INSTRUCTION INTERMINISTÉRIELLE

RELATIVE À LA PROTECTION DES SYSTÈMES D'INFORMATION SENSIBLES

n° 901/SGDSN/ANSSI

NOR : PRMD1503279J

Sommaire

La présente instruction définit les objectifs et les règles
relatifs à la protection des systèmes d'information sensibles,
notamment ceux traitant des informations portant la mention *Diffusion Restreinte*.

La présente instruction s'adresse à l'ensemble des personnes physiques ou morales
intervenant dans ces systèmes.

Le respect des règles contribue à garantir la continuité des activités de l'entité
qui met en œuvre le système d'information, à protéger l'image de cette entité,
à prévenir la compromission d'informations sensibles
et à assurer la sécurité des personnes et des biens.

Ces règles peuvent être précisées au cas par cas en s'appuyant
sur les normes techniques existantes et sur les guides techniques et les recommandations
de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Titre I - Définition et périmètre

Article 1er : Définitions

Les **systèmes d'information sensibles** sont ceux qui traitent d'informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre.

Les **systèmes d'information *Diffusion Restreinte*** sont les **systèmes d'information sensibles** qui traitent d'informations portant la mention *Diffusion Restreinte*[1] ou ses équivalentes européennes ou internationales.

Article 2 : Champ d'application

2.1 L'instruction s'applique :

- aux administrations de l'Etat[2] qui mettent en œuvre des **systèmes d'information sensibles** ;
- aux entités publiques ou privées soumises à la réglementation relative à la protection du potentiel scientifique et technique de la nation (PPST)[3] qui mettent en œuvre des **systèmes d'information sensibles**[4] ;
- à toute autre entité publique ou privée qui met en œuvre des **systèmes d'information *Diffusion Restreinte***.

2.2 La présente instruction a valeur de recommandation pour toute autre entité publique ou privée qui met en œuvre des **systèmes d'informations sensibles**, notamment des systèmes traitant d'informations régies par des obligations de sécurité spécifiques[5].

2.3 La présente instruction ne s'applique pas aux systèmes d'information traitant d'informations couvertes par le secret de la défense nationale[6].

---

[1] Voir l'article 5 et l'annexe 3, intitulée « Règles de protection des informations ou supports portant la mention *Diffusion Restreinte* », de l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 30 novembre 2011 sur la protection du secret de la défense nationale. La mention *Diffusion Restreinte* n'est pas un niveau de classification mais une mention de protection qui signale à l'utilisateur la discrétion dont il doit faire preuve dans la manipulation des informations couvertes par cette mention.

[2] Les administrations de l'Etat au sens de la présente instruction sont les administrations centrales, les établissements publics nationaux, les services déconcentrés de l'État et les autorités administratives indépendantes.

[3] Le cadre réglementaire de la PPST est défini à l'article R. 413-5-1 du code pénal ainsi que par le décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation et par l'arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation.

[4] Sauf lorsqu'ils traitent d'informations classifiées et sont en conséquence régis par les textes relatifs à la protection des informations couvertes par le secret de la défense nationale, les systèmes d'information qui sont mis en œuvre par une entité soumise à la réglementation relative à la PPST et qui traitent d'informations relatives aux spécialités dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs constituent des systèmes d'information *Diffusion Restreinte*.

[5] Sont notamment concernés les systèmes traitant d'informations couvertes par le secret professionnel, constituant des correspondances privées ou mentionnées à l'article 6 de la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal. Sont également concernés les systèmes d'information mentionnés dans l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Article 3 : Principes stratégiques appliqués

Les règles décrites dans la présente instruction s'appuient sur cinq principes stratégiques :

- mettre en place une organisation consacrée à la sécurité des systèmes d'information, incluant des volets préventifs et défensifs et reposant sur des moyens humains, matériels et financiers identifiés ;
- évaluer les risques périodiquement, dans une démarche d'amélioration continue de la sécurité de chaque système pendant leur durée de vie ;
- défendre en profondeur, en s'assurant dès la conception que si l'une des mesures de sécurité est compromise ou défaillante, d'autres assurent la protection des informations sensibles ;
- respecter les règles élémentaires d'hygiène informatique, définies par l'ANSSI, mises en œuvre par des administrateurs de systèmes d'information formés à cet effet ;
- recourir à des produits de sécurité agréés, qualifiés ou, à défaut, certifiés et à des prestataires de services de confiance qualifiés par l'ANSSI.

