République française

PREMIER MINISTRE

Délégation Interministérielle
pour la Sécurité des Systèmes d'Information

N°901/DISSI/SCSSI

Paris, le 2 mars 1994

RECOMMANDATION

POUR LA PROTECTION DES SYSTEMESD'INFORMATION

TRAITANT DES INFORMATIONS SENSIBLES

NON CLASSIFIEES DE DEFENSE

SERVICE CENTRAL DE LA SECURITE DES SYSTEMES D'INFORMATION

S O M M A I R E

INTRODUCTION

Article 1

OBJET DE CETTE RECOMMANDATION

L'accomplissement de la mission des administrations et des entreprises et la recherche permanente d'une meilleure efficacité passent de plus en plus par la mise en oeuvre de moyens de télécommunication, d'informatique et de bureautique. Ce recours très large aux technologies de l'information, rendu nécessaire par le volume croissant des informations à traiter et par l'extension du besoin de communication, a l'inconvénient de rendre ces organismes dépendants de leurs systèmes d'information, donc vulnérables aux multiples menaces qui pèsent sur eux.

Les risques sans cesse croissants qu'implique l'utilisation des systèmes d'information peuvent mettre en cause l'action de l'Etat. C'est pourquoi, protéger l'information doit être un souci général et sécuriser les systèmes d'information est une obligation nationale majeure.

La présente recommandation reprend et adapte certains des grands principes de l'instruction générale interministérielle applicable aux systèmes d'information faisant l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées. Elle définit les grandes orientations de la politique à mettre en oeuvre par les départements ministériels, en matière de sécurité des systèmes d'information, pour assurer la protection des informations sensibles non classifiées de défense, dans le respect des lois et règlements en vigueur.

Elle précise également l'organisation à mettre en place pour appliquer cette politique. Elle définit et répartit les responsabilités entre les différents intervenants dans ce domaine.

Article 2

DEFINITIONS

Est dénommé **système d'information**, au sens du présent document, tout moyen dont le fonctionnement fait appel d'une façon ou d'une autre à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information. Dans le présent document, le terme "traitement" désigne l'ensemble de ces fonctions.

Est dénommé **sécurité d'un système d'information** l'état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer :

- La **confidentialité**, c'est-à-dire le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service ;

- La **disponibilité**, qui est l'aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performances ;

- L'**intégrité** du système et de l'information qui garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire à la garantie de son origine et de sa destination.

Article 3

CHAMP D'APPLICATION

La présente recommandation s'adresse à toutes les administrations et services déconcentrés de l'Etat. Elle concerne également les établissements publics placés sous l'autorité d'un ministre ainsi que les établissements ou organismes placés sous sa tutelle.

En outre, il doit être tenu compte de ses dispositions dans les marchés ou contrats au titre desquels les organismes ci-dessus confieraient des informations sensibles.

Enfin, ces principes veulent être un système de référence pour les entreprises privées qui désirent assurer une protection de leurs propres secrets scientifiques, technologiques, industriels, commerciaux ou financiers, ou qui désirent garantir leur intérêts et leur patrimoine.

CHAPITRE PREMIER

LES INFORMATIONS NECESSITANT UNE PROTECTION

Article 4

LES INFORMATIONS SENSIBLES NON CLASSIFIEES DE DEFENSE

Les informations sensibles non classifiées de défense sont des informations pour lesquelles le non respect de la confidentialité, la disponibilité ou l'intégrité mettrait en cause la responsabilité du propriétaire ou du dépositaire, ou causerait un préjudice à eux-mêmes ou à des tiers.

Les critères de sensibilité d'une information ne peuvent être fixés a priori. A titre d'exemple, on peut citer :

1 - Les informations énumérées à l'article 6 de la loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public, dont la consultation ou la communication, selon les termes de la loi, porteraient atteinte :

- Au secret des délibérations du Gouvernement et des autorités responsables relevant du pouvoir exécutif (si elles ne sont pas, par ailleurs, protégées par le secret de défense) ;

- A la monnaie et au crédit public, à la sécurité publique ;

- Au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures ;

- Au secret de la vie privée, des dossiers personnels et médicaux ;

- Au secret en matière commerciale et industrielle ;

- A la recherche, par les services compétents, des infractions fiscales et douanières ;

- Ou, de façon générale, aux secrets protégés par la loi.

Les mesures de protection mises en oeuvre par les administrations ne sauraient avoir pour effet de soustraire les informations à la liberté d'accès prévue par la loi du 17 juillet 1978 précitée, lorsqu'elles ne figurent pas sur les listes de documents non-communicables fixées par les arrêtés ministériels prévus à l'article 6 de cette loi.

