Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Guide pour l'élaboration d'une politique de sécurité de système d'information

PSSI

SECTION 1
INTRODUCTION

Version du 3 mars 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante
(voir formulaire de recueil de commentaires en fin de guide) :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Version	Objet de la modification	Statut
15/09/1994 (1.1)	Publication du guide d'élaboration de politique de sécurité interne (PSI).	Validé
2002	Révision globale : - actualisation des références, - création d'une méthodologie, - enrichissement et reclassement des principes de sécurité, - séparation en 3 sections (méthodologie, principes de sécurité et compléments).	Draft
2003	Restructuration, remise en forme, amélioration de la méthode, mise en cohérence avec les outils méthodologiques et meilleures pratiques de la DCSSI suite à une consultation d'experts internes.	Prétest
23/12/2003	Séparation en 4 sections (introduction, méthodologie, principes de sécurité et références SSI) et améliorations diverses suite à une consultation d'experts externes (notamment le Club EBIOS) et à plusieurs mises en pratique (ministère de la Défense, CNRS, Direction des Journaux Officiels…).	Prétest pour validation
03/03/2004	Publication du guide pour l'élaboration d'une politique de sécurité de système d'information (PSSI)	Validé

Table des matières

Avant-propos

Le présent document est un guide destiné aux administrations et aux entreprises.

Ce document édité par le Secrétariat général de la défense nationale est un guide, il n'a pas de caractère obligatoire.

Le guide s'appuie sur des documents législatifs ou normatifs ainsi que sur l'expérience et le savoir-faire d'administrations et d'acteurs du secteur privé.

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

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

Concepts manipulés

Voici les trois définitions essentielles des concepts manipulés dans le document :

Politique de Sécurité de Système d'Information (PSSI)	Ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme.
Principe de sécurité	Les principes de sécurité sont l'expression des orientations de sécurité nécessaires et des caractéristiques importantes de la SSI en vue de l'élaboration d'une PSSI.
Règle de sécurité	Les règles de sécurité définissent les moyens et les comportements définis dans le cadre de la PSSI. Elles sont construites par déclinaison des principes de sécurité dans un environnement et un contexte donnés.

Conventions d'écriture

Dans la suite des guides PSSI, nous utiliserons les conventions suivantes :

Organisme	Entreprise, association, établissement, ministère, département ministériel, administration particulière, organisme sous-tutelle, collectivité territoriale…
Responsable SSI	Ministre, Haut fonctionnaire de défense, Fonctionnaire de sécurité des systèmes d'information, Responsable de la sécurité des systèmes d'information…
Validation	Reconnaissance officielle par l'autorité responsable de l'organisme
[ ]	Les crochets encadrent une référence placée en bibliographie
italique	Le texte en italique indique un extrait de référence

1 Présentation du guide

1.1 Objectif

Ce guide a pour objectif majeur de fournir un support aux responsables SSI pour élaborer une politique de sécurité du ou des systèmes d'information (PSSI) au sein de leur organisme.

Ce guide présente une méthode et un ensemble de principes de sécurité et de références, pour élaborer une PSSI adaptée à son environnement. Il ne constitue pas un résultat final qu'un responsable SSI peut recopier.

Ainsi, les responsables SSI pourront suivre une démarche structurée et décliner les principes de sécurité sous la forme de règles de sécurité adaptées à leurs métiers et activités.

1.2 Champ d'application

La portée de ce guide couvre les besoins du secteur public et du secteur privé.

Appliqué aux ministères, il est plus particulièrement destiné aux acteurs de la voie fonctionnelle SSI, tels que les fonctionnaires de sécurité des systèmes d'information (FSSI) ou autorités qualifiées, afin de mettre en place une PSSI, conformément aux instructions interministérielles et pour satisfaire les besoins de leurs métiers.

Appliqué aux autres types d'organismes, il s'adresse plus particulièrement aux responsables de la sécurité des systèmes d'information (RSSI) et propose une approche pour l'application des actions de sécurité conformes à l'état de l'art en matière de principes de protection appliqués aux systèmes d'information.