Article 4 : Application des règles

4.1 Application des règles aux **systèmes d'information sensibles**

Les administrations de l'Etat qui mettent en œuvre des **systèmes d'information sensibles** appliquent la politique de sécurité des systèmes d'information de l'Etat (PSSIE)[7]. Une administration de l'Etat qui respecte la PSSIE est réputée se conformer à l'ensemble des dispositions du titre II.

Les entités publiques ou privées mentionnées à l'article 2.1 qui mettent en œuvre des **systèmes d'information sensibles** appliquent les règles prévues au titre II ainsi que celles prévues à l'annexe 1. Ces dernières sont les règles de la PSSIE adaptées aux entités situées hors du champ d'application de cette politique de sécurité.

4.2 Application des règles aux **systèmes d'information *Diffusion Restreinte***

Les administrations de l'Etat qui mettent en œuvre des **systèmes d'information *Diffusion Restreinte*** appliquent la PSSIE ainsi que les règles prévues au titre III.

Les entités publiques ou privées qui mettent en œuvre des **systèmes d'information *Diffusion Restreinte*** appliquent les règles prévues aux titres II et III ainsi qu'à l'annexe 1.

---

[6] Ces systèmes sont régis par les articles R. 2311-1 et suivants du code de la défense et par l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 30 novembre 2011 sur la protection du secret de la défense nationale, notamment son titre V.

[7] La PSSIE a été approuvée par une circulaire du Premier ministre signée le 17 juillet 2014.

Titre II - Protection des systèmes d'information sensibles

Article 5 : Détermination de la sensibilité des informations

Chaque entité mettant en œuvre un **système d'information sensible** :

- identifie l'information sensible qu'elle traite ;
- marque cette information par les moyens de son choix ;
- détermine, si besoin, une échelle de sensibilité correspondant à des niveaux en matière de disponibilité, d'intégrité et de confidentialité des informations de son système d'information sensible ;
- applique des mesures de protection adaptées.

Lorsque les informations sensibles transitent entre plusieurs entités, leur niveau de sensibilité est explicitement mentionné par l'entité émettrice afin qu'elles soient protégées en conséquence par l'entité destinataire en termes de disponibilité, d'intégrité et de confidentialité, pendant et après leur transit.

Article 6 : Gouvernance de la protection des systèmes d'information

Chaque entité :

- applique une politique de sécurité des systèmes d'information (PSSI), validée au plus haut niveau de l'entité et couvrant tous les aspects, techniques ou non, de la sécurité (communication, ressources humaines et financières, aspects juridiques, *etc.*) ;
- organise la gouvernance et attribue les responsabilités en matière de sécurité des systèmes d'information.

Article 7 : Maîtrise des risques

La PSSI de l'entité résulte d'une analyse des risques menée :

- pour tous les risques, pas seulement techniques, qu'ils soient d'origine humaine ou non ;
- pour chacun des systèmes d'information de l'entité ;
- en appréciant l'impact qu'une menace sur un composant du système pourrait avoir sur les missions de l'entité, son image, son patrimoine ou la sécurité des biens et des personnes.

Article 8 : Homologation des systèmes d'information sensibles

Tout **système d'information sensible** doit faire l'objet d'une homologation de sécurité avant sa mise en service. Dans le dossier d'homologation figurent notamment les risques résiduels, c'est-à-dire ceux qui ne sont pas couverts par des mesures de protection.

L'autorité d'homologation doit être choisie au sein de l'entité, au niveau hiérarchique suffisant pour assumer la responsabilité afférente à la décision d'homologation. Elle accepte notamment les risques résiduels. Elle est en principe l'autorité qui emploie le système.

En prononçant sa décision d'homologation, l'autorité d'homologation déclare que le système d'information est conforme aux règles prévues par la présente instruction.

Article 9 : Protection des systèmes d'information

L'entité dispose d'une cartographie de l'ensemble des systèmes d'information dont elle est responsable. Cette cartographie est tenue à jour. Elle est nécessaire à l'entité pour assurer la protection de ses systèmes d'information.

L'entité protège ses systèmes d'information contre les menaces identifiées pendant toute leur durée de vie. La protection repose sur plusieurs volets :

- physique : elle retarde ou empêche l'accès physique des personnes non autorisés aux locaux, aux systèmes et aux informations, tout en maintenant la disponibilité des accès pour les personnes autorisées. Elle permet également d'éviter et de détecter les incidents physiques tels les défauts d'alimentation, les défauts de climatisation, les incendies et les dégâts des eaux ;
- logique : elle permet de se prémunir contre les attaques informatiques malveillantes et accidentelles mais surtout de protéger les réseaux, les équipements, les données et leurs supports, les accès logiques ainsi que l'administration des systèmes ;
- organisationnel : elle est mise en œuvre selon des processus explicitement définis dans la PSSI de l'entité.