2 - Les informations qui ne présentent pas un caractère de secret mais qui restent soumises à l'obligation de réserve ou de discrétion professionnelle.

3 - Les informations constitutives du patrimoine scientifique, industriel et technologique.

Il est recommandé que les informations sensibles reçoivent une mention rappelant leur sensibilité en considération de la gravité des conséquences qu'aurait une divulgation, une altération, une indisponibilité ou une destruction. A cette fin, on pourra utiliser les mentions suivantes :

- CONFIDENTIEL
- DIFFUSION LIMITEE

La mention de sensibilité désigne le **niveau de protection** qu'il faut assurer à l'information.

Le choix de cette mention de sensibilité ne saurait avoir pour effet d'entraver de façon injustifiée la libre circulation nationale et internationale des informations.

Chacune de ces mentions de sensibilité peut être assortie d'une mention spécifique, caractéristique du domaine protégé :

- **PERSONNEL** (information nominative au sens de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) ;

- **PROFESSIONNEL** (protégé par l'article 226-13 du code pénal) ;

- **INDUSTRIEL, COMMERCIAL, NOM d'une société ou d'un organisme, NOM d'un programme, etc.** (protégés par les articles 80-3° et 378 du code pénal).

La mention spécifique assure le **cloisonnement** de l'information, en réservant son accès aux seules personnes ayant besoin de les connaître pour l'accomplissent de leur fonction ou de leur mission.

Article 5

LES INFORMATIONS VITALES POUR LE FONCTIONNEMENT D'UN SYSTEME

Le traitement des informations et notamment des données par un système nécessite la mise en oeuvre d'une suite d'actions élémentaires internes dont l'association représente les fonctionnalités du système d'information. L'agencement et le déroulement de ces actions élémentaires sont commandés par un ensemble de programmes de base permettant d'atteindre toutes ces fonctionnalités.

L'ensemble de ces actions élémentaires et de ces programmes de base constitue **les informations traitantes, vitales pour le fonctionnement du système.** Il convient d'en garantir la disponibilité et l'intégrité, leur modification ou leur altération pouvant entraîner le dysfonctionnement ou l'arrêt du système. D'autres informations sont liées aux fonctions de sécurité du système et assurent la continuité, la non répudiation des transactions et l'intégrité des données. L'ensemble de ces informations est à **protéger** au même titre que les informations traitées mentionnées à l'article 4.

CHAPITRE 2

LES MOYENS DE PROTECTION

Il convient de garantir la protection des informations en prenant des mesures de sécurité au niveau des systèmes de traitement afin d'empêcher quiconque de nuire à leur fonctionnement et d'interdire à des tiers non autorisés à les connaître, d'avoir accès aux informations visées aux articles 4 et 5 ci-dessus. Ces mesures seront adaptées à la sensibilité des informations traitées.

Outre le contrôle d'accès aux installations internes de traitement et de télécommunication et leur surveillance, les principales mesures de sécurité reposent sur l'emploi :

- De moyens de cryptologie qui permettent le chiffrement des informations stockées ou acheminées sur des réseaux de télécommunications, ainsi que d'autres mécanismes de sécurité ;

- De matériels respectant les normes de compatibilité électromagnétique en vigueur et installés suivant des règles appropriées ;

- De moyens informatiques munis de fonctions de sécurité visant à empêcher leur usage illicite.

Ce document est complété par des guides techniques du service central de la sécurité des systèmes d'information (S.C.S.S.I.), élaborés en concertation avec la commission interministérielle pour la sécurité des systèmes d'information (C.I.S.S.I.).

Article 6

MOYENS DE CRYPTOLOGIE

Les moyens de cryptologie sont des matériels ou des logiciels qui transforment, à l'aide de conventions secrètes, des informations ou des signaux clairs en informations ou signaux inintelligibles pour des tiers ou qui réalisent l'opération inverse. Ils sont également à la base des mécanismes de nombreuses fonctions de sécurité :

- Intégrité des informations stockées ou transmises, y compris l'authentification mutuelle de deux entités ou la non répudiation d'un échange ;

- Confidentialité avec le chiffrement des informations stockées ou transmises.

Lorsque les mesures de sécurité générales et particulières déjà prises ne permettent pas de traiter (en fait d'acheminer ou de stocker) les informations sensibles avec une protection correspondant à leur sensibilité, il peut être éventuellement fait appel à des moyens de cryptologie devant alors avoir reçu la caution du S.C.S.S.I.

La fourniture, l'utilisation et l'exportation des moyens et prestations de cryptologie sont soumises à une réglementation spécifique prise en application de l'article 28 de la loi n°90-1170 du 29 décembre 1990 modifiée.