De façon plus globale, ce guide s'adresse aux personnes qui ont la responsabilité de définir ou de faire évoluer une organisation de la sécurité au sein d'un organisme, public ou privé. Il apporte une aide à la préparation d'un projet de définition et/ou de déploiement d'une PSSI applicable à l'ensemble des systèmes d'information de l'organisme ou à un système d'information spécifique.

Il est finalement destiné à l'ensemble des acteurs de l'organisme dans un but de sensibilisation et d'adhésion aux principes.

1.3 Description

Le guide PSSI est décomposé en quatre sections :

- l'introduction, ce présent document, permet de situer la place de la PSSI dans le référentiel normatif de la SSI au sein de l'organisme et de préciser les bases de légitimité sur lesquelles elle s'appuie ;

- la méthodologie présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité ;

- le référentiel de principes de sécurité ;

- une liste de documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthiques, notes complémentaires...).

L'attention du lecteur est attirée sur le fait que les sections composant le guide PSSI seront mises à jour indépendamment par le Secrétariat général de la défense nationale sur la base des retours d'expérience et des contributions de lecteurs.

Un formulaire de recueil de commentaires figure en annexe de chaque section du guide afin de renvoyer des propositions et remarques au Bureau Conseil de la DCSSI.

1.4 Historique

Ces documents sont une mise à jour de la version 1.1 du "Guide pour l'élaboration d'une politique de sécurité interne (PSI)", paru en septembre 1994.

La DCSSI a souhaité présenter des éléments pragmatiques et mieux adaptés aux environnements des administrations, entreprises et autres organismes du secteur public et du secteur privé. Il a également souhaité profiter de cette évolution pour réaliser une mise à niveau des documents de références utilisables et approfondir des thèmes de la sécurité non traités dans la précédente version.

Cette nouvelle version est organisée différemment pour assurer une maintenance plus efficace des principes de sécurité et des meilleures pratiques.

Les évolutions des sections du guide PSSI consistent à :

- actualiser l'ensemble des références ;

- enrichir les principes de sécurité afin de mieux couvrir l'ensemble des domaines de la SSI en utilisant des normes internationales ([ISO 15408], [ISO 13335], [ISO 17799]…) et les réorganiser sur la base d'une étude comparative des principaux référentiels SSI nationaux et internationaux ;

- développer une approche méthodique pour élaborer une PSSI, s'appuyant sur le référentiel de l'organisme et une analyse des risques SSI ;

- permettre l'élaboration de PSSI spécifiques (à un métier, à un système d'information…) dans le cadre de PSSI globales afin de réduire les coûts de réalisation et de garantir une cohérence de tout le référentiel d'un organisme ;

- séparer le guide en quatre sections autonomes (introduction, méthodologie, principes de sécurité et références SSI).

2 Présentation et rôle de la PSSI

2.1 Contexte de la sécurité des systèmes d'information

2.1.1 La SSI comme élément de la qualité

La sécurité du système d'information est devenue un facteur indispensable au bon fonctionnement de l'organisme.

Le développement rapide des technologies de l'information a entraîné une dépendance croissante des organismes envers leur système d'information, devenu une composante stratégique.

Par ailleurs, l'utilisation croissante des systèmes d'information pour des applications variées 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 et sûrs (disponibilité, intégrité, confidentialité et parfois preuve).

2.1.2 La gestion des risques par la sécurisation est globale

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 PSSI.

Les qualifications requises pour assumer la responsabilité de sécurité des systèmes d'information ont elles aussi évolué. Là où une formation technique était suffisante, l'évolution des enjeux qui pèsent sur le système d'information rend obligatoire une compétence multiple des responsables sécurité et l'adoption d'une approche systémique (prenant en compte les différents systèmes, tels que le système entreprise, le système de gestion de la sécurité, ou le système d'information, et leurs interactions). 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 de gestion des personnels liés), à l'organisation et aux méthodes et techniques utilisées.

