adoption d'une classification ou d'une typologie, les mesures de gestion de ces biens et les mesures de protection tout au long de leur vie.

L'article 10 de l'IGI n°900 définit ainsi les biens physiques faisant l'objet d'une classification de défense : "Tout document, logiciel ou matériel qui, par son intégrité ou sa confidentialité contribue à la sécurité d'un système d'information, reçoit la mention ACSSI qui rappelle que sa gestion et sa protection doivent être assurées conformément aux prescriptions de l'instruction ministérielle relative aux Articles Contrôlés de la Sécurité des Systèmes d'Information".

Pour les biens physiques non classifiés de défense, l'adoption d'une typologie permet de les regrouper suivant leur nature et leur affectation. Des classes de protection sont établies en fonction du niveau d'exigence de sécurité, c'est-à-dire des critères de confidentialité, d'intégrité et de disponibilité attachés à ces biens pour en garantir une surveillance continue. La typologie adoptée est spécifique à la mission ou au métier, à la culture et aux contraintes propres à l'organisme.

Chapitre 4
Principes liés à l'organisation de la sécurité

Rappel : "✓" : règle de base - "▲" : règle à caractère majeur pour les organismes sensibles

L'adhésion de la hiérarchie à une politique de sécurité interne ne peut suffire à garantir la protection d'un système d'information en l'absence d'une organisation dédiée à la sécurité. En effet, les responsables de tout niveau doivent pouvoir faire appel à des spécialistes capables de prendre en charge l'élaboration de la réglementation, la formation du personnel, la coordination et le contrôle des actions de sécurité. Les principes préconisés dans ce chapitre pour atteindre ces objectifs, reposent sur la mise en place d'une structure de sécurité et sur la continuité de l'action de contrôle.

4.1. Principe d'une structure de la sécurité

La structure de sécurité est l'organisation mise en place pour la gestion des différentes composantes de la sécurité et de leurs évolutions ; elle implique un partage des responsabilités entre les différents niveaux hiérarchiques, à savoir :

- le niveau décisionnel,
- le niveau de pilotage,
- le niveau opérationnel.

Le principe de responsabilité du personnel est formulé au chapitre 5.

✓ ▲ **OGS-001 Une règle prévoit les responsabilités du niveau décisionnel**

Il appartient au niveau décisionnel de prendre toute disposition pour concevoir et mettre en place une sécurité adaptée aux besoins de l'organisme et de s'assurer du respect de la politique de sécurité interne.

Pour un organisme ministériel, ce niveau est celui ***du haut fonctionnaire de défense*** *(HFD) qui reçoit délégation du ministre ; il est responsable de l'application des dispositions relatives à la sécurité de défense, à la protection du secret et à la sécurité des systèmes d'information.*

*Il peut être aidé dans sa mission par un **fonctionnaire de sécurité des systèmes d'information** (FSSI) dont les principales missions sont (IGI 900, article 19) :*

- *de préciser les modalités d'application des instructions interministérielles,*
- *d'élaborer et de contrôler l'application des instructions particulières à son ministère,*
- *d'organiser la sensibilisation des autorités,*
- *d'assurer la liaison avec les commissions interministérielles et ministérielles spécialisées.*

*Pour un organisme public ou privé, ce niveau est celui **d'un haut responsable de la sécurité** qui reçoit délégation du **comité de direction** ; il est aidé dans sa mission par un **comité de sécurité.***

Le comité de direction fixe, sur proposition du haut responsable de la sécurité, les grandes orientations en matière de sécurité du système d'information, en accord avec les objectifs de l'organisme et les différentes politiques mises en œuvre (politique de gestion du personnel, budgétaire, de production, etc.). Ce comité peut être, par ailleurs, l'instance de validation de la politique de sécurité interne.

Le haut responsable de la sécurité veille à l'application de la politique de sécurité. Il participe aux délibérations du comité de direction dont il est le conseiller pour toutes les questions relatives à la sécurité telles que la définition des objectifs, l'allocation des ressources et du personnel.

Le comité de sécurité, présidé par le haut responsable de la sécurité, réunit les responsables de la sécurité des différentes fonctions de l'organisme. Il veille à la coordination de la mise en œuvre de la politique de sécurité interne : il vérifie tout particulièrement la cohérence des règles de sécurité et arbitre les conflits éventuels avec les autres règles et pratiques en usage dans l'organisme.

*Une **équipe de sécurité** du système d'information, à la disposition du haut fonctionnaire de défense (ou du haut responsable de la sécurité), peut être constituée si les besoins de l'organisme l'exigent. Elle rassemble des spécialistes en informatique et en réseaux de télécommunication, formés à la sécurité et dont les principales missions sont :*

- *la préparation et la coordination des activités de sécurité,*
- *l'évaluation périodique des vulnérabilités,*
- *la recherche des solutions techniques et l'élaboration des procédures,*

- *la mise en place de programmes de sensibilisation et de formation,*
- *les expertises de sécurité sur demande du comité de direction.*

▲ OGS-002 Une règle prévoit les responsabilités du niveau de pilotage

*Ce niveau est celui des **autorités qualifiées** qui sont responsables de la sécurité du système d'information dont ils ont la charge (IGI 900, article 20 et Recommandation 901, article 19).*

Leur mission est d'adapter la politique de sécurité interne à leur niveau (direction, service, établissement, etc.) et, plus précisément :

- *de s'assurer du respect des dispositions contractuelles et réglementaires,*
- *d'élaborer les consignes et les directives internes,*
- *de s'assurer que les contrôles internes de sécurité sont correctement effectués,*
- *d'organiser la sensibilisation du personnel.*

Ces autorités peuvent s'appuyer sur les compétences de l'équipe de sécurité.

▲ OGS-003 Une règle prévoit les responsabilités du niveau opérationnel

A tous les niveaux, les autorités hiérarchiques sont personnellement responsables de l'application des mesures, définies par les autorités qualifiées, destinées à assurer la sécurité des systèmes d'information (IGI 900, article 20 et Recommandation 901, article 19).

*Pour permettre à chaque site, service ou unité la mise en œuvre des consignes et des procédures, les autorités hiérarchiques se font assister par un ou plusieurs **agents de la sécurité** chargés principalement :*

- *de la gestion et du suivi des articles contrôlés de sécurité des systèmes d'information se trouvant sur le ou les sites où s'exercent leurs responsabilités,*
- *du contrôle des personnes, des informations et de la sécurité des systèmes et des réseaux.*

Ces agents sont les correspondants privilégiés de l'équipe de sécurité.

Ils peuvent également avoir en charge les ressources communes à plusieurs unités opérationnelles. Leur rôle est alors la mise en œuvre des mesures de protection compatibles avec les objectifs des unités et la résolution locale des problèmes de sécurité. En l'absence de telles mesures, il pourrait s'ensuivre un arbitrage difficile entre une tâche fonctionnelle et une action de sécurité.

4.2. Principe de continuité du contrôle de la sécurité

La notion de continuité utilisée dans ce principe fait référence à la nécessité de l'action de contrôle et à la régularité de sa mise en œuvre :

- la nécessité de contrôle signifie qu'il est exercé par tous les niveaux de responsabilités précédemment définis et selon leurs prérogatives respectives,

- la régularité de mise en œuvre signifie que les actions de contrôle sont prévues dans le plan de charge de tous les niveaux de responsabilités.

▲ **OGS-004 Une règle prévoit les circonstances retenues par le niveau décisionnel pour mettre en œuvre les contrôles de sécurité**

Le responsable de la sécurité contrôle la cohérence et la validité des programmes d'équipement de son organisme par rapport aux grandes orientations de la sécurité.

Par ailleurs, et dans la cadre d'enquêtes déclenchées à sa demande, des contrôles sont mis en œuvre par l'équipe de sécurité : ces contrôles sont caractérisés par leur portée et leur ampleur :

- *leur portée fait référence à la définition du niveau de détail (c'est la composante verticale),*

- *leur ampleur fait référence aux divers éléments pris en compte dans le contrôle (c'est la composante horizontale).*

Il est essentiel, pour le climat de confiance du personnel et le bon déroulement de la mission de l'organisme, d'adopter une gradation dans les contrôles de sécurité, fonction de circonstances clairement énoncées par le niveau décisionnel ; en dehors d'un contexte judiciaire ou disciplinaire, ces contrôles devraient être accompagnés d'une action de communication et de préparation du personnel.

OGS-005 Une règle prévoit les modalités des contrôles par le niveau de pilotage

L'évaluation périodique des vulnérabilités est nécessaire pour apprécier le niveau de sécurité du système d'information.

Les autorités qualifiées, aidées par l'équipe de sécurité de l'organisme, fixent les modalités techniques, les méthodes et les outils nécessaires à la sécurité ; elles en contrôlent le bon usage et l'efficacité selon des critères énoncés par le niveau décisionnel.

Ces contrôles qui s'inscrivent dans le cadre d'inspections ou d'audits de sécurité planifiés, couvrent les différents domaines de la sécurité des systèmes d'information (sécurité des informations, sécurité physique, organisation de la sécurité, sécurité du personnel, sécurité du fonctionnement du système d'information).

Pour les contrôles nécessitant le recours au personnel opérationnel et aux ressources techniques, une planification par le niveau du pilotage s'impose pour qu'ils ne constituent pas une gêne au bon déroulement de la mission de l'organisme.

▲ **OGS-006 Une règle prévoit la continuité du contrôle de sécurité par le niveau opérationnel**

Les agents de sécurité effectuent les contrôles qui leur sont impartis par application de seuils de tolérance fixés par l'autorité qualifiée. L'observation d'écarts répétés, liés par exemple aux contraintes de l'exploitation, ou bien le changement d'état du système d'information peuvent conduire le niveau de pilotage à une modification de ces seuils.

Leurs actions de contrôle sont étroitement liées à l'exécution des tâches opérationnelles et elles intéressent (IGI 900, art.20):

- *la protection des personnes comme, par exemple, la tenue à jour de la liste du personnel employé à titre permanent et, le cas échéant, affecté au traitement des informations,*

- *la protection des informations comme, par exemple, le contrôle de la destruction des informations classifiées qui doivent être expurgées du système,*

- *la protection des systèmes et réseaux comme, par exemple, le contrôle de la diffusion aux utilisateurs des éléments d'authentification pour les applications classifiées.*

Ces contrôles sont complémentaires de ceux confiés aux ingénieurs système, qui exploitent les journaux d'audits.

Page laissée blanche

Chapitre 5
Principes de sécurité liés au personnel

Rappel : "✓" : règle de base - " ▲ " : règle à caractère majeur pour les organismes sensibles

Le comportement et les agissements du personnel dans le cadre de ses activités peuvent avoir une forte incidence sur la préservation des intérêts de l'organisme et, tout particulièrement, sur la sécurité des systèmes d'information.

Les principes présentés dans ce chapitre sont :

- le principe de sélection du personnel, qui a pour but la protection de l'organisme contre la malveillance interne,
- le principe de contrôle de l'affectation du personnel à un poste de travail sensible, qui prend en compte les résultats d'enquêtes individuelles et les statuts particuliers du personnel (stagiaire, vacataire, etc.),
- le principe de sensibilisation, qui permet une plus grande compréhension et l'adhésion du personnel aux divers aspects de la sécurité des systèmes d'information,
- le principe de responsabilité du personnel, qui vise l'intégration des procédures et des contrôles de sécurité dans les activités opérationnelles.

5.1. Principe de sélection du personnel

D'après l'observatoire de la sinistralité des risques informatiques[31], la principale menace pesant sur les systèmes d'information est la malveillance interne, qui représente plus de la moitié des sinistres déclarés (vol d'informations, détournement de logiciels, sabotage de matériels ou de locaux, etc.).

Le principe de sélection du personnel vise à réduire la vulnérabilité de l'organisme face à cette menace ; il énonce les règles portant sur l'adoption de critères de sélection spécifiques pour le personnel travaillant sur le système d'information et d'une procédure d'habilitation pour les postes de travail sensibles.

[31] Mis en place depuis 1983 par l'APSAD, puis le CLUSIF et dont les statistiques établies, qui ne concernent pas le secteur gouvernemental, sont corroborées par le Comité européen des assurances.

✓ ▲ PER-001 Une règle prévoit l'adoption de critères de sélection pour le personnel travaillant sur les systèmes d'information sensibles

Cette règle concerne toutes les catégories de personnel qui sont amenées à travailler sur les systèmes d'information sensibles. Elle précise, pour les emplois touchant au fonctionnement et à l'utilisation du système, le mode de sélection à appliquer par l'organisme pour le recrutement du personnel et, tout particulièrement, les critères de sécurité requis pour chaque poste de travail[32]. Par exemple, l'exigence de références à des postes sensibles peut être prise en compte lors de procédures d'embauche.

Cette règle implique la possibilité de vérification des références de travail d'un candidat à un emploi ainsi que celles des personnes affectées temporairement à une activité nécessitant l'utilisation du système d'information.

▲ PER-002 Une règle prévoit l'adoption d'une procédure d'habilitation pour les postes de travail sensibles

La sensibilité d'un poste de travail fait référence au besoin de confidentialité et d'intégrité attaché aux informations, aux logiciels et aux matériels qu'il rassemble ; elle se définit selon les critères énoncés aux chapitres 1 et 2, mais peut aussi être lié à la localisation : un poste de responsable des relations humaines dans une région à fort risque social peut être considéré comme un poste sensible.

Pour un poste comportant des manipulations d'informations relevant du secret de défense, les habilitations du personnel sont définies par l'article 3 de l'IGI 1300 : "La procédure d'habilitation consiste à vérifier qu'une personne peut, sans risque pour la défense nationale, la sûreté de l'État ou sa propre sécurité, connaître des informations classifiées d'un niveau déterminé dans l'exercice de ses missions. Au terme de la procédure d'habilitation, l'autorité compétente décide d'admettre ou non la personne concernée à prendre connaissance d'informations classifiées au niveau exigé".

Pour les postes de travail sensibles n'utilisant pas des informations relevant du secret de défense, une procédure d'habilitation peut être utilisée sur le modèle de celle qui doit être appliquée dans le cadre des marchés de défense.

[32] Un poste de travail est un ensemble défini de tâches, de devoirs et de responsabilités qui constituent le travail habituel d'une personne.

5.2. Principe de contrôle de l'affectation du personnel aux postes de travail sensibles

Le principe de contrôle de l'affectation du personnel aux postes de travail sensibles a pour objet la prise en compte des résultats d'enquêtes individuelles et des statuts particuliers (stagiaire, vacataire, etc.).

Les règles attachées à ce principe visent principalement à réduire le risque de fuites d'informations sensibles vers l'extérieur de l'organisme ; elles traitent du cloisonnement des postes de travail sensibles et de la rotation du personnel à ces postes.

▲ PER-003 Une règle prévoit le cloisonnement des postes de travail sensibles

Le cloisonnement des postes de travail sensibles vise à lutter contre la fuite des informations représentant un enjeu pour les intérêts de l'État ou de l'organisme.

Pour la préservation des intérêts de l'État et, tout particulièrement dans le cadre de la protection du secret de défense, les décisions d'admission ou d'agrément aux informations classifiées d'un niveau donné, telles que définies dans les articles 10 à 12 de l'IGI n°1300, n'autorisent pas pour autant le bénéficiaire à accéder à toutes les informations relevant de ce niveau ; le besoin de connaître ces informations reste fonction de l'activité de la personne ou des dossiers particuliers qui lui sont confiés.

D'une manière identique, pour la préservation des intérêts propres à un organisme dont les informations ne relèvent pas du secret de défense, la connaissance des besoins en informations pour l'accomplissement de la mission ou du métier permet la mise en place d'un cloisonnement efficace des postes de travail.

PER-004 Une règle prévoit la rotation du personnel affecté aux postes de travail sensibles

La rotation du personnel peut, dans certains cas, éviter les risques de collusion et de diminution de la vigilance :

- *face au risque de collusion, elle permet de limiter les pressions de toute origine sur le personnel pouvant entraîner la divulgation des informations classifiées,*

- *face au risque de diminution de la vigilance, elle permet de limiter les erreurs, d'éviter la perte du réflexe du contrôle de la confidentialité et de l'intégrité des informations et des ressources du système allouées.*

5.3. Principe de sensibilisation pour la sécurité des systèmes d'information

Le principe général de sensibilisation de l'OCDE énonce : "Pour favoriser la confiance envers les systèmes d'information, les propriétaires, les fournisseurs, les utilisateurs et toute autre entité concernée doivent pouvoir connaître, de façon compatible avec le maintien de la sécurité, à tout moment, l'existence et l'ampleur des mesures, pratiques et procédures visant à la sécurité des systèmes d'information".

Le principe présenté dans ce paragraphe comprend les règles portant sur la définition des objectifs de la sensibilisation à la sécurité et son adaptation aux différentes classes d'utilisateurs.

▲ **PER-005** **Une règle prévoit la définition des objectifs de la sensibilisation à la sécurité**

La sensibilisation vise à faire prendre conscience à chaque utilisateur qu'il détient une part importante de responsabilité dans la lutte contre la malveillance.

La définition des objectifs de cette sensibilisation est étroitement liée à la mission ou au métier de l'organisme, à la sensibilité du patrimoine d'informations et de biens physiques ainsi qu'aux menaces connues. Ils peuvent être, par exemple, la recherche de l'adhésion du personnel vis-à-vis de la protection du patrimoine de l'organisme, ou bien encore l'émergence et l'efficacité d'un réseau d'alerte impliquant tous les utilisateurs du système d'information.

Une action de sensibilisation qui ne répond pas à des objectifs clairement exprimés n'apporte qu'une illusion de confiance en la capacité du personnel à réagir efficacement lors d'une atteinte au système d'information.

PER-006 **Une règle prévoit l'adaptation de la sensibilisation aux différentes classes d'utilisateurs**

En matière de sécurité, les niveaux de préoccupations diffèrent considérablement suivant qu'il s'agit du personnel de direction ou d'exécution. La sensibilisation est, en conséquence, adaptée aux niveaux de responsabilité détenus et aux spécificités des postes de travail.

Le personnel concerné appartient à trois grandes catégories :

- *celle liée aux activités de direction, d'encadrement, de gestion, de relations extérieures, etc.,*

- *celle liée aux emplois du système d'information (ingénieurs et techniciens, utilisateurs de la bureautique, etc.),*
- *celle liée à la sécurité des systèmes d'information (ingénieurs et techniciens de l'équipe de sécurité, agents de la sécurité, etc.) qui nécessitent une formation spécialisée.*

Une sensibilisation qui ne tient pas compte des particularités opérationnelles de chaque classe d'utilisateurs et des exigences plus ou moins fortes liées aux responsabilités ou aux postes de travail n'atteint pas les objectifs assignés et laisse voir la sécurité comme une contrainte supplémentaire sans valeur ajoutée par rapport à l'aspect productivité du poste de travail.

5.4. Principe de responsabilité du personnel

Le principe général de sensibilisation de l'OCDE énonce : "Les attributions et responsabilités des propriétaires, des fournisseurs, des utilisateurs de système d'information et des autres parties concernées par la sécurité des systèmes d'information, doivent être explicitement exprimées".

La responsabilité du personnel peut être engagée dès qu'il détient ou manipule des informations, des logiciels ou des matériels pour l'accomplissement de sa tâche.

Les règles énoncées dans ce paragraphe concernent l'application de la notion de responsable-détenteur, de responsable-dépositaire, de profil d'utilisateur du système d'information et l'application de la notion de reconnaissance de responsabilités.

✓ ▲ **PER-007 Une règle prévoit l'application de la notion de responsable-détenteur**

La notion de responsable-détenteur concerne le responsable hiérarchique d'une unité organique (établissement, service, centre de responsabilités ou de profit) ou l'autorité qualifiée telle qu'elle est définie à la règle OGS-002 du chapitre 4 du présent guide, et qui dispose de ses propres ressources humaines et matérielles pour mener à bien sa mission.

Le terme de détention s'applique au patrimoine d'informations, aux logiciels et aux matériels constitutifs du système d'information et implique l'obligation de respecter les lois, règlements et règles en vigueur dans l'organisme.

Le responsable-détenteur détermine les niveaux de risques acceptables et les conditions d'accès aux fichiers, de mises à jour des informations (en accord avec les règles de classification en vigueur

dans l'organisme), ou de modifications des logiciels et des matériels dont il dispose.

PER-008 **Une règle prévoit l'application de la notion de responsable-dépositaire**

Le responsable-dépositaire reçoit délégation du responsable-détenteur pour l'application des lois, règlements et des règles de protection concernant les informations, logiciels et matériels durant les phases de collecte, de traitement, de diffusion et de stockage.

Le responsable-dépositaire peut être, par exemple, un informaticien de l'équipe d'exploitation, un documentaliste, un secrétaire, etc.

Il est le gardien d'une partie du patrimoine de l'organisme et il est alors tenu, tout particulièrement, de se porter garant de l'application de la loi concernant la protection juridique des logiciels qui lui sont confiés (copies illicites).

▲ **PER-009** **Une règle prévoit l'application de la notion de reconnaissance de responsabilité**

Pour les postes de travail comprenant des informations relevant du secret de défense, l'attestation de reconnaissance de responsabilité est l'engagement que prend une personne de respecter les lois, règlements et règles de sécurité du système d'information.

Elle fait l'objet d'une déclaration écrite et signée conforme à l'IGI 1300. En particulier, l'article 16 stipule : "...cette attestation signifie que le titulaire de l'admission reconnaît avoir pris connaissance des obligations particulières et des sanctions imposées par le Code pénal à tout gardien ou détenteur d'informations intéressant la défense nationale et la sûreté de l'État... il appartient au directeur de l'organisme ou à l'autorité hiérarchique compétente d'appeler l'attention de l'intéressé sur le sens de la portée de cette attestation".

Pour les postes ne relevant pas de cette catégorie, des clauses spécifiques de confidentialité, de fin de contrat de travail ou de non-concurrence peuvent être insérées, si besoin est, dans le contrat de travail[33].

Au caractère essentiellement dissuasif de cette mesure, il peut être adjoint l'application de sanctions. Les incidences sur le plan disciplinaire du non respect des règles internes de sécurité doivent dans ce cas être expliquées dès la prise de fonction du personnel nouvellement affecté.

[33] À titre d'exemple les décrets 93-1229 et 1230 du 10 novembre 1993 relatifs au serment professionnel prêté respectivement par les personnels de la Poste et de France Télécom.

✓▲ PER-010 Une règle prévoit l'application des modalités d'accueil et de circulation des visiteurs

Les modalités d'accueil et de circulation des visiteurs sont généralement fixées par le service de sécurité générale. Mais, loin d'interférer avec celui-ci, il est un devoir pour chaque utilisateur du système d'information de prendre à sa charge l'application de cette règle dans sa propre zone de travail ou à proximité de son poste de travail. Le responsable-dépositaire est, en effet, le mieux placé pour vérifier la non atteinte au patrimoine informationnel qui lui est confié.

Cette règle est à rapprocher de celle préconisant le découpage de l'infrastructure en zones de sécurité laquelle apporte une grande facilité pour le contrôle des visiteurs (BPH-005).

Page laissée blanche

Chapitre 6

Principes de sécurité liés au cycle de vie du système d'information

Rappel : "✓" : règle de base - " ▲ " : règle à caractère majeur pour les organismes sensibles

Les principes de sécurité énoncés dans ce chapitre s'attachent à définir les règles essentielles liées au cycle de vie du système d'information dont les principales phases sont :

- la spécification, la conception et le développement,
- la validation et la mise en service,
- le fonctionnement et ses différents états (régime normal, reconfiguration, mode de secours, etc.),
- la maintenance logicielle, matérielle et documentaire,
- l'évolution,
- la mise hors service et la destruction partielle ou totale.

Ces principes s'appliquent à tous les constituants qui permettent le fonctionnement et le soutien logistique du système d'information (logiciels, matériels et documentation). Toutefois, ils n'ont pas pour but de reprendre une à une les étapes du cycle de vie d'un système d'information pour décrire, sous forme de règles, les procédures qu'il conviendrait de leur appliquer.

Ces principes peuvent couvrir une ou plusieurs phases du cycle de vie du système d'information comme, par exemple, la mise en place de la documentation de sécurité.

Les principes présentés dans ce chapitre ont été choisis en fonction de leur impact sur la sécurité et concernent :

- les spécifications pour le développement du système d'information sécurisé,
- l'autorisation d'utilisation du système d'information,
- l'exploitation sécurisée du système d'information,
- la sécurité pour les communications,
- la sécurité pour la maintenance du système d'information,
- la mise en place d'une documentation de sécurité,
- la limitation des sinistres touchant le système d'information,
- l'application des ITSEC lorsqu'une évaluation de la sécurité est envisagée,
- l'anticipation sur l'évolution de la sécurité du système d'information.

6.1. Principe de spécification pour le développement du système d'information sécurisé

Le principe de spécification pour le développement s'applique à tout système candidat ou non à une évaluation.

Il appartient au responsable de la sécurité d'identifier les ressources sensibles en fonction, d'une part, du prix qu'il attache à leur niveau de disponibilité, de confidentialité et d'intégrité et, d'autre part, des menaces contre lesquelles il estime nécessaire de se protéger ; il lui revient aussi de déterminer les protections non techniques à mettre en place, mesures d'organisation et protections physiques par exemple. Des mesures techniques - système d'exploitation sécurisé, par exemple - sont généralement indispensables pour compléter ces mesures non techniques ; l'utilisateur pourra s'appuyer sur une offre commerciale de produits dans lesquels il aura une confiance justifiée et dont il pourra comparer les mérites. De façon symétrique, pour développer leur offre de produits de sécurité, les vendeurs ont également besoin de la situer par rapport à une échelle de mesure largement admise.

L'expérience de plusieurs pays a montré que l'adoption des critères d'évaluation de la sécurité des systèmes informatiques (ITSEC) favorise l'émergence d'une offre commerciale de bonne qualité et constitue donc un point de départ pour promouvoir et développer la sécurité.

Les règles afférentes au principe de spécification pour le développement du système d'information sécurisé sont :

- la définition des besoins de sécurité,
- l'élaboration d'une cible de sécurité,
- l'adoption de méthodes et d'outils approuvés pour garantir la sécurité du système d'information,
- l'adoption d'un standard de programmation et de codage des données,
- les conditions de mise en exploitation de tout nouveau constituant du système d'information,
- la séparation des tâches de développement et des tâches techniques ou opérationnelles,
- la gestion des prestations de services externes à l'organisme,
- les critères d'acquisition et les conditions d'usage de progiciels.

Ce chapitre ne traite pas de la méthodologie pour le développement de systèmes d'information sécurisés : les guides méthodologiques développés par le SCSSI, et correspondant aux différentes phases du développement sécurisé d'un système d'information pour les départements ministériels et les administrations de l'État, sont donnés en annexe 8. Pour le domaine public, d'autres méthodes sont également proposées par le CLUSIF.

✓ ▲ CVE-001 Une règle prévoit la définition des besoins de sécurité

La définition des besoins de sécurité permet de décrire de façon non ambiguë les niveaux de confidentialité, d'intégrité de disponibilité et de preuve et contrôle[34] qu'il convient d'assurer aux constituants d'un système d'information.

La sécurité qu'on attend du système d'information doit être précisée dans ses spécifications car elle est une dimension essentielle de ce système au même titre que ses performances ou les services qu'il doit rendre ; ***cette expression des besoins de sécurité*** *devrait faire l'objet d'un examen approfondi, conduit selon une démarche référentielle.*

Compte tenu de la mission ou du métier de l'organisme, il convient de définir ce qui devrait être protégé dans le système en analysant les aspects suivants :

- *qu'il s'agisse d'informations, de services ou de supports, il faut préciser si la protection de ces entités concerne leur disponibilité, leur intégrité, leur confidentialité, et leur besoin en preuve et contrôle,*
- *il faut expliquer* ***pourquo****i les entités ainsi définies doivent être protégées : ce peut être en raison de leur valeur, de leur sensibilité, de leur caractère stratégique, etc.,*
- *il faut préciser les* ***menaces*** *accidentelles ou volontaires auxquelles ces entités sont soumises en envisageant tous les acteurs ou les causes susceptibles de provoquer une agression et en étudier les motivations et les origines,*
- *il faut enfin indiquer quelles sont les* ***contraintes*** *auxquelles est soumis le système d'information ; il peut s'agir de choix fixés a priori ou de toute autre contrainte, d'ordre budgétaire, technique, etc.*

Une analyse de risques[35] doit permettre, à ce stade, de mettre en évidence les vulnérabilités du système et les conséquences d'éventuelles atteintes à sa sécurité de façon à pouvoir justifier la mise en place de certaines parades dont on aura évalué le rapport coût / efficacité. C'est ainsi que, par exemple, les résultats d'une analyse de risques peuvent conduire à recourir à des assurances pour pallier un manque de compétences ou de ressources budgétaires.

[34] Par preuve et contrôle, il faut entendre la prévention de non répudiation en émission et réception ainsi que la prévention permettant d'assurer l'auditabilité.

[35] Pour une étude de diagnostics rapide, le SCSSI met à disposition des départements ministériels la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité).
Dans le domaine public, les méthodes MARION, MELISA et les méthodes qui leur sont dérivées sont les plus utilisées pour les études détaillées d'un système d'information.

▲ CVE-002 Une règle prévoit l'élaboration d'une cible de sécurité

La cible de sécurité[36] *constitue* ***la spécification du système en matière de sécurité*** *; c'est une étape très importante qui fixe à la fois l'objectif à atteindre et les moyens pour y parvenir.*

En premier lieu, la réflexion approfondie qu'ont permis l'étude des besoins de sécurité et l'analyse de risques doit permettre de fixer ce que l'on décide finalement de protéger, en précisant pourquoi, contre qui et contre quoi ; la synthèse de cette réflexion constitue les ***objectifs de sécurité*** *du système. Ceux-ci sont clairement définis dès la phase de spécification pour que l'on puisse ensuite apprécier si la sécurité du système est en mesure de les satisfaire.*

De ces objectifs de sécurité on déduit les mesures à mettre en place, qu'elles soient techniques ou non techniques. L'ensemble de ces objectifs de sécurité et des mesures associées constitue la ***politique de sécurité du système****.*

Les mesures non techniques sont les procédures et règles de mise en œuvre, l'habilitation des personnes, les mesures concourant à protéger l'environnement du système et toutes les dispositions à caractère réglementaire.

Les mesures techniques sont les fonctions de sécurité qu'il faut prévoir dans la conception du système de façon à satisfaire les objectifs ; ces fonctions sont réalisées au moyen de mécanismes de sécurité intégrés au système.

Objectifs et fonctions constituent l'essentiel de la ***cible de sécurité*** *; celle-ci représente le fondement de la sécurité dans la conception du système d'information.*

Cependant, pour que l'on puisse être sûr que les objectifs sont satisfaits, il faut d'une part que ces fonctions et mécanismes existent et, d'autre part, que l'on puisse leur accorder une confiance suffisante. La cible de sécurité *indique aussi le niveau de confiance qui est estimé nécessaire par l'intermédiaire d'un niveau d'assurance ITSEC.*

[36] La cible de sécurité est un concept développé dans les ITSEC, chapitre 2, page 19 , §2.3.

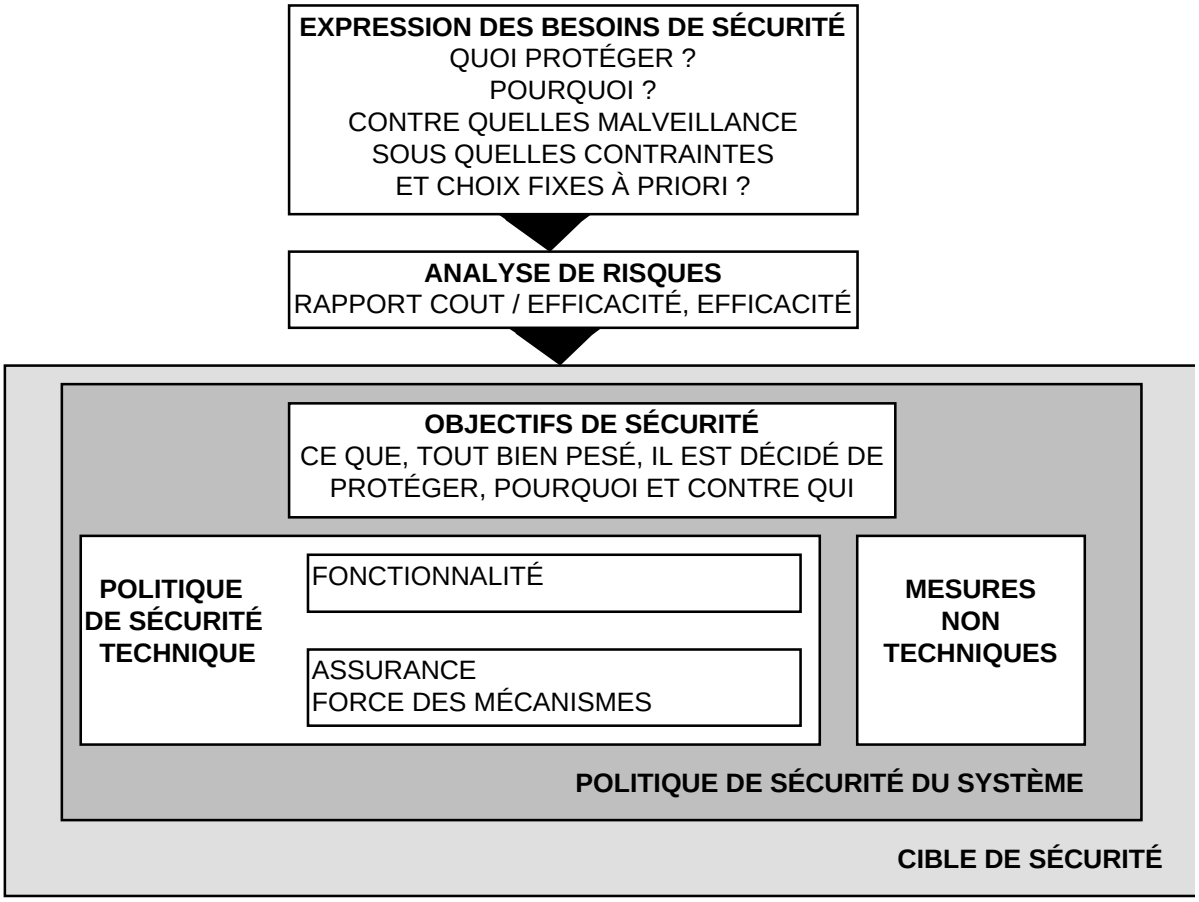


Schéma de principe pour la conception d'une cible de sécurité

▲ CVE-003 Une règle prévoit l'adoption de méthodes et d'outils de développement approuvés pour garantir la sécurité du système d'information

L'adoption, dès la conception du système d'information, de méthodes et d'outils de développement approuvés marque la volonté de l'organisme de maîtriser la sécurité[37].

L'application de cette règle permet d'acquérir une confiance justifiée dans la conception et la réalisation de la cible de sécurité ; elle contribue à la mise en place de protections homogènes et cohérentes constituant ainsi un gage de réussite pour une éventuelle évaluation du système d'information.

Toutefois, cette règle ne sous-entend pas l'emploi d'une méthode unique pour le développement du système d'information mais elle

[37] Le SCSSI met à la disposition des départements ministériels les guides ROSCOF (Réalisation des Objectifs de Sécurité par le ChOix des Fonctions) et DSIS (Développement de Systèmes d'Information Sécurisés).
Dans le domaine public, le CLUSIF propose la méthode INCS (Intégration dans la Conception des Applications de Sécurité)

appelle à veiller sur la nécessaire cohérence qui doit exister entre les différentes méthodes utilisées par l'organisme.

CVE-004 Une règle prévoit l'adoption d'un standard de programmation et de codage des données

L'adoption d'un standard de programmation intéresse tous les développements d'applications informatiques, y compris les parties logicielles que peuvent contenir les matériels ou dispositifs divers du système d'information.

La première recommandation liée à l'adoption d'un standard de programmation est celle de préciser les configurations matérielles et logicielles utilisées pour le développement.

La deuxième obligation concerne le choix d'une représentation et d'une structuration des programmes qui permet d'avoir des références uniformes et reconnues de tous, facilitant ainsi les opérations de maintenance logicielles et le suivi de la documentation technique.

Le codage des données concerne le formatage et la représentation des champs de données qui, pour des raisons similaires à la structuration des programmes, nécessitent l'adoption d'un standard.

Les divers états de sortie des données obéissent également à des standards de présentation qui prennent en compte les particularités fonctionnelles des utilisateurs de l'organisme.

L'administrateur de données est responsable de la bonne définition des données et de la structure des fichiers et bases de données.

▲ CVE-005 Une règle prévoit la séparation des tâches de développement et des tâches techniques ou opérationnelles

La séparation des tâches de développement et des autres activités liées au fonctionnement du système d'information (exploitation, gestion du système et du réseau, saisie des données, maintenance, audit de sécurité, etc.) réduit le risque de mauvaise utilisation délibérée ou accidentelle des ressources du système.

Cette règle influe sur le niveau de sécurité et sur l'efficacité dans la répartition des tâches et des responsabilités ; en effet, elle permet :

- *d'accroître la sécurité, en réduisant le risque de modifications malveillantes des programmes grâce à la séparation des tâches caractérisant le fonctionnement opérationnel du système d'information qui nécessitent des ressources différentes et des privilèges d'accès à des instructions machines critiques eu égard à la sécurité,*

- *d'améliorer l'efficacité par le fait que le cumul de plusieurs fonctions techniques peut inciter un informaticien d'une équipe d'exploitation à dépanner "à chaud" un logiciel au mépris des règles de programmation dont il est fait mention à la règle précédente (par exemple, l'absence de commentaires dans les lignes de code modifiées).*

Cette séparation des fonctions concourt à une meilleure délimitation des responsabilités en cas d'incident.

CVE-006 Une règle prévoit les critères d'acquisition et les conditions d'usage de progiciels

Si les critères d'achat de progiciels sont essentiellement économiques et opérationnels (disponibilité immédiate du produit, coût accessible, maintenance et assistance technique), il n'en demeure pas moins un problème de sécurité vis-à-vis de l'intégrité des logiciels livrés et de leur utilisation au sein de l'organisme.

Il est donc essentiel qu'une règle prévoie les critères permettant de justifier l'acquisition de progiciels et leurs conditions d'usage portant, par exemple, sur les aspects suivants :

- *la vérification du respect des principes de sécurité en vigueur dans l'organisme avant la décision d'acquisition,*
- *les tests de conformité et d'intégrité avant la mise en service des progiciels,*
- *les restrictions d'utilisation en fonction de la sensibilité des postes de travail.*

▲ **CVE-007 Une règle prévoit la gestion des prestations de services externes**

Pour le développement du système d'information, le recours à des prestataires de services externes (dûment habilités dans le cadre de marchés de défense) impose l'application stricte des règles précédemment énoncées et un contrôle renforcé des ressources mises à disposition (applications et fichiers sensibles, compilateurs, éditeurs, documentation technique, etc.).

La décision de mise à disposition de ressources sensibles doit être prise par rapport aux exigences opérationnelles de disponibilité du système d'information.

Les responsabilités et les procédures doivent être clairement établies entre l'organisme et les prestataires pour l'imputabilité d'éventuels incidents.

Le recours aux prestations de service, dès lors que la sécurité d'un système d'information représente un enjeu majeur pour les intérêts de l'État ou de l'organisme, ne doit jamais dériver vers une sous-traitance de la gestion de l'exploitation (traduction du terme anglo-saxon "facility management").

▲ **CVE-008 Une règle prévoit les conditions de mise en exploitation de tout nouveau constituant du système d'information**

Un nouveau constituant du système d'information (logiciel ou matériel) même réputé efficace et conforme aux spécifications de fabrication doit être soumis à des tests d'intégration dans son nouvel environnement.

Cette règle vise à réduire les risques inhérents au manque de coopération sur le plan de la sécurité avec les autres constituants de l'environnement ou l'inadaptation des consignes techniques et humaines en vigueur qui peuvent être à l'origine d'erreurs d'exploitation.

Les conditions préconisées par cette règle peuvent prévoir, par exemple, une recette complète du constituant pour l'identification des modifications techniques et procédurales à effectuer ainsi que la possibilité, en cas d'échec, de restaurer l'environnement technique dans l'état qui existait avant sa mise en exploitation.

6.2. Principe d'autorisation pour l'utilisation du système d'information

Le principe d'autorisation pour l'utilisation du système d'information est la conséquence pour la sécurité de la présence, au sein du système, d'applications et de services sensibles ou critiques pour la mission ou les activités de l'organisme. Ce principe, en permettant de réduire les risques de perte de confidentialité, d'intégrité et de disponibilité (par exemple, la lecture ou la modification illicite d'un fichier, la saturation d'un réseau), constitue la base du fonctionnement sécurisé.

Le terme "autorisation pour l'utilisation" se rapporte aux fonctionnalités décrites dans les critères harmonisés européens[38] à savoir :

- l'identification et l'authentification des utilisateurs désirant accéder au système,
- le contrôle des accès aux ressources du système d'information,
- l'imputabilité des actions dans le cadre de la recherche de responsabilité,

[38] ITSEC, § 2.31 à 2.58

- l'audit des informations lié aux événements survenus dans la phase de fonctionnement,
- la réutilisation d'objets garantissant que les ressources telles que la mémoire centrale ou les zones de stockage peuvent être réutilisées tout en préservant la sécurité.

Toutefois, ce principe ne vise pas à reprendre une à une les fonctionnalités précédentes pour décrire les règles qui s'y rapportent : en revanche, ce principe contient les concepts majeurs qui peuvent s'appliquer à une ou plusieurs de ces fonctionnalités.

L'autorisation d'utilisation du système d'information repose sur la correspondance entre les classes d'utilisateurs (ou sujets) pouvant accéder à des classes de ressources (ou objets). En pratique, la gestion de l'utilisation du système d'information se fait grâce à une matrice croisant les entités sujets et objets qui nécessite une protection adaptée (usage d'un codage voire, pour les applications plus vulnérables, un chiffrement des tables résidant en mémoire centrale) repose sur le triplet constitué par l'objet manipulé, le rôle du sujet dans le système et les privilèges associés.

L'objet manipulé et le rôle du sujet dans le système permettent l'énoncé d'une règle portant sur :

- la notion de profil d'utilisateur du système d'information.

De plus, le rôle du sujet dans le système induit deux autres règles permettant d'assurer le contrôle :

- la notion d'unicité des utilisateurs,
- la notion de complétude des moyens d'authentification.

Enfin, les privilèges associés induisent deux règles liées à la gestion :

- l'administration des privilèges d'utilisation du système d'information,
- le contrôle des privilèges des utilisateurs du système d'information.

▲ CVE-009 Une règle prévoit l'application de la notion de profil d'utilisateur du système d'information

L'application de la notion de profil d'utilisateur du système d'information sous-entend, au préalable, la structuration des données (ou objets) par fonction ou activités de l'organisme qui est une prérogative du responsable-détenteur (règle PER-007). Les données manipulées par les utilisateurs sont structurées, en fonction des applications qui les utilisent au sein d'une unité fonctionnelle (par exemple, la gestion des stocks pour un service d'approvisionnement), dans le cadre d'utilisation de ressources partagées (par exemple, les réseaux locaux), ou lors d'une mission

ou d'une activité particulière nécessitant le cloisonnement des postes de travail (règle PER-003).

Il faut, de la même manière, structurer les diverses catégories de personnel (ou sujets) par la définition de profils d'utilisateur du système d'information qui permettent de spécifier les privilèges d'accès aux informations liés à la lecture (visualisation, impression) et les privilèges de traitements liés à l'écriture (création, modification, destruction) dans le cadre de leurs responsabilités ou activités.

▲ CVE-010 Une règle prévoit l'unicité de l'identité des utilisateurs

L'identité des utilisateurs doit être gérée sous le contrôle conjoint de la direction du système et du responsable de la sécurité d'un site ou d'une unité opérationnelle (niveau de l'agent de sécurité). Il faut considérer qu'il y a infraction à la sécurité lorsque deux personnes ou plus connaissent, par exemple, le mot de passe correspondant à une identité d'utilisateur à moins que cela ne soit prévu pour assurer la continuité des fonctions d'administration de système.

S'il est inévitable, dans certains cas, de permettre le partage d'une identité et d'un élément d'authentification, des mesures spéciales telles que l'emploi d'enveloppes scellées peuvent être mises au point pour prévenir toute utilisation abusive ou incorrecte.

▲ CVE-011 Une règle prévoit la notion de complétude des moyens d'authentification

L'accès au système d'information implique que les utilisateurs justifient leur identité en début de session (et, dans certains cas, en cours de cession) en présentant un élément d'authentification. Les techniques actuelles d'authentification reposent sur trois concepts :

- *ce que l'on sait comme, par exemple, les mots de passe,*
- *ce que l'on détient comme, par exemple, les cartes à puce,*
- *ce que l'on est, c'est-à-dire une caractéristique personnelle (empreintes digitales, examen du fond de l'œil, signature dynamique, etc.).*

La réunion de ces trois concepts constitue une authentification complète et efficace mais représente un coût relativement élevé. En conséquence, le responsable-détenteur doit déterminer avec l'aide de l'agent de sécurité, à partir de ces trois concepts, quelles sont les combinaisons les plus adaptées pour son sous-système d'information ou ses applications sensibles.

Le choix d'une authentification basée sur le seul concept de "ce que l'on sait" représente le profil minimum de sécurité pour un système d'information ; il convient alors d'opter pour des mécanismes dynamiques comme les mots de passe utilisables une fois ou bien ceux assujettis à une limite du nombre d'utilisations ; dans ce cas, le mécanisme utilisé est un compteur d'accès sur lequel doit porter l'effort de protection.

Ainsi, les mécanismes utilisés reposent sur des éléments d'authentification dont il convient expressément de prévoir une gestion rigoureuse.

✓ ▲ **CVE-012 Une règle prévoit l'administration des privilèges d'utilisation du système d'information**

Un utilisateur possède des privilèges d'utilisation pour les ressources du système d'information correspondant au profil qui lui est attribué. Toutefois, lorsque ces privilèges sont dynamiques, il est indispensable de les administrer pour vérifier que les règles de sécurité en vigueur sont entièrement respectées.

Les critères d'application de cette règle sont clairement énoncés ; ils peuvent, par exemple, s'inspirer des éléments suivants :

- *les profils d'utilisateurs soumis à l'administration des privilèges,*
- *les privilèges existant entre les divers profils d'utilisateurs,*
- *les personnes qualifiées pour accorder ou modifier ces privilèges,*
- *les conditions à remplir préalablement à toute modification ou tout octroi de privilèges,*
- *les privilèges d'utilisateur incompatibles entre eux.*

La protection particulière de l'intégrité des tables contenant les privilèges doit être la préoccupation majeure du responsable du système et de l'agent de sécurité pour l'aspect du contrôle.

▲ **CVE-013 Une règle prévoit le contrôle des privilèges des utilisateurs du système d'information**

Il apparaît important de spécifier une règle pour la vérification du droit de possession des privilèges indépendamment des contrôles suggérés plus loin dans le principe portant sur l'exploitation sécurisée et qui s'attachent à la façon dont ces privilèges sont utilisés.

Le contrôle a pour mission, dès qu'un utilisateur tente d'exercer ses privilèges sur une ressource du système d'information, de ne permettre cette action que dans la mesure où elle n'outrepasse pas les règles de sécurité en vigueur dans l'organisme.

Les mesures qui découlent de cette règle peuvent reposer sur les aspects suivants :

- *les actions pour lesquelles un contrôle des privilèges doit être mené,*
- *les mesures à prendre si une action est tentée sans que le droit approprié soit possédé,*
- *les passe-droits au contrôle des privilèges et leurs conditions de validité.*

6.3. Principe d'exploitation sécurisée du système d'information

L'exploitation sécurisée du système d'information dépend essentiellement des acteurs qui interviennent pour l'application des procédures et des contrôles approuvés par l'organisme.

Les prérogatives qui leur sont attribuées couvrent l'ensemble du contrôle de sécurité sans qu'un seul acteur ne monopolise tous les privilèges. Or, la maîtrise de l'exploitation du système d'information, de par l'étendue des compétences qu'elle requiert, génère, de fait, un clivage entre les principaux rôles et responsabilités, à savoir :

- le responsable de l'exploitation du système d'information pour le traitement des données,
- l'ingénieur réseau pour la supervision des canaux de télécommunication,
- l'ingénieur système pour la supervision du système d'exploitation,
- le responsable de l'exploitation téléphonique et matériels périphériques associés (Minitel, fax, etc.).

Le principe d'exploitation sécurisée du système d'information concerne la sécurité des informations et des données[39] et la protection des constituants permettant le fonctionnement et le soutien logistique du système d'information.

[39] Les données sont la représentation des informations sous une forme conventionnelle destinée à faciliter leur traitement.

Les règles émanant de ce principe intéressent les procédures d'exploitation et les contrôles de sécurité durant la phase de fonctionnement du système d'information, à savoir :

- l'exploitation sécurisée des informations et des données,
- le contrôle des logiciels avant leur mise en exploitation,
- le contrôle des supports amovibles avant leur mise en exploitation,
- les contrôles de sécurité en phase d'exploitation du système d'information,
- l'analyse des enregistrements des données de contrôle de sécurité,
- l'exploitation sécurisée des moyens décentralisés, dédiés ou déportés hors de leur zone de sécurité.

▲ CVE-014 Une règle prévoit les procédures d'exploitation sécurisée des informations et des données

Les données et les supports associés devraient hériter du même niveau de protection que les informations qui leur ont donné naissance.

En fonction de leur classification, les informations et les données font l'objet d'une exploitation spécifique. Ainsi l'exploitation de données vitales ou sensibles peut nécessiter la mise en œuvre de mesures techniques particulières (par exemple, l'usage de systèmes à tolérance de pannes ou de disques miroir) ou organisationnelles (par exemple, la règle PER-003 sur le cloisonnement des postes de travail sensibles) afin d'éviter les incidents durant la phase de traitement. De même, les informations nominatives doivent recevoir les protections imposées par la loi.

La présente règle portant sur les procédures d'exploitation sécurisée se justifie par la vulnérabilité des données qui existe du fait de leur passage par des états différents (traitements, sauvegardes et transferts sur des supports, stockage, destruction, etc.) : aussi les procédures et contrôles de sécurité s'attachent à assurer la continuité de la protection à ces divers stades de l'exploitation.

Parmi les procédures à mettre en place, celles concernant la sauvegarde des données et la destruction des supports classifiés ont un impact majeur sur la sécurité.

La sauvegarde des données vise le maintien de leur intégrité et disponibilité : elle doit être faite régulièrement et les supports résultants sont stockés en des lieux éloignés de la zone de traitement et offrant le même niveau de protection ; des tests d'intégrité des sauvegardes apportent la garantie de la continuité de service.

La destruction des supports classifiés implique que les données enregistrées sont effacées ou surchargées avant que leur support magnétique ne soit détruit (bandes magnétiques, disquettes, disques amovibles et fixes, mémoires à disques, etc.).

Pour les données relevant du secret de défense, il peut être prévu, en conformité avec la réglementation en vigueur, un chiffrement des données permettant ainsi le stockage intermédiaires des supports associés lors de traitements discontinus.

▲ CVE-015 Une règle prévoit le contrôle des logiciels avant leur mise en exploitation

Les contrôles des logiciels avant leur mise en exploitation visent à lutter tout particulièrement contre la menace de contamination par virus[40] et le risque de non conformité des logiciels.

Les virus posent un problème de plus en plus grave pour la sécurité des systèmes d'information. Leur existence touche tous les organismes et institutions quel que soit leur niveau de vulnérabilité : les organismes les plus ouverts au public sont les plus exposés aux pirates informatiques dont les motivations sont assez souvent la prouesse technique et l'effet médiatique.

Le risque de non conformité des logiciels concerne les organismes sensibles qui, dans le cadre du recours à des prestataires de service pour le développement de logiciels, doivent vérifier l'exactitude et la conformité de la programmation du code afin de vérifier que le programme ne fait que ce pourquoi il a été conçu et qu'il n'existe pas de portes dérobées permettant ultérieurement une modification illicite de ces fonctionnalités.

Des précautions peuvent être prises pour prévenir et détecter l'introduction de logiciels frauduleux (virus, vers, chevaux de Troie, bombes logiques, etc.). Toutes les disquettes en provenance de l'extérieur de l'organisme et, tout particulièrement celles dont l'origine est incertaine, sont soumises à un contrôle. La mise en

[40] Le virus est l'exemple le plus connu de programme écrit dans le but de causer un dommage. Le glossaire de l'OTAN (version 1993) en donne la définition suivante : "Élément de programme qui s'ajoute à d'autres programmes, y compris à des systèmes d'exploitation mais qui ne peuvent s'exécuter indépendamment , ne devenant actif qu'avec l'exécution du programme hôte"

place de matériels dédiés à un dépistage systématique constitue une contre-mesure à cette menace.

▲ **CVE-016** **Une règle prévoit le contrôle des supports amovibles avant leur mise en exploitation**

Cette règle, portant sur le contrôle des supports amovibles, vise principalement la confidentialité des informations et intéresse les organismes traitant d'informations sensibles relevant du secret de défense ou des informations jugées stratégiques pour leurs activités.

Une mesure fondamentale précédant le contrôle des supports amovibles, avant leur réutilisation dans une autre installation protégée, consiste à effacer les informations qui y sont enregistrées en opérant un recouvrement complet au moyen de caractères numériques ou alphanumériques. Un contrôle de la non rémanence des données originelles peut être effectué avant leur réaffectation.

Pour les informations relevant du secret de défense, les supports de mémoire conservent la plus haute catégorie de classification des données pour lesquelles ils ont été utilisés depuis l'origine (sauf en cas de déclassification).

✓ ▲ **CVE-017** **Une règle prévoit les contrôles de sécurité en phase d'exploitation du système d'information**

Le contrôle de sécurité en phase d'exploitation permet de réduire les risques d'atteinte à la disponibilité et à l'intégrité des informations et des données. Ces contrôles se traduisent, par exemple, par des vérifications de l'usage des ressources autorisées pour le traitement.

Le premier aspect de ces contrôles vise les utilisateurs du système d'information. Ils échoient aux ingénieurs système et réseau qui assurent une surveillance en direct à partir de moyens de visualisation : examen des transactions en cours, fichiers en ligne, tentatives de connexions, etc.

Le second aspect de ces contrôles vise les informaticiens pour la vérification de la bonne application des procédures de sécurité, par exemple :

- *le respect du séquencement des opérations planifiées,*
- *les manipulations correctes de fichiers,*
- *l'utilisation des macro-instructions autorisées,*
- *le respect des instructions pour les récupérations d'erreurs ou pour les événements exceptionnels,*
- *la tenue à jour des registres d'exploitation,*

- *le respect des instructions concernant les états de sortie, principalement pour les imprimantes déportées.*

✓ ▲ **CVE-018** **Une règle prévoit l'analyse des enregistrements des données de contrôle de sécurité**

L'exploitation sécurisée du système d'information implique l'enregistrement des données de contrôle de sécurité dans un journal d'audit afin de vérifier que la sécurité est bien respectée, en particulier, pour ce qui concerne les accès au système d'information, qu'ils soient le fait d'utilisateurs, de techniciens ou d'informaticiens.

L'analyse des données de contrôle constitue une vérification ex post mais elle peut révéler des tentatives infructueuses de pénétration du système ou, de façon plus insidieuse, la préparation d'une attaque par récupération de fichiers ou de comptes périmés. Cet examen apporte plus de renseignements que la supervision en direct, à condition qu'il soit exécuté avec régularité et minutie.

Une protection efficace des mécanismes permettant l'enregistrement des données de contrôle est une condition essentielle pour justifier la confiance accordée à l'analyse des enregistrements ; en effet, tout intrus cherche d'abord à inhiber les mécanismes d'enregistrement et à faire disparaître les preuves de son méfait.

La mise en œuvre de journaux d'audits peut être une contrainte en période de forte charge d'exploitation : il faut néanmoins être conscient du risque pour la sécurité que représente leur désactivation.

▲ **CVE-019** **Une règle prévoit les procédures d'exploitation sécurisée des moyens décentralisés, dédiés ou déportés hors de leur zone de sécurité**

Les moyens décentralisés, dédiés ou déportés hors de leur zone de sécurité (micro-ordinateurs, matériels portables, imprimantes déportées, photocopieuses, télécopie, etc.) se caractérisent souvent par des équipes d'exploitation réduites voire des utilisateurs isolés. Sans assistance immédiate et sans le recours aux protections physiques d'une zone de sécurité, la probabilité d'incident ou d'atteinte à la confidentialité et à l'intégrité des données et des matériels reste très élevée : l'indiscrétion et la malveillance représentent une menace majeure dans la mesure où les consignes de vérification sont plus difficiles à mettre en œuvre. C'est la raison pour laquelle l'exploitation de ces moyens nécessite des mesures spécifiques adaptées à leur environnement ; en

particulier et, dans la mesure du possible, les équipements périphériques sont situés dans une zone surveillée.

Le cas des matériels portables mérite un examen particulier. En effet, avec l'accroissement de capacité de mémoire et de puissance de traitement, les machines portables sont de plus en plus utilisées. Cependant, elles sont exposées à des menaces plus variées que les matériels fixes et leur utilisation rend beaucoup plus difficile le contrôle nécessaire à la sauvegarde des informations. Leur portabilité et leur petite taille accroissent fortement la probabilité de perte ou de vol.

Dans la mesure du possible, les informations à protéger ne peuvent être traitées sur des machines portables qu'en des endroits désignés en fonction de leur niveau de classification.

Lorsque ces matériels sont emportés à l'extérieur de l'organisme, il faut appliquer la même procédure que pour la sortie des documents classifiés.

6.4. Principe de sécurité pour les communications

On entend par communication le transfert des informations.

La sécurité des communications[41] est la protection résultant de toutes les mesures générales et particulières destinées à interdire aux personnes non autorisées de tirer des renseignements du fonctionnement des communications.

Les transmissions sont l'ensemble des moyens permettant d'assurer l'acheminement des informations à distance entre plusieurs entités : ce terme désigne le moyen physique utilisé pour véhiculer l'information.

On emploie le terme de télécommunications pour désigner les transmissions qui font appel à des systèmes électroniques (radioélectriques, optiques, filaires, hertziens, acoustiques) permettant l'émission ou la réception de signes, de signaux, d'écrits, d'images ou du son.

La sécurité des transmissions repose sur trois critères fondamentaux et généralement antinomiques :

- la sûreté qui est la garantie de la régularité du fonctionnement d'un moyen de transmission c'est-à-dire, la certitude pour l'autorité origine que tous les messages parviennent sans déformation ni omission à tous les destinataires prévus,

[41] Instruction interministérielle

- la discrétion qui est le facteur assurant le degré de protection contre les risques d'interception, d'analyse, de localisation et d'intrusion,
- la rapidité qui définit l'aptitude à acheminer les informations dans les délais minimaux et à assurer un débit maximal.

▲ **CVE-020 Une règle prévoit le cadre contractuel pour les échanges de données sécurisés**

Les propositions d'accès à des services ou à des applications télématiques internes ou externes à l'organisme posent le problème de la coopération entre les différents systèmes d'information. Cette règle vise à prévenir la perte, la modification et la mauvaise utilisation des données.

Il importe, en conséquence, de prévoir les responsabilités et les obligations contractuelles des divers intervenants, tant au niveau des transmissions que des applications qui les intègrent.

L'échange de données sécurisé se situe dans le cadre de transmissions telles que définies plus haut. Le cadre contractuel désigne les accords entre plusieurs parties pour les échanges de données faisant appel ou non aux technologies de l'information : cette règle englobe le cas des échanges de données informatisées (EDI).
Les accords ou contrats passés par l'organisme avec tous les utilisateurs du système d'information comportent des clauses de contrôles précisant, par exemple :

- *la responsabilité de la gestion des flux d'échanges,*
- *les procédures de sécurité utilisées pour les échanges,*
- *les standards de structuration des données,*
- *les responsabilités en cas de pertes des informations,*
- *les mesures spécifiques pour la protection des clés de chiffrement.*

▲ **CVE-021 Une règle prévoit les modalités d'utilisation sécurisée des réseaux de télécommunication de l'organisme**

L'utilisation sécurisée des réseaux de télécommunication de l'organisme ne doit pas remettre en cause les mesures de sécurité qui sont prises au plan de l'infrastructure (par exemple, la création de zones réservées), du personnel (par exemple, le besoin de connaître les informations) ou des ressources matérielles et logicielles.

Les modalités d'utilisation des réseaux de télécommunication de l'organisme sont d'autant plus importantes à définir que les possibilités d'accès des utilisateurs sont augmentées par les éventuelles interconnexions des réseaux internes.

L'utilisation sécurisée des réseaux de télécommunication fait appel à la mise en place de fonctions et de mécanismes (au sens des ITSEC) destinés à garantir la sécurité des données au cours de leur transmission. Il est recommandé de découper ces fonctions suivant les rubriques tirées de l'architecture de sécurité OSI, à savoir :

- *l'authentification,*
- *le contrôle d'accès,*
- *la confidentialité des données,*
- *l'intégrité des données,*
- *la non répudiation.*

Parmi ces fonctions, le contrôle d'accès repose sur des mesures de gestion et de contrôle continues dans le temps et portant, par exemple, sur les aspects suivants :

- *l'accès des utilisateurs aux services pour lesquels ils sont autorisés,*
- *la connexion au système d'information des ordinateurs isolés ou extérieurs à l'organisme,*
- *la séparation des réseaux dédiés à des domaines particuliers,*
- *le routage des communications sur les canaux autorisés.*

▲ **CVE-022 Une règle prévoit les modalités d'utilisation sécurisée des réseaux de télécommunication externes à l'organisme**

L'utilisation des réseaux de télécommunication externes à l'organisme met en relation des utilisateurs qui n'ont pas, a priori, les mêmes exigences de sécurité.

Les modalités d'utilisation sécurisée des réseaux de télécommunication externes à l'organisme concernent tout particulièrement le contrôle des moyens qui peuvent échapper à la gestion centralisée du système d'information comme, par exemple, l'installation de modems ou de Minitels. Le cas particulier du courrier électronique devrait inciter à l'adoption de mesures visant à contrôler l'envoi de messages considérés comme vulnérables face aux interceptions et modifications non autorisées et sur les considérations légales liées à la non répudiation du message émis ou reçu.

Les rubriques, tirées de l'architecture OSI et énumérées à la règle précédente, s'appliquent au cas des réseaux externes à l'organisme.

▲ **CVE-023 Une règle prévoit la protection des informations durant leur transmission**

L'organisme doit prendre en compte le niveau de protection offert par les canaux de transmission utilisés.

La règle s'attache à contrôler que le niveau de protection requis par les informations communiquées est correctement atteint.

La protection des informations sensibles durant leur transmission est organisée de façon à rendre aussi peu efficace que possible les différents types d'attaques sur le réseau de transmission.

L'organisation de cette protection vise à :

- *l'acheminement du trafic même en ambiance de brouillage ou de saturation (qui consistent à empêcher ou gêner le fonctionnement des liaisons),*
- *la garantie contre l'intrusion (qui consiste à introduire ou à modifier des messages dans l'intention de tromper),*
- *la défense contre l'interception (qui est la réception d'émissions non autorisées),*
- *la défense contre l'analyse de trafic (qui permet d'obtenir des renseignements à partir de l'étude du trafic).*

Le recours au chiffre et à l'emploi de matériels protégés contre l'émission de signaux parasites compromettants constitue les moyens de protection classiques en matière de sécurité des communications.

- *Le chiffre*[42]*.*

  Il est défini comme l'ensemble des moyens cryptologiques permettant de protéger les informations transmises, de façon à les rendre inintelligibles pour toute personne qui n'est pas autorisée à les connaître. On utilise soit le chiffrement des messages soit le chiffrement des voies de transmission.

  La règle intègre le fait que, si les mesures de sécurité correspondant au niveau de protection requis nécessitent des

[42] Instruction interministérielle 500 bis

moyens de chiffrement, l'usage de ces moyens est soumis au respect de la loi et de la réglementation et doit s'accompagner de mesures organisationnelles permettant leur gestion spécifique.

- *Les matériels qualifiés de matériels à la norme TEMPEST (Transient ElectroMagnetic Pulse Emanations STandard)*[43]*.*

  Tout matériel ou système qui traite des informations sous forme électrique est le siège de perturbations électromagnétiques. Ces perturbations, provoquées par le changement d'état des circuits qui composent le matériel considéré, sont qualifiées de signaux parasites. Certains de ces signaux sont représentatifs des informations traitées. Leur interception et leur traitement permettent de reconstituer ces informations. Ces signaux sont, de ce fait, dénommés signaux parasites compromettants.

6.5. Principe de sécurité pour la maintenance du système d'information

La maintenance a pour objet la prévention contre les pannes (maintenance préventive) et la réparation des matériels et des logiciels suite à des incidents de fonctionnement du système d'information (maintenance corrective).

L'absence ou la mauvaise application des procédures de maintenance peut entraîner des erreurs de manipulation ou faciliter des opérations frauduleuses et provoquer, de ce fait, des pannes du système d'information.

Les règles énoncées dans ce paragraphe portent sur les conditions de sécurité pour la mise en maintenance et la remise en fonctionnement d'un constituant, sur les opérations de suivi et sur les conditions d'usage de la télémaintenance.

✓ ▲ **CVE-024 Une règle prévoit les conditions de sécurité pour la mise en maintenance des constituants du système d'information**

Le non respect des consignes pour la préparation d'un constituant avant sa mise en maintenance peut exposer l'organisme à des compromissions ou à des atteintes au bon fonctionnement de son système d'information.

Le conditionnement consiste à préparer le constituant en vue de sa réparation c'est-à-dire, à vérifier les points suivants :

[43] Instruction interministérielle 900, article 8

- *le retrait du support de la mémoire rémanente ayant contenu des informations classifiées ou confidentielles,*

- *la superposition d'écriture sur la mémoire restante afin d'éviter toute possibilité d'interprétation des enregistrements précédents,*

- *la vérification des installations de maintenance externes qui doivent répondre aux mêmes normes de sécurité matérielle et personnelle que celles appliquées dans les zones d'utilisation pour les constituants mis en réparation.*

Si pour des raisons techniques, il n'est pas possible d'enlever le support de la mémoire rémanente, il peut être nécessaire d'imposer que la maintenance d'un constituant soit effectuée sur place par du personnel possédant l'habilitation adéquate.

▲ **CVE-025** **Une règle prévoit les conditions de sécurité pour la remise en fonctionnement des constituants après leur maintenance**

Les conditions de sécurité pour la remise en fonctionnement des constituants après leur maintenance visent à démasquer tout piégeage éventuel : ajout d'un composant ou d'un microprogramme, non conforme à la configuration initiale, dans le but de capturer des signaux ou des informations ou bien encore retrait ou modification d'un composant altérant les caractéristiques du constituant.

En conséquence, des conditions de remise en fonctionnement peuvent être édictées, par exemple :

- *en fonction des conditions locales, de l'évaluation de la menace et, dans le cas d'ordinateurs, de la sensibilité des informations mises en mémoire, le constituant fait l'objet de mesures de détection lorsqu'il est réintégré dans sa zone de sécurité,*

- *pour le cas particulier de matériels répondant à la norme TEMPEST, toute modification entraîne une nouvelle vérification de l'aptitude antirayonnante.*

▲ **CVE-026** **Une règle prévoit le suivi des opérations de maintenance des constituants du système d'information**

Cette règle qui s'applique à tous les constituants du système d'information (matériels et logiciels) prend un caractère majeur pour le cas de constituants ayant des fonctions de sécurité.

L'absence de suivi des opérations de maintenance a pour conséquence la méconnaissance du degré d'aptitude des constituants à assurer de nouveau leurs fonctions : elle peut

conduire à leur attribuer une confiance injustifiée sur le plan de la sécurité.

Le suivi des opérations de maintenance nécessite l'ouverture d'un registre complet et détaillé sur les interventions subies par les composants afin que le personnel connaisse les nouvelles configurations et applique les procédures correctes.

Par ailleurs, lorsque l'organisme dispose d'un infocentre dont la mission principale est le support aux utilisateurs, il est nécessaire de veiller à ce qu'il applique ces mêmes règles pour les interventions dont il a la charge et tout particulièrement lorsque ses attributions consistent à faire installer sur les machines de l'organisme les progiciels ou les cartes électroniques demandées par les utilisateurs.

▲ CVE-027 Une règle prévoit les conditions d'usage de la télémaintenance

La généralisation des services de télémaintenance permet l'optimisation des coûts par la réduction des déplacements de personnel. En contrepartie, l'installation d'une ligne de communication entre le système d'information et l'organisme de maintenance et la nécessité de donner des droits d'accès de haut niveau augmentent les risques d'attaques du système d'information.

Pour ces raisons, les conditions d'usage de la télémaintenance sont rigoureusement définies, voire interdites pour certaines applications sensibles.

6.6. Principe de mise en place d'une documentation de sécurité

L'absence ou la mise à jour incomplète d'une documentation décrivant les fonctionnalités ou les mécanismes de sécurité peut entraîner des erreurs ou des incidents d'exploitation ou de maintenance portant atteinte à la confidentialité, à l'intégrité et à la disponibilité du système d'information.

Le principe de mise en place d'une documentation de sécurité s'inscrit dans toutes les phases du cycle de vie du système d'information : il permet de s'assurer que les dossiers de sécurité sont faciles d'emploi, précis, complets et utilisés seulement par le personnel ayant qualité pour les détenir.

▲ CVE-028 Une règle prévoit l'adoption d'un standard d'élaboration de la documentation de sécurité

La diversité des équipements, des logiciels et des procédures impose la définition d'un standard d'élaboration de la documentation de sécurité.

Ce standard concerne, en premier lieu, le modèle de présentation et le contenu de la documentation : tous les constituants de sécurité sont décrits selon le même formalisme facilitant ainsi les interventions du personnel autorisé pour leur exploitation et leur maintenance.

En second lieu, le standard concerne la manière de réaliser la documentation c'est-à-dire, la rédaction, l'impression et la classification des documents. De plus, tous les éléments ayant servis à l'élaboration de la documentation sont manipulés et protégés au même titre et dans les mêmes conditions que les documents de sécurité qui en résultent.

▲ CVE-029 Une règle prévoit la gestion de la documentation de sécurité

La gestion de la documentation de sécurité comprend la comptabilité, la mise à jour, la reproduction et la destruction :

- *la gestion de la documentation de sécurité repose sur une comptabilité précise et efficace basée sur la tenue à jour d'un registre inventaire*,
- *la mise à jour régulière de la documentation de sécurité est imposée par la constante évolution du système d'information*,
- la reproduction et la destruction de la documentation sont exécutées sur ordre du responsable de la sécurité qui vérifie que l'opération porte sur la totalité des documents désignés et n'affecte qu'eux seuls.

✓ ▲ CVE-030 Une règle prévoit la protection de la documentation de sécurité

La documentation de sécurité doit être protégée contre les accès non autorisés. Sa protection est du même niveau que les constituants auxquels elle se rapporte.
Les mesures suivantes peuvent être suggérées:

- *tout responsable-détenteur de documents de sécurité doit connaître la position des documents qui lui sont confiés et contrôler leur utilisation*,

- *la manipulation de ces documents ne peut être faite que par du personnel autorisé,*

- *les documents sont rangés dans des lieux sûrs,*
- *la diffusion, émanant du responsable de la sécurité, peut être restreinte au minimum de personnes.*

6.7. Principe de limitation des sinistres touchant le système d'information

L'objectif du principe de limitation des sinistres est de réduire les dommages dus aux incidents et aux dysfonctionnements du système d'information, que leur origine soit de nature accidentelle ou malveillante.

Ce principe suppose que soit établi le répertoire des types d'incidents qui justifient un déclenchement d'alerte ainsi que les priorités portant sur les moyens d'intervention adaptés à chaque cas ; par exemple, pour les sinistres accidentels, un début d'incendie ou une panne informatique grave ; pour le cas de malveillance, une tentative de compromission ou d'intrusion dans le système d'information.

Les règles qui découlent de ce principe comprennent :

- la mise en place d'un réseau d'alerte pour la détection des incidents de sécurité,

- la maîtrise des incidents de sécurité durant la phase de l'intervention,

- la reprise d'activité du système d'information,

- le suivi des incidents de sécurité.

▲ **CVE-031** **Une règle prévoit la mise en place d'un réseau d'alerte pour la détection des incidents de sécurité**

La finalité d'un réseau d'alerte est de provoquer une intervention aussi rapide que possible, limitant ainsi les conséquences d'un arrêt du système d'information ou l'activation de procédures suite, par exemple, à une compromission des mots de passe impliquant leur changement immédiat.

Tous les utilisateurs, et particulièrement ceux opérant sur des postes de travail sensibles, constituent les maillons de ce réseau d'alerte. Il s'agit d'apprendre aux utilisateurs à protéger leurs matériels et à déceler les indices de manipulations frauduleuses ou d'activités inhabituelles.

L'efficacité d'un réseau d'alerte repose sur la structure de l'organisation mise en place et, tout particulièrement, sur les agents de sécurité. Elle dépend du niveau technique des moyens de détection et de la mobilisation des utilisateurs du système d'information : l'intervention qui en découle est d'autant plus efficace qu'elle fait intervenir les moyens adéquats au moment opportun.

Pour le cas de compromission d'informations relevant du secret de défense, l'organisme doit rechercher la rapidité de réaction : "Si la sécurité d'une information a été ou semble avoir été compromise de quelque façon que ce soit, la rapidité et la discrétion de l'intervention revêtent une particulière importance pour en limiter les conséquences ; un compte rendu non fondé et démenti par les faits est toujours préférable à un retard dans l'intervention[44]".

▲ CVE-032 Une règle prévoit la maîtrise des incidents de sécurité

La maîtrise des incidents de sécurité consiste à s'assurer de la continuité de la sécurité durant toute la durée de l'intervention faisant suite à une alerte : le recours à des spécialistes extérieurs et l'obligation de leur faciliter l'accès au site et au système d'information ne doit pas dispenser le personnel de l'organisme d'appliquer les règles de sécurité.

Deux cas d'urgence peuvent nécessiter des actions différentes:

- *ceux provenant d'accidents physiques touchant à l'infrastructure d'une zone sensible ou au système d'information qu'elle contient et qui n'entraînent pas d'actions hostiles visant à capturer des constituants du système d'information ; l'action consiste alors à surveiller les matériels, les logiciels et les documents durant l'intervention comme par exemple, le transfert d'équipements vers une salle blanche ou la mise en mode dégradé de mécanismes de sécurité jusqu'au retour à la normale du système d'information,*

- *ceux provenant d'actions hostiles visant à capturer des constituants du système d'information : un plan de destruction d'urgence simple et pratique de mise en œuvre peut être, dans certains cas, le seul moyen d'éviter une compromission grave.*

✓ ▲ CVE-033 Une règle prévoit l'élaboration et le test d'un plan de reprise d'activité du système d'information

Un plan de reprise d'activité est nécessaire pour protéger les tâches opérationnelles critiques du système d'information face aux défaillances majeures, aux erreurs humaines, aux catastrophes naturelles ou aux attaques délibérées. Il a pour but de limiter les

[44] Instruction générale interministérielle 1300, article 51

atteintes à la sécurité suite à un incident majeur et de remettre le système d'information dans les conditions de fonctionnement initiales.

Le plan de reprise d'activité impose la prise en compte de toutes les exigences opérationnelles du système d'information pour assurer un retour à un fonctionnement normal. Les procédures qui découlent de ce plan fournissent une alternative et des moyens temporaires de continuité du service, dans le cas d'endommagement ou de défaillance d'un équipement.

Toutefois, un élément fondamental pour l'établissement d'un plan de reprise d'activité est l'étude de disponibilité du système information car l'importance des préjudices subis est généralement fonction de la durée d'indisponibilité. Ainsi, l'étude de disponibilité a pour but de définir des tranches temporelles où le préjudice est considéré à un niveau donné en correspondance avec le niveau de procédure d'urgence du plan de reprise d'activité.

Mais, pour mériter un niveau de confiance élevé, le plan de reprise d'activité doit être testé régulièrement. Tout particulièrement, la procédure de sauvegardes régulières des données vitales et des logiciels est une mesure fondamentale : un nombre minimum de sauvegardes des informations est stocké dans un lieu éloigné à une distance suffisante pour résister à un désastre sur le site principal ; les protections physiques des sauvegardes sont du même niveau que les standards appliqués sur le site principal.

Le plan de reprise d'activité définit, en outre, l'ordre de priorité dans la reprise des différentes fonctions du système d'information et accepter, si la disponibilité du système d'information est l'objectif prioritaire pour l'organisme, que certains mécanismes de sécurité soient temporairement inhibés.

✓ ▲ CVE-034 Une règle prévoit le suivi des incidents de sécurité

L'absence de suivi des incidents de sécurité expose l'organisme à méconnaître les vulnérabilités de son système d'information et le condamne à ne pas être en mesure de réagir efficacement face à des sinistres répétés de même nature.

De ce fait, les responsabilités du suivi des incidents et des procédures doivent être établies ; les procédures couvrent alors tous les types d'incidents potentiels y compris les défaillances du système ou pertes de service, les erreurs résultant de données fausses ou inadéquates, les failles de la confidentialité.

Pour ce faire, le suivi des incidents de sécurité s'appuie sur les comptes rendus pour les interventions immédiates, sur les relevés des dysfonctionnements pour les actions différées et, dans les deux cas, sur l'analyse et l'identification des causes du sinistre.

L'adoption d'un standard de compte rendu et de directives pour leur exploitation sont des mesures qui visent à rendre uniforme et obligatoire la procédure d'alerte évoquée.

Les incidents de toute nature, décelés par exemple en phase d'exploitation, font l'objet d'un compte rendu au niveau du responsable de sécurité aussi rapidement que possible.

Les dysfonctionnements et les faiblesses du système d'information doivent être notés et corrigés. En particulier, il apparaît nécessaire de passer en revue les dysfonctionnements pour s'assurer que les mesures correctives ont été effectivement mises en œuvre et qu'elles correspondent à des actions autorisées.

L'analyse et l'identification des causes de l'incident impliquent une planification de la collecte des comptes rendus d'audit, de la mise en place de mesures de protection et de la communication avec les utilisateurs affectés par l'incident.