Article 7

PROTECTION CONTRE LES SIGNAUX PARASITES COMPROMETTANTS

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 exploitation qui permettent de reconstituer ces informations constituent une menace. Ces signaux sont, de ce fait, dénommés signaux parasites compromettants.

Les matériels ou systèmes qui traitent des informations sensibles nécessitent une protection contre cette menace. Pour limiter les risques de compromission des informations sensibles, il est recommandé d'utiliser des matériels respectant les normes de comptabilité électromagnétique en vigueur, en association avec les règles d'installation diffusées par le S.C.S.S.I.

D'autres méthodes telles que l'utilisation de cages de Faraday ou le zonage peuvent être utilisées. Il convient alors de s'assurer du maintien de leur efficacité dans le temps.

Article 8

MOYENS DE SECURITE INFORMATIQUE

La sécurité informatique exige que des équipements et des mécanismes (matériels et logiciels) soient incorporés dans le système informatique pour réaliser la disponibilité, l'intégrité et la confidentialité des informations prévues par les objectifs de sécurité.

Elle exige également que l'intégration de ces équipements et mécanismes dans le système ne compromette pas leur efficacité, et que leur exploitation soit assurée conformément aux consignes de sécurité du système.

Elle exige enfin, que des assurances suffisantes soient données, d'une part, que ces mécanismes et équipements ont bien été réalisés conformément à leurs spécifications et, d'autre part, qu'ils n'ont été ni modifiés ni contournés au cours de leur intégration dans le système, ni altérés lors de la mise en service ou pendant l'exploitation de celui-ci.

Les moyens permettant de réaliser la sécurité informatique sont :

a) Les mécanismes, leurs spécifications et le dossier de leur réalisation, qui permettent de les évaluer. Ils réalisent, conformément au plan de sécurité, les grandes fonctions de la sécurité informatique qui sont :

- L'identification des utilisateurs et leur authentification (assurance que l'utilisateur est bien celui qui affirme l'être) ;

- L'administration et la vérification des droits, que la politique de sécurité confère à chaque utilisateur ;

- L'enregistrement de ces droits, ainsi que celui des tentatives infructueuses de leur exercice, afin de pouvoir d'une part attribuer les responsabilités et, d'autre part, détecter les anomalies et y remédier dans les meilleurs délais ;

- Le maintien de la disponibilité et de la cohérence du service tout au long de la vie du système ;

- La réutilisation des ressources informatiques (fichiers, mémoires, programmes, etc) ;

- Le maintien de la cohérence et de l'exactitude des données de sécurité ;

- La sécurité des échanges.

b) Les moyens, techniques et non techniques, utilisés pour garantir au cours du développement que les objectifs de sécurité ont bien été atteints ; il s'agit notamment de l'organisation des équipes de développement, des outils éventuellement certifiés et du système de gestion de configuration.

c) La documentation d'exploitation du système.

Pour les produits informatiques qui comportent des moyens de sécurité informatique, le S.C.S.S.I. délivre un certificat qui atteste de leur niveau de sécurité. Ce certificat est délivré à l'issue d'une évaluation effectuée par un laboratoire agréé, conformément aux critères d'évaluation de la sécurité des systèmes informatiques (critères européens harmonisés : ITSEC - Information Technology Security Evaluation Criteria).

Il est recommandé qu'un système informatique qui traite des informations sensibles donne lieu à la définition d'une **cible de sécurité** au sens des critères d'évaluation de la sécurité des systèmes informatiques précités.

Article 9

SURVEILLANCE DES MOYENS DE PROTECTION DES SYSTEMES D'INFORMATION

Les moyens de protection, objet des articles précédents, et les documents qui les accompagnent sont les moyens auxquels il est fait confiance pour assurer la protection des informations traitées. Le maintien de cette confiance justifie un contrôle de ces moyens tout au long de leur durée de vie : ils sont conçus, réalisés, utilisés, réparés puis réformés ou détruits. Ce contrôle est l'un des éléments qui permet de garantir leur intégrité.

Ainsi, les documents, logiciels ou matériels qui contribuent directement à la sécurité d'un système d'information, font-ils l'objet d'une protection visant à garantir leur intégrité ou leur confidentialité. Cette protection peut être concrétisée par :

- L'attribution d'une mention spécifique qui rappelle la sensibilité des documents, logiciels ou matériels visés. Cette mention est délivrée sur décision de la voie hiérarchique :

  - Par la structure SSI du département ministériel concerné lorsqu'elle existe (cf. articles 18 et 19) ;

  - Par le Haut fonctionnaire de défense dans le cas contraire ;

  - Par l'autorité qualifiée de l'organisme ou de l'entreprise ayant en charge la sécurité des systèmes d'information.

- La mise en oeuvre d'une gestion particulière des moyens de sécurité concernés dont l'objectif est d'assurer une surveillance continue des moyens afin d'en garantir l'efficacité. Les principales mesures de cette gestion particulière pourraient être par exemple :

  - Le marquage des moyens concernés ;

  - Le suivi individualisé de ces moyens au travers d'une comptabilité rigoureuse qui débute dès le stade de la production en usine ;

  - La prise en charge des moyens par des détenteurs responsables de leur protection ;

  - La mise en place d'un registre inventaire dans chaque organisme ou entreprise où se trouve un détenteur responsable ; ce registre est notamment utilisé aux fins d'inventaire annuel à adresser à l'autorité responsable.

- La désignation nominative des personnes ayant besoin d'accéder à ces moyens dans le cadre de leurs fonctions, en limitant au strict minimum les personnes ayant accès à ces moyens.

CHAPITRE 3

PRINCIPES GENERAUX DE SECURISATION DES SYSTEMES D'INFORMATION

Article 10

MENACES ET VULNERABILITE DES SYSTEMES

Les systèmes d'information, qu'ils soient utilisés en local ou par l'intermédiaire des réseaux de télécommunications, présentent une vulnérabilité en raison des menaces qui pèsent sur eux. Une telle vulnérabilité croît avec la banalisation, la complexité, l'automatisme et le nombre d'utilisateurs de ces systèmes, ainsi qu'avec le volume et la diversité des informations traitées.

Les agressions que peuvent subir ces systèmes résultent généralement d'actes frauduleux ou malveillants et visent dans la majorité des cas à détruire, altérer, prendre connaissance des informations sensibles et à nuire au bon fonctionnement du système lui-même pour le rendre inopérant ou altérer sa sécurité.

Elles peuvent s'exercer localement ou à distance, notamment à travers les réseaux de télécommunications, et affecter les informations à tout instant de leur traitement.

Suivant les informations traitées et les missions de l'organisme qui les traite, les menaces peuvent revêtir des aspects différents :

- la menace ludique :

  Les nouvelles techniques de traitement de l'information ont créé cette nouvelle menace qui procède davantage, dans l'esprit de ses auteurs, d'un jeu. Ceux-ci, motivés par la recherche d'une prouesse technique valorisante destinée à démontrer la fragilité d'un système, se recrutent parmi des jeunes soucieux de s'affirmer. Les victimes sont des organismes socialement importants à leurs yeux.

- la menace cupide :

  Elle consiste en la recherche d'un gain financier important et rapide par des individus ou des groupes sans considération morale ; ses victimes se choisissent parmi ceux qui détiennent l'argent (banques, compagnies d'assurance, etc.).

- la menace terroriste :

  Un groupuscule, un groupe, voire un Etat veulent frapper l'opinion par une action la plus spectaculaire possible, amplifiée par les médias, afin de déclencher une psychose de peur. Ce moyen d'action peut viser par exemple le sabotage de systèmes vitaux.

- la menace stratégique :

Un Etat peut utiliser avec efficacité les faiblesses éventuelles des systèmes d'information afin d'entrer, par la télématique, en relation plus ou moins discrète avec un agent implanté dans un pays. Il peut prendre connaissance d'informations sensibles, notamment en accédant frauduleusement à des banques de données. Au-delà, on peut envisager l'attaque massive de tous les systèmes vitaux d'un pays pour le neutraliser, le paralyser et le forcer à négocier.

Cette réflexion sur la menace doit aussi intégrer un phénomène d'interpénétration : le "pirate" ludique acquiert un savoir-faire en matière d'attaque de systèmes d'information dont il peut ensuite chercher à tirer un profit financier (menace cupide). Déçu par la société, il peut accepter les propositions de recruteurs de réseaux terroristes ou d'agents de renseignement (menace ludique devenant terroriste ou stratégique)...

De manière générale, dès qu'une menace se manifeste, la personne qui en a connaissance doit rendre compte rapidement des incidents réels ou supposés, susceptibles de porter atteinte à la sécurité.

Article 11

METHODOLOGIE DE SECURISATION D'UN SYSTEME D'INFORMATION

La sécurité d'un système d'information est l'un des besoins opérationnels que ce système doit satisfaire, au même titre que les fonctions qu'il doit assurer et les performances qu'il doit atteindre.

Dans le développement d'un système d'information, une prise en compte tardive des contraintes et des exigences de la sécurité conduit inévitablement à des modifications du projet initial et ainsi à des surcoûts, à des baisses de performance ou à des limitations d'emploi.

La sécurité doit donc être prise en compte dès l'expression du besoin, puis tout au long de la vie d'un système d'information.

C'est l'objet de la politique de sécurité du système que le rassembler en un tout cohérent les règles, règlements et pratiques qui gouvernent la gestion, la protection et l'affectation des informations visées aux articles 4 et 5 et des autres ressources de ce système.

Il est donc recommandé de rédiger une **fiche d'expression rationnelle des objectifs de sécurité (FEROS)**, précisant la nature et la sensibilité des informations que traitera ou utilisera le système d'information, rappelant les obligations légales et réglementaires, analysant les menaces et les risques, et indiquant, le cas échéant, les contraintes a priori, techniques ou non, qui restreignent les choix du concepteur du système et dont une incidence sur la sécurité. Cette fiche est établie par l'autorité utilisatrice suivant le modèle défini par le SCSSI.

Il est également recommandé d'établir, selon des règles définies par chaque ministère pour ses besoins propres :

- Un **plan de sécurité**, qui décrit le système développé et présente les mesures techniques et non techniques prises pour atteindre les objectifs définis par la **FEROS** ; il expliquera en particulier, en quoi les mesures prises permettent d'atteindre l'ensemble des objectifs de sécurité ; pour un système informatique, le **plan de sécurité** et la **FEROS** constituent la **cible de sécurité** comme indiqué dans les critères d'évaluation de la sécurité des systèmes informatiques (**ITSEC**) ;

- Un **plan d'organisation du développement**, rappelant les réglementations générales et spécifiques, précisant les contrats à conclure et les conditions de choix des contractants. Il comprend une annexe précisant la sensibilité de tous les produits créés pour la mise en oeuvre du projet, ainsi que les outils et procédures à utiliser pour garantir la sécurité au cours du développement ;

- Une **documentation d'administration et d'utilisation** du système qui traite notamment, sous l'angle de la sécurité :

  - De la nature et du niveau de responsabilité des exploitants ;
  - Des procédures d'installation et de mise en ordre de marche ;
  - Des procédures d'exploitation ;
  - Des procédures de sauvegarde et de remise en configuration ;
  - Des procédures de modification de configuration ;
  - Des procédures de maintenance et de dépannage.

Enfin, le concepteur devra s'efforcer de séparer clairement les parties du système qui ne concernent pas la sécurité de celles qui ont une incidence sur la sécurité. Ces dernières devront être aussi simples et réduites que possible, afin que l'on puisse acquérir dans leur bon fonctionnement la confiance nécessaire. Une telle exigence de simplicité pourra d'ailleurs, parfois, conduire à extraire du projet envisagé les informations et les traitements dont l'altération ou la divulgation aurait les conséquences les plus graves.

Article 12

PRINCIPE DE PROTECTION GLOBALE

La sécurité d'un système d'information résulte de mesures générales et de mesures particulières :

1- les **mesures générales** consistent à adapter aux systèmes d'information les mesures prises pour la protection des informations objet des articles 4 et 5 ; il s'agit pour l'essentiel de mesures administratives et techniques ainsi que de contrôles (appréciation et application du besoin d'en connaître, protection périmétrique des installations où sont traitées les informations sensibles, contrôle d'accès aux locaux, etc.) ;
2- les **mesures particulières** consistent, d'une part, à inclure dans les systèmes tous les dispositifs de sécurité permettant de protéger les informations en précisant les

modalités de leur mise en oeuvre et, d'autre part, à limiter l'accès aux informations relatives à ces dispositifs eux-mêmes.

Aucune de ces mesures ne permet, isolément, de garantir la confidentialité, l'intégrité et la disponibilité recherchées. Il faut considérer leur association pour évaluer la sécurité d'un système d'information. Une protection globale, seule, peut garantir la sécurité d'un système d'information. Dans le cas de l'interconnexion de systèmes d'information relevant de responsabilités différentes, il convient de préserver la cohérence de la sécurité.

Article 13

PRINCIPE D'INTEGRITE DES MOYENS DE PROTECTION

L'intégrité des moyens de protection est la condition fondamentale de l'efficacité des dispositifs de sécurité.

Cette intégrité est, en particulier, garantie par la mise en oeuvre de mesures de gestion de ces moyens, depuis leur conception jusqu'à leur déclassement ou leur destruction. Ces mesures sont complétées par des mesures visant, notamment, à limiter le nombre des personnes ayant accès aux informations relatives aux dispositifs de sécurité.

Article 14

PRINCIPE DE REEVALUATION DE LA SECURITE DU SYSTEME

L'efficacité de la sécurité d'un système d'information a été évaluée avant sa mise en service, en fonction des principes développés dans les articles précédents. Elle résulte de l'adéquation du plan de sécurité aux objectifs initiaux.

Conserver cette efficacité impose de prendre en compte l'évolution et l'environnement du système pendant sa durée de vie. Une réévaluation périodique de la sécurité globale du système est donc nécessaire.

En outre, un contrôle à l'issue de chaque intervention à titre préventif ou curatif sur le système permet de vérifier que les conditions de sécurité restent satisfaites.

Article 15

AUTORISATION D'ACCES DES PERSONNELS

Lors de la conception des systèmes d'information, on s'efforcera d'en rendre la sécurité transparente et l'utilisation accessible sans qualification particulière.

En revanche, la conception des moyens de protection d'un système d'information, leur gestion, leur maintenance ainsi que l'exploitation des fonctions de sécurité ne peuvent être confiées qu'à des personnes justifiant le besoin d'en connaître et formées à cet effet tant sur le plan technique que sur le plan réglementaire. Ces personnes sont nommément désignées par l'autorité qualifiée (cf. article 19-1) pour l'exercice de leurs attributions.

De même, l'emploi de certains systèmes d'information nécessite une qualification analogue, concrétisée par une désignation nominative.

CHAPITRE 4

ROLES, ORGANISATION ET MISSIONS DES DIVERS INTERVENANTS

Article 16

LE PREMIER MINISTRE

La sécurité des systèmes d'information est assurée sous l'autorité du Premier ministre.

En outre, des structures interministérielles permettent d'orienter, d'harmoniser et de renforcer l'efficacité de l'action des départements ministériels.

Article 17

LES INSTANCES INTERMINISTERIELLES PLACEES SOUS L'AUTORITE DU PREMIER MINISTRE

1- Le directoire de la sécurité des systèmes d'information (DSSI)

Instance de décision placée sous l'autorité du Premier ministre, le directoire est présidé par le Secrétaire général du Gouvernement. Il a pour rôle de proposer la politique à suivre en matière de sécurité des systèmes d'information et d'en contrôler l'application.

L'organisation et les missions du directoire font l'objet du décret n°86-316 du 3 mars 1986 modifié (Journal Officiel du 8 mars 1986).

2- La délégation interministérielle pour la sécurité des systèmes d'information (DISSI)

La préparation et la mise en oeuvre des décisions du directoire sont confiées à une délégation interministérielle pour la sécurité des systèmes d'information, dirigée par un délégué assisté par deux adjoints.

ABROGÉ Décret n°96-67

Le délégué interministériel pour la sécurité des systèmes d'information veille à la cohérence des actions entreprises en matière de sécurité des systèmes d'information. Il coordonne l'activité des départements ministériels, fait contrôler l'application de la réglementation, propose les arbitrages et s'assure que les relations entre les organismes concernés et avec les utilisateurs privés répondent à l'intérêt général.

Le délégué interministériel, placé sous l'autorité du Premier ministre, dispose du service central de la sécurité des systèmes d'information.

Les attributions de la D.I.S.S.I. font l'objet du décret n°86-317 du 3 mars 1986 (Journal Officiel du 8 mars 1986) modifié par le décret n°87-862 du 26 octobre 1987 (Journal Officiel du 28 octobre 1987) et par le décret n°93-26 du 8 janvier 1993 (Journal Officiel du 9 janvier 1993).

ABROGE

3- Le service central de la sécurité des systèmes d'information (S.C.S.S.I.)

Le service central de la sécurité des systèmes d'information est le centre focal de l'Etat pour la sécurité des systèmes d'information. En temps qu'expert, il est chargé, dans ce domaine, d'assurer la symbiose entre les organismes impliqués.

Ses principales fonctions sont :

- L'agrément de la sécurité des équipements et des systèmes ;

- L'évaluation :
  . Evaluation des technologies de sécurisation ;
  . Evaluation de la sécurité des équipements et systèmes ;

- La fabrication des clés pour les organismes ministériels ;

- La coordination et l'harmonisation du développement des technologies et des équipements sécurisés ;

- La participation aux actions de normalisation nationales et internationales ;

- La formation dans le domaine de la sécurité des systèmes d'information dans le cadre du centre d'études supérieures de la sécurité des systèmes d'information (C.E.S.S.S.S.I.).

Les attributions de la S.C.S.S.I. font l'objet du décret n°86-318 du 3 mars 1986 modifié (Journal Officiel du 8 mars 1986)

Celles du C.E.S.S.S.S.I. font l'objet du décret n°87-354 du 25 mai 1987 modifié (Journal Officiel du 30 mai)

4- La commission interministérielle pour la sécurité des systèmes d'information (C.I.S.S.I.)

La commission interministérielle pour la sécurité des systèmes d'information a pour mission d'harmoniser les conceptions, les méthodes et les programmes d'équipement au niveau national. Structure de concertation, elle est présidée par le délégué interministériel pour la sécurité des systèmes d'information.

Ses attributions font l'objet d'un arrêté du Premier ministre du 3 mars 1986 modifié (Journal Officiel du 8 mars 1986).

Article 18

LES MINISTRES

La sécurité des systèmes d'information relève de la responsabilité de chaque ministre, pour le département dont il a la charge.

A ce titre, chaque ministre prend, dans les conditions fixées par le Premier ministre et sous son contrôle, des dispositions en vue de :

- Développer à tous les échelons le souci de la sécurité ;
- Apprécier en permanence le niveau de sécurité des installations ;
- Recenser les besoins en matière de protection des systèmes d'information et veiller à ce qu'ils soient satisfaits.

Dans les départements autres que celui de la Défense, ces attributions sont exercées par les hauts fonctionnaires de défense.

Le respect des règles applicables en matière de sécurité des systèmes d'information se traduit par l'existence, dans chaque département ministériel, d'un réseau de responsabilités spécifiques. Lorsqu'il existe une structure mise en place au titre des informations classifiées de défense, il est recommandé d'étendre sa compétence à l'ensemble des informations sensibles.

1- Le Haut fonctionnaire de défense

Dans chaque département ministériel, à l'exception de celui de la défense, le ministre est assisté par un ou, exceptionnellement, plusieurs Hauts fonctionnaires de défense (décret n°80-243 du 3 avril 1980 - Journal Officiel du 5 avril 1980, modifié par le décret n°86-446 du 14 mars 1986 - Journal Officiel du 16 mars 1986).

Le Haut fonctionnaire de défense 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 contrôle en particulier les programmes d'équipement de son département. Il fait appel aux compétences du service central de la sécurité des systèmes d'information pour la spécification et l'homologation des produits et des installations.

2- Le fonctionnaire de sécurité des systèmes d'information

Dans les départements ministériels qui utilisent des systèmes d'information justifiant une protection ou qui assurent la tutelle d'organismes ou d'entreprises utilisant de tels systèmes, le ministre désigne un **fonctionnaire de sécurité des systèmes d'information (FSSI)**, placé sous l'autorité du Haut fonctionnaire de défense.

Lorsque la charge de travail n'est pas suffisante, le ministre peut charger le Haut fonctionnaire de défense d'assurer lui-même les fonctions de FSSI.

Ces fonctions consistent à :

- Porter la réglementation interministérielle à la connaissance des organismes et entreprises concernés et à en préciser les modalités d'application ;

- Elaborer la réglementation propre à son ministère en définissant, pour chaque type de système d'information, les mesures de protection nécessaires. Un catalogue des informations à protéger doit être actualisé chaque année ;

- Contrôler dans son département l'application de cette réglementation et l'efficacité des mesures prescrites ;

- Organiser en permanence la sensibilisation des autorités définies à l'article 19, et contrôler la formation des cadres ;

- Assurer la liaison avec les commissions interministérielles et ministérielles spécialisées.

Une équipe de sécurité des systèmes d'information, à la disposition du Haut fonctionnaire de défense et du fonctionnaire de sécurité des systèmes d'information, peut être constituée si les besoins du département ministériels l'exigent.

Article 19

AUTORITES QUALIFIEES ET AGENTS DE SECURITE

1 - L'autorité qualifiée

Les **autorités qualifiées** sont les autorités responsables de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'Etat, ainsi que dans les établissements publics visés à l'article 3 et dans les organismes et entreprises ayant conclu avec l'administration des marchés ou des contrats visés par ce même article.

Leur responsabilité ne peut pas se déléguer.

Sous le contrôle du Haut fonctionnaire de défense et du fonctionnaire de sécurité des systèmes d'information, **l'autorité qualifiée** est chargée de :

- Définir une politique de sécurité des systèmes d'information adaptée à son organisme ou à son entreprise et d'en fixer les objectifs ;

- S'assurer que les dispositions contractuelles et réglementaires sur la sécurité des systèmes d'information sont appliquées aux différents niveaux et selon les structures propres à l'organisme ou à l'entreprise ;

- Elaborer les consignes et les directives internes ;

- S'assurer que les contrôles internes de sécurité sont régulièrement effectués ;

- Organiser la sensibilisation et la formation du personnel aux questions de sécurité ;

- Mettre en oeuvre les procédures prescrites pour le contrôle des personnes ainsi que pour l'homologation des produits et des installations.

Dans les administrations et services déconcentrés de l'Etat, ainsi que dans les établissements publics visés à l'article 3, de ministre désigne les **autorités qualifiées** aux niveaux convenables (directions, services, établissements...)

2 - L'agent de sécurité des systèmes d'information (ASSI)

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.

Elles peuvent, à cet effet, se faire assister par un ou plusieurs **agents de sécurité des systèmes d'information (ASSI)**, chargés de la gestion et du suivi des moyens de sécurité des systèmes d'information se trouvant sur le ou les sites où s'exercent leurs responsabilités, notamment lorsque la gestion et le suivi de ces articles nécessitent une comptabilité individuelle.

L'agent de sécurité des systèmes d'information assure les missions suivantes :

a) la protection des personnes.

A cet effet, l'ASSI :
- Tient à jour la liste des personnels employés à titre permanent et, le cas échéant occasionnel, affectés au traitement des informations ;

- Fait surveiller en permanence les activités des personnes extérieures, appelées à effectuer des travaux temporaires ;

- S'assure de l'application, par les personnels d'exploitation et les utilisateurs, des règles de sécurité prescrites ;

- Assure la formation et la sensibilisation des personnels en matière de sécurité.

b) la protection des informations :

A cet effet, l'ASSI :
- Veille à la mise en oeuvre des mesures de protection prescrites, il établit des consignes particulières et contrôle leur application ;

- Tient la comptabilité d'entrée et de sortie des supports d'informations ayant reçu une mention de sensibilité, et en assure périodiquement l'inventaire ;

- Etablit les consignes de sécurité relatives à la conservation et au stockage des supports des informations classifiées ;

- Contrôle la destruction des informations ayant une mention de sensibilité qui doivent être expurgées du système.

c) la sécurité des systèmes et réseaux.

A cet effet, l'ASSI :
- Vérifie périodiquement le bon fonctionnement des dispositifs de sécurité ;

- Veille au respect des procédures opérationnelles de sécurité propres au système de traitement utilisé ;

- S'assure de l'installation correcte, au plan technique, des différents matériels utilisés ;

- Selon les règles de sécurité en vigueur, établit et diffuse aux utilisateurs les éléments d'authentification pour les applications ayant reçu une mention de sensibilité ;

- Surveille les opérations de maintenance ;

- Assure la liaison avec le responsable de la sécurité protection incendie du centre informatique ;

- Rend compte de toute anomalie constatée.

Pour l'exercice de ses attributions, l'ASSI peut disposer d'une équipe de sécurité dont l'effectif dépend de la dimension de l'organisme ou de l'entreprise, et de la nature des systèmes à protéger.

CHAPITRE 5

DISPOSITIONS DIVERSES

Article 20

INSPECTIONS ET CONTROLES

I. A l'échelon interministériel.

Des inspections et contrôles portant sur la sécurité des systèmes d'information sont organisés par la délégation interministérielle pour la sécurité des systèmes d'information.

II. A l'échelon ministériel.

Chaque ministre prescrit, à l'intérieur de son département, les inspections et contrôles nécessaires pour vérifier l'application effective de la réglementation traitant de la sécurité des systèmes d'information.

III. Rapport annuel d'évaluation

Chaque Haut fonctionnaire de défense[1] adresse en début d'année au délégué interministériel pour la sécurité des systèmes d'information, un rapport sur l'état de la sécurité des systèmes d'information dans son département. Ce rapport fait notamment le bilan des enseignements tirés des inspections et contrôles effectués durant l'année.

Chaque année, le délégué interministériel pour la sécurité des systèmes d'information adresse au Premier ministre un rapport sur la sécurité des systèmes d'information.

Fait à Paris, le 2 mars 1994

Pour le Premier ministre et par délégation
Le secrétaire général du Gouvernement
Renaud DENOIX de SAINT MARC

Pour ampliation
Le Chef du Service central
de la sécurité des systèmes d'information :
Michel DAGES

[1]. pour le ministère de la défense, le chef du cabinet militaire

ANNEXE

GLOSSAIRE

Les termes suivis d'un astérisque (*) sont définis conformément à l'arrêté du 22 décembre 1981 du ministre de l'industrie et du ministre de l'éducation nationale, relatif à l'enrichissement du vocabulaire de l'informatique (Journal Officiel du 17 janvier 1982).

Agrément :

Reconnaissance formelle que le produit ou système évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies.

Agrément d'un laboratoire :

Reconnaissance formelle qu'un laboratoire possède la compétence pour effectuer des évaluations d'un produit ou d'un système par rapport à des critères d'évaluation définis.

Donnée* :

Représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement.

Evaluation :

Estimation de la sécurité d'un produit ou d'un système par rapport à des critères d'évaluation définis.

Homologation :

Autorisation d'utiliser, dans un but précis ou dans des conditions prévues, un produit ou un système (en anglais : accreditation). C'est l'autorité responsable de la mise en oeuvre du produit ou du système qui délivre cette autorisation, conformément à la réglementation en vigueur.

Information* :

Renseignement ou élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.

Système d'information :

Tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information (c.f. article 2).

Système informatique :

Ensemble formé par un ordinateur et les différents éléments qui lui sont rattachés. Ceci concerne les matériels et les logiciels.