2.1.3 Des risques étendus et parfois nouveaux

Les menaces ont pris une nouvelle dimension tant du point de vue de leur origine que du point de vue de leurs objectifs et de l'importance de leurs impacts. L'interconnexion des réseaux est aujourd'hui réelle et transfrontière. Cette évolution facilite la transmission de l'information mais aussi son agression (modifications et vols) et les moyens d'attaque ne sont plus l'apanage d'une élite gouvernementale.

De nombreux organismes sensibilisés à la SSI ont pris conscience de la nécessité de disposer de règles de sécurité des systèmes d'information pour leur permettre de mettre en place des espaces de confiance. Cette prise de conscience a donné lieu à la formalisation de méthodes et de référentiels de sécurité.

2.2 Nécessité d'une PSSI

Compte tenu du niveau des risques liés à la pression continue de la menace, une défaillance de la sécurité du système d'information pourrait entraîner des conséquences irréversibles sur la réalisation des objectifs stratégiques de l'organisme ou vis à vis du respect de ses obligations ou engagements. C'est pourquoi la PSSI (le référentiel final) doit être prise en compte et validée au niveau de responsabilité le plus élevé comme un instrument de gestion des risques SSI.

La PSSI traduit la reconnaissance formelle de l'importance accordée par la direction générale de l'organisme à la sécurité de son ou ses systèmes d'information.

Face aux menaces qui pèsent sur les systèmes d'information, l'usager exige une protection adaptée des informations et des services de traitement, d'archivage et de transport de l'information. La sécurité est donc devenue l'une des dimensions essentielles de la stratégie de l'organisme et elle doit être

prise en compte dès la conception d'un système d'information afin d'assurer la protection des biens et des personnes et du patrimoine de l'organisme. Ainsi, la sécurité des systèmes d'information vise en particulier à protéger les composantes suivantes du patrimoine :

- le patrimoine matériel, composé des biens matériels nécessaires au fonctionnement de ses activités et dont la détérioration pourrait interrompre, diminuer ou altérer son activité ; ce patrimoine est essentiellement composé des technologies de l'information et de communication (serveurs, réseau, postes de travail, téléphonie...), mais aussi des procédures et applications logicielles traduisant les processus et les fonctions métiers de l'organisme ;
- le patrimoine immatériel et intellectuel, composé de toutes les informations concourant au métier de l'organisme (données scientifiques, techniques, professionnelles, administratives…) ;
- les informations relatives aux personnes (physiques et morales) avec qui l'organisme est en relation, dont la destruction, l'altération, l'indisponibilité ou la divulgation pourrait entraîner des pertes ou porter atteinte à son image de marque voire entraîner des poursuites judiciaires.

La PSSI définit la politique de sécurité d'une entité spécifique qui peut être un système technologique, une fonction automatisée ou une application mais aussi un organisme entier comme une entreprise ou un département ministériel. Une entreprise repose sur son personnel, sa culture, ses informations et ses processus de gestion (traitement, stockage ou/et transfert) des informations. Ce sont ces processus d'entreprise qui font toute la différence entre deux "organisations" au but similaire, dans le même secteur économique.
Chaque processus repose sur l'organisation, les procédures et la technologie. Se limiter aux aspects technologiques est donc insuffisant car il est nécessaire de considérer également les aspects non techniques.
La démarche de gestion des risques, dont les risques SSI, est une activité fonctionnelle, opérationnelle et managériale comme les autres.

Rappelons que les risques informatiques, tout comme les risques informationnels, sont des risques opérationnels pour les systèmes d'information malgré leur caractère partiellement immatériel.

La PSSI constitue un cadre de référence et de cohérence :

- pour l'intégration de la sécurité lors de la conception d'un système d'information ;
- pour l'ensemble des activités et des acteurs de l'organisme par rapport auxquels toute évolution du système d'information devra être justifiée ;
- pour aider les personnes chargées 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.

