

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT

Version 1.0

HISTORIQUE DES VERSIONS		
DATE	**VERSION**	**ÉVOLUTION DU DOCUMENT**
17/07/2014	1.0	*Publication de la première version de la Politique de sécurité des systèmes d'information de l'Etat.*

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information
SGDSN/ANSSI
Bureau de la maitrise des risques
et de la réglementation
51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

reglementation [at] ssi.gouv.fr

Le présent document a été approuvé par la circulaire du Premier ministre n° 5725/SG (NOR : PRMX1420095C) du 17 juillet 2014. Il est disponible en ligne sur le site institutionnel de l'ANSSI (www.ssi.gouv.fr).

Préambule 5
Première Partie : instruction 7
Article 1. Objet de l'instruction 8
Article 2. Champ d'application 8
Article 3. Date d'entrée en vigueur 8
Article 4. Dispositions transitoires 8
Article 5. Formation des agents 8
Article 6. Pilotage et évolutions de la PSSIE 9
Article 7. Organisation de l'État pour la mise en application de la PSSIE 9
Article 8. Mise en application ministérielle de la PSSIE 10
Article 9. Contrôle et suivi de l'application de la PSSIE 11
Article 10. Traitement des incidents et gestion de crise 12
Deuxième Partie : objectifs et règles 13
Politique, organisation, gouvernance 14
Organisation de la sécurité des systèmes d'information 14
Ressources humaines 16
Gestion des biens 17
Intégration de la SSI dans le cycle de vie des systèmes d'information 18
Gestion des risques et homologation de sécurité 18
Maintien en condition de sécurité des systèmes d'information 18
Produits et services labellisés 19
Gestion des prestataires 19
Sécurité physique 20
Sécurité physique des locaux abritant les SI 20
Sécurité physique des centres informatiques 21
SI de sûreté 22
Sécurité des réseaux 23
Sécurité des réseaux nationaux 23
Sécurité des réseaux locaux 23
Accès spécifiques 24
Sécurité des réseaux sans fil 24
Sécurisation des mécanismes de commutation et de routage 24
Cartographie réseau 25
Architecture des SI 26
Architecture des centres informatiques 26
Exploitation des SI 27
Protection des informations sensibles 27

Sécurité des ressources informatiques 27
Gestion des autorisations et contrôle d'accès logique aux ressources 27
Exploitation sécurisée des ressources informatiques 29
Défense des systèmes d'information 32
Exploitation des centres informatiques 33
Sécurité du poste de travail 35
Sécurisation des postes de travail 35
Sécurisation des imprimantes et copieurs multifonctions 37
Sécurisation de la téléphonie 37
Contrôles de conformité 37
Sécurité du développement des systèmes 38
Développement des systèmes 38
Développements logiciels et sécurité 38
Applications à risques 39
Traitement des incidents 40
Chaînes opérationnelles 40
Continuité d'activité 41
Gestion de la continuité d'activité des SI 41
Conformité, audit, inspection, contrôle 42
Contrôles 42

Préambule

La *politique de sécurité des systèmes d'information de l'État* (PSSIE) contribue à :

- assurer la continuité des activités régaliennes ;
- prévenir la fuite d'informations sensibles ;
- renforcer la confiance des citoyens et des entreprises dans les téléprocédures.

Le présent document définit les mesures de sécurité applicables aux systèmes d'information de l'État. Il s'appuie sur 10 principes stratégiques :

- P1. Lorsque la maîtrise de ses systèmes d'information l'exige, l'administration fait appel à des opérateurs et des prestataires de confiance.
- P2. Tout système d'information de l'État doit faire l'objet d'une analyse de risques permettant une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une démarche d'amélioration continue de la sécurité du système, pendant toute sa durée de vie. Cette démarche doit également permettre de maintenir à jour une cartographie précise des systèmes d'information en service.
- P3. Les moyens humains et financiers consacrés à la sécurité des systèmes d'information de l'État doivent être planifiés, quantifiés et identifiés au sein des ressources globales des systèmes d'information.
- P4. Des moyens d'authentification forte des agents de l'État sur les systèmes d'information doivent être mis en place. L'usage d'une carte à puce doit être privilégié.
- P5. Les opérations de gestion et d'administration des systèmes d'information de l'État doivent être tracées et contrôlées.
- P6. La protection des systèmes d'information doit être assurée par l'application rigoureuse de règles précises. Ces règles font l'objet de la présente PSSIE.
- P7. Chaque agent de l'État, en tant qu'utilisateur d'un système d'information, doit être informé de ses droits et devoirs mais également formé et sensibilisé à la cybersécurité. Les mesures techniques mises en place par l'État dans ce domaine doivent être connues de tous.
- P8. Les administrateurs des systèmes d'information doivent appliquer, après formation, les règles élémentaires d'hygiène informatique.
- P9. Les produits et services acquis par les administrations et destinés à assurer la sécurité des systèmes d'information de l'État doivent faire l'objet d'une évaluation et d'une attestation préalable de leur niveau de sécurité, selon une procédure reconnue par l'ANSSI (« labellisation »).
- P10. Les informations de l'administration considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, sont hébergées sur le territoire national.

La PSSIE s'adresse à l'ensemble des agents de l'État, et tout particulièrement :

- aux autorités hiérarchiques, qui sont responsables de la sécurité des informations traitées au sein de leurs services ;
- aux agents chargés des fonctions de directeurs des systèmes d'information (DSI) ;
- aux personnes chargées de la sécurité et de l'exploitation des systèmes d'information.

La PSSIE énonce des mesures techniques générales, qui constituent un socle minimal. Pour certaines applications, ce socle minimal ne devra pas être considéré comme suffisant. Chaque ministère s'appuiera sur la PSSIE, sur les normes existantes et sur les guides techniques de l'ANSSI pour élaborer des mesures techniques détaillées.

Première Partie : instruction

Article 1. Objet de l'instruction

La présente instruction fixe les conditions de mise en œuvre de la *politique de sécurité des systèmes d'information de l'État* (PSSIE).

Article 2. Champ d'application

La PSSIE s'applique à tous les systèmes d'information (SI) des administrations de l'État : ministères, établissements publics sous tutelle d'un ministère, services déconcentrés de l'Etat et autorités administratives indépendantes. Ces administrations sont dénommées « entités » dans le reste du texte.

La PSSIE concerne l'ensemble des personnes physiques ou morales intervenant dans ces SI, qu'il s'agisse des administrations de l'État et de leurs agents ou bien de tiers (prestataires ou sous-traitants) et de leurs employés.

La PSSIE ne s'impose pas aux systèmes aptes à traiter des informations classifiées de défense, soumis à un corpus réglementaire spécifique. Il appartient aux responsables des entités concernées d'assurer une cohérence entre les dispositions de la présente PSSIE et la réglementation relative à la protection des informations classifiées de défense.

La plupart des règles de sécurité de la PSSIE constituent des règles de base qui devraient pouvoir être appliquées plus largement, au-delà des administrations de l'État.

Article 3. Date d'entrée en vigueur

La PSSIE entre en vigueur le jour de sa publication.

Article 4. Dispositions transitoires

La mise en application de la PSSIE s'effectue selon les règles suivantes :

- les SI des administrations de l'État devront être en conformité totale dans les trois ans suivant la publication de la PSSIE ;
- les entités devront, au 1er janvier 2015, avoir mis en conformité leur politique de sécurité des systèmes d'information (PSSI) et défini un plan d'action. Celui-ci tiendra compte des impacts sur les activités ainsi que des moyens financiers et humains à mettre en œuvre. Il sera établi un calendrier de mise en conformité indiquant les mesures à prendre dans l'immédiat puis à court et à long terme.

Article 5. Formation des agents

Les ministères forment leurs agents chargés d'appliquer la PSSIE. Ces derniers doivent être sensibilisés à la sécurité des SI (SSI) et au respect des règles de sécurité. Les agents exploitant les SI ou assurant des missions en lien avec la SSI font l'objet de formations adaptées, dispensées par les ministères eux-mêmes.

Article 6. Pilotage et évolutions de la PSSIE

La PSSIE est amenée à évoluer dans le temps. Elle pourra notamment être revue afin de prendre en compte :

- les évolutions des menaces et les retours d'expérience des traitements d'incidents ;
- les résultats d'analyses de risques ainsi que les actions découlant de contrôles ou d'inspections ;
- les évolutions des contextes organisationnel, juridique, réglementaire et technologique.

Le suivi de ces évolutions est assuré par un groupe de pilotage présidé par l'ANSSI, composé de représentants de la Présidence de la République, des services du Premier ministre, de la direction interministérielle des systèmes d'information et de communication (DISIC) et des ministères. Ce groupe a pour principales missions :

- de suivre la mise en œuvre de la PSSIE ;
- de proposer des mises à jour ;
- de proposer des documents complémentaires et des directives permettant d'en faciliter ou d'en préciser la mise en œuvre ;
- de suivre les évolutions des documents techniques.