En cas d'élévation du niveau de la menace, l'entité renforce les mesures de vigilance et de protection de ses systèmes.

Article 10 : Gestion des incidents de sécurité des systèmes d'information

Même protégée, l'entité se prépare à subir des attaques sur ses systèmes d'information. Elle intègre la sécurité des systèmes d'information (SSI) dans ses procédures de gestion de crise et dans ses exercices périodiques. Pour être en mesure d'agir pour réduire l'impact des attaques et des incidents, elle se dote :

- d'une capacité de détection, d'analyse, de qualification et de réaction, afin notamment d'assurer la continuité de ses missions ;
- d'un dispositif de gestion des incidents afin de détecter et d'analyser les attaques et de réagir face à des événements anormaux.

Des retours d'expérience de traitement des incidents sont prévus après chaque événement.

Article 11 : Évaluation du niveau de sécurité

L'entité évalue en permanence le niveau de sécurité de ses systèmes d'information et les risques résiduels. Elle effectue régulièrement des vérifications et réalise des audits fonctionnels et techniques de sécurité des systèmes d'information. Cette évaluation permet de réduire l'impact des attaques et des incidents et d'assurer la continuité de service de l'entité.

Article 12 : Relations avec les autorités de l'État

Sans préjudice des dispositions législatives et réglementaires spéciales, notamment celles applicables aux opérateurs d'importance vitale, chaque entité coopère avec les autorités de l'État telles que l'ANSSI ou les ministères de tutelle pour assurer la sécurité de ses systèmes d'information. Elle répond, en cas de crise, aux sollicitations de ces autorités.

Titre III - Protection des systèmes d'information *Diffusion Restreinte*

Article 13 : Homologation des systèmes d'information *Diffusion Restreinte*

Tout système d'information *Diffusion Restreinte* est homologué à ce titre dans les conditions prévues à l'article 8. L'homologation prévoit en particulier la manière dont est contrôlée et maîtrisée la destruction du système lui-même ou d'autres supports ayant contenu des informations portant la mention *Diffusion Restreinte*.

Article 14 : Traitement des informations portant la mention *Diffusion Restreinte*

En fonction de son besoin et de ses moyens techniques, humains et financiers, l'entité choisit, conformément aux dispositions du présent article et de l'annexe 2, la classe du réseau sur lequel sont traitées les informations portant la mention *Diffusion Restreinte*.

Le traitement en clair des informations portant la mention *Diffusion Restreinte*, notamment leur stockage et leur diffusion, s'effectue sur des réseaux de classe 1 ou 2.

Le choix d'un réseau de classe 2 est fortement recommandé. En effet, toute connexion à un réseau public constitue en elle-même une vulnérabilité qui peut facilement conduire à la compromission d'informations.

Les informations portant la mention *Diffusion Restreinte* sont chiffrées à l'aide de moyens agréés à ce niveau par l'ANSSI dès lors qu'elles transitent ou sont stockées en dehors d'une zone physiquement protégée dans les conditions prévues à l'article 15.

Article 15 : Protection physique des locaux

Les mesures de sécurité physique sont choisies en proportion des menaces déterminées par l'analyse des risques prévue à l'article 7. Elles ont pour objectif à la fois de prévenir la perte, l'altération ou la détérioration d'une information portant la mention *Diffusion Restreinte* et de recueillir des informations pour résoudre des incidents informatiques en :

- défendant par une barrière périmétrique physique les limites de la zone à protéger ;
- dissuadant l'accès non autorisé par toute mesure physique appropriée ;
- contrôlant l'accès des locaux de façon électronique, électromécanique ou humaine ;
- conservant la traçabilité des accès ;
- protégeant des intrusions par un système de détection (ce système peut remplacer une barrière périmétrique ou la compléter pour renforcer le niveau de sécurité).

Article 16 : Externalisation

En cas d'externalisation d'une prestation qui met en œuvre un système d'information *Diffusion Restreinte*, l'entité et son prestataire tiennent compte des recommandations figurant dans le guide de l'ANSSI relatif à l'externalisation[8]. Le contrat qui les lie garantit la conformité du système d'information aux règles prévues par la présente instruction. La prestation s'effectue, dans la mesure du possible, à partir du territoire national.

[8] Guide de l'ANSSI « Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information », http//www.ssi.gouv.fr/infogerance.