La PSSI offre les bénéfices suivants :

- une vision stratégique de la gestion des risques globaux, dont la SSI, visant à informer les maîtrises d'ouvrage des enjeux et susciter la confiance dans le système d'information,
- la mise en évidence des objectifs, obligations et engagements de l'organisme vis-à-vis de ses usagers et partenaires en fonction des lois applicables, ainsi que les principes de sécurité régissant la protection de son propre patrimoine,
- la promotion de 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,
- l'assurance de la cohérence et de la pérennité des actions de sécurité (analyses de risques, mise en œuvre des mesures…) en indiquant les directives nécessaires, notamment pour tout choix technique mais aussi organisationnel ou contractuel, en matière de sécurité,
- une gradation des moyens (avec une proportionnalité assurée par l'analyse des risques) par application des principes et règles de sécurité à respecter pour l'ensemble des activités et des systèmes,
- la sensibilisation aux risques menaçant les systèmes d'information et aux moyens disponibles pour s'en prémunir et informer l'ensemble des acteurs sur leurs responsabilités,
- une aide aux Directeurs de programmes et chefs de projet pour intégrer la sécurité au plus tôt dans les développements de nouveaux services du système d'information.

De plus, l'élaboration ou la révision d'une PSSI est l'occasion de repenser dans une démarche structurée et à finalité opérationnelle, la sécurité du système d'information en commençant par l'organisation mise en place pour répondre à ce besoin en modifiant la culture de l'organisme.

La PSSI est un document général diffusable qui :

- satisfait les objectifs de sécurité identifiés pour l'organisme ;
- doit être connu de l'ensemble des acteurs internes, ainsi que, le cas échéant, de l'ensemble des personnes accédant au système d'information de l'organisme (sous-traitants, prestataires, stagiaires…) ;

- doit, après validation par l'autorité responsable (par exemple : la direction générale), être largement diffusé, éventuellement sous une forme simplifiée et didactique, à l'ensemble du personnel. Cette diffusion sera accompagnée d'une sensibilisation de l'ensemble du personnel, portant sur le rappel des principes, de l'organisation et des règles de sécurité.

2.3 Domaines d'application de la PSSI

La Politique de Sécurité des Systèmes d'Information (PSSI) peut s'appliquer à la totalité ou à une partie du système d'information de l'organisme.

La PSSI :
- s'applique à un système existant ou à développer,
- concerne toute personne ayant accès au système d'information de l'entreprise qu'il soit interne ou externe à l'organisme (sous-traitant, stagiaire, prestataire),
- concerne l'ensemble des aspects du système d'information (l'organisation, l'environnement physique, le développement, l'exploitation, la maintenance…),
- concerne l'ensemble du cycle de vie du système d'information et de l'information.

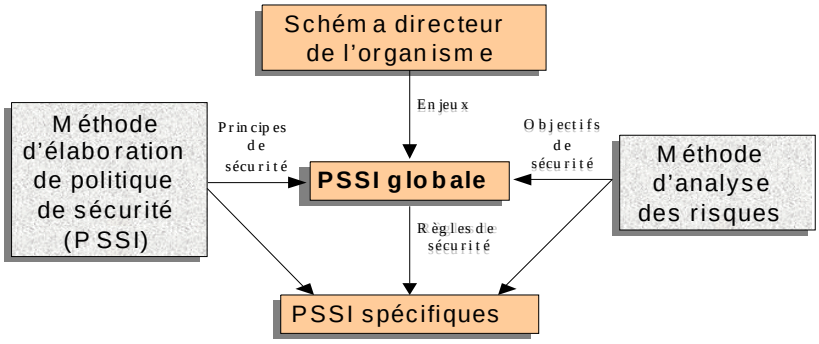
Telle qu'elle est décrite dans la suite de ce guide, elle couvre l'ensemble des systèmes d'information de l'administration, de l'organisme ou de l'entreprise.

2.4 Place de la PSSI dans le référentiel documentaire

La PSSI est un élément de la politique générale de l'organisme et elle est en accord avec le schéma directeur du système d'information et la stratégie de sécurité de l'information.

