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 3
PRINCIPES DE SÉCURITÉ

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

Introduction

Le guide PSSI est décomposé en quatre sections :

- l'introduction 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 (ce document) ;

- 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.

Un formulaire de recueil de commentaires figure en annexe de chaque guide afin de renvoyer des propositions et remarques à la DCSSI.

Objet du document

Cette section du guide PSSI présente la liste des principes utiles pour l'élaboration d'une politique de sécurité des systèmes d'information (PSSI).

Ces principes couvrent 16 domaines de la sécurité des systèmes d'information.

- **Principes organisationnels**
  1. Politique de sécurité
  2. Organisation de la sécurité
  3. Gestion des risques SSI
  4. Sécurité et cycle de vie
  5. Assurance et certification

- **Principes de mise en œuvre**
  6. Aspects humains
  7. Planification de la continuité des activités
  8. Gestion des incidents
  9. Sensibilisation et formation
  10. Exploitation
  11. Aspects physiques et environnementaux

- **Principes techniques**
  12. Identification / authentification
  13. Contrôle d'accès logique
  14. Journalisation
  15. Infrastructures de gestion des clés cryptographiques
  16. Signaux compromettants

Chacun des principes pourra être décliné en règles d'application pour rédiger une PSSI.

La DCSSI recommande :

- de conserver les conventions d'écriture,

- d'éviter la recopie des principes de sécurité sans analyse approfondie.

1 Principes organisationnels

PSI : Politique de sécurité

PSI-01 : Évolutions de la PSSI

Un organisme peut changer au cours du temps (organisation, missions, périmètre, axes stratégiques, valeurs). Son système d'information est donc l'objet de modifications fréquentes, tout comme les menaces et vulnérabilités qui s'y appliquent. Il convient alors de prévoir un réexamen de la PSSI :

- lors de toute évolution majeure du contexte ou du SI ;
- dans le cas d'une évolution de la menace ;
- dans le cas d'une évolution des besoins de sécurité ;
- à la suite d'un audit ;
- à la suite d'un incident de sécurité ;
- systématiquement à intervalle défini ;
- sur demande d'une autorité (responsable de la sécurité, direction…) dans le cadre d'une procédure à définir dans la PSSI.

PSI-02 : Diffusion de la PSSI

La PSSI ainsi que toutes ses déclinaisons opérationnelles doivent être parfaitement documentées et les versions de références à jour doivent être facilement accessibles à tous les personnels de l'organisme.
La PSSI doit être connue 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…) ;
Cependant, elle peut contenir des informations confidentielles et les personnels de l'organisme peuvent être concernés de façon différenciée en fonction de leur rôle. De ce fait, il est recommandé, le cas échéant, d'élaborer et de diffuser des synthèses, incluant des extraits plus détaillés pour les informations pertinentes en fonction des lecteurs. Le but de ces synthèses est de permettre à chacun de connaître les enjeux et les règles de sécurité en fonction de ses besoins.

PSI-03 : Contrôle d'application de la PSSI

Il est judicieux de prévoir des procédures et moyens de contrôle interne de l'application de la PSSI et de les compléter par des procédures et moyens d'audits externes. Éditer des règles sans se donner les moyens de contrôler leur application ne constitue pas une situation acceptable, en particulier sur le plan de la sécurité.

PSI-04 : Protection des informations confiées à l'organisme

Ce principe permet de s'assurer de l'exhaustivité des références réglementaires.
Les informations détenues provisoirement par l'organisme et qui comportent, du fait de leur propriétaire, une classification ou une mention particulière de protection devraient être protégées rigoureusement selon les mêmes mesures que celles appliquées par l'organisme d'origine. Ces mesures peuvent découler de l'application des textes de loi (Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés…), d'instructions interministérielles comme, par exemple, celle traitant du respect de la classification des informations liées au secret de défense [IGI 900], de la protection des informations concernant le patrimoine national [II 486] ou de l'établissement d'un marché de défense [II 2000].
Dans le cas où ces règles ne découlent pas de réglementations communes, ils convient de contractualiser l'engagement des parties vis-à-vis des informations échangées.

PSI-05 : Adoption d'une échelle de besoins

Une échelle de besoins selon différents critères de sécurité (disponibilité, intégrité, confidentialité…) permettra de faciliter la classification objective des éléments essentiels de l'organisme (informations et fonctions).

La démarche méthodologique du guide PSSI propose une approche pour élaborer une échelle de besoins. Elle précise qu'une pondération et des valeurs de référence doivent être déterminées pour chacun des critères de sécurité. Les valeurs de référence doivent être objectives, propres à l'organisme et liées à ses orientations stratégiques.
Par ailleurs, dans le plan-type proposé dans le guide PSSI, il est recommandé d'inclure cette échelle dans la PSSI.

PSI-06 : Critères de détermination des besoins de sécurité

La démarche méthodologique du guide PSSI propose une approche pour déterminer les besoins de sécurité (en termes de disponibilité, d'intégrité, de confidentialité…) des éléments essentiels (informations et fonctions) selon l'échelle de besoins adoptée.

Deux cas se présentent pour les éléments essentiels identifiés :

- l'utilisation directe de cette échelle de besoins pour ceux qui ne possèdent pas de classification ;

- la mise en correspondance avec cette échelle de besoins pour ceux qui possèdent déjà une classification (par exemple les informations relevant du secret de défense, sensibles, vitales…).

En dehors, principalement, des informations relevant du secret de défense et des informations nominatives pour lesquelles les textes législatifs en vigueur doivent être appliqués, les besoins de sécurité seront déterminés selon le contrôle de l'origine des informations, l'appréciation de leur intérêt et de leur validité par rapport à leur cycle de vie dans le processus opérationnel de production :

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

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

Remarque concernant les **informations sensibles** :

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

- d'une part, les informations relevant du secret de défense au sens de l'article 5 de l'[IGI 900] ; l'organisme est alors tenu de respecter les règles de classification spécifiées dans la réglementation ; de plus, l'organisme a obligation de mettre en œuvre les moyens pour être conforme à la réglementation ;

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

La classification retenue vise en premier lieu à donner à l'utilisateur une juste appréciation de la sensibilité des informations qu'il traite, puis à faciliter le contrôle et, par conséquent, à améliorer la protection des informations sensibles. Pour celles qui ne sont pas du ressort de l'[IGI 900] la classification choisie doit être approuvée par l'organisme.

Remarque concernant les **informations vitales** :

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

- d'une part, les informations relevant du secret de défense au sens de l'article 6 de l'[IGI 900],

- d'autre part, les informations ne relevant pas du secret de défense au sens de l'article 5 de la [REC 901] mais nécessaires pour le fonctionnement du système, ainsi que des informations sortant du champ de l'article 5 (par exemple, les nomenclatures d'articles pour une unité de production).

La classification retenue vise en premier lieu à donner à l'utilisateur une juste appréciation de la sensibilité des informations qu'il traite, puis à faciliter le contrôle et, par conséquent, à améliorer la protection des informations vitales. Pour celles qui ne sont pas du ressort de l'[IGI 900], la classification choisie doit être approuvée par l'organisme. En particulier, il peut être prévu la spécification d'un seuil minimal de disponibilité des informations vitales (traitées ou traitantes) en dessous duquel le système d'information est déclaré inopérant.

Remarque concernant les **informations stratégiques** :

Les informations stratégiques sont des informations dont la connaissance est nécessaire pour atteindre les objectifs correspondant aux orientations stratégiques de l'organisme. Elles peuvent être protégées par des textes législatifs, mais peuvent également faire l'objet de contrats, de conventions ou de protocoles d'accord protégés par le Code Civil.
La classification retenue vise en premier lieu à donner à l'utilisateur une juste appréciation de la sensibilité des informations qu'il traite puis à faciliter le contrôle et, par conséquent, à améliorer la protection des informations stratégiques ; elle peut s'appuyer sur des critères propres à l'organisme comme, par exemple, un secteur particulier (études, innovations, marchés…), le niveau de valeur accordé et la durée de validité.

Remarque concernant les **informations nominatives** :

L'article 4 de la loi "Informatique et Libertés" définit la notion d'information nominative : "les informations nominatives sont celles qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale".
La classification retenue vise à faciliter le contrôle et, par conséquent, à améliorer la protection des informations nominatives conformément à la loi ; elle peut s'appuyer sur des critères propres à l'organisme comme, par exemple, un domaine particulier (médical, recrutement…), le type de sondage ou d'enquête, le lieu de traitement ou de stockage.

Remarque concernant les **informations coûteuses** :

Les informations coûteuses sont des informations qui font partie du patrimoine de l'organisme et dont la collecte, le traitement, le stockage ou la transmission nécessitent un délai important ou un coût d'acquisition élevé. Les dispositions législatives énumérées pour les informations stratégiques peuvent être appliquées à cette catégorie.
La classification retenue vise en premier lieu à donner à l'utilisateur une juste appréciation de la sensibilité des informations qu'il traite puis à faciliter le contrôle et, par conséquent, à améliorer la protection des informations coûteuses ; elle peut s'appuyer sur des critères propres à l'organisme comme, par exemple, un secteur particulier (études, innovations…), la provenance et le niveau de coût.

PSI-07 : « Déclassification » des informations

La classification d'une information est parfois attribuée pour une période de temps. Des règles devront définir les périodes minimales selon la nature des informations.

PSI-08 : « Surclassification » des informations

Le degré de protection doit être proportionnel à la classification des informations et des systèmes.
Si l'emploi d'une classification élevée semble garantir une meilleure protection, un recours systématique à la surclassification risque d'entraîner une perte de confiance vis à vis de la méthode de classification. Pour éviter cela il convient :
- d'éviter de surclasser l'information ;
- de revoir périodiquement la classification attribuée.

PSI-09 : Identification et portée de la classification d'une information

L'identification de la classification doit être claire, connue de tous et immédiatement reconnaissable. Pour les documents, elle doit être intégrée aux chartes graphiques ; pour les disquettes et autres supports informatiques, aux procédures de gestion des supports ; pour les fichiers, aux procédures d'organisation des ressources informatiques. Les machines appartenant à un réseau traitant d'informations confidentielles ou hébergeant des informations de ce type doivent également être identifiées.
Il est important que les personnels aient conscience que la classification de leur organisme peut ne pas être équivalente à une classification portée sur des informations provenant d'autres organismes. À l'inverse la classification définie pour l'organisme peut n'avoir de sens que dans le périmètre de la PSSI.

PSI-10 : Définition et contrôle des habilitations

L'organisme propriétaire des informations doit être en mesure d'attribuer des habilitations liées à l'utilisation des informations et il a pour mission de définir les règles de gestion des habilitations et d'effectuer les contrôles correspondants.
Sans être nécessairement le propriétaire des informations à un instant donné, l'organisme peut néanmoins en être le dépositaire. Dans ce cas, il ne dispose pas de pouvoir de décision vis à vis des informations traitées mais doit respecter les règles de gestion définies par le propriétaire (clients, sous-traitants...) en fonction de la classification affectée.

PSI-11 : Critères de diffusion interne des informations

Afin d'éviter les indiscrétions et les fuites, les informations et généralement les supports associés, ne doivent pouvoir être utilisés que dans un environnement répondant aux exigences de sécurité définies par l'organisme.
Le contrôle de la diffusion interne a pour but de s'assurer que les informations sont rendues disponibles exclusivement aux personnes ayant le besoin de les connaître dans le cadre de leur travail. Un contrôle permet également de vérifier que la recopie d'informations est conforme aux prérogatives prévues par la loi (droit d'auteur, copyright), à la réglementation (secret de défense) et aux contraintes spécifiques de l'organisme.
Le besoin d'en connaître (pour la confidentialité) peut être étendu aux besoins d'en modifier (pour l'intégrité), d'en utiliser (pour la disponibilité)…

PSI-12 : Critères de diffusion externe des informations

La mise à disposition non contrôlée d'informations nécessitant une protection peut porter préjudice à l'organisme (par exemple, perte de crédibilité ou d'image de marque, récupération de savoir-faire…).
La mise en place de critères permet de s'assurer que les informations transmises à l'extérieur d'un organisme, si elles sont de nature confidentielle, imposent un contrôle préalable d'habilitation du récepteur ou une clause contractuelle liant les organismes concernés ; dans le cas d'informations nominatives, la communication doit être en accord avec la loi.
Par ailleurs, dans le cadre de ce principe, il peut être envisagé que la diffusion externe des informations soit effectuée par du personnel habilité et selon une procédure d'autorisation préalable.

ORG : Organisation de la sécurité

ORG-01 : Responsabilités générales pour la sécurité du système d'information de l'organisme

La nomination d'un responsable de la sécurité des systèmes d'information (RSSI ou équivalent) est nécessaire pour assurer la responsabilité globale de l'élaboration, de la mise en œuvre et du

fonctionnement de la gestion de la SSI dans l'organisme. Ce RSSI (terminologie habituelle qui sera employée dans la suite de ce document) est en charge du respect d'une PSSI à tous les échelons et domaines de l'organisme.
Ce responsable, rattaché à la direction de l'organisme doit pouvoir faire prévaloir l'aspect sécuritaire sur les intérêts particuliers et intégrer la sécurité dans tous les projets touchant les systèmes d'information.
La mise en place de cette fonction est un signal fort et nécessaire de l'importance donnée par l'organisme à sa PSSI.
Dans le cadre des administrations, la voie fonctionnelle SSI couvre ces responsabilités.

ORG-02 : Les responsabilités pour l'élaboration et la mise en œuvre d'une PSSI

La PSSI concerne toutes les fonctions vitales d'un organisme ; en effet, celui-ci ne pourrait généralement pas supporter une défaillance prolongée de son ou de ses systèmes d'information.
De ce fait, la PSSI revêt un intérêt stratégique : une règle doit définir les responsabilités pour son élaboration comme pour ses inéluctables évolutions au sein, par exemple, d'un comité de pilotage.
De plus, dans la phase de mise en œuvre de la PSSI, la règle établit les responsabilités des autorités qualifiées dans la mise en place et le contrôle des consignes de sécurité pour l'installation et l'exploitation des moyens composant le système d'information.
Elle met tout particulièrement en évidence, la nécessité d'une intégration de la sécurité dès la conception et le développement de tout nouveau projet intéressant le système d'information. La PSSI indique également que la sécurité du SI ne se limite pas aux aspects et aux évolutions techniques mais qu'elle englobe toute évolution ou modification de l'organisation, des missions….

ORG-03 : Couverture des responsabilités

Le principe général de sensibilisation de l'OCDE énonce : "Les attributions et responsabilités des propriétaires, des fournisseurs, des utilisateurs de système d'information et des autres parties concernées par la sécurité des systèmes d'information, doivent être explicitement exprimées".
Il est fondamental que tous les domaines concernés par la sécurité (sécurité des infrastructures, sécurité dans les projets et familles d'application, sécurité des locaux, documentation de sécurité…) aient un responsable désigné et que l'ensemble des tâches relevant de la sécurité, ait été attribué.
L'organisation de la sécurité dans chacun de ces domaines doit inclure les niveaux stratégique, de pilotage et opérationnel.
En particulier, il doit exister une identification claire et unique de la responsabilité sécurité liée aux réseaux ou systèmes transversaux tel que le réseau bureautique d'entreprise ou le dispositif d'accès aux réseaux externes.

ORG-04 : Responsabilités du niveau décisionnel

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

(1) Pour un organisme ministériel, ce niveau est celui **du haut fonctionnaire de défense** (HFD) qui reçoit délégation du ministre ; il est responsable de l'application des dispositions relatives à la sécurité de défense, à la protection du secret et à la sécurité des systèmes d'information.
Il peut être aidé dans sa mission par un **fonctionnaire de sécurité des systèmes d'information** (FSSI) dont les principales missions sont ([IGI 900], article 19 et [REC 901], article 18) :
- de préciser les modalités d'application des instructions interministérielles, ;
- d'élaborer et de contrôler l'application des instructions particulières à son ministère ;
- d'organiser la sensibilisation des autorités ;
- d'assurer la liaison avec les commissions interministérielles et ministérielles spécialisées.

(2) Pour un organisme public ou privé, ce niveau est celui **d'un haut responsable de la sécurité** qui reçoit délégation du **comité de direction** ; il est aidé dans sa mission par un **comité de sécurité.**
Le comité de direction fixe, sur proposition du haut responsable de la sécurité, les grandes orientations en matière de SSI, en accord avec les objectifs de l'organisme et les différentes politiques mises en œuvre (politique de gestion du personnel, budgétaire, de production…). Ce comité peut être, par ailleurs, l'instance de validation de la PSSI.
Le haut responsable de la sécurité veille à l'application de la PSSI. Il participe aux délibérations du comité de direction dont il est le conseiller pour toutes les questions relatives à la sécurité telles que la définition des objectifs, l'allocation des ressources et du personnel.

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

(3) Une **équipe de sécurité** du système d'information, à la disposition du haut fonctionnaire de défense (ou du haut responsable de la sécurité), peut être constituée si les besoins de l'organisme l'exigent. Elle rassemble des spécialistes en informatique et en réseaux de télécommunication, mais aussi de responsables des aspects non technologiques des systèmes d'information, formés à la sécurité et dont les principales missions sont :
- la préparation et la coordination des activités de sécurité ;
- l'évaluation périodique des vulnérabilités ;
- la recherche des solutions techniques et l'élaboration des procédures ;
- la mise en place de programmes de sensibilisation et de formation ;
- les expertises de sécurité sur demande du comité de direction.

L'équipe de sécurité peut être composée de permanents mais pourra en fonction des besoins (tels de gros projets d'évolution majeure du SI) s'adjoindre temporairement des spécialistes ou experts des domaines concernés.

ORG-05 : Responsabilités du niveau de pilotage

Dès lors que la taille d'un organisme le justifie, il sera identifié des sous-ensembles (sites, parties du SI, divisions…) avec une mise en place de responsables « locaux », une délégation de responsabilité clairement définie et une organisation efficace de la coordination avec la structure centrale.
Pour un organisme ministériel, ce niveau est celui des **autorités qualifiées** qui sont responsables de la sécurité du système d'information dont ils ont la charge ([IGI 900], article 20 et [REC 901], article 19).
Pour un organisme privé, ce niveau est celui d'un correspondant local de sécurité, dont la fonction est dédiée à la SSI et qui appartient à l'équipe dirigée par le RSSI.
Leur mission est de piloter la mise en œuvre de la PSSI à leur niveau (direction, service, établissement…) et, plus précisément :
- de s'assurer du respect des dispositions contractuelles et réglementaires ;
- d'élaborer les consignes et les directives internes ;
- de s'assurer que les contrôles internes de sécurité sont correctement effectués ;
- d'organiser la sensibilisation du personnel.