Il est recommandé à toute entité de choisir des prestataires de services de confiance qualifiés par l'ANSSI.

Article 17 : Utilisation en milieu non maîtrisé

Les informations portant la mention *Diffusion Restreinte* contenues dans des dispositifs nomades (ordinateurs portables, média amovibles, téléphones, *etc.*) sont chiffrées par des moyens agréés par l'ANSSI, afin de limiter le risque de divulgation en cas de perte ou de vol.

La consultation de documents électroniques portant la mention *Diffusion Restreinte* dans les lieux publics est entourée de précautions particulières (utilisation d'un filtre de confidentialité sur l'écran, surveillance continuelle du poste nomade lui-même, des alentours, des supports portant la mention *Diffusion Restreinte* ou des équipements qui les utilisent).

La connexion d'équipements personnels à un système d'informations *Diffusion Restreinte* est proscrite.

Il en va de même de la connexion d'équipements nomades traitant d'informations portant la mention *Diffusion Restreinte* à tout autre système d'information que ceux homologués par l'entité pour traiter de telles informations, sauf si l'homologation du système d'information auquel le dispositif nomade appartient le permet et si les règles prévues par la présente instruction sont respectées.

Article 18 : Supports audiovisuels

Avant de diffuser des informations portant la mention *Diffusion Restreinte* sur un support audiovisuel, le responsable de la diffusion vérifie que les participants ont besoin d'en connaître. Il s'assure également que les systèmes d'information utilisés sont homologués pour traiter des informations portant la mention *Diffusion Restreinte*.

À cette occasion, les éventuelles captations photographiques, vidéo ou audio des informations font l'objet d'une attention particulière. Le cas échéant, ces captations sont interdites.

Article 19 : Autorisations de dérogation

Lorsque les circonstances l'imposent, des dérogations, limitées dans le temps, aux règles prévues par la présente instruction peuvent être accordées à une entité pour un système d'information *Diffusion Restreinte* qu'elle met en œuvre. Les dérogations sont accordées par le haut fonctionnaire de défense et de sécurité du ministère dont relève l'entité qui met en œuvre le système d'information. Les autorisations de dérogation, accompagnées de leur motivation, sont communiquées à l'ANSSI.

Titre IV - Dispositions transitoires et finales

Article 20 : Dispositions transitoires

Les entités disposent d'un délai de trois ans à compter de la date de publication de la présente instruction pour mettre en conformité avec les règles qu'elle prévoit leurs systèmes d'information *Diffusion Restreinte* mis en service avant la date de publication de la présente instruction ou dans les six mois suivant cette date. Durant ce délai, les entités établissent et tiennent à la disposition de l'ANSSI la liste des manquements aux règles prévues par la présente instruction.

Article 21 : Abrogation

La présente instruction abroge la recommandation n° 901/DISSI/SCSSI du 2 mars 1994 pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense et la recommandation n° 600/DISSI/SCSSI de mars 1993 pour la protection des informations sensibles ne relevant pas du secret de défense.

Fait à Paris, le 28 janvier 2015

Guillaume POUPARD
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

Annexe 1 - Règles pour les entités situées hors du champ d'application de la PSSIE[9]

Politique, organisation, gouvernance

Objectif 1 :

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

Organisation SSI

ORG-SSI : organisation de la SSI. Une organisation dédiée à la SSI est déployée au sein de chaque entité. Cette organisation 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'application des mesures sont écrites et portées à la connaissance de tous.

Acteurs SSI

ORG-ACT-SSI : identification des acteurs de la SSI. L'organisation de la SSI s'appuie sur des acteurs clairement identifiés, responsables de la mise en application générale de la PSSI.

Responsabilités internes

ORG-RSSI : désignation du responsable de la SSI. La direction de l'entité s'appuie sur un ou plusieurs responsables de la sécurité des systèmes d'information (RSSI), chargés de l'assister dans le pilotage et la gestion de la SSI. Des correspondants locaux de la 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 PSSI par la direction de l'entité et veille à leur application. Des dénominations alternatives des fonctions mentionnées 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 la direction de l'entité.

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

ORG-PIL-PSSI : définition et pilotage de la PSSI. Chaque entité établit une PSSI, validée par la direction. Une structure de pilotage de la PSSI est définie. Cette structure est chargée de sa mise en place, de son évolution, de son suivi et de son contrôle.

---

[9] Ces règles sont adaptées de la politique de sécurité des systèmes d'information de l'Etat.

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 d'application de la PSSI. Il rend compte régulièrement de l'application des mesures de sécurité auprès de la direction de l'entité.