Bien qu'elle puisse concerner l'ensemble des systèmes d'information de l'organisme, elle peut également être restreinte à un système d'information particulier, par exemple lié à un métier de l'organisme ou à un système transversal (messagerie, intranet…). Dans ce cas, il peut exister plusieurs PSSI dans un organisme ou une entreprise. Elles devront être cohérentes entre elles. Cette cohérence est assurée grâce à la formalisation d'une PSSI globale (objet du présent guide). Les autres politiques sont alors des déclinaisons de la PSSI dans un environnement métier ou technique particulier, pour des instances spécialisées ou des cas particuliers.

Pour élaborer une PSSI adaptée à l'organisme, il est recommandé de réaliser une analyse des risques spécifiques au contexte afin d'en ajuster les règles de sécurité.



2.4.1 Lien entre la PSSI et les lignes directrices de l'OCDE

Les neuf principes généraux exposés dans les lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information constituent un cadre de sécurité applicable aux systèmes d'information d'un État ou d'un organisme privé.

La PSSI d'un organisme, quant à elle, se situe à un niveau d'abstraction moins élevé. Elle peut alors hériter des principes de l'OCDE. Notons que les principes de sécurité proposés dans ce guide sont compatibles avec ceux des lignes directrices de l'OCDE (voir section 4 – Références SSI).

2.4.2 Lien entre la PSSI et les Critères Communs (CC)

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…). 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[1] exige une protection convenable des informations et des services de traitement et de transport de l'information. La SSI 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. Il y a donc un besoin en méthodes et référentiels de sécurité afin d'une part, de spécifier les objectifs de sécurité d'un système de manière pertinente, et d'autre part, d'avoir les moyens d'évaluer la réalisation de ces objectifs de sécurité en mesures afin de garantir un certain niveau de confiance dans la sécurité du système.

Des travaux ont été entrepris au niveau international fondés sur les résultats des initiatives existantes en Europe, aux USA, au Canada… ; ils ont abouti à l'élaboration des critères communs d'évaluation de la sécurité des technologies de l'information [ISO 15408] qui permettent de définir un cadre pour l'évaluation de produits ou de systèmes informatiques.

Ces critères d'évaluation ont été élaborés de façon générique afin de permettre l'évaluation de n'importe quel produit ou système informatique, qu'il s'agisse d'un composant électronique dédié ou d'une application logicielle grand public. Ils sont, de fait, particulièrement adaptés pour la définition des objectifs de sécurité des systèmes ou produits informatiques, pour la définition de leurs exigences fonctionnelles de sécurité et donc pour l'élaboration des spécifications techniques des marchés les concernant. Pour les organismes publics, ces spécifications techniques ont donc valeur de recommandations.

Dans la philosophie des critères communs, il est établi que la sécurisation d'un système d'information nécessite entre autre la mise en place d'une politique de sécurité des systèmes d'information.

Cette politique de sécurité constitue la première étape d'une méthodologie de gestion des risques pour un système d'information avec l'élaboration d'un schéma directeur de sécurité des systèmes d'information. L'exprimer à l'aide du formalisme des Critères Communs permet alors d'entamer les étapes suivantes de la sécurisation du système d'information en accord avec les méthodologies appliquées par les organismes officiels. Notamment, les Critères Communs sont utilisés comme référentiel de certification et cette étape permet d'obtenir le niveau de confiance que l'on peut accorder au produit ou système établi.

2.5 Les bases de légitimité d'une PSSI

Les règles contenues dans une PSSI puisent leur légitimité dans les lois, les réglementations, les normes et les recommandations émanant d'instances internationales, nationales ou professionnelles. Elles trouvent également leur justification dans les composantes de la culture de l'organisme comme les traditions, les habitudes ou les règlements internes.