6.8. Principe d'application des ITSEC pour une évaluation de la sécurité du système d'information

En France, conformément aux directives du Premier Ministre[45], l'évaluation des systèmes d'information des départements ministériels et des administrations de l'État doit être conduite selon la méthodologie de sécurité préconisée par les critères d'évaluation de la sécurité des systèmes informatiques (ITSEC). Pour les organismes publics et privés, ces critères ont valeur de recommandation.

Les règles qui découlent du principe d'application des ITSEC pour une évaluation de la sécurité représentent les étapes qu'il convient de suivre pour sécuriser un système d'information, à savoir :

- l'évaluation et la certification,
- l'agrément et l'homologation,

[45] Lettres n°106/SGDN/DISSI/26007 du 11 mars 1992 et n°110/SGDN/DISSI/25100 du 16 mars 1992.

- les circonstances qui justifient une réévaluation du système d'information selon les ITSEC.

Tous les organismes tenus à l'application des critères d'évaluation de leur système d'information doivent adopter l'approche définie dans les trois règles précédentes. En particulier, l'élaboration d'une cible de sécurité (règle CVE-002) permet de prendre en compte la sécurité dès la phase de conception d'un système d'information. De plus, il faut aussi maintenir des préoccupations de sécurité tout au long du développement du système et durant son exploitation[46].

Une présentation succincte des ITSEC est donnée en annexe 2.

CVE-035 Une règle prévoit l'évaluation du niveau de confiance accordé au système d'information : l'évaluation et la certification

La conception du système est guidée par une démarche cohérente qui conduit à ce que les objectifs de sécurité soient atteints ; les fonctions de sécurité sont choisies pour satisfaire ces objectifs.

*Une fois le système développé et mis en service, il importe de savoir quelle **confiance** on peut avoir que la cible de sécurité est bien atteinte.*

D'une part cette confiance dépend du choix des fonctions, de leur efficacité et de la qualité de leur développement et, d'autre part, elle dépend de la façon dont le système a été installé, mis en service et exploité.

*L'étude de chacun de ces aspects permettra d'avoir une confiance justifiée dans la réalisation de la cible de sécurité ; c'est l'objet de **l'évaluation**. Un système développé selon les principes exposés ci-dessus pourra être évalué et on aura alors la confirmation qu'on peut lui faire confiance quant à la sécurité qu'il assure aux informations qui lui sont confiées.*

*Cette évaluation doit être conduite selon une méthode approuvée obéissant à des règles définies. Les résultats de l'évaluation et le fait que les critères d'évaluation utilisés ont été correctement appliqués sont confirmés par une déclaration formelle appelée **certificat**.*

Toutefois, la certification n'a aucun caractère obligatoire : il appartient au commanditaire de l'évaluation de juger du besoin de certification.

[46] Le SCSSI met à disposition des départements ministériels le guide DSIS (Développement de Systèmes d'Information Sécurisés).

CVE-036 **Une règle prévoit l'agrément et l'homologation du système d'information**

L'évaluation et la certification qui en confirme les résultats permettent seulement d'assurer que la cible de sécurité est bien atteinte. Elle ne constitue qu'un des éléments pour juger si le système ou le produit placé dans son environnement réel, présente bien avec les mesures de sécurité non techniques (en particulier, les procédures d'exploitation effectivement mises en place) les protections adaptées à la sensibilité des ressources qui lui sont confiées et à l'étendue des menaces qu'il doit repousser.

Il y a lieu, de plus, de prononcer un jugement sur la pertinence de la cible de sécurité face à l'environnement réel d'exploitation du système : c'est le rôle de ***l'agrément*** *qui constitue la reconnaissance formelle que le produit ou le système évalué peut protéger des informations jusqu'à un niveau spécifié, dans des conditions d'emploi définies.*

Enfin, ***l'homologation*** *est la décision d'utiliser, dans un but précis ou dans des conditions prévues, un produit ou un système. Cette décision finale est prise par l'autorité responsable de la mise en œuvre du produit ou du système, conformément à la réglementation en vigueur.*

Toutefois, et comme cela a été précisé dans la règle précédente, la décision de l'opportunité de demander un agrément et l'homologation revient, en général, au seul commanditaire.

CVE-037 **Une règle prévoit les circonstances qui justifient une réévaluation du système d'information selon les ITSEC**

Le principe général de réévaluation des Lignes directrices de l'OCDE stipule :
"La sécurité des systèmes d'information devrait être réévaluée périodiquement étant donné que les systèmes d'information et les exigences en matière de sécurité varient dans le temps".

Selon les ITSEC, une évaluation et le certificat qui lui est associé expriment un avis sur la mise en œuvre d'une cible de sécurité en laquelle l'utilisateur place sa confiance.

Mais, une fois qu'un système a été soumis à une évaluation, il est irréaliste de croire qu'il est à l'abri d'erreurs ou impossible à modifier : en effet, le système devra répondre à de nouvelles exigences qui se traduiront par des modifications des matériels, des logiciels et de la documentation.

Dans cette optique, il est évident que certaines modifications exigent une réévaluation comme, par exemple, la restructuration du noyau d'un système d'exploitation, qui peut s'appuyer, en partie, sur les résultats de l'évaluation précédente. En revanche, d'autres modifications peuvent n'entraîner aucune nouvelle évaluation dès lors qu'elles touchent à des parties du système d'information séparées des composantes de sécurité et qui n'influent pas sur celles-ci.

6.9. Principe d'anticipation sur l'évolution de la sécurité du système d'information

CVE-038 Une règle prévoit le recours à une étude prospective sur l'évolution de la sécurité du système d'information

Une étude prospective sur l'évolution de la sécurité du système d'information permet d'anticiper sur les besoins à moyen terme de l'organisme et d'intégrer le plus tôt possible les nouveaux logiciels, matériels ou mécanismes nécessaires à la sécurité. Cette étude prospective ne peut être dissociée des orientations stratégiques (ou d'un schéma directeur des systèmes d'information) portant sur les nouvelles technologies de l'information susceptibles d'être choisies par l'organisme.

Par ailleurs, cette règle vise à vérifier que toute évolution du système d'information reste conforme aux principes de sécurité en vigueur dans l'organisme. Dans le cas contraire, l'étude prospective permet d'en mesurer l'impact sur la sécurité et de proposer les aménagements d'ordre technique ou organisationnel pouvant impliquer une modification des principes et des règles de la politique de sécurité interne de l'organisme.

Page laissée blanche

Annexes

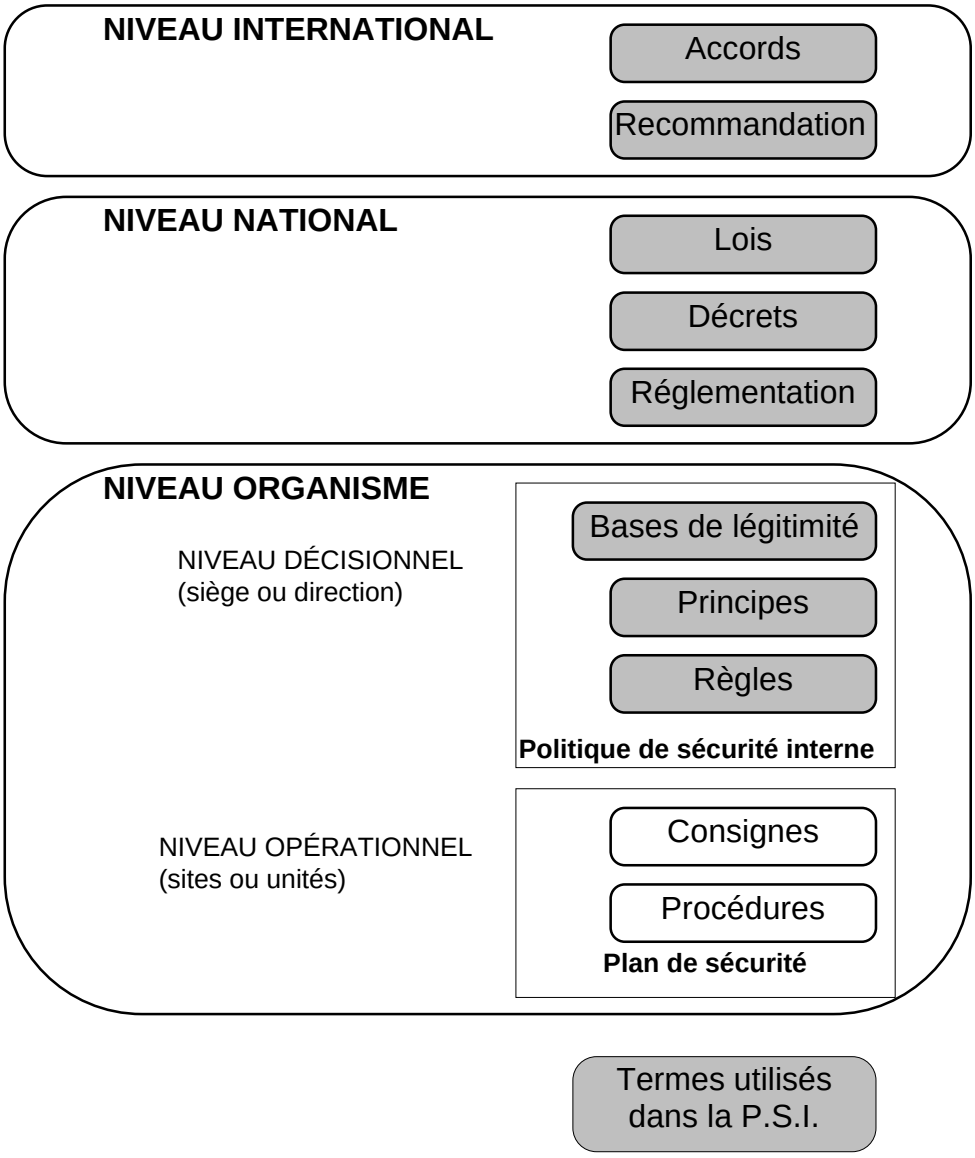
Le contenu des présentes annexes est donné à titre indicatif : sa mise à jour ne sera faite qu'à l'occasion de la rédaction de la version suivante du guide. Par conséquent, le lecteur est invité - tout particulièrement pour les textes juridiques cités - à vérifier leur validité ainsi que la parution éventuelle de nouveaux textes.

Page laissée blanche

Annexe 1

Notes complémentaires

Note complémentaire n°1 :
Hiérarchie des concepts utilisés dans une politique de sécurité interne.



Note complémentaire n°2 :

I. ORGOGOZO, Les paradoxes du management, Les Éditions d'organisation, Paris, 1991, p. 22.
On peut aussi définir un organisme à partir des cinq composantes suivantes :

- le milieu, c'est-à-dire le degré de complexité et d'ouverture sur l'environnement,
- les matières comme, par exemple, l'information et toutes les matières premières,
- la main d'œuvre, c'est-à-dire le personnel, ses qualifications et sa mobilité,
- les méthodes concernant, par exemple, le pilotage, le développement des compétences, l'obtention de l'adhésion du personnel,
- les matériels permettant le traitement, le transport et le soutien logistique.

Note complémentaire n°3 :

FIASI, extrait de la note technique n°1 sur les conditions d'utilisation des entreprises extérieures, 4 mars 1993, page 1.

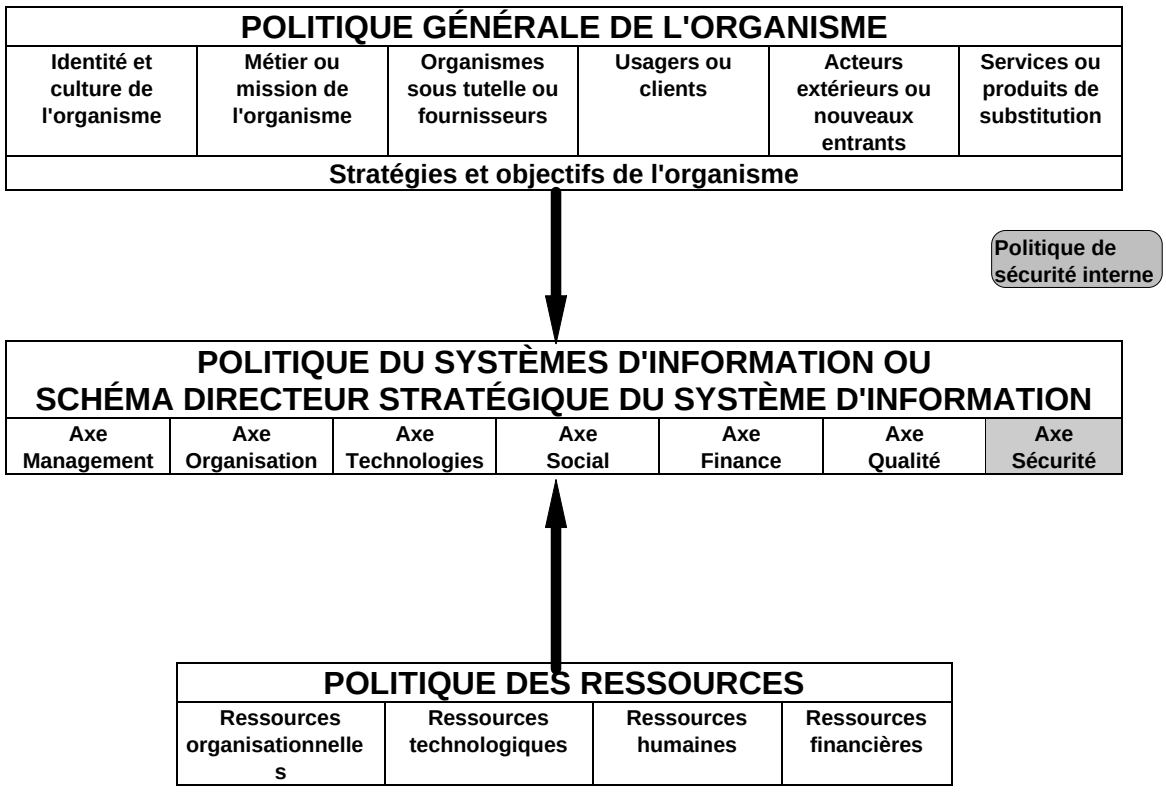
Les règles de sécurité doivent être définies et appliquées en fonction du Décret n°92-158 du 20 février 1992 qui précise :

"Lorsqu'une ou des entreprises, dites entreprises extérieures, font intervenir leur personnel aux fins d'exécuter (ou de participer à l'exécution d') une opération (une ou plusieurs prestations de service ou de travaux afin de recourir à un même objectif), l'entreprise qui accueille devra organiser et assurer la coordination générale des mesures de prévention".

Cette coordination a pour objet de prévenir les risques liés à l'interface entre les activités, les installations et les matériels des différentes entreprises présentes sur le lieu de travail. Ce décret concerne tous les travaux ou prestations effectués sur le site (aménagement de locaux, travaux électriques, développements de logiciels, reportages vidéos,...) sauf la construction de nouveaux bâtiments clos ou indépendants, même s'ils sont situés à l'intérieur de l'enceinte du site.

Note complémentaire n°4 :

G. BALANTZIAN, Les schémas directeurs stratégiques, Masson, 4ème édition, Paris, 1992 : une adaptation, au cas de la sécurité, d'après le schéma sur les facteurs d'influence sur la politique des SIC, page 4.



Place de la politique de sécurité interne
dans la politique générale de l'organisme

Ce schéma précise les caractéristiques qui composent une politique générale de l'organisme ; puis il décrit les différents axes à prendre en compte dans un schéma directeur stratégique d'un système d'information ainsi que l'influence de la politique des ressources sur celui-ci.

La politique de sécurité interne apparaît donc comme une spécification de l'axe sécurité du schéma directeur d'un système d'information.

Note complémentaire n°5 :

Les spécificités liées à la localisation géographique de l'organisme.

La dispersion géographique des sites d'un organisme peut justifier d'importants aménagements aux principes de sécurité en vigueur. Par exemple, pour la sécurité physique, il peut s'agir de la prise en compte des risques locaux de calamités naturelles ; pour la sécurité liée à l'organisation, de l'intégration de l'environnement culturel et humain local ainsi que du niveau d'interopérabilité, lequel détermine la sécurité offerte dans le cadre des communications inter-sites.

Note complémentaire n°6 :

On se réfère généralement à trois grandes familles d'organisation :

- L'organisation fonctionnelle.

  Chaque fonction de l'organisme forme une unité spécialisée (production, logistique, finances, etc.).

  La prise de décision appartient au niveau central et elle est transmise par la structure hiérarchique ce qui peut générer la rétention d'informations et favoriser ainsi l'émergence de flux informels.

- L'organisation opérationnelle ou divisionnelle.

  L'activité est organisée en divisions par produits, marchés, types de clientèle, domaine d'activités stratégiques.

  La prise de décisions se fait de manière décentralisée au niveau de la division.

  Il existe un risque de manque de communication entre les divisions qui peut éventuellement induire des communications informelles plus rapides et plus souples que par la voie de transmission normale.

- L'organisation matricielle.

  Chaque mission est le croisement de moyens communs (fonctions) auxquels elle recourt.

  L'organisation vise à équilibrer la logique des fonctions avec la logique des domaines d'activités.

  L'aspect communication et décision peut se révéler délicat du fait des dépendances hiérarchiques et fonctionnelles différentes pour un même

individu ou une même unité. Cela nécessite donc un effort particulier de clarté dans les procédures de communication et de coordination.

Annexe 2

Les critères d'évaluation de la sécurité des systèmes informatiques (ITSEC)

L'évaluation selon les ITSEC peut concerner un système dont l'environnement d'exploitation est connu dès la conception ou un produit proposé sur catalogue et pour lequel ne peuvent être faites que des hypothèses sur son environnement d'utilisation.

L'évaluation d'un système ou d'un produit permet d'obtenir l'assurance qu'il fournit une sécurité adéquate pour satisfaire ses objectifs de sécurité. Il est prévisible qu'à moyen terme de nombreux produits évalués seront disponibles pour répondre aux besoins des utilisateurs. Ceux-ci pourront, par exemple, utiliser des produits évalués qui leur conviennent pour la conception d'un système ; ou bien ils pourront adapter les objectifs de sécurité qu'ils définissent à ceux de produits déjà évalués ; ils pourront aussi inclure des produits évalués dans un système existant. Les ITSEC constituent le référentiel pour ces évaluations que les utilisateurs adapteront à leurs besoins d'autant plus facilement qu'elles seront nombreuses.

Ces évaluations nécessitent un examen approfondi du système ou du produit, depuis sa conception jusqu'à son exploitation courante.
L'expression anglaise "target of evaluation" est traduite par cible d'évaluation ; elle est utilisée dans les ITSEC pour désigner le système ou le produit à évaluer et qui est une émanation de la cible de sécurité.

2.1. Les acteurs

La démarche des ITSEC identifie trois acteurs principaux qui sont concernés par l'évaluation et définit leurs responsabilités respectives :

- le ***commanditaire*** de l'évaluation est l'autorité propriétaire du système ou du produit qui définit les besoins à satisfaire et qui est à l'origine de la demande d'évaluation. Il doit définir la cible de sécurité pour l'évaluation ; le commanditaire et le développeur peuvent être confondus,

- le ***développeur*** est la personne qui réalise la cible d'évaluation compte tenu de l'expression de besoins du commanditaire,

- l'***évaluateur*** est la personne qui effectue l'évaluation de la sécurité.

Une évaluation nécessite la collaboration de ces trois acteurs, si possible dès le début du développement de la cible d'évaluation. Autant pour préserver le maximum d'objectivité dans les résultats d'une évaluation que pour réduire la charge et les frais de l'évaluation, il est prévu que le commanditaire fournisse les éléments de preuve exigés. Ceux-ci sont vérifiés par l'évaluateur qui doit aussi effectuer des tests complémentaires.

2.2. La cible de sécurité

Cette cible qui a été définie par le commanditaire et qui peut être utilisée pour le développement du système, contient tous les renseignements relatifs aux spécifications de la sécurité.

C'est l'étape fondamentale de la conception d'un système selon les principes exposés dans la première partie ; c'est la référence de base pour l'évaluation selon les ITSEC.

Cette cible caractérise la politique de sécurité du système (ou l'argumentaire du produit) et elle contient :

- les objectifs de sécurité,
- la politique technique de sécurité, donnant
- la spécification des fonctions de sécurité, la définition des mécanismes de sécurité (optionnelle) et l'annonce de la résistance minimum des mécanismes de sécurité,
- les mesures non techniques,
- le niveau d'évaluation visé pour cette cible d'évaluation correspondant au degré de confiance nécessaire.

2.3. La fonctionnalité

Compte tenu de ses objectifs de sécurité, la cible d'évaluation doit contenir des fonctions de sécurité appropriées. Celles-ci peuvent être déclarées de façon explicite, ou bien en référence à des classes prédéfinies ou à des normes.

La spécification des fonctions de sécurité est la partie la plus importante de la cible de sécurité. Pour les niveaux élevés, la spécification en langage naturel doit être précisée par une spécification de type semi-formel ou formel, de façon à éliminer les ambiguïtés du langage. Ces fonctions sont regroupées logiquement suivant les huit rubriques génériques suivantes :

identification et authentification,

- contrôle d'accès,

- imputabilité,
- audit,
- réutilisation d'objet,
- fidélité,
- fiabilité de service,
- échanges de données.

2.4. Les critères d'assurance

L'évaluation est conduite selon des critères permettant d'avoir l'assurance d'une part que les fonctions et mécanismes de sécurité satisfont les objectifs de sécurité et, d'autre part, qu'ils ont été implémentés et qu'ils seront exploités correctement.

- ***assurance-efficacité*** : les fonctions et mécanismes doivent être efficaces pour contrer les menaces identifiées.

  L'estimation de l'efficacité est indépendante du niveau d'évaluation ; elle consiste à vérifier que les fonctions sont efficaces pour satisfaire les objectifs déclarés : elle porte sur la pertinence du choix des fonctions, leur cohésion, les conséquences d'éventuelles vulnérabilités découvertes et la facilité d'emploi.

  Elle est faite sous deux angles différents en examinant les aspects suivants :

  sous l'angle de la ***construction*** :
  - pertinence du choix des fonctions,
  - cohésion des fonctions et mécanismes au sein de la cible d'évaluation,
  - résistance des mécanismes à une attaque directe,
  - vulnérabilités dans la construction de la cible d'évaluation,

  sous l'angle de l'***exploitation*** :
  -facilité d'emploi pour une exploitation sûre,
  -vulnérabilités en exploitation.

- ***assurance-conformité*** : les fonctions et mécanismes doivent être correctement développés et exploités.

  L'estimation de la conformité est directement liée au niveau d'évaluation choisi (E1 à E6), c'est-à-dire que les exigences de conformité sont d'autant plus grandes que le niveau est élevé ; elle consiste à étudier la manière dont la cible d'évaluation a été construite et dont elle sera exploitée.

  L'estimation de la conformité est réalisée à partir des critères correspondant au niveau d'évaluation visé. Ces critères ont tous la même

structure mais ils se différencient par leur niveau de détail, en particulier dans l'examen du processus de développement.

Là encore, la cible d'évaluation est examinée sous les angles de la construction et de l'exploitation puis, dans chaque cas, sous différents aspects ou phases ;

sous l'angle de la ***construction*** :
- le processus de développement,
- l'environnement de développement,

sous l'angle de l'***exploitation*** :
- la documentation d'exploitation,
- l'environnement d'exploitation.

C'est au commanditaire de l'évaluation que revient la charge de fournir toute la documentation nécessaire, en respectant les exigences de contenu et de présentation ainsi que, à partir du niveau E2, les éléments de preuve issus des résultats des tests effectués pendant le développement.

Le résultat de l'évaluation, en cas de succès, est une confirmation que la cible d'évaluation satisfait ses objectifs de sécurité avec un niveau d'assurance correspondant au niveau d'évaluation visé. Si une vulnérabilité exploitable, au niveau considéré, a été découverte au cours de l'évaluation et n'a pas été éliminée, la cible d'évaluation recevra le niveau E0.

2.5. Conclusion

Au delà d'un simple catalogue de critères, les ITSEC proposent une approche méthodique et cohérente pour examiner la façon dont est prise en compte la sécurité dans la conception, le développement et l'exploitation d'un système d'information. Cette approche exige en particulier que les objectifs de sécurité aient été définis au préalable pour que l'on puisse apprécier, grâce à l'évaluation, la manière dont les fonctions de sécurité parviennent à les satisfaire.

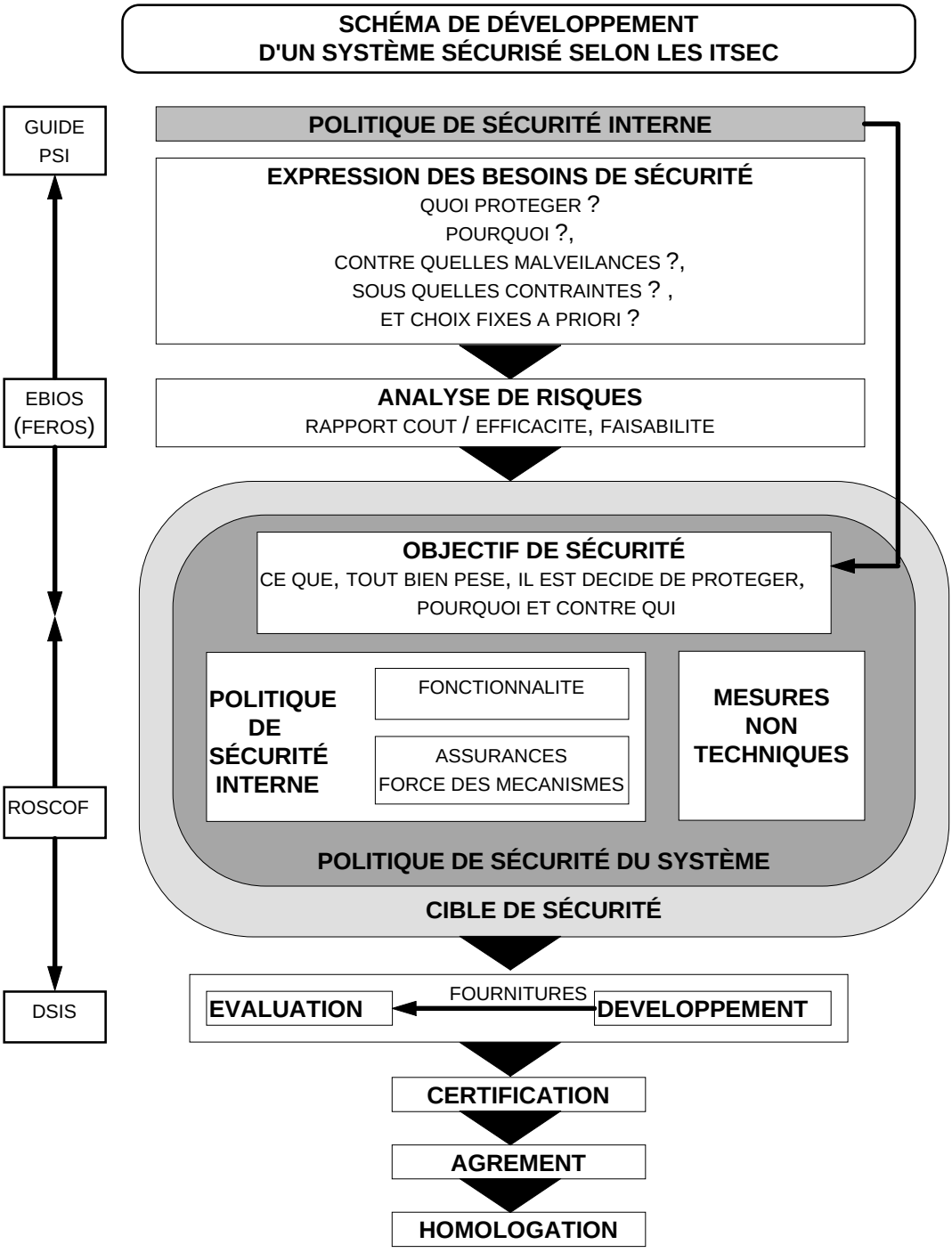
L'élaboration de ces critères a été guidée par le souci de préserver le maximum d'objectivité dans les résultats d'une évaluation. Ils sont utilisables pour l'évaluation d'une gamme très large de produits de sécurité et de systèmes d'information sécurisés. De plus, leur adoption par une communauté internationale est favorable au développement du marché de la sécurité.

La Commission de l'Union Européenne a prévu une recommandation du Conseil pour promouvoir l'utilisation des ITSEC au sein de la Communauté. L'ISO entame des travaux en matière de normalisation de critères d'évaluation sur la base des ITSEC. De même, l'OTAN travaille à la reformulation de ses propres critères.

La prise en compte des ITSEC a été officialisée pour l'administration française. Ils constituent la pièce importante de l'œuvre de sécurisation dont

l'objectif est d'améliorer la sécurité et, pour cela, de faire naître un marché de produits développés conformément aux nouveaux besoins des utilisateurs.

Il est important que ces utilisateurs, au sens large, soient bien persuadés que seule une approche globale comme celle qui a été présentée ci-dessus peut permettre de bien traiter le problème de la sécurité du traitement de l'information, problème qui ne peut être résolu que s'il a été clairement défini.



Page laissée blanche

Annexe 3

Lignes directrices régissant la sécurité des systèmes d'information (OCDE)

3.1. Introduction

Adoptée par les 24 pays membres de l'OCDE, la version actuelle (novembre 1992) de ces lignes directrices constitue un document de référence de portée internationale.
Elles ont pour but de sensibiliser aux risques menaçant les systèmes d'information, d'aider les personnes responsables de la sécurité des systèmes d'information et de promouvoir la coopération internationale dans ce domaine.
Elles se présentent sous la forme des principes résumés ci-après.

3.2. Principe de responsabilité

Les attributions et responsabilités des propriétaires, des fournisseurs, des utilisateurs de systèmes d'information et des autres parties concernées par la sécurité des systèmes d'information, doivent être explicitement exprimées.

3.3. Principe de sensibilisation

Pour favoriser la confiance envers les systèmes d'information, les propriétaires, les fournisseurs, les utilisateurs et toute autre entité concernée doivent pouvoir connaître, de façon compatible avec le maintien de la sécurité, à tout moment l'existence et l'ampleur des mesures, pratiques et procédures visant à la sécurité des systèmes d'information.

3.4. Principe d'éthique

La fourniture et l'utilisation des systèmes d'information, ainsi que la mise en œuvre de leur sécurité doivent être telles que les intérêts légitimes des tiers soient respectés.

3.5. Principe de pluridisciplinarité

Les mesures, pratiques et procédures de sécurité des systèmes d'information doivent prendre en compte toutes les considérations pertinentes qu'elles soient d'ordre technique ou administratif, et concernant l'organisation, l'exploitation, le commerce, l'éducation ou le droit.

3.6. Principe de proportionnalité

Les niveaux, coûts, mesures, pratiques et procédures de sécurité doivent être appropriés et proportionnés à la valeur et au degré de dépendance envers les systèmes d'information, ainsi qu'à la gravité, la probabilité et l'ampleur des éventuels préjudices.

3.7. Principe d'intégration

Les mesures, pratiques et procédures de sécurité des systèmes d'information doivent être coordonnées et harmonisées entre elles et les autres mesures, pratiques et procédures de l'organisme, afin de réaliser un dispositif de sécurité cohérent.

3.8. Principe d'opportunité

Les organismes publics ou privés, au plan national et international, doivent agir en temps opportun de manière coordonnée afin d'empêcher les atteintes à la sécurité des systèmes d'information, ou d'y faire face.

3.9. Principe de réévaluation

La sécurité des systèmes d'information doit être réévaluée périodiquement car les systèmes d'information et les exigences de sécurité varient dans le temps.

3.10. Principe de démocratie

La sécurité des systèmes d'information doit être compatible avec l'utilisation et la circulation légitimes des données et des informations dans une société démocratique.

Annexe 4

Codes d'éthique des métiers des technologies de l'information

4.1. Codes d'éthique de l'IFIP (International Federation for Information Processing)

Un code d'éthique a été élaboré par l'IFIP (International Federation for Information Processing) dont l'AFCET est membre, pour la France.

Ce code s'adresse non seulement aux professionnels de l'informatique mais encore aux organisations multinationales de l'informatique et à tous ceux qui se sentent concernés par les problèmes juridiques internationaux de l'informatique et par les règles publiques en ce domaine.

Le code est constitué des rubriques suivantes:

- éthique professionnelle des personnes,
- éthique des organisations internationales,
- éthique pour la législation internationale,
- éthique pour la politique internationale.

4.2. Codes d'éthique nationaux

4.2.1. Association Française des Informaticiens (AFIN)

Un code d'éthique, élaboré par l'Association française des informaticiens, est destiné à guider l'informaticien sur ses devoirs et droits. Le texte du code peut être adjoint aux contrats de travail et fait référence devant le Conseil des prud'hommes. Le texte s'articule autour de quatre grands chapitres :

- informaticiens et entreprise,
- entreprise et informaticiens,
- informaticien prestataire,
- informaticien vis-à-vis de ses confrères.

4.2.2. CLUb de la Sécurité Informatique Français (CLUSIF)

Code d'Éthique, 13 janvier 1991.

Ce code s'adresse en priorité aux membres du CLUSIF qui doivent s'y conformer sous peine d'exclusion.

Il est recommandé à tous les professionnels ou utilisateurs de l'informatique.
Le code du CLUSIF aborde les principes d'éthique selon les aspects suivants :

- règles générales,
- partie applicable aux consultants, niveau schéma directeur de la sécurité des systèmes d'information,
- partie applicable aux intervenants, niveau conception détaillée,
- partie applicable aux intervenants, niveau réalisation,
- partie applicable aux intervenants, niveau contrôle,
- partie applicable aux intervenants, niveau maintenance.

4.3. Autres codes d'éthique dans le monde

4.3.1. Association for Computing Machinery (ACM)

4.3.1.1. Code of Professionnal Conduct, 1972

Ce code présente des principes généraux, chacun étant décliné sous l'aspect de l'éthique professionnelle et sous formes de règles à appliquer.

Les principes généraux s'adressent à tout membre de l'ACM et sont les suivants :

- l'intégrité,
- la compétence professionnelle,
- la responsabilité professionnelle,
- l'utilisation de ses compétences pour l'amélioration du bien-être de l'humanité.

4.3.1.2. Code of Ethics and Professionnal Conduct

Ce code identifie les situations que les professionnels peuvent rencontrer et fournit des conseils pour y faire face.

Il est découpé en 4 sections :

- impératifs moraux généraux,

- responsabilités professionnelles plus spécifiques,
- impératifs relatifs aux dirigeants,
- respect du code.

4.3.2. British Computer Society (BCS)

Code of Conduct, 1990.

Ce code s'adresse aux membres de la BCS.
Les principes de base du code concernent :

- la conduite professionnelle,
- l'intégrité professionnelle,
- la préservation de l'intérêt public et du droits des tiers,
- la fidélité à l'employeur ou au client et le respect de la confidentialité des informations de l'employeur ou du client,
- la compétence technique,
- l'impartialité.

4.3.3. American Society for Information Science (ASIS)

Code of Ethics for Information Professionals.

Ce code s'applique aux membres de l'ASIS, il aborde les domaines suivants :

- responsabilité envers les employeurs, les clients et les utilisateurs,
- responsabilité envers la profession,
- responsabilité envers la société.

4.3.4. Computer Professionals for Social Responsibility (CPSR) and Privacy International (PI)

Code of Fair Information Practices to promote information privacy.

Les thèmes abordés concernent les données sur les personnes :

- ne pas utiliser de données personnelles dans un autre but que celui initialement prévu sans consentement spécifique,
- ne collecter que l'information nécessaire,
- assurer l'intégrité des données,
- informer les sujets de la mémorisation et de l'usage des informations qui les concernent, leur donner le droit de vérification et de correction,
- établir et diffuser la politique relative à la protection de la vie privée.

Page laissée blanche

Annexe 5

Textes législatifs et réglementaires relatifs aux informations relevant du secret de défense

5.1. Textes fondamentaux

5.1.1. Nouveau Code pénal (1994)

- Art. 410-1 à 414-9 : Des atteintes aux intérêts fondamentaux de la nation.
- Art. 226-13 et 226-14 relatifs au secret professionnel

5.1.2. Décret-loi du 18 avril 1939 modifié par l'ordonnance n°58-917 du 7 octobre 1958 modifié par le décret n°72-743 du 12 juin 1972

fixant le régime des matériels de guerre, armes et munitions, dont les articles 12 et 13, fixant les conditions d'exportation des matériels de cryptologie.
Remarque : Décret d'application n°95-589 du 6 mai 1995 et voir code pénal .

5.1.3. Décret n°79-1160 du 28 décembre 1979

relatif aux conditions d'application aux traitements d'informations nominatives intéressant la sûreté de l'État, la défense et la sécurité publique de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

5.1.4. Décret n°81-514 du 12 mai 1981

relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'État.

5.2. Principales instructions et directives

Ce paragraphe doit être complété - tout particulièrement pour la réglementation sur la cryptologie et les signaux parasites compromettants - par **le Répertoire des documents relatifs à la sécurité des systèmes d'information** n°980/SCSSI (Diffusion restreinte), mise à jour et édité par le SCSSI, 18 rue du Dr Zamenhof, 91131 Issy-les-Moulineaux.

5.2.1. Instruction interministérielle n°500bis/SGDN/TTS/SSI/DR du 18 octobre 1996

relative au chiffre dans la sécurité des systèmes d'information

5.2.2. Instruction interministérielle n°910/SGDN/SSD/DR et n°910/SGDN/DISSI/SCSSI/DR du 19 décembre 1994

sur les articles controlés de la sécurité des systèmes d'information (ACSSI).

5.2.3. Instruction Interministérielle n°300/SGDN/TTS/SSI/DR du 21 juin 1997

relative à la protection contre les signaux parasites compromettants.

5.2.4. Instruction générale interministérielle n°1300/SGDN/SSD/DR du 12 mars 1982

relative à la protection du secret et des informations concernant la Défense nationale et la sûreté de l'État.

5.2.5. Instruction Interministérielle n°2000/SGDN/SSD/DR du 1er octobre 1986

relative à la protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les marchés et autres contrats.

5.2.6 Instructions générales interministérielles n°900/SGDN/SSD/DR et n°900/DISSI/SCSSI/DR du 20 juillet 1993

relative à la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées.

5.2.7. Directive n°485/SGDN/DISSI/SCSSI/DR du 15 décembre 1988

relatif à l'installation des sites et systèmes d'information : protection contre les signaux compromettants.

Annexe 6

Textes législatifs et réglementaires relatifs aux informations ne relevant pas du secret de défense

6.1. Textes fondamentaux

6.1.1. Code pénal

Art. 226-1 et 226-2 : relatifs aux secrets de la vie privée.
Art 226-13 et 226-14 : relatifs au secret professionnel
Art. 411-6 à 411-8, Art. 411-10, Art. 414-1 à 414-9
relatifs aux informations ne relevant pas du secret de défense.

6.1.2. Loi n°68-678 du 26 juillet 1968 Loi n°80-538 du 16 juillet 1980

relatives aux secrets économiques et industriels.
Code de la propriété intellectuelle : Art. L621 relatif au secret de fabrique.

6.1.3. Contrôle de la destination finale

Décret du 30 novembre 1944.
Arrêté du 30 janvier 1967.
Avis n°9 du 24 janvier 1992, modifications du 8 mai et du 27 août 1992, complément du 30 décembre 1992.
Avis du Ministère de l'Économie, des Finances et du Budget du 2 janvier 1992, relatif aux produits et technologies soumis au contrôle de la destination finale, modifié par l'avis du 8 mai 1992 et par l'avis du 30 décembre 1992.
Remarque : un règlement européen est en projet.

6.2. Principaux guides

6.2.1. Guide n°400 SGDN/DISSI/SCSSI du 18 octobre 1991

relatives à l'installation des sites et systèmes traitant des informations sensibles ne relevant pas du secret de défense : protection contre les signaux parasites compromettants.

6.2.2. Guide n°600 DISSI/SCSSI de mars 1993

relatives à la protection des informations sensibles ne relevant pas du Secret de Défense : recommandations pour les postes de travail informatiques.

6.2.3. Guide n°650/DISSI/SCSSI du 28 mars 1994

relatives à la menace et aux attaques informatiques.

6.2.4. Recommandation n°901/DISSI/SCSSI du 2 mars 1994

relative à la sécurité des systèmes d'information traitant des informations sensibles non classifiées de défense.

6.3. Textes particuliers

6.3.1. Loi n°72-662 du 13 juillet 1972, art. 18

portant statut général des militaires relatif à l'obligation de discrétion professionnelle.

6.3.2. Loi n°78-753 du 17 juillet 1978, art. 6

relatif au droit d'accès aux documents administratifs et portant sur diverses mesures d'améliorations des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

6.3.3. Loi n°83-634 du 13 juillet 1983, art. 26 et art. 27

portant droits et obligations des fonctionnaires relatif à l'obligation de discrétion professionnelle.

Annexe 7

Textes législatifs et recommandations relatifs à la lutte contre la malveillance

7.1. Textes sur la protection juridique des informations

7.1.1. Code pénal

Art. 226-15 sur le secret des correspondances,
Art. 226-16 à 226-24 sur les traitements automatisés d'informations nominatives,
Art. 323-1 à 323-7 relatifs aux atteintes aux systèmes de traitements automatisés de données.

7.1.2. Directive n°91/250/CEE du 14 mai 1991, modifiée par la Directive n°93/98/CEE du 29 octobre 1993

concernant la protection juridique des programmes d'ordinateur.

7.1.3. Loi n°57-298 du 11 mars 1957

relative à la propriété littéraire et artistiques

7.1.4. Loi n°85-660 du 3 juillet 1985

relative aux droits d'auteur et aux droits des artistes interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communications audiovisuelle.

7.1.5. Loi n°86-1067 du 30 septembre 1986 modifiée par la loi n°89-25 du 17 janvier 1989

relative à la liberté de communication.

7.1.6. Loi n°89-816 du 2 novembre 1989

relative à la protection des topographies de produits semi-conducteurs.
Art L.622 du code de la propriété intellectuelle

7.1.7. Loi n°91-646 du 10 juillet 1991

relative au secret des correspondances émises par la voie des télécommunications.
L'art. 25 précise les peines encourues par quiconque aura illégalement intercepté, détourné, utilisé ou divulgué des correspondances transmises par la voie des télécommunications.
Art. 226-3 et 226-15 alinéa 2 du Code pénal.
Art. Art. 432-9 du Code pénal.

7.1.8. Loi n°92-546 du 20 juin 1992

relative au dêpôt légal

7.1.9. Loi n°92-597 du 1er juillet 1992

relative au code de la propriété intellectuelle (partie législative)

7.1.10. Loi n°94-361 du 10 mai 1994

relatif à la protection des logiciels.

7.1.11. Décret n°62-53 du 10 janvier 1962

portant publication de la cnvention révisée pour la protection de la propriété intellectuelle.

7.1.12. Décret n°74-743 du 21 août 1974

portant publication de la Convention de Berne pour la protection des œuvres littéraires et artistiques.

7.1.13. Circulaire du 17 octobre 1990 du Premier ministre

relative à la protection juridique des logiciels.

7.1.14. Code de la propriété intellectuelle, issu de la loi n°92-597 du 1 juillet 1992, modifiée par la loi n°94-102 du 5 février 1994

relative aux droits d'auteurs.

7.1.15. Code des Postes et Télécommunications, art. L.41

relatif au secret de la correspondance confiée aux services de télécommunications.

7.2. Textes sur la lutte contre la malveillance

7.2.1. Recommandation n°81-94 du 21 juillet 1981 (Commission nationale informatique et libertés)

relative aux mesures générales de sécurité des systèmes informatiques ; cette recommandation s'adresse aux détenteurs et aux utilisateurs de fichiers nominatifs, en complément de la loi n°78-17 du 6 janvier 1978.

7.2.2. Recommandation du Conseil de l'Europe adoptée par le Conseil des ministres le 19 septembre 1989

relative à la criminalité en relation avec l'ordinateur.

7.2.3. Décision n°92/242/CEE du 31 mars 1992

relative à la sécurité des systèmes d'information.

7.3. Textes sur la cryptologie

7.3.1. Loi n°90-1170 du 29 décembre 1990 modifiée par la loi n°91-648 du 11 juillet 1991, la loi n°93-1 du 1 avril 1993 et la loi n°96-659 du 26 juillet 1996

relative à la réglementation des télécommunications.
L'article 28 de cette loi précise ce qui doit être entendu par moyens cryptologiques.

7.3.2. Loi n°92-1477 du 31 décembre 1992

relative aux produits soumis à certaines restrictions de circulation, notamment l'article 2.

7.3.3. Décret n°92-1358 du 28 décembre 1992

définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie.

7.3.4. Arrêtés du 28 décembre 1992

le premier, concernant les déclarations et demandes d'autorisation relatives aux moyens et prestations de cryptologie, le second, définissant les dispositions particulières auxquelles sont soumises les prestations de cryptologie.

7.3.5. Arrêté du 15 février 1993

fixant les modalités d'établissement de la demande de licence d'exportation des moyens de cryptologie et d'utilisation de cette licence.

Page laissée blanche

Annexe 8

Les guides méthodologiques développés par le Service Central de la Sécurité des Systèmes d'Information

Les ITSEC définissent le cadre de l'évaluation d'un système ou d'un produit conçu selon les principes exposés dans l'annexe précédente ; cette démarche d'ensemble comprend les étapes suivantes :

- **l'expression des besoins et l'identification des objectifs de sécurité**
  cette étape nécessite une analyse complète et rigoureuse selon les principes exposés dans le chapitre 6 du présent guide.
  *Le SCSSI a mis au point un guide méthodologique pour faciliter cette analyse : Le guide **EBIOS** et sa fiche de synthèse **FEROS** (Fiche d'Expression Rationnelle des Objectifs de Sécurité).*
- **le choix des fonctions de sécurité et du niveau d'évaluation pour des objectifs donnés**
  la démarche qui doit guider la conception d'un système conduit à définir ses objectifs de sécurité ; une fois ces objectifs fixés, les fonctions de sécurité et le niveau d'évaluation sont choisis de façon à les satisfaire. Mais ce choix est une étape délicate de la conception qui nécessite de la part du concepteur beaucoup d'expérience et de savoir-faire.
  *Le SCSSI a mis au point un guide pour faciliter ce choix : **ROSCOF** (Réalisation des objectifs de sécurité par le choix de fonctions).*
- **et, un document plus spécifique traitant de Classes de fonctions de sécurité pour Ateliers de Génie Logiciel : F-SEE-1**

- **enfin, la prise en compte de la sécurité au cours du développement**
  une fois la cible de sécurité définie, la phase de développement du système doit également être conduite de façon sûre.
  *Le SCSSI a mis au point un guide pour faciliter cette démarche : **DSIS** (Développement de systèmes d'information sécurisés).*

Page laissée blanche

Annexe 9

Liste des règles contenues dans le guide

Page laissée blanche

Rappel : "3" : règle de base - " s " : règle à caractère majeur pour organismes sensibles

La règle prévoit..... page