ORG-APP-DOCS : formalisation de documents d'application. Le RSSI établit et tient à jour les documents, approuvés par la direction de l'entité, permettant l'application des mesures de la PSSI.

Ressources humaines

Objectif 2 :

Faire des personnes les maillons forts des SI.

Utilisateurs

RH-SSI : charte d'application de la SSI. Une charte d'application de la PSSI, récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques et élaborée sous le pilotage de la chaîne fonctionnelle de la 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.

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 locaux de la SSI et administrateurs de sécurité. Les RSSI et leurs correspondants 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 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. Il doit être formé à l'utilisation des outils de travail conformément aux règles de la 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 doit être formalisée et appliquée strictement. Cette procédure doit couvrir au minimum :

- la gestion et la 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 PSSI s'appliquent à tout personnel non permanent utilisateur d'un SI d'une entité. 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 :

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 la disposition du RSSI 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 réglementation en vigueur.

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 et de l'ANSSI en cas de besoin de coordination opérationnelle.

Objectif 4 :

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 leur création jusqu'à leur éventuelle destruction.

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

Objectif 5 :

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

Gestion des risques et homologation de sécurité

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. L'homologation est l'acte selon lequel une autorité, dite autorité d'homologation, désignée par la direction de l'entité, atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise le cas échéant après avis d'une commission d'homologation. Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré et précise les conditions d'emploi.

Objectif 6 :

Gérer dynamiquement les mesures de protection, tout au long de la vie du SI.

Maintien en condition de sécurité des systèmes d'information

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, d'évolution ou de retrait d'un système.

INT-TDB : créer un tableau de bord SSI. Un tableau de bord de la 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 de la 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.

Objectif 7 :

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

Produits de sécurité et services de confiance labellisés

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

Objectif 8 :

Veiller aux exigences de sécurité lorsqu'il est fait appel à une prestation par des tiers.

Gestion des prestataires

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 phase de production.

INT-REX-AR : analyse de risques. Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à déterminer des objectifs de sécurité et définir des mesures adaptées. L'ensemble des objectifs de sécurité ainsi déterminés 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 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

Objectif 9 :

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 de la SSI et les services chargés 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 au 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 du 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 pour les opérations dites de « dépoussiérage ».

Objectif 10 :

Proportionner les protections physiques des centres informatiques aux 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 chargés 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.

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 de sécurité labellisés, lorsqu'ils sont disponibles, et être maintenu en condition de sécurité de façon rigoureuse.

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 et s'appuyer sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé ou habilité mais néanmoins appelé à intervenir dans les zones internes ou restreintes (entretien ou réparation des bâtiments ou des équipements non informatiques, nettoyage, visiteurs) accède à ces zones sous surveillance permanente et systématique.

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

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

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

PHY-CI-CLIM : climatisation. Une climatisation proportionnée aux besoins énergétiques du système informatique doit être installée. 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 matière inflammable 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.

Objectif 11 :

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 de détection d'intrusion (CAD), 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 toute 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 contre les incendies (INC), regroupant l'ensemble des moyens informatiques mis en œuvre pour détecter, informer, intervenir 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 fondant 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 de sécurité labellisés, quand ils existent, est fortement recommandé.

Sécurité des réseaux

Objectif 12 :

Utiliser les infrastructures maîtrisées de l'entité,
en respectant les règles de sécurité qui leur sont attachées.

Sécurité des réseaux internes

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 maîtrisées de l'entité.

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 des passerelles maîtrisées de l'entité. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par un chiffrement adapté.

Objectif 13 :

Maîtriser les interconnexions de réseaux locaux.
Configurer de manière adéquate les équipements de réseau actifs.

Sécurité des réseaux locaux

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 spécifiques et de passerelles sécurisées.

RES-RESS : cloisonnement des ressources en cas de partage de locaux. Dans le cas où une entité partage des locaux avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Les mesures prises doivent être validées par l'autorité d'homologation si elles ne sont pas physiques.

Objectif 14 :

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

Accès spécifiques

RES-INTERNET-SPECIFIQUE : cas particulier des accès spécifiques dans une entité. Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage professionnel 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.

Objectif 15 :

Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.

Sécurité 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 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.

Objectif 16 :

Configurer les mécanismes de commutation et de routage
pour se protéger des attaques.

Sécurisation des mécanismes de commutation et de routage

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 dynamique 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 que 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 des certificats, la désactivation des interfaces et des services inutiles ainsi que la mise en place de mécanismes de protection du plan de contrôle.