[1] Nous distinguons en fait plusieurs types et niveaux d'utilisateurs :
- le propriétaire décide, définit les exigences, paye et prend la responsabilité des opérations ;
- le gestionnaire ou exploitant a la responsabilité des affaires courantes du système d'information au jour le jour, il est responsable des opérations et du rapport des résultats, il ne peut travailler que si le propriétaire lui précise des objectifs et s'il fournit des moyens, il n'est pas toujours l'administrateur, qui peut dépendre de lui pour des sous-objectifs précis et spécifiques, mais se trouve à ce niveau ;
- l'utilisateur qui emploie le système d'information en suivant des règles et procédures définies par le propriétaire et transmises par le gestionnaire peut assurer l'entretien préventif ou journalier et rendre compte au gestionnaire ; l'opérateur est un utilisateur spécifique dont la compétence permet une utilisation "professionnelle" d'un outil ; l'utilisateur peut être uniquement le destinataire de l'information.

2.5.1 Le respect de la déontologie

L'utilisation croissante des systèmes d'information par un large public conduit à appliquer aux métiers utilisant les technologies de l'information de 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

(1) Déclaration universelle des droits de l'homme adoptée par l'assemblée générale des Nations Unies le 10 décembre 1948 à Paris et en particulier :
- la liberté d'expression et le droit de chercher, recevoir et répandre les informations par quelque moyen d'expression que ce soit ;
- la protection de sa vie privée, sa famille, son domicile ou sa correspondance.

(2) Principes directeurs de l'ONU pour la réglementation des fichiers informatisés contenant des données à caractère personnel :
- les principes concernant les garanties minimales qui devraient être prévues dans les législations nationales ;
- l'application des principes directeurs aux fichiers contenant des données à caractère personnel, détenus par les organisations internationales gouvernementales.

(3) Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel :
- lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (1980) ;
- déclaration des flux transfrontières de données (1985) ;
- déclaration des ministres relative à la protection de la vie privée sur les réseaux mondiaux (1998).

Au niveau de l'Union européenne

(1) Convention de sauvegarde des droits de l'Homme et des libertés fondamentales**,** adoptée par le conseil de l'Europe (Rome 4/11/1950).

(2) Directives du Conseil de l'Union Européenne :
- La directive du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette directive vise à favoriser l'élaboration de codes de conduite nationaux et communautaires destinés à contribuer à la bonne application des dispositions nationales et communautaires.
- La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

Au niveau national

(1) Déclaration des droits de l'homme du 26 août 1789 - article 11 concernant la liberté de penser, de parler, d'écrire et d'imprimer librement.

(2) Loi « Informatique et Libertés » qui réglemente l'emploi et la constitution des fichiers nominatifs, c'est-à-dire, encadre 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,
- la reconnaissance, pour toute personne figurant dans un fichier automatisé ou manuel, des droits d'accès, de rectification et de refus des 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.

(3) Rapport de la CNIL sur la cybersurveillance sur les lieux de travail publié le 5 février 2002

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

(1) Codes d'éthique par secteurs professionnels (métiers juridiques, de la santé, de la recherche, de la banque, de la statistique…) formulant des principes de base, des recommandations de politiques, des codes de conduite 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"... (domaine protégé par le Code pénal).

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

(2) Codes d'éthique des métiers des technologies de l'information : ces codes particuliers 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 partenaires, à savoir le respect du partenaire et la protection des informations confiées dans le cadre d'une mission menée en partenariat,
- les devoirs envers les concurrents, à savoir le respect des principes de loyauté et de libre concurrence
- le respect du secret de fabrique.

2.5.2 La gestion des risques : accidents, erreurs, défaillances et malveillances

Les accidents pouvant survenir à l'intérieur d'un organisme ou être provoqués à l'extérieur de celui-ci par ses activités peuvent entraîner des atteintes aux personnes, aux biens, à l'environnement (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.

Si cette préoccupation est prise en compte au niveau de la sécurité générale (et, tout particulièrement celle qui touche aux personnels), 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 l'eau…).