Article 7. Organisation de l'État pour la mise en application de la PSSIE

Une organisation spécifique, destinée à assurer la sécurité et la défense des SI, est mise en place à tous les niveaux de l'État et au sein de chaque entité.

L'ANSSI assure la fonction d'autorité nationale de sécurité et de défense des systèmes d'information, conformément au décret n° 2009-834 du 7 juillet 2009. A ce titre, et dans le cadre des orientations fixées par le Premier ministre, l'ANSSI décide des mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale. Elle coordonne l'action gouvernementale en la matière.

Dans le cadre de ses missions, l'ANSSI :

- est chargée d'élaborer les mesures de protection des SI proposées au Premier ministre et de veiller à leur application. C'est dans ce cadre que la présente PSSIE a été définie ;
- est chargée de mener des inspections des systèmes d'information au sein des services de l'État ;
- établit et tient à jour en permanence la situation des systèmes d'information de l'État, en liaison avec les chaînes fonctionnelles SSI et les directions des systèmes d'information (DSI) des ministères ;
- met en œuvre un centre de détection chargé de la surveillance permanente des réseaux, afin de réagir au plus tôt en cas d'attaque informatique ;

- assure des échanges d'informations avec les constructeurs de matériels, les éditeurs de logiciels ainsi que les opérateurs de communications électroniques et les opérateurs d'importance vitale, afin de mieux comprendre les mécanismes d'attaques, d'étudier les parades possibles et de favoriser la diffusion rapide des correctifs de sécurité.

Au niveau ministériel, l'organisation fonctionnelle en matière de sécurité des SI s'appuie sur le haut fonctionnaire de défense et de sécurité (HFDS) [1], lui-même assisté par un fonctionnaire de sécurité des systèmes d'information (FSSI), ou sur les personnes assurant ces fonctions au sein de la Présidence de la République. Le HFDS est responsable de l'application générale de la PSSIE.

Chaque entité est placée sous la responsabilité d'une autorité qualifiée en sécurité des systèmes d'informations (appelée AQSSI). Cette autorité a notamment pour mission de désigner, sur son périmètre de compétence, les autorités d'homologation de sécurité des SI. L'autorité qualifiée est assistée par un ou plusieurs responsables de la sécurité d'un système d'information (RSSI[2]).

Chaque entité contribue à la protection et la défense des systèmes d'information de l'Etat par la mise en place d'une « chaîne opérationnelle », qui rend compte régulièrement à la chaîne fonctionnelle SSI. Cette chaîne opérationnelle s'appuie notamment sur les équipes directement en charge des SI et a pour mission :

- d'organiser et de mettre en œuvre la capacité opérationnelle de détection et de traitement des incidents ;
- d'assurer la circulation des informations du ministère vers l'ANSSI (incidents, données techniques d'éléments suspects, traces, cartographie) et de l'ANSSI vers le ministère (vulnérabilités, alertes, mesures).

Article 8. Mise en application ministérielle de la PSSIE

Chaque entité met en place un dispositif de gestion des risques pour ses systèmes d'information. Ce dispositif doit permettre une meilleure maîtrise de la sécurité des SI par la mise en œuvre de mesures de protection proportionnées aux enjeux et en adéquation avec les risques encourus.

Cette gestion s'appuie sur un processus régulier d'identification, d'appréciation et de traitement des risques. Ce dispositif doit aussi permettre de s'assurer que les mesures de sécurité sont adaptées. Le choix de ces mesures est effectué en s'assurant que les actions prévues et les coûts engendrés sont proportionnés à la réduction du risque. Les entités peuvent s'appuyer sur les guides et recommandations publiés par l'ANSSI.

Dans ce but, chaque entité :

- met en place une organisation en application de la PSSIE ;
- établit un inventaire de ses systèmes d'information et en évalue la sensibilité ;

[1] *Dans l'ensemble du texte, ce terme désigne également les hauts-fonctionnaire correspondants de défense et de sécurité (HFCDS), ainsi que le haut fonctionnaire de défense du ministère de l'intérieur (HFD).*

[2] *D'autres titres peuvent désigner la fonction de RSSI.*

- conduit une analyse de risques pour ses systèmes d'information, selon la méthode préconisée dans le *référentiel général de sécurité* (RGS) et met en place les mesures de sécurité applicables ;
- conduit des actions de motivation : sensibilisation et formation à la sécurité des systèmes d'information, communication claire sur les sanctions encourues (par exemple, dans les chartes d'usage des SI) ;
- conduit des actions régulières de contrôle du niveau de sécurité de ses systèmes d'information et met en œuvre les actions correctives nécessaires ;
- met en place les processus lui permettant de faire face aux alertes, aux incidents de sécurité et aux situations d'urgence.

Chaque ministère organise et coordonne l'application de la PSSIE au sein de ses entités. Il adapte les règles lorsque cela est nécessaire et justifié, élabore les documents techniques de référence à portée ministérielle et établit un plan d'action pluriannuel, en précisant le cas échéant les étapes successives menant à l'application de la PSSIE.

Il peut être nécessaire, dans certains cas, de déroger à des règles énoncées par la PSSIE. Il appartient alors à l'autorité de l'entité concernée de leur substituer formellement des règles spécifiques. Pour chacune de ces règles, la dérogation, motivée et justifiée, doit être expressément accordée par le HFDS dont dépend l'entité. La décision de dérogation, accompagnée de la justification, est tenue à la disposition de l'ANSSI.

Chaque ministère élabore un bilan annuel comportant :

- une synthèse de l'état d'avancement de la cartographie des SI et de ses mises à jour ;
- des indicateurs permettant d'appréhender la maturité générale en termes de SSI ;
- l'état d'avancement de l'organisation en sécurité et de l'application des règles édictées par la PSSIE ;
- un récapitulatif des actions réalisées pour la mise en conformité à la PSSIE ;
- un récapitulatif des incidents significatifs constatés (accompagnés éventuellement de descriptifs des dispositions mise en œuvre pour les résoudre) ;
- un récapitulatif des exercices menés (avec les enseignements associés et un descriptif synthétique des plans d'actions qui en sont issus).

Article 9. Contrôle et suivi de l'application de la PSSIE

La cohérence globale de la PSSI de chaque ministère, et sa conformité avec la PSSIE, sont de la responsabilité du HFDS.

Le respect de la PSSIE fait l'objet, pour chaque ministère, de contrôles réguliers à différents niveaux, sous la responsabilité de la chaîne fonctionnelle SSI avec compte-rendu au FSSI. Le HFDS désigne les organismes compétents pour la réalisation de ces contrôles.

Au plan interministériel, l'ANSSI vérifie, en particulier lors des inspections ministérielles, la conformité des dispositions prises par les entités avec les exigences de la présente PSSIE.

En complément, des actions de contrôle peuvent être engagées à la suite d'incidents de sécurité majeurs, ou en cas de forte suspicion de non-conformité. L'ANSSI établit le bilan

annuel de la sécurité des systèmes d'information de l'État à partir du résultat des contrôles menés, et du bilan annuel de la SSI établi par chaque ministère.

Article 10. Traitement des incidents et gestion de crise

La rapidité des attaques informatiques rend nécessaire une veille renforcée et une réaction coordonnée des différents acteurs. Afin de rétablir le fonctionnement rapide des activités vitales de l'État, une stratégie de traitement des incidents et de gestion de crise est mise en place.

L'ensemble des acteurs (utilisateurs, responsables d'applications, des réseaux et des centres serveurs ....) doit remonter tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des systèmes d'information d'une entité. Ces incidents de sécurité doivent être signalés rapidement à la chaîne fonctionnelle SSI du ministère. Les incidents jugés significatifs sont remontés à l'ANSSI sous la responsabilité du HFDS.

Une alerte est une action d'information portant à la connaissance des acteurs concernés des situations ou des faits techniques relatifs à la sécurité des systèmes d'information et nécessitant un traitement et une vérification des mesures prises. Les alertes sont issues de la veille permanente effectuée par les CERT internationaux et par l'ANSSI. Les alertes significatives sont signalées par l'ANSSI aux FSSI. Leur prise en compte au sein de chaque ministère est organisée sous la responsabilité du HFDS.

Une situation d'urgence SSI résulte de toute alerte ou incident sur un ou plusieurs SI générant un dysfonctionnement majeur des activités du ministère. Une situation de cette nature impose une forte réactivité et une coordination planifiée des différents acteurs concernés. Il est donc impératif que les ministères prennent en compte la problématique SSI dans leur organisation de gestion de crise et leurs plans de continuité et de reprise d'activité. Ces actions doivent être menées en cohérence avec la planification interministérielle de gestion de crise.

Deuxième Partie : objectifs et règles

Les 10 principes stratégiques à la base de la PSSIE sont traduits en objectifs à atteindre. Des règles permettant de contribuer à la réalisation de chaque objectif sont énoncées.

Politique, organisation, gouvernance

Organisation de la sécurité des systèmes d'information

Objectif 1 : organisation de la SSI. Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

Organisation SSI

ORG-SSI : organisation SSI. Une organisation dédiée à la SSI est déployée à tous les niveaux de l'État, au sein de chaque ministère et au sein de chaque entité suivant les principes de l'IGI 1300. Cette organisation, établie selon les directives du haut fonctionnaire de défense et de sécurité (HFDS), définit les responsabilités internes et à l'égard des tiers, les modalités de coordination avec les autorités externes, ainsi que les modalités d'application des mesures de protection. Des procédures d'applications sont écrites et portées à la connaissance de tous.

Acteurs SSI

ORG-ACT-SSI : identification des acteurs SSI. L'organisation SSI de l'État s'appuie sur des acteurs SSI clairement identifiés, à tous les niveaux d'organisation de l'État. Les acteurs responsables en matière de SSI pour la protection du secret de la défense désignés dans l'IGI 1300, et les agents chargés de les assister dans cette mission, sont responsables de la mise en application générale de la politique SSI de l'État Ils sont référencés dans un annuaire interministériel. Cette chaîne fonctionnelle s'appuie, pour chaque ministère, sur le le HFDS, assisté par un fonctionnaire de sécurité des systèmes d'information (FSSI).

Responsabilités internes

ORG-RSSI : désignation du responsable SSI. Chaque autorité qualifiée en sécurité des systèmes d'information (AQSSI) s'appuie sur un ou plusieurs responsables de la sécurité des systèmes d'information (RSSI), chargé(s) de l'assister dans le pilotage et la gestion de la SSI. Des « correspondants locaux SSI » peuvent être désignés, le cas échéant, afin de constituer un relais du RSSI. Le RSSI d'une entité fait valider les mesures d'application de la PSSIE par l'autorité qualifiée et veille à leur application. Des dénominations alternatives des fonctions citées ci-dessus peuvent être utilisées si nécessaire.

ORG-RESP : formalisation des responsabilités. Une note d'organisation fixe la répartition au sein de chaque entité et au niveau local des responsabilités et rôles en matière de SSI. Cette note sera, le plus souvent, proposée par le RSSI et validée par l'autorité qualifiée.

Responsabilités vis-à-vis des tiers

ORG-TIERS : gestion contractuelle des tiers. Le RSSI coordonne les actions permettant l'intégration des clauses liées à la SSI dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques.

PSSI ministérielle

ORG-PIL-PSSIM : définition et pilotage de la PSSI ministérielle. Chaque ministère établit une politique SSI ministérielle, sous la responsabilité du HFDS. Cette politique reprend le socle commun établi par la présente PSSIE. Une structure de pilotage de la PSSI

ministérielle est définie. Cette structure est chargée de sa mise en place, de son évolution, de son suivi et de son contrôle.

Application des mesures de sécurité au sein de l'entité

ORG-APP-INSTR : application de l'instruction dans l'entité. Le RSSI planifie les actions de mise en application de la PSSIE. Il rend compte régulièrement de la mise en application des mesures de sécurité auprès de son autorité qualifiée et du FSSI.

ORG-APP-DOCS : formalisation de documents d'application. Le RSSI formalise et tient à jour les documents d'application, approuvés par l'autorité qualifiée, permettant la mise en œuvre des mesures de la PSSIE sur son périmètre.

Ressources humaines

Objectif 2 : ressources humaines. Faire des personnes les maillons forts des SI de l'État.

Utilisateurs

RH-SSI : charte d'application SSI. Une charte d'application de la politique SSI, récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques et élaborée sous le pilotage de la chaîne fonctionnelle SSI, est communiquée à l'ensemble des agents de chaque entité. Cette charte doit être opposable juridiquement et, si possible, intégrée au règlement intérieur de l'entité. Le personnel non permanent (stagiaires, intérimaires, prestataires…) est informé de ses devoirs dans le cadre de son usage des SI de l'État.

Personnel permanent

RH-MOTIV : choix et sensibilisation des personnes tenant les postes clés de la SSI. Une attention particulière doit être portée au recrutement des personnes-clés de la SSI : RSSI, correspondants SSI locaux et administrateurs de sécurité. Les RSSI et leurs correspondants SSI locaux doivent être spécifiquement formés à la SSI. Les administrateurs des SI doivent être régulièrement sensibilisés aux devoirs liés à leur fonction, et doivent veiller à respecter ces exigences dans le cadre de leurs activités quotidiennes.

RH-CONF : personnels de confiance. Toutes les personnes manipulant des informations sensibles doivent le faire avec une attention et une probité particulière, dans le respect des textes en vigueur. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont rappelées.

RH-UTIL : sensibilisation des utilisateurs des systèmes d'information. Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant, et motivé à leur respect. Il doit être formé à l'utilisation des outils de travail conformément aux règles SSI.

Mouvement de personnel

RH-MOUV : gestion des arrivées, des mutations et des départs. Une procédure permettant de gérer les arrivées, les mutations et les départs des collaborateurs dans les SI doit être formalisée, et appliquée strictement. Cette procédure doit couvrir au minimum *:*

- *la gestion/révocation des comptes et des droits d'accès aux SI, y compris pour les partenaires et les prestataires externes ;*
- *la gestion du contrôle d'accès aux locaux ;*
- *la gestion des équipements mobiles ;*
- *la gestion du contrôle des habilitations.*

Personnel non permanent

RH-NPERM : gestion du personnel non permanent (stagiaires, intérimaires, prestataires…). Les règles de la PSSIE s'appliquent à tout personnel non permanent utilisateur d'un SI d'une administration de l'État. Les dispositions contractuelles préexistantes régissant l'emploi de ce personnel sont amendées si nécessaire. Pour tout personnel non permanent, un tutorat par un agent permanent est mis en place, afin de l'informer de ces règles et d'en contrôler l'application.

Gestion des biens

Objectif 3 : cartographie des SI. Tenir à jour une cartographie détaillée et complète des SI.

GDB-INVENT : inventaire des ressources informatiques. Chaque entité établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire est tenu à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle. Il comprend la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes. Il est constitué d'une base de données de configuration, maintenue à jour et tenue à disposition du RSSI.
L'historique des attributions des biens inventoriés doit être conservé, dans le respect de la législation.

GDB-CARTO : cartographie. La cartographie précise les centres informatiques, les architectures des réseaux (sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées) et qualifie le niveau de sécurité attendu. Cette cartographie est maintenue à jour et tenue à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle.

Objectif 4 : qualification et protection de l'information. Qualifier l'information de façon à adapter les mesures de protection.

GDB-QUALIF-SENSI : qualification des informations. La sensibilité de toute information doit être évaluée. Le marquage systématique des documents, en fonction du niveau de sensibilité, est fortement recommandé.

GDB-PROT-IS : protection des informations. L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction.

Intégration de la SSI dans le cycle de vie des systèmes d'information

Gestion des risques et homologation de sécurité

Objectif 5 : risques. Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information.

INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d'information. Tout système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise par l'autorité d'homologation (désignée par l'autorité qualifiée), le cas échéant après avis de la commission d'homologation. Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi.

Maintien en condition de sécurité des systèmes d'information

Objectif 6 : maintien en condition de sécurité. Gérer dynamiquement les mesures de protection, tout au long de la vie du SI.

INT-SSI : intégration de la sécurité dans les projets. La sécurité des systèmes d'information doit être prise en compte dans toutes les phases des projets informatiques, sous le contrôle de l'autorité d'homologation, de la conception et de la spécification du système jusqu'à son retrait du service.

INT-QUOT-SSI : mise en œuvre au quotidien de la SSI. La sécurité des systèmes d'information se traite au quotidien par des pratiques d'hygiène informatique. Des procédures écrites définissent les actes élémentaires du maintien en condition de sécurité lors des phases de conception, évolution ou retrait d'un système.

INT-TDB : créer un tableau de bord SSI. Un tableau de bord SSI est mis en place et tenu à jour. Il fournit au RSSI et aux autorités une vision générale du niveau de sécurité et de son évolution, rendant ainsi plus efficace le pilotage de la SSI. Au niveau stratégique, le tableau de bord SSI permet de suivre l'application de la politique de sécurité et de disposer d'éléments propres à qualifier les ressources devant être allouées à la SSI. Au niveau du pilotage, la mise en place de ce tableau de bord permet de contrôler la réalisation d'objectifs opérationnels, d'améliorer la qualité de service et de détecter au plus tôt les retards dans la réalisation de certains objectifs de sécurité.

Produits et services labellisés

Objectif 7 : produits et services qualifiés ou certifiés. Utiliser des produits et services dont la sécurité est évaluée et attestée selon des procédures reconnues par l'ANSSI, afin de renforcer la protection des SI.

INT-AQ-PSL : acquisition de produits et services de confiance. Lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI doivent être utilisés.

Gestion des prestataires

Objectif 8 : maîtrise des prestations. Veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers.

INT-PRES-CS : clauses de sécurité. Toute prestation dans le domaine des SI est encadrée par des clauses de sécurité. Ces clauses spécifient les mesures SSI que le prestataire doit respecter dans le cadre de ses activités.

INT-PRES-CNTRL : suivi et contrôle des prestations fournies. Le maintien d'un niveau de sécurité au cours du temps nécessite un double contrôle :

- *l'un, effectué périodiquement par l'équipe encadrant la prestation, qui porte sur les actions du sous-traitant et la conformité au cahier des charges ;*
- *l'autre, effectué par une équipe externe, qui porte sur la pertinence du cahier des charges en amont des projets, la conformité des réponses apportées par le sous-traitant en phase de recette et le niveau de sécurité global obtenu en production.*

INT-REX-AR : analyse de risques. Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

INT-REX-HB : hébergement. L'hébergement des données sensibles de l'administration sur le territoire national est obligatoire, sauf accord du HFDS, et dérogation dûment motivée et précisée dans la décision d'homologation.

INT-REX-HS : hébergement et clauses de sécurité. Tout contrat d'hébergement détaille les dispositions mises en œuvre pour prendre en compte la SSI. Ce sont notamment les mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes, etc.).

Sécurité physique

Sécurité physique des locaux abritant les SI

Règles générales

Objectif 9 : sécurité physique des locaux abritant les SI. Inscrire la sécurisation physique des SI dans la sécurisation physique des locaux et dans les processus associés.

PHY-ZONES : découpage des sites en zones de sécurité. Un découpage des sites en zones physiques de sécurité doit être effectué, en liaison avec le RSSI, les correspondants locaux SSI et les services en charge : de l'immobilier, de la sécurité et des moyens généraux. Pour chaque zone de sécurité, des critères précis d'autorisation d'accès sont établis.

Règles de sécurité s'appliquant aux zones d'accueil du public

PHY-PUBL : accès réseau en zone d'accueil du public. Tout accès réseau installé dans une zone d'accueil du public doit être filtré ou isolé du reste du réseau informatique de l'entité.

PHY-SENS : protection des informations sensibles au sein des zones d'accueil. Le traitement d'informations sensibles au sein des zones d'accueil est à éviter. Si un tel traitement est strictement nécessaire, il doit rester ponctuel et exceptionnel. Des mesures particulières sont alors adoptées, notamment en matière de protection audiovisuelle, ainsi qu'en matière de protection des informations stockées sur les supports.

Règles de sécurité complémentaires s'appliquant aux locaux techniques

PHY-TECH : sécurité physique des locaux techniques. L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, ou des équipements de réseau et de téléphonie, doit être physiquement protégé.

PHY-TELECOM : protection des câbles électriques et de télécommunications. Il convient de protéger le câblage réseau contre les dommages et les interceptions des communications qu'ils transmettent. En complément, les panneaux de raccordements et les salles des câbles doivent être placés en dehors des zones d'accueil du public et leur accès doit être contrôlé.

PHY-CTRL : contrôles anti-piégeages. Sur les SI particulièrement sensibles, il convient de mener des contrôles anti-piégeages réguliers, effectués par du personnel formé. Il peut être fait appel à des services spécialisés (opérations dites de « dépoussiérage »).

Sécurité physique des centres informatiques

Objectif 10 : sécurité physique des centres informatiques. Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abrités.

Règles générales

PHY-CI-LOC : découpage des locaux en zones de sécurité. Un découpage du centre informatique en zones physiques de sécurité doit être effectué, en liaison avec le RSSI et les services en charge de l'immobilier, de la sécurité et des moyens généraux. Des règles doivent fixer les conditions d'accès à ces différentes zones.

PHY-CI-HEBERG : convention de service en cas d'hébergement tiers. Dans le cas où un tiers gère tout ou partie des locaux du centre informatique, une convention de service, définissant les responsabilités mutuelles en matière de sécurité, doit être établie entre ce tiers et l'entité ou le ministère.

Règles de sécurité complémentaires s'appliquant aux zones internes et restreintes

PHY-CI-CTRLACC : contrôle d'accès physique. L'accès aux zones internes (autorisées uniquement au personnel du centre informatique ou aux visiteurs accompagnés) et restreintes (autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) doit reposer sur un dispositif de contrôle d'accès physique. Ce dispositif doit s'appuyer sur des produits qualifiés, lorsqu'ils sont disponibles, et bénéficier d'un maintien en condition de sécurité rigoureux.

PHY-CI-MOYENS : délivrance des moyens d'accès physique. La délivrance des moyens d'accès physique doit respecter un processus formel permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles (entretien ou réparation des bâtiments, des équipements non informatiques, nettoyage, visiteurs, …), intervient systématiquement et impérativement sous surveillance permanente.

PHY-CI-TRACE : traçabilité des accès. Une traçabilité des accès, par les visiteurs externes, aux zones restreintes doit être mise en place. Ces traces sont alors conservées un an, dans le respect des textes protégeant les données personnelles.

Règles de sécurité complémentaires s'appliquant aux salles informatiques et aux locaux techniques

PHY-CI-ENERGIE : local énergie. L'alimentation secteur des équipements devra être conforme aux règles de l'art, de façon à se prémunir des atteintes à la sécurité des personnes et équipements liées à un défaut électrique.

PHY-CI-CLIM : climatisation. Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique doit être installé. Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement. Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

PHY-CI-INC : lutte contre l'incendie. L'installation de matériel de protection contre le feu est

obligatoire. Des procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu ne doit être entreposé dans ces locaux.

PHY_CI-EAU : lutte contre les voies d'eau. Une étude sur les risques dus aux voies d'eau doit être réalisée. Cette étude doit notamment prendre en compte le risque de fuite sur un collecteur d'eau douce.

SI de sûreté

Objectif 11 : sécurité du SI de sûreté. Traiter de manière globale la sécurité des systèmes d'information et de communication qui assurent la sûreté d'un site.

Les sites importants (reconnus le cas échéant comme points d'importance vitale) s'appuient sur des services support des activités de sûreté physique. Dans ce cadre, l'appellation « services de systèmes d'information et de communication de sûreté » regroupe :

- les services support des activités de contrôle d'accès et détection d'intrusion (CTA), permettant au personnel de sûreté :
  - d'authentifier, d'autoriser et de tracer l'accès à une ressource physique (contrôle d'accès),
  - de détecter, d'alerter et de tracer en cas de tentative d'accès non autorisé (détection d'intrusion).
- les services support des activités de vidéo-surveillance (VS), fournissant au personnel de sûreté un système de caméras disposées sur l'ensemble du site, de transport des flux vidéo, d'enregistrement, d'archivage et de visionnage de ces vidéos ;
- les services support de la gestion technique des bâtiments (GTB), permettant de superviser et de gérer l'ensemble des équipements des bâtiments du site, et d'avoir une vue globale de l'état de ces bâtiments ;
- les services support de la sécurité incendie (INC), regroupant l'ensemble des moyens informatiques mis en œuvre pour détecter, informer, intervenir et/ou évacuer tout ou partie du site en cas d'incendie.

PHY-SI-SUR : sécurisation du SI de sûreté. Pour les sites physiques considérés comme importants, des mesures de protection doivent être définies et appliquées en se basant sur les conclusions d'une analyse de risques. L'analyse de risques conduit à la désignation des briques essentielles dont il faut assurer la protection contre des actes malveillants. Un système de gestion de la sécurité du SI de sûreté (s'inspirant de la norme ISO 27001) assure le maintien en condition de sécurité. L'emploi de produits labellisés, quand ils existent, est fortement recommandé.

Sécurité des réseaux

Sécurité des réseaux nationaux

Objectif 12 : usage sécurisé des réseaux nationaux. Utiliser les infrastructures nationales, en respectant les règles de sécurité qui leur sont attachées.

RES-MAITRISE : systèmes autorisés sur le réseau. Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'une entité.

RES-INTERCO : interconnexion avec des réseaux externes. Toute interconnexion entre les réseaux locaux d'une entité et un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via les infrastructures nationales.

RES-ENTSOR : mettre en place un filtrage réseau pour les flux sortants et entrants. Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées.

RES-PROT : protection des informations. Les accès à Internet passent obligatoirement à travers les passerelles nationales. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par chiffrement adapté.

Sécurité des réseaux locaux

Objectif 13 : usage sécurisé des réseaux locaux. Maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseau actifs.

RES-CLOIS : cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes. Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.

RES-INTERCOGEO : interconnexion des sites géographiques locaux d'une entité. L'interconnexion au niveau local de réseaux locaux d'une entité n'est possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions dédiées à cet effet, et de passerelles sécurisées et validées par le HFDS.

RES-RESS : cloisonnement des ressources en cas de partage de locaux. Dans le cas où une entité partage des locaux (bureaux ou locaux techniques) avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Si le cloisonnement n'est pas physique, les mesures prises doivent être validées par le ou les HFDS concernés.

Accès spécifiques

Objectif 14 : accès spécifiques. Ne pas porter atteinte à la sécurité du SI par le déploiement d'accès non supervisés.

RES-INTERNET-SPECIFIQUE : cas particulier des accès spécifiques dans une entité. Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage métier ne peuvent être mis en place que sur dérogation dûment justifiée, et sur des machines isolées physiquement et séparées du réseau de l'entité, après validation préalable de l'autorité d'homologation.

Sécurité des réseaux sans fil

Objectif 15 : usage sécurisé des réseaux sans fil. Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.

RES-SSFIL : mise en place de réseaux sans fil. Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, validées par le HFDS concerné, doivent être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio. À défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des SI manipulant des données sensibles est proscrit.

Sécurisation des mécanismes de commutation et de routage

Objectif 16 : sécurité des mécanismes de commutation et de routage. Configurer les mécanismes de commutation et de routage pour se protéger des attaques.

RES-COUCHBAS : implanter des mécanismes de protection contre les attaques sur les couches basses. Une attention particulière doit être apportée à l'implantation des protocoles de couches basses, de façon à se prémunir des attaques usuelles par saturation ou empoisonnement de cache. Cela concerne, par exemple, le protocole ARP.

RES-ROUTDYN : surveiller les annonces de routage. Lorsque l'utilisation de protocoles de routage dynamiques est nécessaire, celle-ci doit s'accompagner de la mise en place d'une surveillance des annonces de routage, et de procédures permettant de réagir rapidement en cas d'incidents.

RES-ROUTDYN-IGP : configurer le protocole IGP de manière sécurisée. Le protocole de routage dynamique de type IGP doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. La configuration du protocole de routage dynamique doit systématiquement s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY.

RES-ROUTDYN-EGP : sécuriser les sessions EGP. Lors de la mise en place d'une session EGP avec un pair extérieur sur un média partagé, cette session doit s'accompagner d'un mot de passe de type message-digest-key.

RES-SECRET : modifier systématiquement les éléments d'authentification par défaut des équipements et services. Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.

RES-DURCI : durcir les configurations des équipements de réseaux. Les équipements de réseaux (comme les routeurs) doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et certificats, la désactivation des interfaces et services inutiles, ainsi que la mise en place de mécanismes de protection du plan de contrôle.

Cartographie réseau

Objectif 17 : cartographie réseau. Tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions.

RES-CARTO : élaborer les documents d'architecture technique et fonctionnelle. L'architecture réseau du système d'information doit être décrite et formalisée à travers des schémas d'architecture, et des configurations, maintenus au fil des évolutions apportées au SI. Les documents d'architecture sont sensibles et font l'objet d'une protection adaptée. La cartographie réseau s'insère dans la cartographie globale des SI.

Architecture des centres informatiques

Objectif 18 : architecture sécurisée des centres informatiques. Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

ARCHI-HEBERG : principes d'architecture de la zone d'hébergement. D'une manière générale, l'architecture des infrastructures des centres informatiques est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité. Le principe de défense en profondeur doit être respecté, en particulier par la mise en œuvre successive de « zones démilitarisées » (DMZ), d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.

ARCHI-STOCKCI : architecture de stockage et de sauvegarde. Le réseau de stockage/sauvegarde pour les besoins des centres informatiques repose sur une architecture dédiée à cet effet.

ARCHI-PASS : passerelle Internet. Les interconnexions Internet passent obligatoirement par les passerelles nationales homologuées.

Exploitation des SI

Protection des informations sensibles

Objectif 19 : protection des informations sensibles. Définir et mettre en œuvre des mesures de protection renforcées pour les informations sensibles.

EXP-PROT-INF : protection des informations sensibles en confidentialité et en intégrité. Des mesures doivent être mises en œuvre afin de garantir la protection des informations sensibles en confidentialité et en intégrité. A défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées à l'aide d'un moyen de chiffrement labellisé.

Sécurité des ressources informatiques

Objectif 20 : surveillance et configuration des ressources informatiques. Durcir les configurations des ressources informatiques, et surveiller les interventions opérées sur celles-ci.

EXP-TRAC : traçabilité des interventions sur le système. Les interventions de maintenance sur les ressources informatiques de l'entité doivent être tracées par le service informatique, et ces traces doivent être accessibles au correspondant SSI local durant au moins un an.

EXP-CONFIG : configuration des ressources informatiques. Les systèmes d'exploitation et les logiciels doivent faire l'objet d'un durcissement. Les configurations et mises à jour sont appliquées dans le strict respect des guides ou procédures en vigueur dans l'entité ou, par défaut, en vigueur au niveau central.

EXP-DOC-CONFIG : documentation des configurations. La configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.

Gestion des autorisations et contrôle d'accès logique aux ressources

Objectif 21 : autorisations et contrôles d'accès. Authentifier les usagers et contrôler leurs accès aux ressources des SI de l'État, en fonction d'une politique explicite d'autorisations.

Contrôle des accès logiques

EXP-ID-AUTH : identification, authentification et contrôle d'accès logique. L'accès à toute ressource non publique doit nécessiter une identification et une authentification individuelle de l'utilisateur. Dans le cas de l'accès à des données sensibles, des moyens d'authentification forte doivent être utilisés. A cette fin, l'usage d'une carte à puce doit être privilégié. Le contrôle d'accès doit être géré et s'appuyer sur un processus formalisé en cohérence avec la gestion des ressources humaines.

EXP-DROITS : droits d'accès aux ressources. Après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes suivants : besoin d'en connaître (chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès), moindre privilège (chaque utilisateur accède aux ressources avec le

minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui).

EXP-PROFILS : gestion des profils d'accès aux applications. Les applications manipulant des données sensibles doivent permettre une gestion fine par profils d'accès. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

Processus d'autorisation

EXP-PROC-AUTH : autorisations d'accès des utilisateurs. Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI, qu'elle soit locale ou nationale, doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ du personnel.

EXP-REVUE-AUTH : revue des autorisations d'accès. Une revue des autorisations d'accès doit être réalisée annuellement sous le contrôle du RSSI, le cas échéant avec l'appui du correspondant local SSI.

Gestion des authentifiants

EXP-CONF-AUTH : confidentialité des informations d'authentification. Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des données sensibles.

EXP-GEST-PASS : gestion des mots de passe. Les utilisateurs ne doivent pas stocker leurs mots de passe en clair (par exemple dans un fichier) sur leur poste de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.

EXP-INIT-PASS : initialisation des mots de passe. Chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique. Si les circonstances l'imposent, un mot de passe plus simple mais à usage unique peut être envisagé.

EXP-POL-PASS : politiques de mots de passe. Les règles de gestion et de protection des mots de passe donnant accès aux applications et infrastructures nationales, telles qu'édictées par les maîtrises d'ouvrage nationales, doivent être respectées dans chaque entité. Pour les ressources dont la politique de mots de passe est gérée localement, les recommandations de l'ANSSI doivent être appliquées pour tous les comptes.

EXP-CERTIFS : utilisation de certificats électroniques. L'utilisation de certificats électroniques doit respecter les règles édictées par le RGS.

EXP-QUAL-PASS : contrôle systématique de la qualité des mots de passe. Des moyens techniques permettant d'imposer la politique de mots de passe (par exemple pour s'assurer du respect de l'éventuelle obligation relative à l'usage de caractères spéciaux) doivent être mis en place. A défaut, un contrôle périodique des paramètres techniques relatifs aux mots de passe doit être réalisé.

Gestion des authentifiants d'administration

EXP-SEQ-ADMIN : séquestre des authentifiants « administrateur ». Les authentifiants permettant l'administration des ressources des SI doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. L'authentifié doit être informé de l'existence de ces opérations de gestion, de leurs finalités et limites. Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit. Les informations d'authentification bénéficiant d'un moyen de protection physique (notamment carte à puce) n'ont, par défaut, pas besoin d'être

l'objet d'opérations de séquestre de la part d'autres personnels que l'authentifié lui-même.

EXP-POL-ADMIN : politique de mots de passe « administrateurs ». Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.

EXP-DEP-ADMIN : gestion du départ d'un administrateur des SI. En cas de départ d'un administrateur disposant de privilèges sur des composants des SI, les comptes individuels dont il disposait doivent être immédiatement désactivés. Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés (exemples : mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur).

Exploitation sécurisée des ressources informatiques

Objectif 22 : sécurisation de l'exploitation. Fournir aux administrateurs les outils nécessaires à l'exercice des tâches SSI et configurer ces outils de manière sécurisée.

Administration des systèmes

EXP-RESTR-DROITS : restriction des droits. Sauf exception dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droits d'administration.

EXP-PROT-ADMIN : protection des accès aux outils d'administration. L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès.

EXP-HABILIT-ADMIN : habilitation des administrateurs. L'habilitation des administrateurs s'effectue selon une procédure validée par l'autorité d'homologation. Le nombre de personnes habilitées pour des opérations d'administration doit être connu et validé par l'autorité d'homologation.

EXP-GEST-ADMIN : gestion des actions d'administration. Les opérations d'administration doivent être tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration.

EXP-SEC-FLUXADMIN : sécurisation des flux d'administration. Les opérations d'administration sur les ressources locales d'une entité doivent s'appuyer sur des protocoles sécurisés. Un réseau dédié à l'administration des équipements, ou au moins un réseau logiquement séparé de celui des utilisateurs, doit être utilisé. Les postes d'administrateurs doivent être dédiés et ne doivent pas pouvoir accéder à Internet.

EXP-CENTRAL : centraliser la gestion du système d'information. Afin de gérer efficacement un grand nombre de postes d'utilisateurs, de serveurs ou d'équipements réseau, les administrateurs doivent utiliser des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur le système d'information.

EXP-SECX-DIST : sécurisation des outils de prise de main à distance. La prise de main à distance d'une ressource informatique locale ne doit être réalisable que par les agents autorisés par l'équipe locale chargée des SI, sur les ressources informatiques de leur périmètre. Des mesures de sécurité spécifiques doivent être définies et respectées.

Administration des domaines

EXP-DOM-POL : définir une politique de gestion des comptes du domaine. Une politique explicite de gestion des comptes du domaine doit être documentée.

EXP-DOM-PASS : configurer la stratégie des mots de passe des domaines . La politique de gestion des mots de passe doit être conçue de façon à protéger contre les attaques par essais successifs de mots de passe. Une complexité minimale dans le choix des mots de passe doit être imposée aux utilisateurs.

EXP-DOM-NOMENCLAT : définir et appliquer une nomenclature des comptes du domaine. La gestion des comptes doit s'appuyer sur une nomenclature adaptée, afin de pouvoir distinguer selon leur usage : comptes d'utilisateur standard, comptes d'administration (domaine, serveurs, postes de travail) et comptes de service.

EXP-DOM-RESTADMIN : restreindre au maximum l'appartenance aux groupes d'administration du domaine. L'appartenance aux groupes du domaine ADMINISTRATEURS DE L'ENTREPRISE et ADMINISTRATEURS DU DOMAINE n'est nécessaire que dans de très rares cas. Les opérations les plus courantes doivent être effectuées avec des comptes du domaine membres des groupes locaux d'administration des ordinateurs ou ayant une délégation d'administration.

EXP-DOM-SERV : maîtriser l'utilisation des comptes de service. Les comptes de service ont la particularité d'avoir généralement leurs mots de passe inscrits en dur dans des applications ou dans des systèmes. Afin de pouvoir être en mesure de changer ces mots de passe en urgence, il est nécessaire de maîtriser leur utilisation.

EXP-DOM-LIMITSERV : limiter les droits des comptes de service. Les comptes de service doivent faire l'objet d'une restriction des droits, en suivant le principe du moindre privilège.

EXP-DOM-OBSOLET : désactiver les comptes du domaine obsolètes. Il est nécessaire de désactiver immédiatement, voire de supprimer, les comptes obsolètes, que ce soient des comptes d'utilisateur (administrateur, de service ou utilisateur standard) ou des comptes de machine.

EXP-DOM-ADMINLOC : améliorer la gestion des comptes d'administrateur locaux. Afin d'empêcher la ré-utilisation des empreintes d'un compte utilisateur local d'une machine à une autre, il faut soit utiliser des mots de passe différents pour les comptes locaux d'administration, soit interdire la connexion à distance via ces comptes.

Envoi en maintenance et mise au rebut

EXP-MAINT-EXT : maintenance externe. Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique. Les opérations de chiffrement doivent faire appel à des produits qualifiés. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.

EXP-MIS-REB : mise au rebut. Lorsqu'une ressource informatique est amenée à quitter définitivement l'entité, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.

Lutte contre les codes malveillants

EXP-PROT-MALV : protection contre les codes malveillants. Des logiciels de protection contre les codes malveillants, appelés communément antivirus, doivent être installés sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail de l'entité. Ces logiciels de protection doivent être distincts pour ces trois catégories au moins, et le dépouillement de leurs journaux doit être corrélé.

EXP-GES-ANTIVIR : gestion des événements de sécurité de l'antivirus. Les événements de sécurité de l'antivirus doivent être remontés sur un serveur national pour analyse statistique et gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

EXP-MAJ-ANTIVIR : mise à jour de la base de signatures. Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail par un dispositif prescrit par les services centraux.

EXP-NAVIG : configuration du navigateur Internet. Le navigateur déployé par l'équipe locale chargée des SI sur l'ensemble des serveurs et des postes de travail nécessitant un accès Internet ou Intranet doit être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).

Mise à jour des systèmes et des logiciels

EXP-POL-COR : définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité. Le maintien dans le temps du niveau de sécurité d'un système d'information impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à chaque système ou applicatif doit être défini, et adapté suivant les contraintes et le niveau d'exposition du système.

EXP-COR-SEC : déploiement des correctifs de sécurité. Les correctifs de sécurité des ressources informatiques locales doivent être déployés par l'équipe locale chargée des SI en s'appuyant sur les préconisations et outils proposés par les services centraux.

EXP-OBSOLET : assurer la migration des systèmes obsolètes. L'ensemble des logiciels utilisés sur le système d'information doit être dans une version pour laquelle l'éditeur assure le support, et tenu à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.

EXP-ISOL : isoler les systèmes obsolètes restants. Il est nécessaire d'isoler les systèmes obsolètes, gardés volontairement pour assurer un maintien en condition opérationnelle des projets, et pour lesquels une migration n'est pas envisageable. Chaque fois que cela est possible, cette isolation doit être effectuée au niveau du réseau (filtrage strict), des éléments d'authentification (qui ne doivent pas être communs avec le reste du SI) et des applications (pas de ressources partagées avec le reste du SI).

Journalisation

EXP-JOUR-SUR : journalisation des alertes. Chaque système doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité. Ces traces doivent être conservées de manière sûre.

EXP-POL-JOUR : définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces. Une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie par le RSSI, validée par l'autorité qualifiée, et mise en œuvre. Le niveau de sécurité d'un système d'information dépend en grande partie de la

capacité de ses exploitants et administrateurs à détecter les erreurs, dysfonctionnements et tentatives d'accès illicites survenant sur les éléments qui le composent.

EXP-CONS-JOUR : conservation des journaux. Les journaux des événements de sécurité doivent être conservés sur douze mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

Défense des systèmes d'information

Objectif 23 : défense des systèmes d'information. Défendre les SI nécessite une vigilance de tous, et des actions permanentes.

EXP-GES-DYN : gestion dynamique de la sécurité. L'équipe en charge de la SSI doit procéder, notamment via l'analyse des journaux, à la surveillance des comportements anormaux au sein du système d'information, et à la surveillance des flux d'entrée et de sortie du système d'information.

Gestion des matériels informatiques fournis à l'utilisateur

EXP-MAIT-MAT : maîtrise des matériels. Les postes de travail - y compris dans le cas d'une location - sont fournis à l'utilisateur par l'entité, gérés et configurés sous la responsabilité de l'entité. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'entité (qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur des équipements et des réseaux professionnels est interdite.

EXP-PROT-VOL : rappel des mesures de protection contre le vol. Les postes fixes bénéficient des mesures de protection physique offertes au titre de la directive de sécurité physique de la présente PSSIE. Chaque utilisateur doit veiller à la sécurité des supports amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr. Il est recommandé de chiffrer les données contenues sur ces supports. Les supports contenant des données sensibles doivent être stockés dans des meubles fermant à clef.

EXP-DECLAR-VOL : déclarer les pertes et vols. Toute perte ou vol d'une ressource d'un système d'information doit être déclarée au RSSI.

EXP-REAFFECT : réaffectation de matériels informatiques. Une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être mise en place et validée par le RSSI. Elle doit définir les conditions de recours à un effacement des données.

Nomadisme

EXP-NOMAD-SENS : déclaration des équipements nomades aptes à traiter des informations sensibles. L'autorité d'homologation du SI valide les usages possibles des équipements nomades vis-à-vis du traitement des informations sensibles ; les usages non explicitement autorisés sont interdits.

EXP-ACC-DIST : accès à distance au système d'information de l'organisme. Les utilisateurs distants doivent s'authentifier sur le réseau de l'entité en utilisant une méthode conforme à l'annexe B3 du RGS.

Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles

EXP-IMP-SENS : impression des informations sensibles. Les impressions d'informations sensibles doivent être effectuées selon une procédure prédéfinie, garantissant le contrôle de l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé.

EXP-IMP-2 : sécurité des imprimantes et copieurs multifonctions. Les imprimantes et copieurs multifonctions sont des ressources informatiques à part entière qui doivent être gérées en tant que telles. Elles ne doivent pas pouvoir communiquer avec l'extérieur.

Exploitation des centres informatiques

Objectif 24 : exploitation sécurisée des centres informatiques. Exploiter de manière sécurisée les centres informatiques en s'appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision.

Sécurité des ressources informatiques

Les règles suivantes sont présentées selon le modèle qui structure l'architecture des applications selon trois Tiers (Présentation – Application – Données).

Les socles techniques déployés dans chaque Tiers – en particulier les règles de sécurité à appliquer – sont précisés dans un cadre de cohérence technique ministériel (CCT).

EXP-CI-OS : systèmes d'exploitation. Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque. Une attention particulière doit être apportée aux comptes administrateurs.

EXP-CI-LTP : logiciels en Tiers Présentation. La mise en œuvre d'une configuration renforcée est obligatoire sur les logiciels déployés pour le tiers présentation (ex : serveur Web, Reverse Proxy).

EXP-CI-LTA : logiciels en Tiers Application. Des règles de développement sécurisé, et les configurations des logiciels en Tiers Application doivent être fixées et appliquées. Elles sont détaillées dans le cadre de cohérence technique (CCT).

EXP-CI-LTD : logiciels en Tiers Données. Des règles très strictes (restrictions d'accès, interdictions de connexions, gestion des privilèges) s'appliquent aux logiciels en tiers données. Ces règles doivent être détaillées dans le cadre de cohérence technique (CCT).

EXP-CI-PROTFIC : passerelle d'échange de fichiers. Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS...).

EXP-CI-MESSTECH : messagerie technique. Pour satisfaire les besoins d'exploitation et de supervision des infrastructures et des applications, une messagerie dite technique peut être déployée en zone de Back-office du centre informatique. Cette messagerie technique ne doit être en aucun cas utilisée directement par un utilisateur.

EXP-CI-FILT : filtrage des flux applicatifs. De façon à garantir un niveau de sécurité satisfaisant face aux attaques informatiques, des mécanismes de filtrage et de cloisonnement doivent être mis en œuvre.

EXP-CI-ADMIN : flux d'administration. D'une manière générale, il convient de différencier deux type de flux d'administration : les flux d'administration de l'infrastructure (réservés aux agents du centre informatique) d'une part, les flux d'administration des applications métier (réservés à la direction métier) d'autre part. L'attribution des droits d'administration doit

respecter cette différenciation, et les 2 types de flux d'administration doivent être dans la mesure du possible cloisonnés.

EXP-CI-DNS : service de noms de domaine – DNS technique. Dans le cas du déploiement d'un serveur de noms de domaines pour les besoins techniques internes au centre informatique, on utilisera les extensions sécurisées DNSSEC.

EXP-CI-EFFAC : effacement de support. Le reconditionnement et la réutilisation des disques durs pour un autre usage (ex : ré-attribution d'une machine/serveur) ne sont autorisés qu'après une opération d'effacement sécurisé des données.

EXP-CI-DESTR : destruction de support. La fin de vie d'un support ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur…) doit s'accompagner d'une opération de destruction avant remise au constructeur.

EXP-CI-TRAC : traçabilité / imputabilité. Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les centres d'exploitation emploient une référence de temps commune (service NTP, Network Time Protocol).

EXP-CI-SUPERVIS : supervision. Un cloisonnement entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) doit être mis en place.

EXP-CI-AMOV : accès aux périphériques amovibles. L'accès aux supports informatiques amovibles fait l'objet d'un traitement adapté, plus particulièrement lorsqu'ils ont été utilisés pour mémoriser de l'information sensible ou lorsqu'ils sont utilisés pour des opérations d'exploitation.

EXP-CI-ACCRES : accès aux réseaux. Dans un centre informatique, le contrôle physique des accès réseaux, l'attribution des adresses IP, le filtrage des informations et l'usage de dispositifs spécifiques (machines virtuelles, cartes d'administration à distance, etc.) font l'objet de procédures sécurisées.

EXP-CI-AUDIT : audit/contrôle. Le RSSI pilote des audits réguliers du système d'information relevant de sa responsabilité.

Sécurité du poste de travail

Sécurisation des postes de travail

Objectif 25 : sécurisation des postes de travail. Durcir les configurations des postes de travail en protégeant les utilisateurs.

Mise à disposition du poste

PDT-GEST : fourniture et gestion des postes des travail. Les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par l'équipe locale chargée des SI.

PDT-CONFIG : formalisation de la configuration des postes des travail. Une procédure formalisée de configuration des postes de travail est établie par chaque entité, conformément aux directives nationales existantes.

Sécurité physique des postes de travail

PDT-VEROUIL-FIXE : verrouillage de l'unité centrale des postes fixes. Lorsque l'unité centrale d'un poste fixe est peu volumineuse, donc susceptible d'être facilement emportée, elle doit être protégée contre le vol par un système d'attache (par exemple un câble antivol).

PDT-VEROUIL-PORT : verrouillage des postes portables. Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation.

Réaffectation du poste et récupération d'informations

PDT-REAFFECT : réaffectation du poste de travail. Une procédure SSI définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.

Gestion des privilèges sur les postes de travail

PDT-PRIVIL : privilèges des utilisateurs sur les postes de travail. La gestion des privilèges des utilisateurs sur leurs postes de travail doit suivre le principe du « moindre privilège » : chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission.

PDT-PRIV : utilisation des privilèges d'accès « administrateur ». Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.

PDT-ADM-LOCAL : gestion du compte « administrateur local ». L'accès au compte « administrateur local » sur les postes de travail doit être strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail.

Protection des informations

PDT-STOCK : stockage des informations. Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des entités et en accord avec les règles de sécurité en vigueur.

PDT-SAUV-LOC : sauvegarde / synchronisation des données locales. Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs.

PDT-PART-FIC : partage de fichiers. Le partage de répertoires ou de données hébergées localement sur les postes de travail n'est pas autorisé.

PDT-SUPPR-PART : suppression des données sur les postes partagés. Les données présentes sur les postes partagés (portable de prêt, par exemple) doivent être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître.

PDT-CHIFF-SENS : chiffrement des données sensibles. Une solution de chiffrement labellisée doit être mise à disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

PDT-AMOV : fourniture de supports de stockage amovibles. Les supports de stockage amovibles (clés USB et disque durs externes, notamment) doivent être fournis aux utilisateurs par l'équipe locale chargée des SI.

Nomadisme

PDT-NOMAD-ACCESS : accès à distance aux Systèmes d'Information de l'entité. Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent être réalisés via les infrastructures nationales. Lorsque l'accès à distance utilise d'autres infrastructures, l'usage de réseaux privés virtuels (VPN) de confiance est nécessaire.

PDT-NOMAD-PAREFEU : pare-feu local. Un pare-feu local conforme aux directives nationales doit être installé sur les postes nomades.

PDT-NOMAD-STOCK : stockage local d'information sur les postes nomades. Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé.

PDT-NOMAD-FILT : filtre de confidentialité. Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité doit être fourni et être positionné sur l'écran dès lors que le poste est utilisé en dehors de l'entité.

PDT-NOMAD-CONNEX : configuration des interfaces de connexion sans fil. La configuration des interfaces de connexion sans fil doit interdire les usages dangereux de ces interfaces.

PDT-NOMAD-DESACTIV : désactivation des interfaces de connexion sans fil. Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 3G…), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être définies et appliquées. Les interfaces sans fil ne doivent être activées qu'en cas de besoin.

Sécurisation des imprimantes et copieurs multifonctions

Objectif 26 : sécurisation des copieurs multifonctions. Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque.

PDT-MUL-DURCISS : durcissement des imprimantes et copieurs multifonctions. Les imprimantes et copieurs multifonctions hébergés localement dans une entité doivent faire l'objet d'un durcissement en termes de sécurité : changement des mots de passe initialement fixés par le « constructeur », désactivation des interfaces réseau inutiles, suppression des services inutiles, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible, configuration réseau statique.

PDT-MUL-SECNUM : sécurisation de la fonction de numérisation. Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans une entité doit être sécurisée. Les mesures de sécurité suivantes doivent notamment être appliquées : envoi de documents uniquement à destination d'une adresse de messagerie interne à l'entité, envoi uniquement à une seule adresse de messagerie.

Sécurisation de la téléphonie

Objectif 27 : sécurisation de la téléphonie. Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes.

PDT-TEL-MINIM : sécuriser la configuration des autocommutateurs. Les autocommutateurs doivent être maintenus à jour au niveau des correctifs de sécurité. Leur configuration doit être durcie. La définition et l'affectation des droits d'accès et des privilèges aux utilisateurs (transfert départ-départ, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé, etc.) doivent faire l'objet d'une attention particulière. Une revue de la programmation téléphonique doit être organisée périodiquement.

PDT-TEL-CODES : codes d'accès téléphoniques. Il est nécessaire de sensibiliser les utilisateurs au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.

PDT-TEL-DECT : limiter l'utilisation du DECT. Les communications réalisées au travers du protocole DECT sont susceptibles d'être interceptées, même si les mécanismes d'authentification et de chiffrement que propose ce protocole sont activés. Il est recommandé d'attribuer des postes téléphoniques filaires aux utilisateurs dont les échanges sont les plus sensibles.

Contrôles de conformité

Objectif 28 : contrôles de la conformité des postes de travail. Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

PDT-CONF-VERIF : utiliser des outils de vérification automatique de la conformité. Un outil de vérification régulière de la conformité des éléments de configuration des postes de travail doit être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration.

Sécurité du développement des systèmes

Développement des systèmes

Objectif 29 : prise en compte de la sécurité dans le développement des SI. Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.

DEV-INTEGR-SECLOC : intégrer la sécurité dans les développements locaux. Toute initiative locale de développement informatique doit respecter les exigences nationales en matière de SSI, concernant la prise en compte de la sécurité dans les projets et les développements informatiques. Le service à l'origine du projet se porte garant de l'application du référentiel général de sécurité*, et de l'application d'une démarche d'homologation du système.*

DEV-SOUS-TRAIT : intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique. Lors de l'écriture d'un contrat de sous-traitance de développement, plusieurs clauses relatives à la SSI doivent être intégrées :

- *formation obligatoire des développeurs sur le développement sécurisé et sur les vulnérabilités classiques ;*
- *utilisation obligatoire d'outils permettant de minimiser les erreurs introduites durant le développement (outils gratuits d'analyse statique de code, utilisation de bibliothèques réputées pour leur sécurité, etc.) ;*
- *production de documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement, etc.) ;*
- *respect de normes de développement sécurisé, qu'elles soient propres au développeur, publiques ou propres au commanditaire ;*
- *obligation pour le prestataire de corriger, dans un temps raisonnable et pour un prix défini, les vulnérabilités introduites durant le développement et qui lui sont remontées, en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation.*

Développements logiciels et sécurité

Objectif 30 : prise en compte de la sécurité dans le développement des logiciels. Mener les développements logiciels selon une méthodologie de sécurisation du code produit.

DEV-FUITES : limiter les fuites d'information. Les fuites d'informations techniques sur les logiciels utilisés permettent aux attaquants de déceler plus facilement d'éventuelles vulnérabilités. Il est impératif de limiter fortement la diffusion d'informations au sujet des produits utilisés, même si cette précaution ne constitue pas une protection en tant que telle.

DEV-LOG-ADHER : réduire l'adhérence des applications à des produits ou technologies spécifiques. Le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. En phases de conception et de spécification technique, il est nécessaire de s'assurer que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent. En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent. En plus du maintien en condition de sécurité propre à l'application, il est donc nécessaire de pouvoir

faire évoluer son environnement pour garantir sa sécurité dans la durée.

DEV-LOG-CRIT : instaurer des critères de développement sécurisé. Une fois passées les phases de définition des besoins et de conception de l'architecture applicative, le niveau de sécurité d'une application dépend fortement des modalités pratiques suivies lors de sa phase de développement.

DEV-LOG-CYCLE : intégrer la sécurité dans le cycle de vie logiciel. La sécurité doit être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

DEV-LOG-WEB : améliorer la prise en compte de la sécurité dans les développements Web. Les développements Web (et les développements en PHP en particulier) font l'objet de problèmes de sécurité récurrents qui ont conduit à la constitution de référentiels de sécurité. Ces référentiels ont pour objectif de fixer des REGLES DE BONNES PRATIQUES à l'usage des développeurs. Ce sont des règles d'ordre générique ou pouvant être spécifiques à un langage (PHP, ASP, NET, etc.).

DEV-LOG-PASS : calculer les empreintes de mots de passe de manière sécurisée. Lorsqu'une application doit stocker les mots de passe de ses utilisateurs, il est important de mettre en œuvre des mesures permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute, etc.

Applications à risques

Objectif 31 : sécurisation des applications à risques. Accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles.

DEV-FILT-APPL : mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque. Devant les applications à risques, il est recommandé de faire usage d'une solution tierce de filtrage applicatif.

Traitement des incidents

Chaînes opérationnelles

Objectif 32 : chaînes opérationnelles. Partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques.

TI-OPS-SSI : chaînes opérationnelles SSI. Les chaînes opérationnelles des ministères concourent à l'effort national de cybersécurité. Les alertes et les incidents sont gérés selon des procédures testées lors d'exercices. La coordination des compétences est organisée à l'échelon ministériel. Les situations d'urgences peuvent faire appel à des mesures définies préalablement dans le cadre des plans gouvernementaux.

Traitement des alertes de sécurité émises par les instances nationales (ANSSI)

TI-MOB : mobilisation en cas d'alerte En cas d'alerte de sécurité identifiée au niveau national, les RSSI de chaque entité s'assurent de la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.

Remontée des incidents de sécurité rencontrés

TI-QUAL-TRAIT : qualification et traitement des incidents. La chaîne fonctionnelle SSI est informée par la chaîne opérationnelle de tout incident de sécurité, et contribue si nécessaire à la qualification de l'incident et au pilotage de son traitement.

TI-INC-REM : remontée des incidents. Tout incident de sécurité, même apparemment mineur, dont l'impact dépasse ou est susceptible de dépasser le SI d'une entité ou d'un ministère, fait l'objet d'un compte-rendu, via la chaîne SSI, au Centre opérationnel de la sécurité des systèmes d'information *(COSSI) de l'ANSSI.*

La remontée d'incidents par les chaînes opérationnelles ministérielles participe à la posture permanente de vigilance. Cette remontée est immédiate pour les incidents dont la portée est susceptible de dépasser à court terme le périmètre de l'entité ou du ministère, et pour les incidents correspondant à des signalements spécifiques, notamment de la part de l'ANSSI. La remontée prend la forme d'une synthèse mensuelle pour les autres incidents.

Les critères et procédures précis de remontée d'incidents sont élaborés sous le pilotage de la chaîne fonctionnelle SSI, en lien avec la chaîne opérationnelle.

Chaque entité doit maintenir à jour un historique clair des suites liées à l'escalade de chaque incident, afin de capitaliser les enseignements associés à la résolution (ou non) de ces incidents.

L'aspect difficile de la caractérisation des attaques (ambiguïté de la source, du dommage, du moyen, de la finalité) rend nécessaire les échanges d'informations interministériels - même sur des « signaux faibles » - ainsi que la coordination continue des actions.

Continuité d'activité

Gestion de la continuité d'activité des SI

Objectif 33 : gestion de la continuité d'activité. Se doter de plans de continuité d'activité, et les tester.

PCA-MINIS : définition du plan ministériel de continuité d'activité des Systèmes d'Information. Chaque ministère définit un plan de continuité d'activité ministériel des systèmes d'information permettant d'assurer, en cas de sinistre, la continuité d'activité des systèmes d'information.

Définition du plan de continuité d'activité des systèmes d'information d'une entité

PCA-LOCAL : définition du plan local de continuité d'activité des systèmes d'information. Le directeur des systèmes d'information ou le RSSI d'une entité définit la structure et les attendus du plan de continuité d'activité des systèmes d'information permettant d'assurer effectivement, en cas de sinistre, la continuité d'activité.

Mise en œuvre du plan local de continuité d'activité des systèmes d'information

PCA-SUIVILOCAL : suivi de la mise en œuvre du plan de continuité d'activité local des Systèmes d'Information (PCA des SI). Le RSSI d'une entité s'assure de la bonne mise en œuvre des dispositions prévues dans le plan de continuité d'activité des systèmes d'information.

PCA-PROC : mise en œuvre des dispositifs techniques et des procédures opérationnelles. Les équipes informatiques mettent en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la continuité des SI, en assurent la supervision au quotidien et la maintenance dans le temps.

PCA-SAUVE : protection de la disponibilité des sauvegardes. Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées.

PCA-PROT : protection de la confidentialité des sauvegardes. Les sauvegardes doivent être traitées de manière à garantir leur confidentialité et leur intégrité.

Maintien en conditions opérationnelles du plan local de continuité d'activité des Systèmes d'Information

PCA-EXERC : exercice régulier du plan local de continuité d'activité des systèmes d'information. Le RSSI d'une entité organise des exercices réguliers, afin de tester le plan local de continuité d'activité des systèmes d'information.

PCA-MISAJOUR : mise à jour du plan local de continuité d'activité des systèmes d'information. Le RSSI d'une entité assure le maintien à jour du plan local de continuité d'activité des Systèmes d'Information.

Conformité, audit, inspection, contrôle

Contrôles

Objectif 34 : contrôles réguliers. Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

CONTR-SSI : contrôles locaux. La conformité à la PSSIE et à la PSSI ministérielle est vérifiée par des contrôles réguliers. Les RSSI de chaque entité conduisent des actions locales d'évaluation de la conformité à la PSSIE et contribuent à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en œuvre.

CONTR-BILAN-SSI : bilan annuel. Chaque ministère établit un bilan annuel mesurant sa maturité SSI globale. L'ANSSI consolide l'ensemble de ces bilans. Le document de synthèse est soumis au Premier ministre.