Objectif 17 :

Tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions.

Cartographie de réseau

RES-CARTO : élaborer les documents d'architecture technique et fonctionnelle. L'architecture en 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 du réseau s'insère dans la cartographie globale des SI.

Architecture des systèmes d'information

Objectif 18 :

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

Architecture 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 et de sauvegarde pour les besoins des centres informatiques repose sur une architecture consacrée.

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

Exploitation des systèmes d'information

Objectif 19 :

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

Protection des 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 termes de confidentialité et d'intégrité. A défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées à l'aide d'un moyen de chiffrement labellisé.

Objectif 20 :

Durcir les configurations des ressources informatiques et surveiller les interventions opérées sur celles-ci.

Sécurité des ressources informatiques

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. Les traces doivent être accessibles au correspondant local de la SSI 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 les mises à jour sont effectuées dans le strict respect des guides ou des procédures en vigueur dans l'entité ou, à 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.

Objectif 21 :

Authentifier les usagers et contrôler leurs accès aux ressources des SI 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 cohérent 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) et 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 de la 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 suivent les recommandations de l'ANSSI.

EXP-CERTIFS : utilisation de certificats électroniques. Les autorités administratives au sens de l'ordonnance n° 2005-1516 du 8 décembre 2005 appliquent les règles du

référentiel général de sécurité pour les certificats électroniques. Les autres entités s'inspirent de ces règles.

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 des administrateurs. 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'administrateur authentifié doit être informé de l'existence de ces opérations de gestion, de leurs finalités et de leurs 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 d'une carte à puce, n'ont, par défaut, pas besoin de faire l'objet d'opérations de séquestre de la part d'autres personnes que l'administrateur authentifié lui-même.

EXP-POL-ADMIN : politique des mots de passe des 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, par exemple les mots de passe des comptes fonctionnels, des comptes génériques ou des comptes de service utilisés dans le cadre des fonctions de l'administrateur.

Objectif 22 :

Fournir aux administrateurs les outils nécessaires à l'exercice des tâches de 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 aux 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 imputer individuellement les 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, tout au moins un réseau logiquement séparé de celui des utilisateurs, doit être utilisé. Les postes d'administrateur 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 en 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[10]

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

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.

Gestion des comptes

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 les comptes d'utilisateur standard, les comptes d'administration (domaine, serveurs, postes de travail) et les 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 mots de passe des comptes de service sont souvent inscrits en dur dans des applications ou dans des systèmes. Cette mauvaise pratique ne permet pas d'être en mesure de changer ces mots de passe, par exemple en urgence. Il est ainsi nécessaire de veiller à pouvoir 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,

[10] La notion de domaine est prise ici dans son sens général, à savoir un regroupement d'équipements. Il s'agirait par exemple, dans une architecture Microsoft, du regroupement de machines partageant des informations d'annuaires.

que ce soient des comptes d'utilisateur (administrateur, service ou utilisateur standard) ou des comptes de machine.

EXP-DOM-ADMINLOC : améliorer la gestion des comptes d'administrateur locaux. Afin d'empêcher la réutilisation des empreintes d'un compte d'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 de sécurité labellisés. L'effacement des données sensibles doit s'appuyer sur des produits de sécurité labellisés 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 de sécurité labellisés 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, des serveurs applicatifs et des 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 envoyés à 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 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 aux contraintes et au 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 les 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 l'être dans une version pour laquelle

l'éditeur assure le support et le tient 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, qui sont 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 par un filtrage strict, au niveau des éléments d'authentification, qui ne doivent pas être communs avec le reste du SI, et au niveau des applications (aucune ressource ne doit être partagée 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 d'homologation et mise en œuvre. Le niveau de sécurité d'un système d'information dépend en grande partie de la capacité de ses exploitants et de ses administrateurs à détecter les erreurs, les dysfonctionnements et les 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 pendant douze mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

Objectif 23 :

Défendre les SI nécessite une vigilance de tous et des actions permanentes.

Défense des systèmes d'information

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 présente PSSI. 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 des 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 autorités administratives au sens de l'ordonnance n° 2005-1516 du 8 décembre 2005 appliquent les règles de l'annexe B3 du référentiel général de sécurité pour l'authentification des utilisateurs distants. Les autres entités s'inspirent de ces règles.

Sécurisation des imprimantes et des copieurs multifonctions manipulant des informations sensibles

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

EXP-IMP-2 : sécurité des imprimantes et des copieurs multifonctions. Les imprimantes et les 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.

Objectif 24 :

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).

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 les 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 (exemples : serveur Web, Reverse Proxy).

EXP-CI-LTA : logiciels en tiers application. Des règles de développement et de configuration sécurisés des logiciels en tiers application doivent être fixées et appliquées.

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.

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

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 types de flux d'administration : les flux d'administration de l'infrastructure, réservés aux agents du centre informatique, et les flux d'administration des applications métier, réservés à la direction métier. L'attribution des droits d'administration doit respecter cette différenciation. Les deux 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, par exemple la réattribution d'une machine ou d'un 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, *etc.*) doit s'accompagner d'une opération de destruction avant remise au constructeur.

EXP-CI-TRAC : traçabilité et 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 lorsque ces supports ont été utilisés pour mémoriser des informations sensibles 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 aux 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 et contrôle. Le RSSI pilote des audits réguliers du système d'information relevant de sa responsabilité.

Sécurité du poste de travail

Objectif 25 :

Durcir les configurations des postes de travail en protégeant les utilisateurs.

Mise à disposition du poste

PDT-GEST : fourniture et gestion des postes de 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 de travail. Une procédure formalisée de configuration des postes de travail est établie par chaque entité, conformément aux recommandations de l'ANSSI.

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 par 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 de 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 des administrateurs. Les privilèges d'accès des administrateurs doivent être utilisés uniquement pour les actions d'administration le nécessitant.

PDT-ADM-LOCAL : gestion du compte de l'administrateur local. L'accès au compte de l'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 en réseau, eux-mêmes sauvegardés selon les exigences des entités et en accord avec les règles de sécurité en vigueur.

PDT-SAUV-LOC : sauvegarde et synchronisation des données locales. Dans le cas où des données doivent être stockées localement 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. Un moyen de chiffrement labellisé doit être mis à la 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 SI de l'entité. Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent intervenir via des réseaux privés virtuels (VPN) de confiance conformes aux recommandations de l'ANSSI.

PDT-NOMAD-PAREFEU : pare-feu local. Un pare-feu local conforme aux recommandations de l'ANSSI 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, *etc.*), 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.

Objectif 26 :

Paramétrer les imprimantes et les copieurs multifonctions afin de diminuer leur surface d'attaque.

Sécurisation des imprimantes et des copieurs multifonctions

PDT-MUL-DURCISS : durcissement des imprimantes et des copieurs multifonctions. Les imprimantes et les 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 en réseau inutiles, suppression des services inutiles, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible, configuration de 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 à une seule adresse de messagerie.

Objectif 27 :

Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes.

Sécurisation de la téléphonie

PDT-TEL-MINIM : sécuriser la configuration des autocommutateurs. Les autocommutateurs doivent être maintenus à jour en ce qui concerne les 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 un 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.

Objectif 28 :

Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

Contrôles de conformité

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

Objectif 29 :

Reconnaître la sécurité comme une fonction essentielle et la prendre en compte dès la conception des projets.

Développement des systèmes

DEV-INTEGR-SECLOC : intégrer la sécurité dans les développements locaux. Toute initiative locale de développement informatique doit respecter les recommandations de l'ANSSI, 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 de 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 portées à sa connaissance, en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation.

Objectif 30 :

Mener les développements des logiciels
selon une méthodologie de sécurisation du code produit.

Développements des logiciels et sécurité

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 à 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 du logiciel. La sécurité doit être intégrée à toutes les étapes 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, en particulier les développements en PHP, 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 règles de bonne pratique 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 dites « arc-en-ciel », attaques par force brute, *etc.*

Objectif 31 :

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

Applications à risques

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

Objectif 32 :

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.

Chaînes opérationnelles

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

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 de la 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, fait l'objet d'un compte-rendu, via la chaîne de SSI, au centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI.

La remontée d'incidents par les chaînes opérationnelles participe à la vigilance permanente. Cette remontée est immédiate pour les incidents dont la portée est susceptible de dépasser à court terme le périmètre de l'entité 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 les procédures précis de remontée d'incidents sont élaborés sous le pilotage de la chaîne fonctionnelle de la SSI, en lien avec la chaîne opérationnelle.

Chaque entité doit maintenir à jour un historique précis des suites de chaque incident, afin de capitaliser les enseignements tirés de la résolution ou non de ces incidents.

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

Continuité d'activité

Objectif 33 :

Se doter de plans de continuité d'activité et les tester.

Gestion de la continuité d'activité des SI

PCA-MINIS : définition du plan de continuité d'activité des SI. Chaque entité définit un plan de continuité d'activité des SI permettant d'assurer, en cas de sinistre, la continuité d'activité des SI.