La liste des altérations spécifiques à la sécurité comprend habituellement, sans y être limitée, le déni d'accès à une information ou une fonction (perte de disponibilité), le dommage provoqué à une information ou une fonction par une modification non autorisée (perte d'intégrité) ou la divulgation nuisible d'une information ou une fonction à des destinataires non autorisés (perte de confidentialité).

Indépendamment de l'obligation faite par la loi, il est un devoir prioritaire pour les responsables d'organismes de renforcer les contrôles de sécurité partout où il existe un risque, aussi minime soit-il, lié à l'utilisation du système d'information.

La sécurité a trait à la protection des biens contre les menaces, ces dernières étant classées selon leur potentiel de nuisance envers les biens à protéger. Toutes les catégories de menaces devraient être prises en compte, mais dans le domaine de la sécurité, une plus grande attention est accordée aux menaces liées à des activités humaines malveillantes ou non. [ISO 15408]

Une menace doit être décrite en citant l'élément menaçant identifié, l'attaque et le bien qui en est la cible. Les éléments menaçants devraient être caractérisés par des aspects tels que l'expertise, les ressources disponibles et la motivation. Les attaques devraient être caractérisées par des aspects tels que les méthodes d'attaque, toutes les vulnérabilités exploitées et l'opportunité. [ISO 15408]

2.5.3 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 spécifiques qui s'y rapportent.

La liste des principaux textes est donnée en section 4 (Références SSI).

Protection des éléments non classifiés de défense

La [REC 901] sur la sécurité des systèmes d'information traitant des informations sensibles non classifiées de défense reprend certains grands principes de l'[IGI 900] et se présente suivant la même articulation. Elle peut s'appliquer à toutes les administrations et tous les services déconcentrés de l'État ainsi qu'aux établissements placés sous l'autorité d'un ministre. Cette recommandation 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.

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.

La [REC 600] présente 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 la sécurité des postes de travail autonomes ou connectés à un réseau.

Les informations relevant du secret de défense

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

(1) La protection du secret et des informations concernant la défense nationale et la sûreté de l'État. L'[IGI 1300], 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 en diffusion restreinte (mention et non classification),
- la sensibilisation aux risques de compromission d'informations classifiées,
- les contrôles et inspections.

(2) La sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées. L'[IGI 900], 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.

(3) Protection du secret dans les rapports entre la France et les États étrangers. L'[II 50] 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 porte sur la protection du patrimoine scientifique et technique français dans les échanges internationaux.

(4) Protection du secret et des informations pour les marchés et autres contrats. L'[II 2000] 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.

2.5.4 La lutte contre la malveillance et le cybercrime

Au niveau de l'Union européenne

La [REC CRIM] sur la criminalité en relation avec l'ordinateur et la [D 250] 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 [CPI] 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.

2.5.5 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.

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 des Systèmes d'Information.

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.

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 interne,
- la communication interne ou externe.

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.

Les orientations stratégiques et la structure de l'organisme

Les choix fondamentaux et les objectifs que se fixe l'organisme découlent de sa mission et de sa propre stratégie organique ; 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 qui rend compte de l'organisation des différentes entités constitutives de l'organisme (directions, départements, services, unités…).

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. Les difficultés relationnelles qui sont souvent difficiles à évaluer, exigent pour être mises en lumière et gérées, 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 de rétention d'informations ; il peut alors se créer au sein de l'organisme des flux qui échappent aux contrôles de la sécurité.

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

Les engagements pris envers d'autres organismes font l'objet de contrats ou de conventions où peuvent figurer en particulier des clauses spécifiques concernant la sécurité des systèmes d'information. 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. Toute relation nouvelle avec l'environnement de l'organisme nécessite un effort préalable de communication à l'intérieur de l'organisme.

À titre d'exemple, dans le cas d'un contrat de sous-traitance de l'exploitation du système d'information, 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 autres contrats de sous-traitance, pour lesquels il existe souvent des clauses spécifiques relatives par exemple à la fourniture de programmes-sources et à leur usage.

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 pérennité de la maintenance et de l'assistance,
- 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.

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.