Ces autorités peuvent s'appuyer sur les compétences de l'équipe de sécurité.
Pour assurer les missions de pilotage de la SSI, il est parfois nécessaire de constituer des comités de pilotage dédiés :
- au suivi de l'application de la PSSI ;
- au traitement de crises, liées à la sécurité du système d'information ;
- à la veille technologique, au suivi des besoins SSI de l'organisme, et à l'évolution de la PSSI.

ORG-06 : Responsabilités du niveau opérationnel

À tous les niveaux, les autorités hiérarchiques sont personnellement responsables de l'application des mesures, définies par les autorités qualifiées, destinées à assurer la sécurité des systèmes d'information ([IGI 900], article 20 et [REC 901], article 19).
Tout personnel appartenant ou intervenant dans l'organisme est impliqué dans la SSI et dispose de responsabilités qui doivent être clairement formalisées et portées à la connaissance de chacun.
Les responsabilités et engagements du personnel (voir les principes de sécurité relatifs aux obligations contractuelles) couvrent notamment :
- le respect des lois et règlements,
- le respect de la politique et règles spécifiques (liées à un projet, à un établissement, à une fonction particulière),
- l'accès à un réseau ou à des locaux dans un autre organisme.

Ces responsabilités peuvent être renforcées en fonction de leurs fonctions et habilitations (voir les principes de sécurité relatifs aux habilitations). Par exemple, les administrateurs des systèmes d'information, détenteurs de secrets et exploitant des fonctions sensibles des SI, auront des responsabilités particulières dans le domaine de la SSI.
D'autre part, les responsabilités des personnels de l'organisme doivent également couvrir le cas où ils interviennent dans un autre SI que celui de l'organisme auquel ils appartiennent (clients, partenaires…).

ORG-07 : Autres responsables de l'organisme jouant un rôle dans la SSI

Il existe d'autres fonctions non dédiées à la sécurité mais jouant néanmoins des rôles particuliers indispensables au fonctionnement de la SSI.
Ces fonctions sont notamment :

- **les agents ou correspondants de la sécurité**
  Pour permettre à chaque site, service ou unité la mise en œuvre des consignes et des procédures, les autorités hiérarchiques se font assister par un ou plusieurs **agents de la sécurité** chargés principalement de l'interface entre les utilisateurs du système d'information et les responsables du suivi de la SSI.
  L'objectif est double :
    - o faciliter la diffusion de l'information de sécurité et l'application des règles de bon usage ;
    - o assurer une remontée d'information des utilisateurs auprès du suivi centralisé de la sécurité.

  Ce rôle doit être assuré par des personnes « proches » des utilisateurs sur les plans géographique et métier.
  Ces agents sont les correspondants privilégiés de l'équipe de sécurité.
  Ils peuvent également avoir en charge les ressources communes à plusieurs unités opérationnelles. Leur rôle est alors la mise en œuvre des mesures de protection compatibles avec les objectifs des unités et la résolution locale des problèmes de sécurité. En l'absence de telles mesures, il pourrait s'ensuivre un arbitrage difficile entre une tâche fonctionnelle et une action de sécurité.
- **les responsables juridiques de l'organisme**
  Ils jouent un rôle indispensable dans le domaine de la SSI de l'organisme. Ils interviennent sur l'initiative du RSSI dans divers domaines dont notamment :
    - o la rédaction des clauses de confidentialité et les engagements de SSI dans les contrats commerciaux et les contrats d'embauche ;
    - o le dépôt de plaintes et l'instruction d'affaires ;
    - o l'intégration dans les divers règlements et chartes de l'organisme des règles de SSI ;
    - o les relations avec les sous-traitants.
- **les responsabilités des auditeurs**
  Outre les responsabilités de contrôle attribuées aux rôles opérationnels, les auditeurs ont en charge les missions suivantes :
    - o définir la stratégie d'audit, comprenant notamment les audits SSI ;
    - o réaliser ou faire réaliser des audits SSI, selon son plan d'audit ou sur demande des Directions, en relation avec le RSSI ;
    - o informer le commanditaire et les entités auditées, selon leur besoin d'en connaître et informer le RSSI de la mise en évidence d'éventuels incidents ou anomalies SSI.
- **d'autres responsabilités** peuvent être nécessaires pour réaliser des actions spécifiques de sécurité définies par exemple dans le cadre de plans d'amélioration de la sécurité, de migration d'applications…

ORG-08 : Entités spécifiques dédiées à la gestion et au pilotage de la sécurité

D'autres entités spécifiques peuvent être créées. Parmi ces entités, on peut notamment citer :

- un comité de sécurité, responsable de la maintenance de la PSSI et du suivi de l'application du plan d'action prioritaire. Il est également chargé de tenir informer la Direction générale de l'efficacité de la politique en place ;
- une cellule de crise, chargée le cas échéant de la mise en œuvre d'une procédure d'urgence pour faire face;
- une équipe de veille technologique, chargée du suivi des alertes sécurité et de leur traitement selon leur pertinence ;
- une cellule d'audit, chargée de la réalisation effective des audits du système d'information.

ORG-09 : Application de la notion de responsable-détenteur

La notion de responsable-détenteur concerne le responsable hiérarchique d'une unité organique (établissement, service, centre de responsabilités ou de profit) ou l'autorité qualifiée telle qu'elle est définie au principe ORG-05, Responsabilités du niveau de pilotage, et qui dispose de ses propres ressources humaines et matérielles pour mener à bien sa mission.
Le terme de détention s'applique au patrimoine d'information, aux logiciels et aux matériels constitutifs du système d'information et implique l'obligation de respecter les lois, règlements et règles en vigueur dans l'organisme. Les informations, logiciels, et matériels concernés peuvent appartenir à l'organisme ou avoir été confiés par un tiers (clients, partenaires, prestataires…).
Le responsable-détenteur détermine les niveaux de risques acceptables et les conditions d'accès aux fichiers, de mises à jour des informations (en accord avec les règles de classification en vigueur dans l'organisme) ou de modifications des logiciels et des matériels dont il dispose.

ORG-10 : Application de la notion de responsable-dépositaire

Le responsable-dépositaire reçoit délégation du responsable-détenteur pour l'application des lois, règlements et des règles de protection concernant les informations, logiciels et matériels durant les phases de collecte, de traitement, de diffusion et de stockage.
Le responsable-dépositaire peut être, par exemple, un informaticien de l'équipe d'exploitation, un documentaliste, un secrétaire… Il est le gardien d'une partie du patrimoine de l'organisme et il est alors tenu, tout particulièrement, de se porter garant de l'application de la loi concernant la protection juridique des logiciels qui lui sont confiés (copies illicites).

ORG-11 : Gestion des relations avec des tiers intervenant dans le cadre de la SSI

La PSSI doit formaliser les types de relation, les consignes et identifier les contacts utiles avec les organismes tiers jouant un rôle (ou susceptible de jouer un rôle) dans le cadre du suivi et du maintien de la SSI.
Parmi ces organismes, il peut y avoir :

- dans la catégorie des autorités et partenaires :
    - les organismes à contacter en cas de détection d'acte malveillant dans le cadre du SI ;
    - les organismes de veille et d'alerte ;
    - des organismes d'audit ;
- dans la catégorie des prestataires :
    - les prestataires de services de télécommunication ;
    - les prestataires intervenants dans l'organisme ;
    - des prestataires sous-traitant et/ou prenant en charge une partie de l'exploitation du SI ;
    - des prestataires experts dans le domaine de la sécurité ;
    - des organismes d'audit externes.

Il est essentiel de maîtriser les accès que ce soit au système d'information ou même à des informations sensibles concernant le SI et sa sécurité. Dès lors que des tiers doivent pour la nécessité du service, avoir ce type d'accès, il convient de s'assurer que les mêmes règles de sécurité s'imposant aux personnels internes sont applicables (documentation et aspects contractuels) et appliquées par les acteurs concernés.

ORG-12 : Cadre contractuel pour les échanges de données sécurisés

Les propositions d'accès à des services ou à des applications télématiques internes ou externes à l'organisme posent le problème de la coopération entre les différents systèmes d'information. Cette règle vise à prévenir la perte, la modification et la mauvaise utilisation des données.
Il importe, en conséquence, de prévoir les responsabilités et les obligations contractuelles des divers intervenants, tant au niveau des transmissions que des applications qui les intègrent.
L'échange de données sécurisé se situe dans le cadre de transmissions telles que définies plus haut.
Le cadre contractuel désigne les accords entre plusieurs parties pour les échanges de données faisant appel ou non aux technologies de l'information : cette règle englobe le cas des échanges de données informatisées (EDI).
Les accords ou contrats passés par l'organisme avec tous les utilisateurs du système d'information comportent des clauses de contrôles précisant, par exemple :

- la responsabilité de la gestion des flux d'échanges ;

- les procédures de sécurité utilisées pour les échanges ;
- les standards de structuration des données ;
- les responsabilités en cas de pertes des informations ;
- les mesures spécifiques pour la protection des clés de chiffrement.

ORG-13 : Modalités d'utilisation des réseaux de télécommunication externes à l'organisme

L'utilisation des réseaux de télécommunication externes à l'organisme met en relation des utilisateurs qui n'ont pas, à priori, les mêmes exigences de sécurité, et qui par ailleurs ne sont pas contrôlables.
Les modalités d'utilisation sécurisée des réseaux de télécommunication externes à l'organisme concernent tout particulièrement le contrôle des moyens qui peuvent échapper à la gestion centralisée du système d'information comme, par exemple, l'installation de modems ou de Minitels. Le cas particulier du courrier électronique devrait inciter à l'adoption de mesures visant à contrôler l'envoi de messages considérés comme vulnérables face aux interceptions et modifications non autorisées et sur les considérations légales liées à la non répudiation du message émis ou reçu.
Le personnel de l'organisme qui travaille depuis son domicile (télétravail) se trouve dans un environnement privé sur lequel l'organisme n'a aucun contrôle, c'est pourquoi il doit mettre en place des règles techniques particulières concernant les droits d'accès mais aussi sensibiliser particulièrement l'utilisateur en l'informant sur ses responsabilités vis à vis des informations que lui confie l'entreprise.
Les rubriques tirées de l'architecture OSI s'appliquent au cas des réseaux externes à l'organisme.

ORG-14 : Clauses spécifiques de protection des informations

Lorsque des échanges sont prévus avec des tiers, des clauses spécifiques peuvent être incluses dans les contrats, régissant le cadre de ces échanges. Elles portent sur les moyens, comme :
- le contrôle de l'absence de codes malveillants ;
- les règles de protection appliquées en interne (définition d'un tableau de classification croisée) ;
- le support d'échange et les moyens de protection contre la divulgation, l'intégrité, la non-répudiation…

Si l'organisme s'est engagé à respecter de telles clauses énoncées par un tiers, elle devra en informer les personnels concernés, voire les inclure dans sa PSSI.

ORG-15 : Sélection, coordination et emploi des moyens cryptographiques

En raison des enjeux, le choix des moyens (par exemple logiciels ou matériels cryptographiques utilisables) et plus encore des services externes (par exemple : autorité de certification, prestataire de service de confiance) doit être validé et approuvé par la structure sécurité de l'organisme quand ce choix n'est pas directement effectué par cette structure.
Un des éléments essentiels à prendre en compte en ce qui concerne la confidentialité est le traitement du besoin (ou non) de recouvrement par l'organisme des documents chiffrés par ses personnels. Les solutions peuvent se jouer au niveau de la gestion des clés (par exemple mise en place de séquestre) ou des fonctions et utilitaires (création systématique de champs de recouvrement).
Pour chacune des fonctions de base (confidentialité, authentification, non-répudiation) il convient que soient élaborées des règles indiquant les exigences minimales (tant de principe qu'opérationnelles) qui devront être respectées.
Le choix des prestataires externes (AC ou PSC par exemple) est une décision structurante qui nécessite l'approbation de la structure sécurité et une validation par la direction générale. Il convient de veiller à ce que des clauses de protection, de sécurité et de garantie convenables soient explicitement présentes dans chacun des contrats avec ces prestataires.

ORG-16 : Mise en place d'une organisation de veille et de prévention

Il est indispensable de définir une organisation qui surveille et maintienne la liste des risques majeurs qui pèsent sur le système d'information (nouvelles menaces, nouveaux besoins de sécurité, évolution majeur du système d'information…).
Cette organisation doit disposer de compétences d'experts internes ou externes et de moyens suffisants pour collecter et qualifier l'information (contacts, abonnements à des organismes spécialisés, voir ORG-12, Gestion des relations avec des tiers intervenant dans le cadre de la SSI.

Elle doit également disposer de moyens contrôlés, de diffusion des informations sécurité pertinentes, à des fins préventives.
Cette veille peut être externalisée ou conduite en lien avec des organismes comme le CERTA qui publie régulièrement des avis, alertes ou recommandations aux administrations françaises.
Cependant, la mise en place d'un système de veille doit s'accompagner d'un suivi des recommandations : la veille n'est pas une fin en soit, il est impératif de contrôler la mise en œuvre des recommandations issues de la veille.

ORG-17 : Organisation de cellules de crise

Le principe est de définir au préalable une organisation (responsabilités, fonctionnement et moyens) capable de répondre à des incidents majeurs survenant dans le système d'information. Il convient pour cela de prévoir des procédures d'escalade, de les tester et de former les personnels à leur exécution.
Le point majeur est d'identifier les acteurs au bon niveau hiérarchique pour être capable de prendre les décisions aussi vite que la situation l'imposera.
Il convient également de définir les moyens et procédures capables de :
- diffuser l'alerte ;
- collecter l'information ;
- constituer une cellule de crise ;
- décider des mesures conservatoires ;
- élaborer un plan d'action regroupant des mesures correctives.

GER : Gestion des risques SSI

GER-01 : Définition du cadre de gestion des risques SSI

La gestion des risques SSI constitue un processus continu dont il convient de définir précisément le cadre (ressources, moyens, responsabilités…) pour chacun de ses aspects :
- appréciation du risque : cette tâche consiste à analyser et évaluer le risque SSI en comparant le niveau de risque à des critères de risques définis au préalable ;
- traitement du risque : cette tâche consiste à réduire, transférer ou prendre le risque apprécié lors de la tâche précédente ;
- acceptation du risque : cette tâche consiste à accepter le risque traité, et le cas échéant à accepter le risque résiduel ;
- communication relative au risque : cette tâche consiste à échanger ou partager des informations concernant le risque.

GER-02 : Identification des objectifs de sécurité

L'identification des objectifs de sécurité permet de définir les besoins réels de l'organisme en matière de SSI. Ce cahier des charges SSI peut être formalisé en respectant les étapes suivantes, compte tenu de la mission ou du métier de l'organisme :
- recueil des éléments stratégiques (contraintes, enjeux, orientations stratégiques, référentiel…),
- expression des besoins de sécurité des éléments essentiels (informations et fonctions) en termes de disponibilité, d'intégrité, de confidentialité… et selon une échelle de besoins objective,
- étude des menaces pesant sur l'organisme (caractérisation des éléments menaçants, étude des vulnérabilités…),
- identification des risques réels pour l'organisme.

Les objectifs de sécurité doivent couvrir l'ensemble des risques identifiés.

La définition des besoins de sécurité permet de décrire de façon non ambiguë les niveaux de sensibilité (en termes de confidentialité, d'intégrité, de disponibilité…) qu'il convient d'assurer aux constituants d'un système d'information.
La sécurité qu'on attend du système d'information doit être précisée dans ses spécifications car elle est une dimension essentielle de ce système au même titre que ses performances ou les services qu'il doit rendre ; **cette expression des besoins de sécurité** devrait faire l'objet d'un examen approfondi conduit selon une démarche méthodologique et une approche globale. Aborder cette analyse par une méthodologie permet de conserver une vision d'ensemble homogène de la problématique SSI, de constituer un référentiel de sécurité complet et de faire prendre conscience au plus grand nombre des risques supportés par le système.

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

C'est sur la base de ces analyses que la décision de prendre en compte ou non les risques pourra être prise.

GER-03 : Circonstances qui justifient une réévaluation de la sécurité du SI

Le principe de réévaluation des lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information stipule :
"Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité. Des vulnérabilités et menaces nouvelles ou évolutives sont constamment découvertes. Toutes les parties prenantes doivent continuellement revoir, réévaluer et modifier tous les aspects de la sécurité pour faire face à ces risques évolutifs".
Une fois qu'un système a été soumis à une évaluation, il est irréaliste de croire qu'il est à l'abri d'erreurs ou impossible à modifier : en effet, le système devra répondre à de nouvelles exigences qui se traduiront par des modifications des matériels, des logiciels et de la documentation. De plus, de nouveaux besoins de sécurité peuvent apparaître et engendrer de nouveaux risques qu'il conviendra d'apprécier et de traiter.
Dans cette optique, il est évident que certaines modifications exigent une réévaluation comme, par exemple, la restructuration du noyau d'un système d'exploitation, qui peut s'appuyer, en partie, sur les résultats de l'évaluation précédente. En revanche, d'autres modifications peuvent n'entraîner aucune nouvelle évaluation dès lors qu'elles touchent à des parties du système d'information séparées des composantes de sécurité et qui n'influent pas sur celles-ci. D'une façon générale, toute évolution du système d'information (évolutions humaines, organisationnelles, financières, géographiques……) doit conduire à une réflexion sur le plan de la sécurité. Cette réflexion peut conduire à une réévaluation du système ou seulement à une modification de certaines règles.

GER-04 : Étude prospective sur l'évolution de la SSI

Une étude prospective sur l'évolution de la SSI permet d'anticiper sur les besoins à moyen terme de l'organisme et d'intégrer le plus tôt possible les nouveaux objectifs, logiciels, matériels ou mécanismes nécessaires à la sécurité. Cette étude prospective ne peut être dissociée des orientations stratégiques (ou d'un schéma directeur des systèmes d'information) portant sur les nouvelles technologies de l'information susceptibles d'être choisies par l'organisme.
Par ailleurs, cette règle vise à vérifier que toute évolution du système d'information reste conforme aux principes de sécurité en vigueur dans l'organisme. Dans le cas contraire, l'étude prospective permet d'en mesurer l'impact sur la sécurité et de proposer les aménagements d'ordre technique ou organisationnel pouvant impliquer une modification des principes et des règles de la PSSI de l'organisme.

GER-05 : Maîtrise et contrôle de certains flux spécifiques

Lorsque les communications permettent des échanges entre l'intérieur et l'extérieur du SI de l'organisme, ainsi qu'à l'intérieur même du SI, voire pour des communications entre périmètres cloisonnés il peut s'avérer nécessaire de mettre en place des règles et des moyens de contrôles spécifiques de ces flux. L'intérêt de conduire une analyse des risques selon une méthodologie apparaît en particulier ici car elle permet d'identifier clairement l'ensemble des flux échangés par le SI ainsi que les menaces qui pèsent qui ces derniers.
Ce sera par exemple le cas des échanges par mail vers l'extérieur avec des règles et donc des dispositifs permettant leur mise en œuvre concernant la taille des messages échangés, la nature des pièces jointes (acceptation ou non de contenus actifs), le contrôle anti-virus et le contrôle contre les codes malicieux. Ces diverses mesures devront être cohérentes avec la charte de sécurité et de bon usage des ressources informatiques que devra avoir signé tout utilisateur, puisque au-delà de son information, des aspects réglementaires (devoir d'information des personnels, respect de la vie privée) entrent en jeu.
Un autre exemple est celui du flux HTTP sortant (consultation de serveurs web externes depuis des postes dans le SI) avec des dispositifs comme par exemple la mise en place –par un proxy sortant- d'une authentification en sortie, la conservation des traces des connexions…

Il ne saurait être question ici ni d'identifier tous les cas de figure, ni encore moins de donner pour chacun les règles et moyens adaptés, la règle à retenir est que chacun de ces flux doit être identifié et analysé sur le plan de la sécurité et pourra/devra donner lieu à la mise en place de solutions spécifiques pour en assurer la sécurité.

GER-06 : Identification des services et moyens justifiant l'utilisation de la cryptographie

Compte tenu des implications tant techniques que légales, il est important d'identifier les applications et services nécessitant l'utilisation de moyens cryptographiques. Les solutions cryptographiques doivent aussi être identifiées pour chaque application ou service. Ce choix est effectué en fonction du type d'informations traitées et du cadre réglementaire. Par exemple, dans le cadre d'un SI manipulant des informations classifiées de défense, l'emploi de moyens cryptographiques agréés est obligatoire. Ici encore l'appréciation des risques fournit les contraintes réglementaires en la matière ainsi que les besoins des utilisateurs.

CDV : Sécurité et cycle de vie

CDV-01 : Intégration de la SSI dans les projets

La PSSI doit prévoir une organisation qui assure une prise en compte des aspects sécurité dans l'ensemble du cycle de vie des projets (étude d'opportunité, étude de faisabilité, conception générale, conception détaillée… jusqu'à la mise au rebut). Cette organisation, bien qu'autonome dans les projets, doit être en étroite relation avec les responsables du pilotage et de la coordination de la SSI globale dans l'organisme.
En particulier, l'organisme doit identifier les domaines et projets dans lesquels des experts reconnus doivent intervenir.

CDV-02 : Conditions de mise en exploitation de tout nouveau constituant du SI

Cette règle vise à réduire les risques inhérents au manque de coopération sur le plan de la sécurité avec les autres constituants de l'environnement ou l'inadaptation des consignes techniques et humaines en vigueur qui peuvent être à l'origine d'erreurs d'exploitation.
Un nouveau constituant du système d'information (logiciel ou matériel), même réputé efficace et conforme aux spécifications de fabrication, doit être soumis à des tests d'intégration dans son nouvel environnement.
Les conditions préconisées par cette règle peuvent prévoir, par exemple, une recette complète du constituant pour l'identification des modifications techniques et procédurales à effectuer ainsi que la possibilité, en cas d'échec, de restaurer l'environnement technique dans l'état qui existait avant sa mise en exploitation.

CDV-03 : Contrôle des logiciels avant leur mise en exploitation

Les contrôles des logiciels avant leur mise en exploitation visent à lutter tout particulièrement contre la menace de contamination par virus[1] ou autres codes malicieux et le risque de non-conformité des logiciels.
Les virus ou autres codes malicieux posent un problème de plus en plus grave pour la sécurité des systèmes d'information. Leur existence touche tous les organismes et institutions quel que soit leur niveau de vulnérabilité : les organismes les plus ouverts au public sont les plus exposés aux pirates informatiques dont les motivations sont assez souvent la prouesse technique et l'effet médiatique.
Le risque de non-conformité des logiciels concerne les organismes sensibles qui, dans le cadre du recours à des prestataires de service pour le développement de logiciels, doivent vérifier l'exactitude et la conformité de la programmation du code afin de vérifier que le programme ne fait que ce pourquoi il a été conçu et qu'il n'existe pas de portes dérobées permettant ultérieurement une modification illicite de ces fonctionnalités.
Des précautions peuvent être prises pour prévenir et détecter l'introduction de logiciels frauduleux (virus, vers, chevaux de Troie, bombes logiques….). Tous les supports de stockage numériques en

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

provenance de l'extérieur de l'organisme et, tout particulièrement ceux dont l'origine est incertaine, sont soumis à un contrôle. La mise en place de matériels dédiés à un dépistage systématique constitue une contre-mesure à cette menace.

CDV-04 : Circonstances retenues pour la mise en œuvre des contrôles de sécurité

Le responsable de la sécurité contrôle la cohérence et la validité des programmes d'équipement de son organisme par rapport aux grandes orientations de la sécurité et aux orientations stratégiques de l'organisme.
Par ailleurs, et dans le cadre d'enquêtes déclenchées à sa demande, des contrôles sont mis en œuvre par l'équipe de sécurité. Ces contrôles sont caractérisés par leur portée et leur ampleur :
- leur portée fait référence à la définition du niveau de détail (c'est la composante verticale) ;
- leur ampleur fait référence aux divers éléments pris en compte dans le contrôle (c'est la composante horizontale).

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

CDV-05 : Modalités des contrôles de sécurité par le niveau de pilotage

La réévaluation périodique des vulnérabilités des entités (matériels, logiciels, réseaux, locaux, organisations, personnels) face aux éléments menaçants (accidentels ou délibérés, et naturels, humains ou environnementaux) et leurs méthodes d'attaque est nécessaire pour apprécier le niveau de sécurité du système d'information.
Les autorités qualifiées, aidées par l'équipe de sécurité de l'organisme, fixent les modalités techniques, les méthodes et les outils nécessaires à la sécurité ; elles en contrôlent le bon usage et l'efficacité selon des critères énoncés par le niveau décisionnel.
Ces contrôles qui s'inscrivent dans le cadre d'inspections ou d'audits de sécurité planifiés, couvrent les différentes entités de la sécurité des systèmes d'information (matériels, logiciels, réseaux, locaux, organisations, personnels).
Pour les contrôles nécessitant le recours au personnel opérationnel et aux ressources techniques, une planification par le niveau du pilotage s'impose pour qu'ils ne constituent pas une gêne au bon déroulement de la mission de l'organisme.

CDV-06 : Continuité du contrôle de sécurité par le niveau opérationnel

Les agents de sécurité effectuent les contrôles qui leur sont impartis par application de seuils de tolérance fixés par l'autorité qualifiée. L'observation d'écarts répétés, liés par exemple aux contraintes de l'exploitation, ou bien le changement d'état du système d'information peuvent conduire le niveau de pilotage à une modification de ces seuils.
Leurs actions de contrôle sont étroitement liées à l'exécution des tâches opérationnelles et elles intéressent ([IGI 900], article 20, [REC 901], article 19) :
- la protection des personnes comme, par exemple, la tenue à jour de la liste du personnel employé à titre permanent et, le cas échéant, affecté au traitement des informations,
- la protection des informations comme, par exemple, le contrôle de la destruction des informations classifiées qui doivent être expurgées du système,
- la protection des systèmes et réseaux comme, par exemple, le contrôle de la diffusion aux utilisateurs des éléments d'authentification pour les applications classifiées.

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

CDV-07 : Contrôle permanent des moyens de protection

Le contrôle de l'intégrité et de la disponibilité des moyens de protection est un aspect fondamental de la sécurité. Cette règle concerne les dispositifs de sécurité auxquels il est fait confiance pour assurer la protection des informations traitées : il s'agit des équipements, des mécanismes (matériels et logiciels) et de la documentation qui leur est associée, nommés dans l'article 10 de l'[IGI 900], "Articles Contrôlés de Sécurité des Systèmes d'Information" (ACSSI), ou de l'article 9 de la [REC 901].
Le maintien de cette confiance justifie un contrôle de l'intégrité et de la disponibilité de ces moyens qui ont un cycle de vie : ils sont conçus, réalisés, utilisés, réparés puis réformés ou détruits. Leur intégrité et leur disponibilité, conditions fondamentales de l'efficacité de la sécurité, sont garanties par la mise

en œuvre de mesures de gestion spécifiques dont un programme de maintenance le plus proactif possible.

CDV-08 : Application de contrôle de code et de procédure de recette

Des procédures de contrôle des développements peuvent être menées pour lutter contre l'introduction de fonctions malveillantes (par exemple : contrôle mutuel des codes, scellement de code sous la responsabilité du développeur, contrôle par échantillonnage…).
Tout développement ou modification de code doit donner lieu avant sa mise en exploitation à l'exécution de procédures de recettes unitaires, d'intégration et de qualification.
Une attention particulière sera alors portée au contrôle des valeurs et aux limites.

CDV-09 : Autres types de contrôles nécessaires

Voici des exemples de contrôles à mettre en œuvre :
- contrôle de l'application dans les projets des normes énoncées dans la PSSI ;
- contrôle de la couverture de la PSSI par rapport à l'évolution des enjeux du SI ;
- contrôle de la bonne application des règles de gestion des accès et des habilitations ;
- contrôle du respect des règles de sécurité par les Tiers (externalisation de service, infogérance) ;
- contrôle de la base d'incident et de l'exhaustivité des traitements ;
- contrôle du respect des règles d'accès physique ;
- contrôle de l'exploitation régulière des traces des activités notamment celles des comptes disposant de privilèges étendus sur le système ou accédant à des informations ou fonctions sensibles / vitales ;
- contrôle de la présence de clauses contractuelles de sécurité dans l'ensemble des contrats de fournisseurs ;
- contrôle de l'efficacité des mesures de protection du réseau public ;
- contrôle de l'application des procédures de recette avant la mise en exploitation d'un nouveau système d'information ou d'une évolution majeure ;
- contrôle du respect des lois, règlements et des différents codes de pratiques ;
- …

CDV-10 : Les processus de contrôle ne doivent pas perturber le fonctionnement des SI

Les procédures de contrôle doivent être clairement définies. Les accès et privilèges nécessaires aux tests et aux contrôles du système d'information doivent être maîtrisés dans le temps et dans leur étendue.
Une attention particulière doit être portée pour vérifier que l'exécution de ces procédures n'a pas d'impact significatif sur le fonctionnement du système d'information.

CDV-11 : Réalisation d'audit de sécurité

L'efficacité de tout moyen de sécurité ne peut s'inscrire dans le temps que si elle est régulièrement vérifiée à l'aide d'éléments tangibles. Des audits de sécurité du système d'information sont réalisés par des personnes qualifiées et habilitées selon des procédures qu'il convient de définir et selon des procédures précises et validées permettant de s'assurer de la bonne application des procédures de sécurité, du fonctionnement opérationnel de ces procédures, de la cohérence de ces procédures, des moyens en place et de la prise en compte effective par ces moyens de l'ensemble du processus visé, incluant les évolutions.
Les résultats de ces audits sont diffusés au commanditaire et aux personnes ayant besoin d'en connaître. La mise en évidence d'incidents ou de failles de sécurité du système d'information doit nécessairement être rapportée au RSSI.
Les audits externes de sécurité du système d'information doivent faire l'objet d'un accord préalable du RSSI. Ce type d'audit doit se faire dans un cadre strict dans lequel les responsabilités de chacun des acteurs sont définies (profondeur de l'investigation, diffusion des résultats…).
En complément de ces audits, des tests intrusifs peuvent être réalisés. Ces tests doivent être définis et encadrés (choix d'un prestataire, engagement de confidentialité, procédures de sauvegarde et plan de remise en route…).

ACR : Assurance et certification

ACR-01 : Exigences minimales sur les applicatifs utilisés dans le SI

Ces exigences doivent être clairement énoncées et concernent principalement :

- la protection des données de configuration ou de paramétrage : elles sont trop souvent oubliées alors qu'elles représentent un des moyens les plus faciles et souvent les plus furtifs de détournement d'un applicatif ;
- la validation et le filtrage éventuel des données en entrée avant tout traitement : cette validation doit être prévue et appliquée systématiquement mais concerne tout particulièrement les « saisies » par des utilisateurs (risques d'erreur ou de tentative malveillante) et les données de provenance externe ;
- la validation des données en sortie : c'est la contre-partie du précédent et cela concerne :
  - la protection des entrées du traitement suivant dans une chaîne applicative,
  - et / ou la fiabilité des résultats en bout de chaîne ;
- les risques de modification ou de corruption des données par l'applicatif lui-même : ces problèmes proviennent le plus souvent d'erreurs de conception et plus encore d'erreurs d'implantation (bugs) qui seraient exploitables par des utilisateurs malveillants ;
- la présence et la pertinence des mécanismes d'autocontrôle présents au sein de l'applicatif lui-même et de leur capacité à générer des notifications d'alerte lors de comportements anormaux ou simplement imprévus ;
- la présence et la pertinence de mécanismes de trace et de journalisation disponibles et configurables selon les besoins.

ACR-02 : Élaboration d'une cible de sécurité

La cible de sécurité constitue la spécification du système en matière de sécurité ; c'est une étape très importante qui fixe à la fois l'objectif à atteindre et les moyens pour y parvenir.
En premier lieu, la réflexion approfondie qu'a permis l'étude des besoins de sécurité et l'analyse de risques doit permettre de fixer ce que l'on décide finalement de protéger, en précisant pourquoi, contre qui et contre quoi ; la synthèse de cette réflexion constitue les objectifs de sécurité du système. Ceux-ci sont clairement définis dès la phase de spécification pour que l'on puisse les atteindre et ensuite apprécier si la sécurité du système est en mesure de les satisfaire.
De ces objectifs de sécurité on déduit les mesures à mettre en place, qu'elles soient techniques ou non techniques.
Les mesures non techniques sont les procédures et règles de mise en œuvre, de gestion et d'organisation, l'habilitation des personnes, les mesures concourant à protéger l'environnement du système et toutes les dispositions à caractère réglementaire.
Les mesures techniques sont les fonctions de sécurité qu'il faut prévoir dans la conception du système de façon à satisfaire les objectifs ; ces fonctions sont réalisées au moyen de mécanismes de sécurité intégrés au système.
Objectifs et fonctions constituent l'essentiel de la cible de sécurité ; celle-ci représente le fondement de la sécurité dans la conception du système d'information.
Cependant, pour que l'on puisse être sûr que les objectifs sont satisfaits, il faut d'une part que ces fonctions et mécanismes existent et, d'autre part, que l'on puisse leur accorder une confiance suffisante.

ACR-03 : Respect des exigences sécuritaires avant mise en service opérationnelle

La vérification du respect des exigences doit être :

- pour une part, mise en oeuvre lors de la sélection (logiciels achetés) ou de la spécification (logiciels développés) afin que les caractéristiques intrinsèques du logiciel soient suffisantes pour permettre une mise en œuvre acceptable d'un point de vue sécuritaire ;
- pour une autre part, effectuée dans les conditions pré-opérationnelles afin que soit garanti le niveau de sécurité dans les conditions effectives d'exploitation (environnement, paramétrage…).

ACR-04 : Vérification périodique du respect des exigences sécuritaires sur les applicatifs

Pour se protéger contre une dérive dans le temps, il est important de mettre en place des procédures conduisant à un contrôle périodique régulier du respect des exigences sécuritaires sur les caractéristiques et le fonctionnement des applicatifs. Une partie de ce contrôle peut être interne.

ACR-05 : Évaluation du niveau de confiance accordé au SI : évaluation et certification

La conception du système est guidée par une démarche cohérente qui conduit à ce que les objectifs de sécurité soient atteints ; les fonctions de sécurité sont choisies pour satisfaire ces objectifs.
Une fois le système développé et mis en service, il importe de savoir quelle confiance continue on peut avoir que la cible de sécurité est bien atteinte.
D'une part cette confiance dépend du choix des fonctions, de leur efficacité et de la qualité de leur développement et, d'autre part, elle dépend de la façon dont le système a été installé, mis en service et exploité.
L'étude de chacun de ces aspects permettra d'avoir une confiance justifiée dans la réalisation de la cible de sécurité ; c'est l'objet de l'évaluation. Un système développé selon les principes exposés ci-dessus pourra être évalué et on aura alors la confirmation qu'on peut lui faire confiance quant à la sécurité qu'il assure aux informations qui lui sont confiées et aux processus qui les utilisent.
L'évaluation contribue de façon significative à réduire les risques d'un comportement non désiré d'une application. Elle consiste à évaluer les propriétés d'un système ou d'un produit par rapport à des critères de sécurité normalisés, par exemple les Critères Communs.
Cette évaluation doit être conduite selon une méthode approuvée obéissant à des règles définies. Les résultats de l'évaluation et le fait que les critères d'évaluation utilisés ont été correctement appliqués sont confirmés par une déclaration formelle appelée **certificat**.
Toutefois, la certification n'a aucun caractère obligatoire : il appartient au commanditaire de l'évaluation de juger du besoin de certification.

ACR-06 : Critères d'acquisition et conditions d'usage de progiciels

Si les critères d'achat de progiciels sont essentiellement économiques et opérationnels (disponibilité immédiate du produit, coût accessible, maintenance et assistance technique), il n'en demeure pas moins un problème de sécurité vis-à-vis de l'intégrité des logiciels livrés et de leur utilisation au sein de l'organisme.
Il est donc essentiel qu'une règle prévoie les critères permettant de justifier l'acquisition de progiciels et leurs conditions d'usage portant, par exemple, sur les aspects suivants :

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

ACR-07 : Adoption de méthodes et d'outils de développement

L'adoption, dès la conception du système d'information, de méthodes et d'outils de développement marque la volonté de l'organisme de maîtriser la sécurité.
L'application de cette règle permet d'acquérir une confiance justifiée dans la conception et la réalisation de la cible de sécurité ; elle contribue à la mise en place de protections homogènes et cohérentes constituant ainsi un gage de réussite pour une éventuelle évaluation du système d'information.
Toutefois, cette règle ne sous-entend pas l'emploi d'une méthode unique pour le développement du système d'information mais elle appelle à veiller sur la nécessaire cohérence qui doit exister entre les différentes méthodes utilisées par l'organisme.

ACR-08 : Adoption d'un standard de programmation et de codage des données

L'adoption d'un standard de programmation intéresse tous les développements d'applications informatiques, y compris les parties logicielles que peuvent contenir les matériels ou dispositifs divers du système d'information.
La première recommandation liée à l'adoption d'un standard de programmation est celle de préciser les configurations matérielles et logicielles utilisées pour le développement.

La deuxième obligation concerne le choix d'une représentation et d'une structuration des programmes qui permet d'avoir des références uniformes et reconnues de tous, facilitant ainsi les opérations de maintenance logicielles et le suivi de la documentation technique.
Le codage des données concerne le formatage et la représentation des champs de données qui, pour des raisons similaires à la structuration des programmes, nécessitent l'adoption d'un standard.
Les divers états de sortie des données obéissent également à des standards de présentation qui prennent en compte les particularités fonctionnelles des utilisateurs de l'organisme.
L'administrateur de données est responsable de la bonne définition des données et de la structure des fichiers et bases de données.

ACR-09 : Homologation du système d'information

L'homologation de sécurité est la déclaration par l'autorité d'homologation (gouvernementale ou spécifique à l'organisme selon le cas), au vu du dossier d'homologation, que le SI considéré est apte à traiter des informations d'un niveau de sensibilité ou de classification donné conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels induits sont acceptés et maîtrisés.
Pour mener à bien une homologation, un comité de pilotage est généralement en charge du suivi du projet. Il pilotera la constitution de l'ensemble du dossier d'homologation que l'autorité d'homologation devra approuver.
L'homologation de sécurité reste valide tant que le SI opère dans les conditions approuvées par l'autorité d'homologation.
Elle traduit l'acceptation d'un niveau de risque résiduel qualifié et quantifié en termes de confidentialité, d'intégrité, de disponibilité, d'authenticité et de non répudiation.

ACR-10 : Agrément du système d'information

L'évaluation et la certification qui en confirme les résultats permettent seulement d'assurer que la cible de sécurité est bien atteinte. Elle ne constitue qu'un des éléments pour juger si le système ou le produit placé dans son environnement réel, présente bien avec les mesures de sécurité non techniques (en particulier, les procédures d'exploitation effectivement mises en place) les protections adaptées à la sensibilité des ressources qui lui sont confiées et à l'étendue des menaces qu'il doit repousser.
Il y a lieu, de plus, de prononcer un jugement sur la pertinence de la cible de sécurité face à l'environnement réel d'exploitation du système : c'est le rôle de l'agrément qui constitue la reconnaissance formelle que le produit ou le système évalué peut protéger des informations jusqu'à un niveau spécifié, dans des conditions d'emploi définies.

ACR-11 : Gestion de la documentation de sécurité

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

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

ACR-12 : Adoption d'un standard d'élaboration de la documentation de sécurité

La diversité des équipements, des logiciels et des procédures impose la définition d'un standard d'élaboration de la documentation de sécurité.
Ce standard concerne, en premier lieu, le modèle de présentation et le contenu de la documentation : tous les constituants de sécurité sont décrits selon le même formalisme facilitant ainsi les interventions du personnel autorisé pour leur exploitation et leur maintenance.
En second lieu, le standard concerne la manière de réaliser la documentation c'est-à-dire, la rédaction, l'impression et la classification des documents. De plus, tous les éléments ayant servis à l'élaboration de la documentation sont manipulés et protégés au même titre et dans les mêmes conditions que les documents de sécurité qui en résultent.

ACR-13 : Production de documents par l'organisme

Tout document produit par l'organisme doit être conforme à la charte graphique et à sa politique d'assurance qualité. Il doit notamment porter une référence unique, permettant d'identifier clairement l'auteur, la date de création, des éléments de gestion de version ainsi que la mention de la classification du document, figurant clairement dans le document.
La sécurité d'une information est affectée dès la publication d'un document. Le créateur du document en est, par défaut, le propriétaire. Il est ainsi responsable de sa classification. En fonction de la classification des informations, le support fera l'objet d'application de règles de protection adaptées.
Des règles spécifiques de sécurité seront applicables en fonction de la classification.

ACR-14 : Maintenance de la documentation de sécurité

Une organisation et des règles doivent être énoncées pour que l'ensemble de la documentation sécurité soit mise à jour lors de l'achèvement de toute modification (*cf. gestion documentaire*) et que l'ancienne documentation est archivée ou mise au rebut.

2 Principes de mise en œuvre

ASH : Aspects humains

ASH-01 : Notion de reconnaissance de responsabilité

Pour les postes de travail comprenant des informations relevant du secret de défense, l'attestation de reconnaissance de responsabilité est l'engagement que prend une personne de respecter les lois, règlements et règles de sécurité du système d'information.
Elle fait l'objet d'une déclaration écrite et signée conforme à l'IGI 1300. En particulier, l'article 16 stipule : "...cette attestation signifie que le titulaire de l'admission reconnaît avoir pris connaissance des obligations particulières et des sanctions imposées par les articles 70 à 85 et R. 24 du Code pénal à tout gardien ou détenteur d'informations intéressant la défense nationale et la sûreté de l'État [...] Il appartient au directeur de l'organisme ou à l'autorité hiérarchique compétente d'appeler l'attention de l'intéressé sur le sens de la portée de cette attestation".

Pour les postes ne relevant pas de cette catégorie, des clauses spécifiques de confidentialité, de fin de contrat de travail ou de non-concurrence peuvent être insérées, si besoin est, dans le contrat de travail. La [REC 600] traite de ces problématiques pour des informations ne relevant de l'[IGI 1300], en particulier elle précise que : « Tout personnel de chaque catégorie devant avoir accès aux ressources informatiques de l'entreprise doit au préalable signer un document d'engagement de responsabilité (cf. section 1.). Ce document peut contenir des éléments spécifiques à chacune des catégories de personnel. »
Au caractère essentiellement dissuasif de cette mesure, il peut être adjoint l'application de sanctions. Les incidences sur le plan disciplinaire du non-respect des règles internes de sécurité doivent dans ce cas être expliquées dès la prise de fonction du personnel nouvellement affecté.

ASH-02 : Clauses de sécurité dans les contrats de travail

Les contrats de travail du personnel doivent :
- soit inclure des clauses explicites de sécurité du système d'information tels que :
    - interdictions,
    - devoir de signalement d'une anomalie ou d'une faille de sécurité,
    - devoir de réserve,
    - clauses de confidentialité,
    - responsabilité dans le respect des règles de protection du patrimoine de l'organisme ;
- soit faire explicitement référence aux divers règlements applicables dans le domaine (cf. chapitre traitant des obligations législatives et réglementaires), tels que :
    - la PSSI,
    - des codes de déontologie liés au métier,
    - des règlements de l'organisme (chartes, règlement intérieur…).

Ces éléments doivent traiter des sanctions ou mesures applicables en cas de non-respect de ces engagements.
Ce principe doit également être étendu à toute convention de stage ou contrat d'intérim.

Les personnels disposant de responsabilités ou chargés de tâches sensibles (administration de sécurité, Inspection…) doivent signer des engagements de nature particulière liés à leur future fonction.
Les engagements divers, y compris s'ils ne sont pas directement intégrés au contrat de travail, doivent être revus et validés par le service juridique de l'organisme (cf. chapitre précédent traitant des responsabilités).

(Cf. Principes d'habilitation et Cf. Obligations légales et réglementaires)

ASH-03 : Adoption de critères de sélection du personnel travaillant sur les SI sensibles

Cette règle concerne toutes les catégories de personnel qui sont amenées à travailler sur les systèmes d'information sensibles. Elle précise, pour les emplois touchant au fonctionnement et à l'utilisation du système, le mode de sélection à appliquer par l'organisme pour le recrutement du

personnel et, tout particulièrement, les critères de sécurité requis pour chaque poste de travail[2]. Par exemple, l'exigence de références à des postes sensibles peut être prise en compte lors de procédures d'embauche.
Cette règle implique la possibilité de vérification des références de travail d'un candidat à un emploi ainsi que celles des personnes affectées temporairement à une activité nécessitant l'utilisation du système d'information.

ASH-04 : Principes généraux d'habilitation

Le SI ne doit être accessible, physiquement et logiquement, qu'à des personnes nominativement autorisées. Ainsi, des restrictions d'accès aux systèmes et informations sont définies conformément à leur sensibilité (cf. classification) et à la criticité des actions autorisées sur ces données et ressources.
Les habilitations sont attribuées à une personne physique et sont incessibles.
L'attribution d'habilitations à un système ou à une information est décidée par leurs propriétaires.
La définition des habilitations doit respecter le principe du besoin d'en connaître : tout acteur aura exclusivement accès aux informations dont il a besoin dans l'accomplissement de sa tâche.
Il est recommandé que le principe du moindre accès (habilitation nulle par défaut) soit appliqué lors de l'ouverture / mise en service de tout nouveau système.

ASH-05 : Catégories d'habilitations

Les catégories d'habilitation doivent être prises en compte dans les processus de recrutement du personnel ou de sélection de fournisseurs qui font appel à une procédure d'habilitation. Aux habilitations doivent correspondre des exigences sur le personnel : vérifications et contrôles à effectuer (identité, compétence), signature d'acte d'engagement spécifique…

ASH-06 : Règles d'attribution et d'engagement (responsabilités)

L'attribution des habilitations est déterminée dès le recrutement du personnel. Il doit être fixé dans le temps et dans l'espace.
La personne à qui est attribuée l'habilitation doit donner acte formellement de sa connaissance des responsabilités qui incombent à l'habilitation qu'on lui attribue.
Toute habilitation pour un domaine ou un projet du système d'information doit être autorisée formellement par son propriétaire (responsable de la protection des traitements et informations traités par le SI).

ASH-07 : Volants de personnel

Des mesures organisationnelles peuvent être prises pour qu'il n'y ait pas de vacance sur un poste vital, même temporaire (congés…). L'organisme devrait prévoir pour tous les postes de travail vitaux un volant de personnel suffisant et expérimenté. Toute personne occupant au poste vital devrait disposer d'un remplaçant ayant des compétences équivalentes et le même niveau de connaissance du dossier.

ASH-08 : Procédure d'habilitation pour les postes de travail sensibles

La sensibilité d'un poste de travail fait référence au besoin de confidentialité, de disponibilité et d'intégrité attaché aux informations, aux logiciels et aux matériels qu'il rassemble ; elle se définit selon les critères de classification (cf. chapitre traitant de la sécurité des informations), mais peut aussi être liée à la localisation : un poste de responsable des relations humaines dans une région à fort risque social peut être considéré comme un poste sensible.
Pour un poste comportant des manipulations d'informations relevant du secret de défense, les habilitations du personnel sont définies par l'article 3 de l'[IGI 1300] : "La procédure d'habilitation consiste à vérifier qu'une personne peut, sans risque pour la défense nationale, la sûreté de l'État ou sa propre sécurité, connaître des informations classifiées d'un niveau déterminé dans l'exercice de ses missions. Au terme de la procédure d'habilitation, l'autorité compétente décide d'admettre ou non la personne concernée à prendre connaissance d'informations classifiées au niveau exigé".
Pour les postes de travail sensibles n'utilisant pas des informations relevant du secret de défense, une procédure d'habilitation peut être utilisée sur le modèle de celle qui doit être appliquée dans le cadre des marchés de défense. Dans ce cas, il est possible de se référer à [REC 600].

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

ASH-09 : Cloisonnement des postes de travail sensibles

Le cloisonnement des postes de travail sensibles vise à lutter contre la fuite des informations représentant un enjeu pour les intérêts de l'État ou de l'organisme.
Pour la préservation des intérêts de l'État et, tout particulièrement dans le cadre de la protection du secret de défense, les décisions d'admission ou d'agrément aux informations classifiées d'un niveau donné, telles que définies dans les articles 10 à 12 de l'[IGI n°1300], n'autorisent pas pour autant le bénéficiaire à accéder à toutes les informations relevant de ce niveau ; le besoin de connaître ces informations reste fonction de l'activité de la personne ou des dossiers particuliers qui lui sont confiés.
D'une manière identique, pour la préservation des intérêts propres à un organisme dont les informations ne relèvent pas du secret de défense, la connaissance des besoins en information pour l'accomplissement de la mission ou du métier permet la mise en place d'un cloisonnement efficace des postes de travail.

ASH-10 : Délégation

Les propriétaires ou détenteurs d'information peuvent déléguer la mise en œuvre de moyens de protection à des personnels de l'organisme. Cependant, ils conservent la responsabilité de la sécurité. C'est pourquoi, ils doivent disposer de moyens pour contrôler le respect des règles de sécurité.
Les habilitations sont attribuées à une personne physique et sont incessibles.

PSS : Planification de la continuité des activités

Le plan de continuité d'activités (BCP – *Business Continuity Plan*) est un document qui définit les procédures permettant de maintenir les activités critiques de l'organisme pendant et après un désastre (événement majeur ayant des effets sur le long terme).
Ce plan traite essentiellement des activités "métier". Les systèmes d'information ne sont évoqués qu'en tant que support des activités "métier".
Différents plans correspondants à des situations particulières peuvent être annexés au plan de continuité :

- le **plan de reprise des activités** traitant de la récupération des activités "métier" en cas de désastre. Ce plan traite essentiellement des activités "métier" et non des systèmes d'information. Les systèmes d'information ne sont évoqués qu'en tant que support des activités "métier".
- le **plan de reprise après désastre** traitant de la récupération des systèmes d'information en cas de désastre,
- le **plan de contingence** traitant de la reprise d'un système d'information en cas d'interruption,
- …

Dans un premier temps, ces plans complémentaires doivent permettre de récupérer partiellement les fonctionnalités des systèmes d'information et des activités critiques reposant sur ceux-ci.
Dans un second temps, ils doivent permettre de restaurer l'intégralité des fonctionnalités des systèmes d'information et des activités reposant sur ceux-ci.
Enfin ils doivent permettre de compenser complètement l'impact des interruptions ou désastres sur l'organisme.

L'appréciation et le traitement des risques SSI contribuent à l'élaboration de ces plans, notamment en définissant la criticité des activités et des systèmes d'information, ainsi que les risques résiduels et les mesures de sécurité à intégrer.

PSS-01 : Définition du périmètre d'un plan de continuité

Il convient de définir précisément l'ensemble du cadre du plan de continuité (ressources, responsabilités, périodicité des tests…) pour chacun des aspects suivants :

- les installations, matériels et réseaux informatiques ;
- les programmes et données informatiques ;
- les utilisateurs du système d'information.

Une analyse des risques SSI apportera les éléments permettant de décider des plans nécessaires pour l'organisme. Ces plans ont en effet un coût important qu'il convient de justifier.

PSS-02 : Prise en compte des services externalisés

La gestion de plan de continuité impliquant des partenaires externes doit être approfondie, notamment lors de la contractualisation. Elle doit comporter des éléments relatifs à des exercices réguliers visant à vérifier le bon fonctionnement des plans.

PSS-03 : Élaboration d'un plan de reprise

Un plan de reprise informatique (ou plan de reprise d'activité) est nécessaire pour protéger les tâches opérationnelles critiques du système d'information face aux défaillances majeures, aux erreurs humaines, aux catastrophes naturelles ou aux attaques délibérées. Il a pour but de limiter les atteintes à la sécurité suite à un incident majeur et de remettre le système d'information dans les conditions de fonctionnement initiales.
Le plan de reprise d'activité impose la prise en compte de toutes les exigences opérationnelles du système d'information pour assurer un retour à un fonctionnement normal. Les procédures qui découlent de ce plan fournissent une alternative et des moyens temporaires de continuité du service, dans le cas d'endommagement ou de défaillance d'un équipement.
Toutefois, un élément fondamental pour l'établissement d'un plan de reprise d'activité est l'étude de disponibilité du système information car l'importance des préjudices subis est généralement fonction de la durée d'indisponibilité. Ainsi, l'étude de disponibilité a pour but de définir des tranches temporelles où le préjudice est considéré à un niveau donné en correspondance avec le niveau de procédure d'urgence du plan de reprise d'activité.

PSS-04 : Positionnement des applications dans le plan de continuité

En fonction de l'analyse de risques de l'organisme, chaque application doit faire l'objet d'une notation en terme de priorité de reprise. Cette notation correspond à une mesure de l'impact qu'aurait l'indisponibilité de l'application sur l'activité de l'organisme.

PSS-05 : Mise en place des procédures de sauvegarde

Un plan de sauvegarde tenant compte des exigences de délai de reconstruction des informations par type d'activité et/ou de processus doit être mis en place. On distinguera les sauvegardes système des applicatifs et des données.
Pour mériter un niveau de confiance élevé, le plan de sauvegarde doit être testé régulièrement. La procédure de sauvegardes régulières des données vitales et des logiciels est une mesure fondamentale, classiquement, un nombre minimum de sauvegardes des informations est stocké dans un lieu éloigné à une distance suffisante pour résister à un sinistre sur le site principal ; les protections physiques des sauvegardes sont du même niveau que les standards appliqués sur le site principal. Des moyens de contrôle de la cohérence et de l'intégrité des informations sauvegardées doivent être mis en place et gérés.

PSS-06 : Tests réguliers des plans

Pour mériter un niveau de confiance élevé, le plan de continuité et les plans liés doivent être testés régulièrement. À la fin de chacun de ces exercices, il sera mis en place un groupe « retour d'expérience » qui mettra à jour les plans après analyse des disfonctionnements ou lenteurs

INC : Gestion des incidents

INC-01 : Définition des situations anormales envisageables

Les types de situation anormale potentielle couvrent entre autres :
- les pannes ou anomalies de fonctionnement des équipements matériels ;
- les pannes ou anomalies de fonctionnement des logiciels et applicatifs ;
- les problèmes dus à des données en entrées absentes, incomplètes ou anormales ;
- la production de résultats manquants, incomplets ou anormaux ;
- …

L'analyse de risques fournira des éléments à prendre en compte dans le choix des alertes à faire remonter. Ces choix sont en particulier liés aux objectifs de sécurité retenus.

INC-02 : Mise en place d'un réseau de détection et d'alerte des incidents de sécurité

La finalité d'un réseau d'alerte est de provoquer une intervention aussi rapide que possible, dès qu'un incident est détecté, limitant ainsi les conséquences d'un arrêt du système d'information ou l'activation de procédures suite à la survenance de l'incident.

Tous les utilisateurs, et particulièrement ceux opérant sur des postes de travail sensibles, constituent les maillons de ce réseau d'alerte. Il s'agit d'apprendre aux utilisateurs à protéger leurs matériels et à déceler les indices de manipulations frauduleuses ou d'activités inhabituelles.
L'efficacité d'un réseau d'alerte repose sur la structure de l'organisation mise en place et, tout particulièrement, sur les agents de sécurité. Elle dépend du niveau technique des moyens de détection et de la mobilisation des utilisateurs du système d'information : l'intervention qui en découle est d'autant plus efficace qu'elle fait intervenir les moyens adéquats au moment opportun.
Pour le cas de compromission d'informations relevant du secret de défense, l'organisme doit rechercher la rapidité de réaction : "Si la sécurité d'une information a été ou semble avoir été compromise de quelque façon que ce soit, la rapidité et la discrétion de l'intervention revêtent une particulière importance pour en limiter les conséquences ; un compte rendu non fondé et démenti par les faits est toujours préférable à un retard dans l'intervention.

INC-03 : Maîtrise des incidents de sécurité

La maîtrise des incidents de sécurité consiste à s'assurer de la continuité de la sécurité durant toute la durée de l'intervention faisant suite à une alerte : le recours à des spécialistes extérieurs et l'obligation de leur faciliter l'accès au site et au système d'information ne doit pas dispenser le personnel de l'organisme d'appliquer les règles de sécurité. Cette maîtrise est obtenue par le respect de procédures préétablies.
Deux cas d'urgence peuvent nécessiter des actions différentes :

- ceux provenant d'accidents physiques touchant à l'infrastructure d'une zone sensible ou au système d'information qu'elle contient et qui n'entraînent pas d'actions hostiles visant à capturer des constituants du système d'information ; l'action consiste alors à surveiller les matériels, les logiciels et les documents durant l'intervention comme par exemple, le transfert d'équipements vers une salle blanche ou la mise en mode dégradé de mécanismes de sécurité jusqu'au retour à la normale du système d'information,
- ceux provenant d'actions hostiles visant à capturer des constituants du système d'information : un plan de destruction d'urgence simple et pratique de mise en œuvre peut être, dans certains cas, le seul moyen d'éviter une compromission grave.

INC-04 : Contrôle des incidents de sécurité

L'absence de suivi des incidents de sécurité expose l'organisme à méconnaître les vulnérabilités de son système d'information et le condamne à ne pas être en mesure de réagir efficacement face à des sinistres répétés de même nature.
De ce fait, les responsabilités du suivi des incidents et des procédures doivent être établies ; les procédures couvrent alors tous les types d'incidents potentiels y compris les défaillances du système ou pertes de service, les erreurs résultant de données fausses ou inadéquates, les failles de la confidentialité.
Pour ce faire, le suivi des incidents de sécurité s'appuie sur les comptes rendus pour les interventions immédiates, sur les relevés des dysfonctionnements pour les actions différées et, dans les deux cas, sur l'analyse et l'identification des causes du sinistre et des statistiques que l'on peut établir sur leur survenance.
L'adoption d'un standard de compte rendu et de directives pour leur exploitation sont des mesures qui visent à rendre uniforme et obligatoire la procédure d'alerte évoquée.
Les incidents de toute nature, décelés par exemple en phase d'exploitation, font l'objet d'un compte rendu au niveau du responsable de sécurité aussi rapidement que possible.
Les dysfonctionnements et les faiblesses du système d'information doivent être notés et corrigés. En particulier, il apparaît nécessaire de passer en revue les dysfonctionnements pour s'assurer que les mesures correctives ont été effectivement mises en œuvre et qu'elles correspondent à des actions autorisées.
L'analyse et l'identification des causes de l'incident impliquent une planification de la collecte des comptes rendus d'audit, de la mise en place de mesures de protection et de la communication avec les utilisateurs affectés par l'incident.

INC-05 : Moyens de détection d’intrusion ou d’utilisation frauduleuse

Il est recommandé que des dispositifs et/ou procédures puissent détecter des tentatives d’intrusion ou d'utilisation frauduleuse et permettre ainsi, en réaction, de prendre les mesures nécessaires pour faire échouer ces tentatives.
Il conviendra donc pour chaque composant ou applicatif sensible du SI de déterminer et mettre en place les moyens ad-hoc, qui peuvent aller d’un mécanisme de supervision bien configuré à des outils spécifiques comme les systèmes de détection d’intrusion.

INC-06 : Mise en œuvre d'un service d'alerte efficace

Le principe est de déterminer le plus rapidement l'occurrence d'un événement constituant (ou susceptible de constituer) les prémices d'une attaque, d'un incident majeur ou à l'origine d'une malveillance.
Le service d'alerte doit organiser la remontée et la centralisation des détections d'incident par l'intermédiaire de processus simples d'information (*cf. fonctionnement des rôles*) et doit sensibiliser les utilisateurs et les exploitants au devoir de signalement de toute anomalie. Il convient de prévoir plusieurs niveaux d'alerte. Ces différents niveaux doivent être détectables par les utilisateurs c'est à dire que chacun doit connaître dans quel niveau le SI se trouve à un instant donné.

INC-07 : Prévision des réactions réflexes face à des situations d'urgence

Le principe est de sélectionner des scénarios types de sinistre et de formaliser les meilleures réactions en terme de mesures conservatoires pour limiter, voire éviter, la propagation des impacts de l'incident ou de l'attaque, en terme de pouvoir de décision et d'information interne et externe, le cas échéant. Ceci permet d'éviter que les incident ne dégénèrent en sinistres aux conséquences fâcheuses ou insupportables pour l'organisme.
À chaque niveau d'alerte correspond une procédure claire des actions à conduire. Ce type de procédure s'appuie sur le principe de défense en profondeur qui permet d'établir des barrières de protection indépendantes et en fonction de l'alerte.

FOR : Sensibilisation et formation

FOR-01 : Documentation des responsabilités

Il est fondamental que l'ensemble des responsabilités de SSI soit rédigé sans ambiguïté et porté à la connaissance des personnes qui en ont la charge. La description de ces responsabilités doit comporter les limites associées à chacun dans le temps et l'espace.
Il est également indispensable que tous les acteurs concernés s'engagent formellement à prendre connaissance et à accepter ces responsabilités.

FOR-02 : Sensibilisation générale à la sécurité

La sensibilisation vise à faire prendre conscience à chaque utilisateur qu'il détient une part importante de responsabilité dans la lutte contre la malveillance.
La définition des objectifs de cette sensibilisation est étroitement liée à la mission ou au métier de l'organisme, à la sensibilité du patrimoine d'informations et de biens physiques ainsi qu'aux menaces connues. Ils peuvent être, par exemple, la recherche de l'adhésion du personnel vis-à-vis de la protection du patrimoine de l'organisme ou bien encore l'émergence et l'efficacité d'un réseau d'alerte impliquant tous les utilisateurs du système d'information.
Une action de sensibilisation qui ne répond pas à des objectifs clairement exprimés n'apporte qu'une illusion de confiance en la capacité du personnel à réagir efficacement lors d'une atteinte au système d'information.
Un programme de sensibilisation régulier doit être prévu et piloté par le RSSI. Ce programme a pour but de rappeler les messages majeurs de la PSSI de l'organisme et notamment d'informer chaque personne sur :

- les enjeux de sécurité ;
- les principales menaces ;
- les lois, règlements, chartes ;
- l'organisation de la sécurité ;
- les principes et les règles de la sécurité de l'organisme ;
- les comportements à adopter ;
- les règles spécifiques (postes nomades, télé-actions…).

FOR-03 : Communication sur la SSI

L'information concernant l'organisation et les exigences générales de la SSI doit être diffusée le plus largement dans l'organisme.
Un moyen de diffusion doit donc être défini et connu de tous, qui permette de retrouver toute information liée à la SSI dans l'organisme (procédure, contact, ..). L'un des moyens utilisés peut être par exemple la mise en place d'un domaine dédié à la sécurité dans l'intranet de l'organisme.

La PSSI globale devra être connue de tous les personnels de l'organisme, les PSSI spécifiques devront être portées à la connaissance des personnels amenés à exploiter ces systèmes particuliers. La diffusion d'une partie ou de la totalité des PSSI à des personnes extérieures, amenées à intervenir sur le système d'information, devra être fonction de leur besoin d'en connaître et dans tous les cas validée par l'organisation en charge de la SSI (Cf. ORG).
Un dossier d'entrée doit être constitué pour s'assurer que toute nouvelle personne intervenant dans le SI est informée de l'organisation, des règles de sécurité et de ses devoirs. De manière analogue, un dossier de sortie est constitué pour informer les personnels quittant l'organisme des procédures et règles à respecter.

FOR-04 : Application pour la protection juridique des informations de l'organisme

Cette règle vise à sensibiliser le personnel sur le devoir de protection juridique des informations qu'il utilise ou qui lui sont confiées afin de diminuer le risque de détournement ou d'appropriation par des tierces personnes.
Les directives d'application se réfèrent, en partie, au principe de responsabilité du personnel et, plus particulièrement, à la règle relative à la notion de responsable-détenteur (cf. chapitre responsabilités ORG).

FOR-05 : Adaptation de la sensibilisation aux différentes classes d'utilisateurs

En matière de sécurité, les niveaux de préoccupations diffèrent considérablement suivant qu'il s'agit du personnel de direction ou d'exécution. La sensibilisation est, en conséquence, adaptée aux niveaux de responsabilité détenus et aux spécificités des postes de travail.
Le personnel concerné appartient à trois grandes catégories :
- celle liée aux activités de direction, d'encadrement, de gestion, de relations extérieures…,
- celle liée aux emplois du système d'information (ingénieurs et techniciens, utilisateurs de la bureautique…),
- celle liée à la sécurité des systèmes d'information (ingénieurs et techniciens de l'équipe de sécurité, agents de la sécurité…) qui nécessitent une formation spécialisée.

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

FOR-06 : Sensibilisation régulière des personnels à la SSI

L'information permanente des personnes vise à obtenir un niveau de vigilance constant. Cette information concerne en particulier les évolutions de la PSSI et des menaces. Elle permet d'actualiser l'information, de communiquer de nouvelles informations, et également de faire un rappel concernant les règles ou consignes qui ne sont pas correctement appliquées. Toute évolution concernant l'organisation et les exigences générales de la SSI doit être également diffusée.

FOR-07 : Sensibilisation au traitement des incidents

Au-delà du simple fonctionnement, les personnels concernés doivent être sensibilisés et formés au niveau qu'il convient aux aspects sécurité des opérations dont ils sont en charge.
Un des points essentiels des obligations sécurité dans les taches d'exploitation concerne le respect des exigences :
- de consignation dans une main-courante des incidents,
- de notification/alerte de qui de droit (cf. suite).

FOR-08 : Préparation et entraînement à la gestion des situations de crise

Outre prévoir les possibilités et le traitement (procédures) des situations anormales et des incidents (FOR-07), il est essentiel de préparer et d'entraîner les personnels concernés, ce qui implique notamment :
- la présentation des plans ad-hoc (plan de secours, plan de continuité, plan de reprise…),
- l'entraînement des personnels au moyen de simulations (exercices comparables aux exercices incendie).

(Cf. Gestion de crise)
Il doit exister un programme de formation spécifique pour chaque profil d'agents pour assurer des réactions réflexes adaptées en cas d'incident ou d'alerte sécurité.

FOR-09 : Sensibilisation du personnel à l'usage des TIC

Une action de sensibilisation du personnel doit être réalisée pour prévenir des risques de divulgation externe (volontaire ou non), liée à l'utilisation des médias des technologies de l'information et de communication (TIC), tels que vidéo, téléphone, fax, voix… En particulier, concernant le contrôle de leur destinataire, les écoutes clandestines, les personnes se trouvant à proximité.

FOR-10 : Formation du personnel à l'usage des TIC

Cette formation s'attachera à présenter la responsabilité de chacun dans le domaine de l'informatique et des communications (technologies de l'information et de communication – TIC) et à former chaque utilisateur à l'utilisation des moyens informatiques et de communication, ainsi qu'aux moyens de protection mis à sa disposition.

FOR-11 : Sensibilisation des utilisateurs aux moyens de supervision

L'emploi de moyens techniques pour détecter des malveillances informatiques ou pour maintenir les systèmes, oblige l'organisme à :
- contrôler les flux d'information,
- accéder aux ressources « personnelles »,
- réglementer les échanges et transferts (Réseau, Messagerie, Internet)
- conserver les éléments de preuve.

C'est pour trouver un équilibre entre contrôle et respect de la vie privée de l'individu et éviter les litiges, voire porter atteinte à l'image de marque de l'organisme, que doivent s'inscrire des actions d'information auprès des acteurs du système d'information.
Ainsi, il est recommandé de rédiger une charte réglementant et expliquant l'objectif, des moyens de surveillance et de récolte des preuves informatiques.

EXP : Exploitation

EXP-01 : Documentation des procédures et règles d'exploitation

Toutes les activités d'exploitation, éventuellement regroupées en familles, doivent être identifiées. Chacune de ces activités doit faire l'objet d'une documentation précise des procédures et règles d'exploitation. Cette documentation pourra, selon les besoins donner lieu à plusieurs documents, chacun étant destiné à une catégorie d'acteurs concernés en fonction de son rôle, de ses responsabilités et de son besoin d'en connaître. Elle devra être tenue à jour.

EXP-02 : Intégration de la SSI dans les procédures et règles d'exploitation

Les documents d'exploitation doivent tous comprendre un volet sécurité qui aura été validé par la structure sécurité mise en place dans l'organisme.

EXP-03 : Séparation du développement et des opérations ou de la production

La séparation des tâches et environnements de développement, de recette et des autres activités liées au fonctionnement du système d'information (exploitation, gestion du système et du réseau, saisie des données, maintenance, audit de sécurité…) réduit le risque de mauvaise utilisation délibérée ou accidentelle des ressources du système.
Cette règle influe sur le niveau de sécurité et sur l'efficacité dans la répartition des tâches et des responsabilités ; en effet, elle permet :
- d'accroître la sécurité, en réduisant le risque de modifications malveillantes ou accidentelles des programmes grâce à la séparation des tâches caractérisant le fonctionnement opérationnel du système d'information qui nécessitent des ressources différentes et des privilèges d'accès à des instructions machines critiques eu égard à la sécurité,
- d'améliorer l'efficacité par le fait que le cumul de plusieurs fonctions techniques peut inciter un informaticien d'une équipe d'exploitation à dépanner "à chaud" un logiciel au mépris des règles de programmation dont il est fait mention à la règle précédente (par exemple, l'absence de commentaires dans les lignes de code modifiées).

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

EXP-04 : Conditions d'usage de l'infogérance

On distingue divers types d'infogérance : l'externalisation, les téléservices (dont la télémaintenance), l'infogérance sur site…
Les conditions d'usage de l'infogérance doivent être rigoureusement définies, et dans la mesure du possible, sur la base d'une analyse des risques spécifique.

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

(Cf. opérations de telé-action)

EXP-05 : Conditions de sécurité pour la maintenance des constituants du SI

Le non-respect des consignes pour la préparation d'un constituant avant sa mise en maintenance peut exposer l'organisme à des compromissions ou à des atteintes au bon fonctionnement de son système d'information.
Le conditionnement consiste à préparer le constituant en vue de sa réparation c'est-à-dire, à vérifier les points suivants :

- le retrait du support de la mémoire rémanente ayant contenu des informations classifiées ou confidentielles,
- la superposition d'écriture sur la mémoire restante afin d'éviter toute possibilité d'interprétation des enregistrements précédents,
- la vérification des installations de maintenance externes qui doivent répondre aux mêmes normes de sécurité matérielle et personnelle que celles appliquées dans les zones d'utilisation pour les constituants mis en réparation.

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

EXP-06 : Conditions de sécurité pour la reprise après maintenance

Les conditions de sécurité pour la remise en fonctionnement des constituants après leur maintenance visent à démasquer tout piégeage éventuel ou dysfonctionnement.
En conséquence, des conditions de remise en fonctionnement peuvent être édictées, par exemple :

- en fonction des conditions locales, de l'évaluation de la menace et, dans le cas d'ordinateurs, de la sensibilité des informations mises en mémoire, le constituant fait l'objet de mesures de détection lorsqu'il est réintégré dans sa zone de sécurité,
- pour le cas particulier de matériels répondant à la norme TEMPEST, toute modification entraîne une nouvelle vérification de l'aptitude anti-rayonnante.

EXP-07 : Suivi des opérations de maintenance des constituants du SI

Cette règle qui s'applique à tous les constituants du système d'information (matériels et logiciels) prend un caractère majeur pour le cas de constituants ayant des fonctions de sécurité.
L'absence de suivi des opérations de maintenance a pour conséquence la méconnaissance du degré d'aptitude des constituants à assurer de nouveau leurs fonctions : elle peut conduire à leur attribuer une confiance injustifiée sur le plan de la sécurité.
Le suivi des opérations de maintenance nécessite l'ouverture d'un registre complet et détaillé sur les interventions subies par les composants afin que le personnel connaisse les nouvelles configurations et applique les procédures correctes.
Par ailleurs, lorsque l'organisme dispose d'un infocentre dont la mission principale est le support aux utilisateurs, il est nécessaire de veiller à ce qu'il applique ces mêmes règles pour les interventions dont il a la charge et tout particulièrement lorsque ses attributions consistent à faire installer sur les machines de l'organisme les progiciels ou les cartes électroniques demandées par les utilisateurs.

EXP-08 : Gestion des prestations de services externes

Pour le développement du système d'information, le recours à des prestataires de services externes (dûment habilités dans le cadre de marchés de défense) impose l'application stricte des règles

précédemment énoncées et un contrôle renforcé des ressources mises à disposition (applications et fichiers sensibles, compilateurs, éditeurs, documentation technique…).
La décision de mise à disposition de ressources sensibles doit être prise par rapport aux exigences opérationnelles de disponibilité du système d'information.
Les responsabilités et les procédures doivent être clairement établies entre l'organisme et les prestataires pour l'imputabilité d'éventuels incidents.
Le recours aux prestations de service, dès lors que la sécurité d'un système d'information représente un enjeu majeur pour les intérêts de l'État ou de l'organisme, ne doit jamais dériver vers une sous-traitance de la gestion de l'exploitation (traduction du terme anglo-saxon "*facility management*").

(Cf. externalisation de services)

EXP-09 : Intégration de la SSI dans les contrats d'infogérance

Les contrats d'infogérance et leurs annexes devront comprendre un volet SSI qui spécifie clairement les engagements du prestataire et de chacun de ses personnels concernés. Ils devront notamment spécifier très précisément :
- les exigences de sécurité auxquelles le prestataire s'engage (et qui ne pourront être inférieures à celles qui seraient en vigueur en interne) ;
- les procédures de contrôle du respect de ces exigences ;
- l'attribution de responsabilités spécifiques pour une coordination efficace en cas d'incident ou d'anomalies ;
- la possibilité d'évolution des exigences et des procédures –en conformité avec une évolution de la PSSI ou de ses déclinaisons opérationnelles– et l'obligation pour le prestataire de se conformer à ces évolutions.

EXP-10 : Sécurité dans les services externalisés

La décision et la contractualisation de services externalisés doivent être précédés d'une analyse de risques et d'enjeux pour l'organisme. Les problématiques suivantes doivent aussi être prises en compte :
- la responsabilité de l'organisme et des prestataires des services d'exploitation externalisés doivent être clairement définies et contractualisées ;
- la mutualisation des ressources fournies par les prestataires pour répondre aux besoins de plusieurs clients peut ne pas correspondrent aux objectifs de sécurité ;
- les moyens mis en oeuvre sur les systèmes d'information du prestataire utilisés pour s'interfacer avec le système d'information de l'organisme ne sont pas nécessairement adaptés, cohérents, voire compatibles, avec les moyens de sécurité mis en œuvre ;
- les possibilités et modalités de contrôle et d'audit de la part du donneur d'ordre se trouvent souvent limitées, compte tenu notamment de dispositions contractuelles figées ou des modalités pratiques d'intervention du donneur d'ordre sur le site d'exploitation ;
- les personnes utilisant et manipulant le système d'information ne sont pas toujours connues de l'organisme, or ces personnes se trouvent par ailleurs simultanément en contact avec des données d'entreprises pouvant être concurrentes, ou avec des responsables de sociétés concurrentes ;
- sur le plan technique, les privilèges accordés au prestataire pour réaliser sa tâche sont, en général, particulièrement étendus en terme de sécurité (cf. protection des accès de maintenance) et peuvent être utilisés pour s'introduire dans le système d'information.

Ainsi, une analyse des risques relatifs à ces problématiques devrait être conduite afin de déterminer des objectifs et mesures de sécurité couvrant les risques identifiés, notamment sur le plan des clauses contractuelles, de la traçabilité et du suivi des opérations réalisées.

EXP-11 : Contrôle antiviral des logiciels et données avant leur mise en exploitation

Les contrôles des logiciels et des fichiers de données avant leur mise en exploitation visent à lutter tout particulièrement contre la menace de contamination par virus.
Des précautions peuvent être prises pour prévenir et détecter l'introduction de logiciels frauduleux (virus, vers, chevaux de Troie, bombes logiques…). Tous les supports en provenance de l'extérieur de l'organisme et, tout particulièrement ceux dont l'origine est incertaine, sont soumis à un contrôle. La mise en place de moyens dédiés à un dépistage systématique constitue une contre-mesure à cette menace. Ces moyens doivent être mis en place de façon à s'assurer que tous les points d'entrée du système informatique sont contrôlés (Internet, réseau, serveurs, postes de travail).

Les éléments du système possédant de forts besoins de sécurité et les chemins de contamination doivent également être identifiés et protégés. Il faut tenir compte des nombreux moyens de récupérer des fichiers (disquettes, cédéroms, pièces chiffrées jointes aux courriers électroniques…).
D'autre part des consignes claires doivent être communiquées aux utilisateurs afin qu'ils n'installent aucun logiciel sur leur poste de travail.

EXP-12 : Contrôles de sécurité en phase d'exploitation du système d'information

Le contrôle de sécurité en phase d'exploitation permet de réduire les risques d'atteinte à la disponibilité et à l'intégrité des informations et des données. Ces contrôles se traduisent, par exemple, par des vérifications de l'usage des ressources autorisées pour le traitement.
Le premier aspect de ces contrôles vise les utilisateurs du système d'information. Ils échoient aux ingénieurs système et réseau qui assurent une surveillance en direct à partir de moyens de visualisation : examen des transactions en cours, fichiers en ligne, tentatives de connexions…
Le second aspect de ces contrôles vise les informaticiens pour la vérification de la bonne application des procédures de sécurité, par exemple :
- le respect du séquencement des opérations planifiées,
- les manipulations correctes de fichiers,
- l'utilisation des macro-instructions autorisées,
- le respect des instructions pour les récupérations d'erreurs ou pour les événements exceptionnels.

EXP-13 : Réduction des vulnérabilités

De plus en plus de services sont offerts au travers des réseaux bureautiques, qui véhiculent toutes sortes d'informations possédant des besoins de sécurité très hétérogènes.
Une politique de veille de sécurité doit être établie de manière à suivre l'état de l'art dans ce domaine et à réagir de manière adéquate lors de la découverte de vulnérabilités significatives sur les systèmes et applications standard du système d'information. La veille concernera les méthodes d'attaque, les vulnérabilités et les solutions de sécurité.

EXP-14 : Procédures d'exploitation sécurisée des informations et des données

Les données et les supports associés devraient hériter du même niveau de protection que les informations qui leur ont donné naissance.
En fonction de leur classification, les informations et les données font l'objet d'une exploitation spécifique. Ainsi l'exploitation de données vitales ou sensibles peut nécessiter la mise en œuvre de mesures techniques particulières (par exemple, l'usage de systèmes à tolérance de pannes ou de disques miroir) ou organisationnelles (par exemple, la règle sur le cloisonnement des postes de travail sensibles) afin d'éviter les incidents durant la phase de traitement. De même, les informations nominatives doivent recevoir les protections imposées par la loi.
La présente règle portant sur les procédures d'exploitation sécurisée se justifie par la vulnérabilité des données qui existe du fait de leur passage par des états différents (traitements, sauvegardes et transferts sur des supports, stockage, destruction…) : aussi les procédures et contrôles de sécurité s'attachent à assurer la continuité de la protection à ces divers stades de l'exploitation.
Parmi les procédures à mettre en place, celles concernant la sauvegarde des données et la destruction des supports classifiés ont un impact majeur sur la sécurité.
- La sauvegarde des données vise le maintien de leur intégrité et disponibilité : elle doit être faite régulièrement et les supports résultants sont stockés en des lieux éloignés de la zone de traitement et offrant le même niveau de protection ; des tests d'intégrité des sauvegardes apportent la garantie de la continuité de service.
- La destruction des supports classifiés implique que les données enregistrées sont effacées ou surchargées avant que leur support magnétique ne soit détruit (bandes magnétiques, disquettes, disques amovibles et fixes, mémoires à disques…).
- Pour les données relevant du secret de défense, il peut être prévu, en conformité avec la réglementation en vigueur, un chiffrement des données permettant ainsi le stockage intermédiaire des supports associés lors de traitements discontinus.

EXP-15 : Mise en place d'une organisation pour la lutte contre le code malveillant

La mise en place d'une organisation et d'une PSSI contre la menace virale permet de diminuer les risques de perte d'intégrité, de disponibilité et de confidentialité de l'information. Cette organisation doit disposer des entités suivantes :
- cellule anti-virus (Administration, exploitation, mise à jour …) ;
- cellule de support ;
- gestion de crise ;
- organisation de la veille.

Dans la lutte contre les codes malveillants il est primordial de bien définir les relations entre les différents intervenants en particulier pour ce qui concerne la veille, les intervenants en cas de crise, et la mise à jour des outils et des procédures
La définition d'une organisation de sécurité contre le code malveillant devra définir notamment l'organisation à mettre en place et les rôles et les responsabilités de chaque acteur.
Il faudra également mettre en place une architecture technique de protection contre les virus pour l'ensemble des composants du système informatique (Postes de travail, serveurs de messagerie, serveurs Internet, serveurs de sauvegardes, de données…)

EXP-16 : Consignes de sécurité concernant la télé-action

La télé-action regroupe toutes les opérations d'exploitation du réseau et des postes de travail réalisées à distance : sauvegarde, prise en main à distance, installations d'application à distance, traitement d'anomalie à distance, opération de maintenance à distance…
Les accès de télé-actions sont particuliers lorsqu'ils doivent s'appliquer à des postes de travail qui ont été attribués à des utilisateurs. En effet, il faut notamment garantir à l'utilisateur qu'il conserve la maîtrise de son environnement et qu'aucune intervention sur ses fichiers ou sa session de travail ne peut avoir lieu sans son aval préalable – ceci doit concourir à garantir une relation de confiance mutuelle entre les exploitants du réseau et les utilisateurs.

EXP-17 : Protection et utilisation de la messagerie

Des règles claires et simples doivent être émises pour assurer la confiance dans l'utilisation de la messagerie électronique.
Ainsi, il conviendra d'établir une liste de mesures techniques et non techniques pour lutter contre :
- la propagation et l'exécution de codes malveillants ;
- l'interception d'informations sensibles véhiculées en clair par le courrier électronique ;
- la désinformation ou le *spamming* ;
- la publication d'informations illégales, diffamatoires ou de harcèlement ;

Il conviendra de surcroît de définir les règles relatives à :
- la conservation de preuves des échanges électroniques ;
- l'utilisation de moyens de sécurité (authentification, chiffrement signature) ;
- l'utilisation de la messagerie depuis l'extérieur de l'organisme (cf. accès distant) ;
- la surcharge du système de messagerie.

EXP-18 : Règles spécifiques de filtrage aux accès

Des règles techniques de filtrage pourront être mises en place sur les routeurs, les pare-feu et les serveurs de messagerie afin de n'autoriser que l'accès à certains serveurs identifiés. En effet, tout ce qui n'est pas explicitement autorisé devrait être interdit pour le filtrage des accès. Ce principe est valable en interne également.

EXP-19 : Normes de conservation et de destruction des informations à protéger

Certaines catégories d'informations nécessitent des conditions de conservation et de destruction adaptées. En ce qui concerne les informations relevant du secret de défense, la réglementation précise les mesures à prendre suivant leur niveau de classification. Pour les autres catégories, les mesures sont adaptées à l'environnement propre à l'organisme et doivent demeurer cohérentes entre elles.
En particulier, le contrôle préalable des bonnes conditions de stockage revêt un aspect fondamental dès lors que l'information est confiée contractuellement à un organisme. La destruction d'urgence peut, pour certains organismes, revêtir un aspect majeur en situations exceptionnelles (émeutes,

guerre civiles…) mais, plus couramment, des normes précises peuvent être adoptées pour l'élimination de l'information périmée qui conserve un caractère résiduel de confidentialité.
De plus, l'archivage de documents magnétiques fait l'objet d'obligations juridiques en termes de durée de conservation et de protection des supports, selon la nature des informations concernées (informations comptables ou fiscales, relatives au personnel…).

EXP-20 : Contrôle des supports amovibles avant leur mise en exploitation

Cette règle, portant sur le contrôle des supports amovibles, vise principalement la confidentialité des informations et intéresse les organismes traitant d'informations sensibles relevant du secret de défense ou des informations jugées stratégiques pour leurs activités.
Une mesure fondamentale précédant le contrôle des supports amovibles, avant leur réutilisation dans une autre installation protégée, consiste à effacer les informations qui y sont enregistrées en opérant un recouvrement complet au moyen de caractères numériques ou alphanumériques.
Pour les informations relevant du secret de défense, les supports de mémoire conservent la plus haute catégorie de classification des données pour lesquelles ils ont été utilisés depuis l'origine (sauf en cas de déclassification).
Ce principe peut être appliqué aux informations non classifiées particulièrement sensibles.

EXP-21 : Les supports, sources d'infection et de risque de divulgation

Les organismes sont sensibilisés à la sécurité des systèmes. Néanmoins, la protection des supports amovibles (disquette, bande sauvegarde, listing, rapport…) est souvent délaissée, bien qu'ils contiennent des informations de l'organisme.
On entend par supports tout moyen incluant des informations : principalement les supports informatiques, les supports papier (listing, documentation, impression de rapports…).
Les supports doivent être protégés conformément aux règles associées à la classification des informations qu'ils hébergent. Ainsi, il doit exister, en fonction de la classification, des règles de sécurité concernant la gestion, le contrôle, le stockage (contre le vol et la destruction), le transport et la mise au rebut des supports.
Bien qu'aujourd'hui la menace virale (codes malveillants) provienne principalement des réseaux publics, l'introduction de virus par des supports reste une problématique importante (cf. lutte anti-virale).
Des règles spécifiques existent concernant l'entrée/sortie de supports informatiques en zone classifiée (gestion d'un registre des supports, de leur contenu…) – (cf. continuité dans la protection des informations).

EXP-22 : Mise au rebut des supports ou sortie de matériel informatique

Les matériels informatiques contiennent des supports de données de l'organisme. L'entrée et surtout la sortie de ces supports de l'organisme doivent être maîtrisées.
Ces données, au même titre que les données contenues dans tout autre support de l'organisme, doivent être détruites lors des dons ou lors de la mise au rebut, soit par destruction physique des supports, soit par effacement logique sécurisé (sur-écritures multiples). Ainsi, l'organisme doit définir les règles de destruction par type de support et, le cas échéant, selon le niveau de classification.
Dans le cas de support papier, l'organisme peut soit installer des broyeuses, soit centraliser ces supports à détruire et confier à des organismes spécialisés cette tâche (avec engagement de destruction). Dans les deux cas, une attention particulière devra être portée à la protection du stockage des supports avant leur destruction.

EXP-23 : Photocopie de documents

Des directives de sécurité doivent être énoncées pour réglementer le photocopillage en fonction de la classification du document.
Ces directives devront prendre en compte les obligations relatives au « photocopillage » qui font l'objet d'une législation spécifique.

EXP-24 : Stockage des informations par l'organisme

Des règles de sécurité pour le stockage des informations doivent être définies et appliquées par tout le personnel en fonction de la classification. Ces règles visent principalement à assurer la protection des informations contre toute divulgation ou vol par des personnes non autorisées ou encore altération.

EXP-25 : Connexion des postes nomades et PDA

Des règles de sécurité doivent être rédigées pour réglementer les types d'information pouvant être stockées dans ces unités. Des moyens de protection et/ou de contrôles doivent être mis en place pour assurer le respect de ces règles.
Leur connexion au système d'information de l'organisme doit avoir été autorisée et respecter sa PSSI.
Une attention particulière doit également être portée pour éviter que ces équipements ne puissent servir de passerelle entre le système d'information et un réseau public.

ENV : Aspects physiques et environnement

ENV-01 : Continuité dans la gestion des biens physiques

La gestion des biens physiques est assurée tout au long de leur cycle de vie : phases d'affectation, d'installation, de fonctionnement, d'entretien, de mise au rebut et de destruction. Ces biens peuvent également être amenés à changer de propriétaire ou de responsable, d'environnement ou d'usage (prêt de matériels pour une exposition, ré-affectation d'un matériel dans le cadre d'un nouveau projet).
La règle prévoit que les mesures choisies offrent une protection continue quelles que soient les évolutions ou les changements d'utilisation des biens physiques.
Cette continuité de gestion repose sur l'adoption d'une classification (incluant, le cas échéant, la classification de défense au sens de l'[IGI 900]), sur le suivi des biens physiques depuis leur mise en service, leur évolution jusqu'à leur remplacement. Les principales mesures qui découlent de cette règle intéressent le recensement, le marquage des biens et les mesures spécifiques de protection physique correspondant à leur état (prêt, maintenance…) ou à leur classification :

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

ENV-02 : Prise en compte des contraintes opérationnelles de l'organisme

La mise en place de moyens et procédures de sécurité physique qui ne prend pas en compte les contraintes de l'organisme peut constituer une entrave au bon fonctionnement des tâches opérationnelles et engendrer un rejet de la part du personnel vis-à-vis de la sécurité.
Il est donc nécessaire de prendre en compte les contraintes opérationnelles de l'organisme dans la mise en place des moyens et procédures de sécurité physique.

ENV-03 : Complétude des mesures de sécurité physique

Les différents types de mesures suivants devraient être pris en compte.
Les mesures de protection des biens physiques ont pour objectif de réduire l'ampleur des atteintes, principalement dans les domaines de la disponibilité, de l'intégrité et de la confidentialité.
L'absence de solutions universelles capables de répondre à toutes les formes de menaces oblige l'organisme à mettre en œuvre un ensemble de mesures susceptibles de contrecarrer le cheminement d'une attaque et de réparer les dommages causés : ce sont les mesures de prévention, de détection, de réaction et de recouvrement.
Les mesures de prévention visent à diminuer la probabilité d'apparition d'un sinistre. Elles consistent, par exemple, à porter attention à la localisation de certains locaux (comme les bandothèques, les salles d'archives, les canalisations, les salles de rangement de produits dangereux) face aux risques d'incendie ou d'inondation ou à surveiller la conformité de l'utilisation des matériels.
Les mesures de détection visent à donner l'alerte lors d'une tentative d'intrusion ou du déclenchement d'un sinistre dans le périmètre du système d'information. Elles doivent également permettre de localiser cette alerte. Ces mesures se traduisent par la mise en place aux endroits critiques de moyens de détection et d'alerte comme, par exemple, des capteurs de chaleur ou des caméras de surveillance.
Les mesures de réaction visent à lutter contre un sinistre déclaré en vue de réduire son impact. Ces mesures se traduisent par le déclenchement de moyens d'interventions prévus par l'organisme comme, par exemple, un service de lutte contre l'incendie.
Les mesures de recouvrement visent à limiter les conséquences d'un sinistre et à faciliter le retour au fonctionnement normal du système d'information. Elles peuvent se traduire par l'activation de moyens de secours ou par la désactivation de fonctions de sécurité comme, par exemple, la

suppression temporaire du contrôle d'accès physique dans le cadre d'un fonctionnement de la sécurité en mode dégradé.
Pour l'ensemble des sinistres redoutés par l'organisme, les mesures choisies devraient être graduelles, afin d'offrir un niveau de résistance suffisant pour contrecarrer ou atténuer l'attaque.

ENV-04 : Isolement des systèmes sensibles ou vitaux

Isoler les systèmes sensibles ou vitaux permet de minimiser l'exposition des biens par rapport aux menaces. Les risques sont ainsi réduits. De plus, ceci offre la possibilité de proportionner au mieux les mesures de sécurité en réduisant les coûts d'une protection globale.

ENV-05 : Adéquation des mesures de sécurité physique aux types de biens

Les mesures de sécurité physique doivent être appliquées à l'ensemble des locaux. Elles visent tout d'abord à protéger le personnel puis à réduire les risques de destruction ou de divulgation qui pourraient porter atteinte directement ou indirectement aux intérêts vitaux de l'entreprise ou de l'organisme.
Cette règle indique que les mesures dont il est fait mention à la règle précédente peuvent être déclinées selon les trois catégories de biens physiques à savoir, l'infrastructure, les matériels et les équipements de soutien.

ENV-06 : Protection contre les accidents et pannes

Dans les locaux hébergeant des équipements vitaux pour le système d'information (sans oublier les composants de l'infrastructure réseau) en tenant compte des menaces de l'environnement proche, prévoir les mesures :

- contre les dégâts des eaux – détection et réaction - (le mieux est d'éviter d'héberger des équipements dans des locaux à risques comme des salles dans lesquelles existent des conduites d'eau ou situé dans des sites inondables) ;
- la détection et l'extinction incendie ;
- contrôle et secours de l'alimentation électrique (au minimum les éléments de protection doivent garantir un délai minimum d'alimentation pour réaliser toutes les opérations de sauvegarde nécessaire) ;
- secours des réseaux de télécommunication (porter une attention particulière aux procédures de basculement vers des lignes de secours en cas d'interruption de ligne) ;
- de climatisation et de conditionnement d'air (tenir compte de la fourniture des consommables tels que eau, gaz et filtre, ainsi que les mesures pour lutter contre les poussières) ;
- procédures formalisées de réaction en cas de sinistre ou de pannes (y compris pendant les heures non ouvrées) ;
- procédures d'urgence.

Le contrôle de l'environnement doit tenir compte de la température, de l'humidité, des poussières et des vibrations.
Il faut également prévoir un plan de situation d'urgence si des sinistres non maîtrisables se produisent.
(Cf. gestion de crise)
Tous les équipements de protection installés doivent être régulièrement contrôlés. Des contrôles (notamment concernant les mesures incendie) sont exigés dans les réglementations. Il est fortement recommandé d'appliquer ces contrôles aux équipements pour lesquels ils ne sont pas obligatoires (par exemple, la détection de présence d'eau).

ENV-07 : Protection physique du câblage et des réseaux télécoms

Le câblage télécom et informatique doit, dans la mesure du possible, être protégé contre tout accès malveillant pouvant conduire à des écoutes (lignes enterrées, câbles cachés…).
Il est indispensable de garantir la protection des accès aux équipements de terminaison et de routage.
La protection des accès aux câblages et autres composants réseaux (qu'ils soient autorisés ou non) consiste non seulement à empêcher l'écoute passive (et parfois active) mais aussi à éviter que, par accident, ces moyens ne soient endommagés.

ENV-08 : Découpage de l'infrastructure en zones de sécurité

Les sites, les bâtiments et les locaux contenant des biens matériels ou immatériels (les informations et leurs supports associés, les matériels constitutifs du système d'information) ou abritant des activités

critiques au regard de la sécurité, doivent être contrôlés tout particulièrement au niveau de leurs accès.
Une zone de sécurité est une zone dans laquelle des dispositions permanentes sont prises pour contrôler les mouvements du personnel et des matériels, ainsi que pour détecter et empêcher toute écoute.
Un découpage de l'infrastructure en zones de sécurité facilite la mise en place de dispositifs adaptés, tout particulièrement pour le contrôle de la circulation du personnel par attribution de droits d'accès spécifiques aux zones. Ces droits peuvent être liés aux postes de travail et aux niveaux de responsabilité.

ENV-09 : Application des modalités d'accueil et de circulation des visiteurs

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

ENV-10 : Gestion spécifique des biens physiques nécessitant une protection

La gestion des biens physiques nécessitant une protection comprend l'adoption d'une classification ou d'une typologie, les mesures de gestion de ces biens et les mesures de protection tout au long de leur vie.
Le principe à respecter est d'adapter ces moyens de protection physique, comme toute mesure de sécurité, à la valeur des biens à protéger, mais aussi en cohérence avec les autres mesures de sécurité appliquées.
L'article 10 de l'[IGI 900] définit ainsi : "Tout document, logiciel ou matériel qui, par son intégrité ou sa confidentialité contribue à la sécurité d'un système d'information, reçoit la mention ACSSI qui rappelle que sa gestion et sa protection doivent être assurées conformément aux prescriptions de l'instruction ministérielle relative aux Articles Contrôlés de la Sécurité des Systèmes d'Information".
Pour les biens physiques non classifiés de défense, l'adoption d'une typologie permet de les regrouper suivant leur nature et leur affectation. Des classes de protection sont établies en fonction du niveau d'exigence de sécurité, c'est-à-dire des critères de confidentialité, d'intégrité et de disponibilité attachés à ces biens pour en garantir une surveillance continue. La typologie adoptée est spécifique à la mission ou au métier, à la culture et aux contraintes propres à l'organisme.

ENV-11 : Procédures d'exploitation sécurisée des moyens décentralisés

Les moyens décentralisés, dédiés ou déportés hors de leur zone de sécurité (micro-ordinateurs, matériels portables, imprimantes déportées, photocopieuses, télécopie…) se caractérisent souvent par des équipes d'exploitation réduites voire des utilisateurs isolés. Sans assistance immédiate et sans le recours aux protections physiques d'une zone de sécurité, la probabilité d'incident ou d'atteinte à la sécurité des biens reste très élevée : l'indiscrétion et la malveillance représentent une menace majeure dans la mesure où les consignes de vérification sont plus difficiles à mettre en œuvre. C'est la raison pour laquelle l'exploitation de ces moyens nécessite des mesures spécifiques adaptées à leur environnement ; en particulier et, dans la mesure du possible, les équipements périphériques sont situés dans une zone surveillée.
Le cas des matériels portables mérite un examen particulier. En effet, avec l'accroissement de capacité de mémoire et de puissance de traitement, les machines portables sont de plus en plus utilisées. Cependant, elles sont exposées à des menaces plus variées que les matériels fixes et leurs utilisations rendent beaucoup plus difficile le contrôle nécessaire à la sauvegarde des informations. Leur portabilité et leur petite taille accroissent fortement la probabilité de perte ou de vol.
Dans la mesure du possible, les informations à protéger ne peuvent être traitées sur des micro-ordinateurs portables qu'en des endroits désignés en fonction de leur niveau de classification.
Lorsque ces matériels sont emportés à l'extérieur de l'organisme, il faut appliquer la même procédure que pour la sortie des documents classifiés.

ENV-12 : Protection de la documentation de sécurité

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

- tout responsable-détenteur de documents de sécurité doit connaître la position des documents qui lui sont confiés et contrôler leur utilisation ;
- la manipulation de ces documents ne peut être faite que par du personnel autorisé ;
- les documents sont rangés dans des lieux sûrs ;
- la diffusion, émanant du responsable de la sécurité, peut être restreinte au minimum de personnes.

ENV-13 : Protection de l'équipement contre le vol

L'agent a qui sera attribué l'équipement, même de manière temporaire, sera responsable dès son attribution de sa protection en utilisant des moyens cohérents et adaptés.
Dans la mesure du possible, lorsque son détenteur doit sortir l'équipement du site, il est recommandé qu'il ne stocke sur l'équipement que les informations strictement nécessaires pour réaliser sa mission à l'extérieur, le cas échéant, il transportera les informations sur un support externe amovible.
Les risques de vol de micro-ordinateurs portables étant important même sur le site de l'organisme, un inventaire et un contrôle fréquent des machines doivent être réalisés.
Une procédure spécifique doit être formalisée pour définir les actions à mener par le détenteur et par l'organisme en cas de vol de l'équipement.

ENV-14 : Protection des supports de sauvegarde

Les supports de sauvegarde doivent être protégés contre les risques de destruction, de divulgation et de vol. Une attention particulière doit être portée à ces types de supports car, par nature, en contenant une partie des informations hébergées par un système, ils constituent une cible de choix pour réaliser un vol d'information et détruire la capacité de l'organisme à récupérer d'un sinistre.

ENV-15 : Protection de la documentation système

La documentation des systèmes (architecture réseaux, plan de nommage…) contiennent des informations qui associées à d'autres (informations de vulnérabilités…) constituent des éléments vitaux pour conduire avec succès des attaques. Leur divulgation à l'extérieur peut être l'opportunité pour certains de mener des tentatives d'intrusion.
Il est donc essentiel de veiller à classifier ces documentations et à en contrôler leur diffusion à l'extérieur, y compris auprès de fournisseurs.

ENV-16 : Utilisation à l'extérieur du site

La sortie et l'utilisation à l'extérieur de l'organisme de tout équipement informatique doivent avoir été autorisées. Des règles doivent être formulées pour restreindre leurs utilisations dans les lieux publics ou sur d'autres systèmes d'information.
Leur connexion au système d'information d'un client ou partenaire doit avoir été autorisée par cet autre organisme, et son propriétaire devra respecter la PSSI.
L'équipement informatique doit être protégé afin d'éviter tout accès non autorisé aux informations qu'il stocke et traite.

3 Principes techniques

AUT : Identification / authentification

AUT-01 : Utilisation d'un même secret pour accéder à plusieurs services

Selon les applications et les systèmes, les moyens utilisés pour protéger les secrets d'authentification sont de niveaux d'assurances différents. Il est fondamental que les utilisateurs s'informent sur la robustesse des systèmes d'authentification pour utiliser un même secret dans des systèmes dont la protection est cohérente (exemple : utilisation d'un même mot de passe pour s'authentifier sur le système d'exploitation et différentes applications).
Ainsi, il convient de n'utiliser un même secret que pour des services de niveaux d'assurance équivalents.

AUT-02 : Combinaison des moyens d'authentification

L'accès au système d'information implique que les utilisateurs justifient leur identité en début de session (et, dans certains cas, en cours de session) en présentant un élément d'authentification. Les techniques actuelles d'authentification reposent sur trois moyens :
- ce que l'on sait comme, par exemple, les mots de passe ;
- ce que l'on détient comme, par exemple, les cartes à puce ;
- ce que l'on est, c'est-à-dire une caractéristique personnelle (empreintes digitales, examen du fond de l'œil, signature dynamique…).

La réunion de ces trois moyens constitue une authentification complète et efficace mais représente un coût relativement élevé. En conséquence, le responsable-détenteur doit déterminer avec l'aide de l'agent de sécurité, à partir de ces trois concepts, quelles sont les combinaisons les plus adaptées pour son sous-système d'information ou ses applications sensibles.
La réunion d'au moins deux de ces concepts est communément appelée authentification forte.
Le choix d'une authentification basée sur le seul concept de "ce que l'on sait" représente le profil minimal de sécurité pour un système d'information ; il convient alors d'opter pour des mécanismes dynamiques comme les mots de passe utilisables une fois ou bien ceux assujettis à une limite du nombre d'utilisations ; dans ce cas, le mécanisme utilisé est un compteur d'accès sur lequel doit porter l'effort de protection.
Ainsi, les mécanismes utilisés reposent sur des éléments d'authentification dont il convient expressément de prévoir une gestion rigoureuse.

AUT-03 : Unicité de l'identité des utilisateurs

L'identité des utilisateurs doit être gérée sous le contrôle conjoint de la direction du système et du responsable de la sécurité d'un site ou d'une unité opérationnelle (niveau de l'agent de sécurité).
L'identification unique (et sans équivoque) du propriétaire d'un accès est fondamentale pour assurer la traçabilité des opérations et le diagnostic d'une anomalie de sécurité (cf. contrôle et audit).

AUT-04 : Délivrance et recouvrement des moyens d'authentification

Les technologies utilisées pour maîtriser les accès à un système d'information peuvent être aussi sophistiquées que possible, la délivrance, l'utilisation et la gestion de ces moyens restent des éléments vitaux du système. Ainsi, les règles suivantes doivent être clairement formalisées et scrupuleusement respectées :
- la délivrance d'un accès à un utilisateur doit être précédée d'un engagement formel de ce dernier au respect des règles élémentaires de protection des moyens d'accès fournis et du devoir d'avertissement en cas de vol (ou seulement de suspicion de divulgation du secret) (cf. responsabilités, cf. attribution de postes sensibles) ;
- la délivrance des moyens d'accès (mots de passe, carte à puce…) doit être réalisée en s'assurant que seul son propriétaire aura connaissance des secrets ;
- le traitement d'une déclaration de vol ou de perte d'un secret doit garantir la protection contre l'usurpation de l'identité de l'utilisateur ;
- le départ d'un personnel (voir sa mutation) doit conduire systématiquement à la suppression de tous ses accès au système d'information.

Il faut considérer qu'il y a infraction à la sécurité lorsque deux personnes ou plus connaissent, par exemple, le mot de passe correspondant à une identité d'utilisateur à moins que cela ne soit prévu pour assurer la continuité des fonctions d'administration du système.
S'il est inévitable, dans certains cas, de permettre le partage d'une identité et d'un élément d'authentification, des mesures spéciales telles que l'emploi d'enveloppes scellées avec prise en compte peuvent être mises au point pour prévenir toute utilisation abusive ou incorrecte.

CAL : Contrôle d'accès logique aux biens

CAL-01 : Dispositifs et procédures de protection contre les intrusions

L'architecture des infrastructures de communication doit comprendre les dispositifs et procédures assurant le niveau adéquat de protection contre les intrusions
L'accès au SI et à ses principales ressources (applicatifs) doit être contrôlé afin de se protéger contre des accès frauduleux –intrusions-. Les moyens à mettre en place varient en fonction des objectifs de sécurité et peuvent comprendre des mesures telles que des dispositifs garde-barrière (*firewall*) et des systèmes d'authentification et de contrôle d'accès.
Après une analyse des risques SSI comprenant un recensement de chacune des cibles potentielles et des moyens d'accès possibles pour des attaquants, il conviendra de mettre en place les dispositifs défensifs adaptés pour couvrir les objectifs de sécurité identifiés.

CAL-02 : Cloisonnement des réseaux et maîtrise des flux

Le cloisonnement des réseaux a pour objectif :
- de faciliter le contrôle d'accès ;
- de mieux se protéger contre les intrusions ;
- d'empêcher la fuite d'information :
    - vers des réseaux ou des postes de travail internes à l'entreprise à destination de personnes qui n'ont pas à connaître ces informations ;
    - vers des réseaux ou des postes externes à l'entreprise ;
    - par la connexion depuis l'extérieur de l'entreprise en utilisant la technique du rebond par exemple, via un poste connecté en même temps au réseau interne de l'entreprise et à un modem.

Il permet de créer des zones réservées –périmètres de sécurité bien identifiés- en prenant en compte le besoin d'en connaître. De tels périmètres internes doivent être mis en place chaque fois qu'une analyse identifie des sous-ensembles ou applications sensibles qui justifient d'une politique de sécurité et de contrôle des accès et des communications particuliers.
Les communications entre l'intérieur et l'extérieur d'un périmètre de sécurité doivent systématiquement passer par un dispositif (garde-barrière) prévu à cet effet qui a en charge de contrôler le respect des exigences particulières à ce périmètre. A cette fin, il est indispensable qu'existe et que soit documenté une « matrice des flux » à la frontière : quelle communication, depuis qui, vers qui, avec quel contenu, dans quelles conditions ?
Le cloisonnement de réseaux qui permet de contrôler les flux d'information se base sur les droits d'accès des personnes, des fonctions et des processus.

Une des solutions de cloisonnement réside dans la protection des informations sensibles durant leur transmission.
Le principe s'attache à contrôler que le niveau de protection requis par les informations communiquées est correctement atteint.
La protection des informations sensibles durant leur transmission est organisée de façon à rendre aussi peu efficace que possible les différents types d'attaques sur le réseau de transmission.
L'organisation de cette protection vise à :
- l'acheminement du trafic même en ambiance de brouillage ou de saturation (qui consistent à empêcher ou gêner le fonctionnement des liaisons) ;
- la garantie contre l'intrusion (qui consiste à introduire ou à modifier des messages dans l'intention de tromper) ;
- la défense contre l'interception (qui est la réception d'émissions non autorisées) ;
- la défense contre l'analyse de trafic (qui permet d'obtenir des renseignements à partir de l'étude du trafic).

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

Le chiffrement est défini comme l'ensemble des moyens cryptologiques permettant de protéger les informations transmises, de façon à les rendre inintelligibles pour toute personne qui n'est pas autorisée à les connaître. On utilise soit le chiffrement des messages soit le chiffrement des voies de transmission.
Le principe intègre le fait que, si les mesures de sécurité correspondant au niveau de protection requis nécessitent des moyens de chiffrement, l'usage de ces moyens est soumis au respect de la loi et de la réglementation et doit s'accompagner de mesures organisationnelles permettant leur gestion spécifique.

CAL-03 : Modalités d'utilisation sécurisée des réseaux de télécommunication de l'organisme

L'utilisation sécurisée des réseaux de télécommunication de l'organisme ne doit pas remettre en cause les mesures de sécurité qui sont prises au plan de l'infrastructure (par exemple, la création de zones réservées), du personnel (par exemple, la gestion du besoin d'en connaître), de l'organisation de la sécurité ou des ressources matérielles et logicielles.
Les modalités d'utilisation des réseaux de télécommunication de l'organisme sont d'autant plus importantes à définir que les possibilités d'accès des utilisateurs sont augmentées par les éventuelles interconnexions des réseaux internes.
L'utilisation sécurisée des réseaux de télécommunication fait appel à la mise en place de fonctions et de mécanismes destinés à garantir la sécurité des données au cours de leur transmission. Il est possible d'adopter le découpage suivant :
- l'authentification ;
- le contrôle d'accès ;
- la confidentialité des données ;
- l'intégrité des données ;
- la non-répudiation ;
- la disponibilité.

Parmi ces fonctions, le contrôle d'accès repose sur des mesures de gestion et de contrôle continues dans le temps et portant, par exemple, sur les aspects suivants :
- l'accès des utilisateurs aux services pour lesquels ils sont autorisés ;
- la connexion au système d'information des ordinateurs isolés ou extérieurs à l'organisme ;
- la séparation des réseaux dédiés à des domaines particuliers ;
- le routage des communications sur les canaux autorisés.

CAL-04 : Organisation des accès au système d'information

L'organisme doit énoncer des règles et identifier des normes techniques pour assurer le contrôle et la gestion des accès au système d'information.
Ainsi, elles doivent définir les niveaux d'assurance des moyens de contrôles d'accès pour :
- l'accès au réseau d'entreprise (à l'intranet) et aux services transversaux - principalement messagerie et services Internet - depuis les sites de l'organisme ;
- le cas échéant, l'accès à un sous-réseau sécurisé ;
- l'accès aux applications de l'organisme ;
- l'accès depuis l'extérieur aux services transversaux de l'entreprise, en particulier la messagerie ;
- l'accès aux équipements connectés au réseau de l'organisme ;
- l'accès des postes de travail de l'organisme à d'autres réseaux – depuis le site de l'organisme ou hors du site ;
- l'accès par des fournisseurs au système d'information ;
- les accès public ou « invité ».

Les caractéristiques suivantes doivent être définies selon les besoins de sécurité des informations et/ou des fonctions du système d'information :
- technologie à utiliser (algorithme d'authentification, mot de passe joué qu'une fois…) ;
- protection des secrets (fichiers de mots de passe gérés par les systèmes ou les applications)
- conditions d'attribution d'un accès (engagement de l'utilisateur au respect des règles élémentaires de protection de l'accès) ;
- exigences de robustesse des moyens d'accès et des mots de passe - règles de construction - fréquence de changement des mots de passe - historique de mots de passe non ré-utilisables.
- durée de vie de l'attribution de l'accès ;
- toute procédure d'authentification à des accès sensibles ou utilisant des médias qui ne sont pas considérés comme de confiance (réseaux publics) doit assurer la non divulgation des éléments d'authentification ;

- procédure en cas de tentatives de connexion infructueuses répétées ;
- limitation des temps de connexion ;
- procédure en cas de déclaration de perte d'un secret – lutter contre des usurpations d'identité ;
- procédure de suppression des accès en cas de départ de personnel ou de vol de matériel.

Une attention particulière doit être portée sur la protection (notamment contre le vol de session, la divulgation de secrets, l'usurpation d'identité, la saturation volontaire de l'accès…) des accès au système d'information, utilisables à distance, hors des locaux de l'organisme (accès Internet, accès réseau commuté).
Pour chacun de ces accès, des procédures doivent être rédigées pour la définition des profils (y compris les profils des exploitants du réseau et des applications), d'attribution et de gestion des accès *(cf. habilitations)*.
Il est fortement recommandé de respecter le principe de n'attribuer un accès et des privilèges que lorsqu'ils sont nécessaires pour la réalisation d'une tâche.
Il est fondamental que les utilisateurs soient sensibilisés à la protection des informations et aux moyens qui leur ont été attribués pour accéder au système d'information de l'organisme (les postes de travail sont les points d'accès principaux au système d'information).

CAL-05 : Fichiers contenant des mots de passe

Dans la mesure du possible, tout fichier contenant des mots de passe (ou secrets) doit être banni ou chiffré (par exemple, script de connexion).

CAL-06 : Suppression des accès non maîtrisés au système d'information

Il est important de pouvoir maîtriser l'ensemble des accès au système d'information. C'est pourquoi une attention particulière doit notamment être portée aux accès suivants :
- équipement connecté au système d'information disposant également d'un accès public direct (par exemple micro-ordinateur portable connecté à la fois à un modem et au réseau d'entreprise) ;
- connexion non autorisée d'un poste de travail sur un accès physique du réseau.

CAL-07 : Attribution de privilèges d'accès aux services

L'attribution d'un accès et des privilèges associés doit être validée par le ou les propriétaires des systèmes accédés afin qu'il(s) vérifie(nt) qu'il est conforme aux habilitations de l'utilisateur et qu'il respecte les principes de responsabilités (séparation des pouvoirs, moindre privilège).
Il est souhaitable pour les services sensibles de maintenir un inventaire des accès et privilèges qui ont été autorisés.

CAL-08 : Protection des accès particuliers (accès de maintenance) au SI

Les accès de maintenance sont des accès octroyant des privilèges élevés sur les systèmes. Quand ils sont utilisés depuis l'extérieur de l'organisme (par exemple par des fournisseurs de service), il est fondamental de définir des moyens de protection renforcés contre toute utilisation malveillante et des moyens de traçabilité.
Des engagements de responsabilités spécifiques devront être inclus dans les contrats de prestations de service (cf. contrat de prestation).

CAL-09 : Vérification des listes d'accès au système d'information

Pour maintenir la maîtrise des accès au système d'information, il est fondamental de procéder périodiquement (voir de manière impromptue) à un contrôle de la liste des accès et des privilèges associés. Ce contrôle peut être réalisé sur la base d'un croisement entre l'inventaire des accès, l'archivage des engagements signés par les utilisateurs et la liste du personnel. Ces contrôles peuvent être renforcés dans le cas d'accès à des informations et/ou fonctions sensibles.
Une procédure doit prévoir les actions à mener en cas de détection d'incident (par exemple, accès apparaissant comme non justifié, privilèges apparaissant comme trop élevés…). Ces procédures devront tenir compte des impacts sur le système d'information d'une réduction des privilèges.

CAL-10 : Contrôle des privilèges des utilisateurs du système d'information

Il apparaît important de spécifier une règle de vérification du droit de possession des privilèges. Et ceci indépendamment des contrôles portant sur l'exploitation sécurisée, qui s'attachent à la façon dont ces privilèges sont utilisés.

Le contrôle a pour mission, dès qu'un utilisateur tente d'exercer ses privilèges sur une ressource du système d'information, de ne permettre cette action que dans la mesure où elle n'outrepasse pas les règles de sécurité en vigueur dans l'organisme.
Les mesures qui découlent de cette règle peuvent reposer sur les aspects suivants :
- les actions pour lesquelles un contrôle des privilèges doit être mené ;
- les mesures à prendre si une action est tentée sans que le droit approprié soit possédé ;
- les passe-droits au contrôle des privilèges et leurs conditions de validité.

CAL-11 : Application de la notion de profil d'utilisateur du système d'information

L'application de la notion de profil d'utilisateur du système d'information sous-entend, au préalable, la structuration des données (ou objets) par fonctions ou activités de l'organisme qui sont des prérogatives du responsable-détenteur. Les données manipulées par les utilisateurs sont structurées, en fonction des applications qui les utilisent au sein d'une unité fonctionnelle (par exemple, la gestion des stocks pour un service d'approvisionnement), dans le cadre d'utilisation de ressources partagées (par exemple, les réseaux locaux), ou lors d'une mission ou d'une activité particulière nécessitant le cloisonnement des postes de travail.
Il faut, de la même manière, structurer les diverses catégories de personnel (ou sujets) par la définition de profils d'utilisateur du système d'information qui permettent de spécifier les privilèges d'accès aux informations liés à la lecture (visualisation, impression) et les privilèges de traitements liés à l'écriture (création, modification, destruction) dans le cadre de leurs responsabilités ou activités.
Il faut également définir et formaliser les règles de délégations.

CAL-12 : Administration des privilèges d'utilisation du système d'information

Un utilisateur possède des privilèges d'utilisation pour les ressources du système d'information correspondant au profil qui lui est attribué. Il est indispensable d'administrer ces privilèges pour vérifier que les règles de sécurité en vigueur sont entièrement respectées.
Les critères d'application de ce principe devront être clairement énoncés ; ils peuvent, par exemple, s'inspirer des éléments suivants :
- les profils d'utilisateurs soumis à l'administration des privilèges ;
- les privilèges existants entre les divers profils d'utilisateurs ;
- les personnes qualifiées pour accorder ou modifier ces privilèges ;
- les conditions à remplir préalablement à toute modification ou tout octroi de privilèges ;
- les privilèges d'utilisateur incompatibles entre eux.

La protection de l'intégrité des tables contenant les privilèges doit faire l'objet d'un contrôle particulier du responsable du système et de l'agent de sécurité.

CAL-13 : Verrouillage des sessions de travail

Les postes de travail sont les points d'entrée principaux du système d'information. Les utilisateurs doivent être sensibilisés à rendre leur environnement de travail inaccessible en leur absence (verrouillage de la session, arrêt du poste de travail). Pour renforcer cette mesure et éviter des négligences, des mesures de protection automatique d'une session de travail après un délai d'inactivité sont fortement recommandées (déconnexion automatique, verrouillage…).

CAL-14 : Protection de l'environnement de travail

La liste des actions de chaque profil utilisateur (administration, intervenants de maintenance, utilisateur principal du poste de travail, utilisateur temporaire) doit être établie et protégée par des droits d'accès.

JRN : Journalisation

JRN-01 : Moyens de journalisation des intrusions ou des utilisations frauduleuses

Le SI devra comprendre des moyens (dispositifs et/ou procédure) de journalisation des intrusions ou des utilisations frauduleuses.
Comme il ne sera pas toujours possible de « bloquer » à temps des tentatives d'intrusion, il convient, dans une logique de gestion des risques, de mettre en place les mécanismes de journalisation et de traces permettant en cas d'intrusion réussie, ou de tentative d'intrusion, de disposer :

- des éléments de traces permettant la meilleure identification possible des causes et origines de l'intrusion (remonter vers les éléments menaçants) ;
- des éléments de traces suffisamment fiables permettant à un juge, si nécessaire, en cas de dépôt de plainte, de les accepter en tant que **preuves** de l'intrusion (ou tentative d'intrusion) ou de l'utilisation frauduleuse.

Il convient donc de mettre en place les procédures –avec les moyens techniques et humains nécessaires - d'exploitation des traces et journaux, pour détecter –même après coup- les intrusions et rassembler les éléments de preuve nécessaires.
Ces éléments seront également indispensables pour remettre le système dans son état initial.

JRN-02 : Enregistrement des opérations

En respect du « Principe de proportionnalité » et de la volumétrie, engendrée par l'enregistrement des traces de sécurité, il est fondamental de définir les règles de génération de traces en fonction des éléments recherchés. Les ressources susceptibles d'exploiter utilement ces traces peuvent influer sur ces règles.
La définition et la mise en œuvre de ces systèmes de journalisation devront tenir compte des contraintes législatives et réglementaires concernant notamment le traitement des informations nominatives.

JRN-03 : Constitution de preuves

La constitution d'éléments de preuves informatiques doit respecter la législation et les codes de pratiques en vigueur pour être présentable le cas échant devant un tribunal. Il s'agit en particulier :
- du respect du principe de proportionnalité et transparence ;
- de l'admissibilité de la preuve ;
- de la qualité et de l'exhaustivité de la preuve ;
- du respect de la vie privée ;
- de la qualité de fabrication des éléments de preuve et de leur stockage jusqu'à leur présentation.

JRN-04 : Gestion des traces

La gestion des traces de sécurité comporte plusieurs tâches qu'il faut définir et organiser :
- télécollecte sécurisée des traces de sécurité ;
- archivage des traces ;
- effacement des fichiers des traces obsolètes (obsolescence et durée d'archivage doivent être fixées) ;
- filtrage et analyse des traces ;
- protection des traces contre toute altération ou accès non autorisé ;
- alerte en cas de détection d'événements majeurs ;
- contrôle de l'intégrité des mécanismes de traces ;
- procédure d'exploitation des traces : sachant qu'il est nécessaire de différencier celui qui analyse les traces et l'administrateur du réseau ;
- destruction des traces au-delà du délai légal.

JRN-05 : Alerte de sécurité

Les règles qui suivent la détection d'un incident de sécurité dépendent de la gravité de l'incident. De la classification peut dépendre, la méthode de transmission de l'alerte, les destinataires, la vitesse et la nature de la réaction (*Cf. Gestion d'incidents et gestion de crise*).
De manière générale, tout incident de sécurité pertinent doit être tracé et doit pouvoir être exploitable (identification de l'auteur, de la date, du type d'opération, de la cible…).
Les règles de journalisation et d'analyse d'un incident de sécurité dépendent de la classification de l'incident.

JRN-06 : Analyse des enregistrements des données de contrôle de sécurité

L'exploitation sécurisée du système d'information implique l'enregistrement des données de contrôle de sécurité dans un journal d'audit afin de vérifier que la sécurité est bien respectée, en particulier, pour ce qui concerne les accès au système d'information, qu'ils soient le fait d'utilisateurs, de techniciens ou d'informaticiens.
L'analyse des données de contrôle constitue une vérification a posteriori mais elle peut révéler des tentatives infructueuses de pénétration du système ou, de façon plus insidieuse, la préparation d'une

attaque par récupération de fichiers ou de comptes périmés. Cet examen apporte plus de renseignements que la supervision en direct, à condition qu'il soit exécuté avec régularité et minutie.
Une protection efficace des mécanismes permettant l'enregistrement des données de contrôle est une condition essentielle pour justifier la confiance accordée à l'analyse des enregistrements ; en effet, tout intrus cherche d'abord à inhiber les mécanismes d'enregistrement et à faire disparaître les preuves de son méfait.
La mise en œuvre de journaux d'audits peut être une contrainte en période de forte charge d'exploitation : il faut néanmoins être conscient du risque pour la sécurité que représente leur désactivation, en particulier du risque juridique que prend l'organisme si il sert de plate-forme de rebond dans une attaque.

IGC : Infrastructures de gestion des clés cryptographiques

IGC-01 : Politique de gestion des clés

L'utilisation de clés cryptographiques dans le cadre d'une infrastructure de gestion des clés (IGC) requiert d'établir, de mettre en œuvre, de contrôler et de maintenir une politique de gestion des clés.
Celle-ci prend généralement la forme d'une **politique de certification (PC)** et d'une **déclaration des procédures de certification (DPC)** qui formalisent les exigences relatives à la gestion des clés. Elles traitent notamment de la vie et de l'échange des clés.
Il est préférable que la structure et le contenu de ces documents respectent les normes internationales (telles que le RFC 2527).
On note aussi que l'établissement d'une PC est grandement facilité par la réalisation préalable d'une analyse de risques SSI et l'étude d'autres PC portant sur le même type de besoin (authentification de serveur, authentification de personne, signature, chiffrement…).

IGC-02 : Protection des clés secrètes ou clés privées

Que ce soit pour du chiffrement en confidentialité ou pour de l'authentification ou de la signature, les utilisateurs vont devoir utiliser des clés secrètes ou clés privées. L'assurance d'intégrité et de non-divulgation de ces clés est par construction absolument fondamentale pour la solidité du système mis en place. Une attention spécifique devra être consacrée à ce problème afin de s'assurer que dans chaque cas, les choix et moyens adoptés sont en cohérence avec les enjeux de l'utilisation de ces clés. On pourra ainsi exiger pour les documents classés « sensibles » que tout chiffrement soit réalisé à l'aide d'un dispositif garantissant que la clé privée est stockée et utilisée dans un dispositif matériel (tel une crypto carte à puce), alors qu'une solution logicielle pourrait être acceptable pour d'autres utilisations.

IGC-03 : Certification des clés publiques

Dans un système de cryptographie asymétrique, il existe un risque d'usurpation de la clé publique. La sécurité du système repose sur la fiabilité de l'infrastructure de gestion des clés et notamment sur le processus de certification qui relie un élément (personne, serveur) à une clé publique. Il est essentiel de maîtriser cet aspect en rédigeant une politique de certification.

SCP : Signaux 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 traitement permettent de reconstituer ces informations. Ces signaux sont, de ce fait, dénommés "signaux parasites compromettants".

D'autre part, le développement des systèmes sans fil montre l'apparition de signaux compromettants non parasites, dits "signaux compromettants intentionnels". Ces signaux intentionnels peuvent devenir compromettants si la portée du système dépasse la limite de la zone de sécurité.

La protection contre les signaux compromettants est :
- obligatoire pour le traitement d'informations classifiées de défense (instruction générale interministérielle 900 du 20 juillet 1993)
- recommandée pour le traitement d'informations sensibles (recommandation 901 du 2 mars 1994)

SCP-01 : Zonage

Un des moyens de se protéger contre les signaux compromettants est le zonage.
Il comporte deux volets :
- le zonage des locaux conformément à la directive 495 du 19 septembre 1997,
- le zonage des équipements conformément au guide 430 du 1 juin 1999.

Au vu des résultats du zonage les équipements devront être installés conformément à la directive 485 du 1 septembre 2000.

SCP-02 : Matériel TEMPEST

Un des moyens de se protéger contre les signaux parasites compromettants est l'utilisation de matériel TEMPEST (*Transient ElectroMagnetic Pulse Emanations Standard*).
Ces matériels qui ont fait l'objet de mesures particulières lors de leur développement pour réduire en émission et en conduction leurs émissions de signaux parasites compromettants sont de 4 catégories :
- A (conforme à la norme AMSG 720),
- B (conforme à la norme AMSG 788),
- C (conforme à la norme AMSG 784),
- D ne répondant à aucune des normes ci-avant.

Les matériels devront être installés conformément à la directive 485 du 1 septembre 2000.
Cette solution est à envisager quand le zonage ne permet pas répondre au besoin.

SCP-03 : Cages de Faraday

Un des moyens, plus onéreux, de se protéger contre les signaux parasites compromettants est l'utilisation de cage de Faraday ou la faradisation des locaux.

SCP-04 : Signaux compromettants intentionnels

Les systèmes de transmission sans-fil, lorsqu'ils sont utilisés pour transmettre de l'information deviennent potentiellement des émetteurs de signaux compromettants, lesquels sont dénommés "signaux compromettants intentionnels" et concernent tous les systèmes de transmission sans-fil : infrarouge, radiofréquence, optique…
Pour se protéger contre l'émission de signaux compromettants intentionnels il convient d'appliquer les recommandations de la DCSSI et dans la majorité des cas, d'avoir recourt à un moyen de chiffrement et/ou d'effectuer un zonage des équipements et des locaux.
D'autre part, il convient de prendre conscience du risque associé à l'utilisation de tels moyens dans la transmission d'information.

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