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 objectifs du plan de continuité d'activité des systèmes d'information permettant d'assurer effectivement, en cas de sinistre, la continuité de l'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 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. Elles en assurent la supervision quotidienne et la maintenance dans le temps.

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

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 SI

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 la tenue à jour du plan local de continuité d'activité des SI.

Conformité, audit, inspection, contrôle

Objectif 34 :

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

Contrôles

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

Annexe 2 - Différentes classes de réseau

Un réseau de classe 0 est un réseau public (Internet, *etc.*) ou un réseau connecté à un réseau public qui ne respecte pas les exigences de la classe 1 ci-dessous.

Un réseau de classe 1 est un réseau qui est isolé de tout réseau de classe 0 à l'aide de dispositifs de filtrage et de rupture de flux de la façon suivante[11] :

- au moins un dispositif de filtrage qualifié au niveau standard est mis en coupure de tous les flux depuis et vers le réseau de classe 0 ;
- un dispositif de rupture de tous les flux (proxy) depuis et vers le réseau de classe 0, si possible qualifié au niveau élémentaire, est positionné entre deux dispositifs de filtrage ;
- une sonde de détection qualifiée au moins au niveau élémentaire contrôle l'ensemble des flux échangés avec le réseau de classe 0.

Les interconnexions entre réseaux de classe 1 sont autorisées[12]. La définition de la passerelle d'interconnexion est à la charge des entités concernées. L'interconnexion fait l'objet d'une homologation distincte de celle des réseaux.

Un réseau de classe 2 est un réseau qui :

- est isolé, c'est-à-dire non connecté, même indirectement, à Internet ;
- ne comprend aucune interconnexion « descendante »[13] permettant l'envoi de flux en clair ou chiffrés à destination des réseaux de classe 0 ou 1, sauf à utiliser des dispositifs agréés spécifiquement pour cet usage ;
- comprend éventuellement des interconnexions « montantes » permettant la réception de flux en provenance des réseaux de classe 0 ou 1 au travers d'une diode agréée par l'ANSSI pour de tels usages.

Les interconnexions entre réseaux de classe 2 sont autorisées[14]. La définition de la passerelle d'interconnexion est à la charge des entités concernées. L'interconnexion fait l'objet d'une homologation distincte de celle des réseaux.

---

[11] Voir la note technique de l'ANSSI sur son site web : « Définition d'une architecture de passerelle d'interconnexion sécurisée » présentant les principes de conception de dispositifs d'interconnexion.

[12] L'interconnexion est autorisée compris via un réseau de classe 0 dès lors que des équipements de chiffrement agréés par l'ANSSI sont utilisés en coupure (voir article 14).

[13] Un flux descendant est un flux dont l'origine est un réseau de classe 2 et la destination un réseau de classe inférieure ; un flux montant est, à l'inverse, un flux dont la destination est un réseau de classe 2 et l'origine un réseau de classe inférieure ; il ne s'agit pas d'un flux de transit, entre deux composants d'un réseau de classe 2, au travers d'un réseau de classe inférieure.

[14] L'interconnexion est autorisée y compris via un réseau de classe 0 dès lors que des équipements de chiffrement agréés par l'ANSSI sont utilisés en coupure (voir article 14).

Annexe 3 - Textes de référence

Mention *Diffusion Restreinte* et équivalents étrangers

Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale (IGI n° 1300), approuvée par arrêté du 30 novembre 2011.

Instruction générale interministérielle n° 2100/SGDN/SSD du 1er décembre 1975 sur la protection en France des informations classifiées de l'Organisation du Traité de l'Atlantique Nord (IGI n° 2100).

Instruction générale interministérielle n° 2102/SGDSN/PSE/PSD du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union Européenne (IGI n° 2102).

Protection du potentiel scientifique et technique de la nation

Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation.

Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation.

Circulaire interministérielle de la mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation du 7 novembre 2012.

Référentiel général de sécurité

Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n°2005-1516 du 8 décembre 2005.

Arrêté du 13 juin 2014 portant approbation du RGS V2 et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.

Politique de sécurité des systèmes d'information de l'Etat

Circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 portant politique de sécurité des systèmes d'information de l'Etat.

Guides de l'ANSSI

Guide d'hygiène informatique.

Guide « L'homologation de sécurité en neuf étapes simples ».

Note technique « Définition d'une architecture de passerelle d'interconnexion sécurisée ».

Guide « Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information ».

Guide d'élaboration de politiques de sécurité des systèmes d'information.