2.5.6 La conformité technologique et légale

Le contrôle étatique dans le domaine de la cryptologie

L'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications définit les prestations de cryptologie par : « *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.* »

La réglementation française (section 4 – Références SSI) 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.

Le contrôle des communications

La loi relative à la liberté de communication concerne le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications

La signature électronique

Suite à la loi du n° 2000-230 du 13 mars 2000, le code civil précise : *« La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission ».*

Il précise également que : *l'écrit sur support électronique a la même force probante que l'écrit sur support papier*.

La loi précise que : « lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support ».

La [D 93] précise le cadre communautaire pour les signatures électroniques.

Les instructions techniques particulières pour la lutte contre les signaux compromettants

On entend par signal 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.

2.5.7 Le contrôle par les consommateurs

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.

Normalisation

L'utilisation de produits normalisés est recommandée 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. Elle est reprise par un décret national fixant le statut de la normalisation"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".

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,
- d'exigences de sécurité des personnes et des biens.

Certification des technologies de l'information

La situation juridique communautaire s'appuie sur une résolution portant sur l'approche globale en matière d'évaluation de la conformité.

En France, une évaluation réussie suivant les critères harmonisés européens peut donner lieu à la délivrance d'un certificat par la DCSSI selon le schéma français d'évaluation et de certification. Ce dernier précise le contexte réglementaire et l'organisation nécessaires à la conduite d'une évaluation par une tierce partie et à son contrôle, conduisant à la délivrance de certificats.

Le décret n°2002-535 du 18 avril 2002 définit le cadre réglementaire du schéma

Bibliographie

Les références suivantes apparaissent dans le guide entre crochets :

[CPI]	Code de la propriété intellectuelle, article L621 relatif au secret de fabrique.
[D 250]	Directive n°91/250/CEE du Conseil des communautés européenne du 14 mai 1991 concernant la protection des programmes d'ordinateur.
[D 93]	Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, relative au cadre communautaire pour les signatures électroniques.
[IGI 1300]	Instruction générale interministérielle nº1300/SGDN/PSE/SSD/DR du 12 mars 198225 août 2003 sur la protection du secret et des informations concernant de la défense nationale et la sûreté de l'État.
[IGI 900]	Instruction générale interministérielle nº900/SGDN/SSD/DR ou nº900/DISSI/SCSSI/DR du 20 juillet 1993 sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées.
[II 2000]	Instruction interministérielle nº2000/SGDN/SSD/DR du 01 octobre 1986 sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les marché et autres contrats.
[II 486]	Instruction interministérielle nº486/SGDN/STS/TSE/CVS/DR du 01 mars 1993 sur la protection du patrimoine scientifique et technique dans les échanges internationaux.
[II 50]	Instruction interministérielle nº50/SGDN/SSD du 09 janvier 1971 sur la protection du secret dans les rapports entre la France et les pays étrangers.
[ISO 13335]	Technologies de l'information – Lignes directrices pour le management de sécurité IT – ISO/IEC, 2001.
[ISO 15408]	Technologies de l'information – Techniques de sécurité– Critères d'évaluation pour la sécurité TI – ISO/IEC, 1999
[ISO 17799]	Technologies de l'information – Code de pratique pour la gestion de sécurité d'information – ISO/IEC, 2000.
[REC 600]	Recommandations nº600/SGDN/DISSI/SCSSI de mars 1993 pour les postes de travail informatiques. Protection des informations sensibles ne relevant pas du secret de défense
[REC 901]	Recommandation nº901/SGDN/DISSI/SCSSI du 02 mars 1994 pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.
[REC CRIM]	Recommandation du Conseil de l'Europe du 19 septembre 1989 adoptée par le conseil des ministres, relative à la criminalité en relation avec l'ordinateur.

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) :
Adresse électronique :
Date :

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui □ Non □

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui □ Non □

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui □ Non □

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension □
- présentation □
- autre □

Précisez vos souhaits quant à la forme :

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :

Quels autres sujets souhaiteriez-vous voir traiter ?

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution