



Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS)

Ce document a été réalisé par

le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI)
du Service du Haut Fonctionnaire de Défense et de Sécurité (HFDS)
des ministères chargés des affaires sociales

en relation avec le bureau conseil
de l'agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
du Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN)

Ministères chargés des affaires sociales
Service du Haut Fonctionnaire de Défense et de Sécurité
14 avenue Duquesne
75350 PARIS 07 SP

hfds@sg.social.gouv.fr

ET APPROUVE LE 1^{ER} OCTOBRE 2015

PAR

LE SECRETAIRE GENERAL, HAUT FONCTIONNAIRE DE DEFENSE ET DE SECURITE (HFDS)
DES MINISTERES CHARGES DES AFFAIRES SOCIALES

NOR : AFSZ1523362A

SOMMAIRE

Préambule	6
1. Objet du document	7
2. Champ d'application	7
2.1. Périmètre d'application.....	7
2.2. Gestion des évolutions	8
3. Enjeux et objectifs de la SSI	8
3.1. Enjeux en matière de SSI	8
3.2. Objectifs en matière de SSI.....	9
4. Organisation de la SSI pour les ministères chargés des affaires sociales	10
4.1. Organisation de la cybersécurité (Sécurité des Systèmes d'Information)	11
4.1.1. Chaîne décisionnelle de cyberdéfense (SSI)	12
4.1.2. Chaîne fonctionnelle de cyberdéfense (SSI)	15
4.1.3. Chaîne opérationnelle de cyberdéfense (SSI)	16
5. Pilotage de la cybersécurité	17
6. Mesures particulières pour les MCAS	18
ANNEXE 1 Cybersécurité – Mise en œuvre simplifiée.....	19
<i>De la mise en place d'une gouvernance de la sécurité des systèmes d'information : Une approche graduelle .</i>	<i>20</i>
Organisation :	20
Cartographie : Savoir ce que l'on possède et ce que l'on veut protéger	20
Analyser des risques	21
Protéger	21
ANNEXE 2 Règles	22
<i>Politique, organisation, gouvernance</i>	<i>22</i>
Organisation de la sécurité des systèmes d'information	22
Organisation SSI	22
Acteurs SSI	22
Responsabilités internes	22
Responsabilités vis-à-vis des tiers	22
PSSI ministérielle.....	22
Application des mesures de sécurité au sein de l'entité	23
<i>Ressources humaines</i>	<i>23</i>
Utilisateurs.....	23
Personnel permanent	23
Mouvement de personnel	23
Personnel non permanent	24
<i>Gestion des biens</i>	<i>24</i>
<i>Intégration de la SSI dans le cycle de vie des systèmes d'information</i>	<i>25</i>
Gestion des risques et homologation de sécurité	25
Maintien en condition de sécurité des systèmes d'information	25
Produits et services labellisés	26

Gestion des prestataires	26
<i>Sécurité physique</i>	27
Sécurité physique des locaux abritant les SI	27
Règles de sécurité s'appliquant aux zones d'accueil du public	27
Règles de sécurité complémentaires s'appliquant aux locaux techniques	27
Sécurité physique des centres informatiques	28
Règles générales	28
Règles de sécurité complémentaires s'appliquant aux zones internes et restreintes	28
Règles de sécurité complémentaires s'appliquant aux salles informatiques et aux locaux techniques	28
SI de sûreté	29
<i>Sécurité des réseaux</i>	29
Sécurité des réseaux nationaux	29
Sécurité des réseaux locaux	30
Accès spécifiques	30
Sécurité des réseaux sans fil	30
Sécurisation des mécanismes de commutation et de routage	30
Cartographie réseau	31
<i>Architecture des SI</i>	31
<i>Exploitation des SI</i>	32
Protection des informations sensibles	32
Sécurité des ressources informatiques	32
Gestion des autorisations et contrôle d'accès logique aux ressources	32
Contrôle des accès logiques	32
Processus d'autorisation	33
Gestion des authentifiants	33
Gestion des authentifiants d'administration	33
Exploitation sécurisée des ressources informatiques	34
Administration des systèmes	34
Administration des domaines	34
Envoi en maintenance et mise au rebut	35
Lutte contre les codes malveillants	35
Mise à jour des systèmes et des logiciels	36
Journalisation	36
Défense des systèmes d'information	36
Gestion des matériels informatiques fournis à l'utilisateur	37
Nomadisme	37
Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles	37
Exploitation des centres informatiques	38
Sécurité des ressources informatiques	38
<i>Sécurité du poste de travail</i>	39
Sécurisation des postes de travail	39
Mise à disposition du poste	39
Sécurité physique des postes de travail	39
Réaffectation du poste et récupération d'informations	39
Gestion des privilèges sur les postes de travail	40
Protection des informations	40
Nomadisme	40
Sécurisation des imprimantes et copieurs multifonctions	41
Sécurisation de la téléphonie	41
Contrôles de conformité	41
<i>Sécurité du développement des systèmes</i>	42
Développement des systèmes	42
Développements logiciels et sécurité	42
Applications à risques	43

<i>Traitement des incidents</i>	43
Chaînes opérationnelles	43
Traitement des alertes de sécurité émises par les instances nationales (FSSI / ANSSI)	43
Remontée des incidents de sécurité rencontrés (Cf. Annexe 3).....	43
<i>Continuité d'activité</i>	44
Gestion de la continuité d'activité des SI.....	44
Définition du plan de continuité d'activité des systèmes d'information d'une entité	44
Mise en œuvre du plan local de continuité d'activité des systèmes d'information	44
Maintien en conditions opérationnelles du plan local de continuité d'activité des Systèmes d'Information ...	45
Contrôles.....	45
ANNEXE 3 gestion des incidents	46
ANNEXE 4 Homologation	52
<i>Options qui s'offrent à l'autorité d'homologation ?</i>	52
<i>Définition de la stratégie d'homologation</i>	52
<i>Maîtrise des risques</i>	52
<i>Prise de décision</i>	53
<i>Suivi a posteriori</i>	53
<i>Exemple de document de stratégie :</i>	53
<i>Exemple de décision d'homologation</i>	58
ANNEXE 5 GLOSSAIRE	59

Préambule

Les évolutions des modes de travail dans les administrations et des relations avec les citoyens et usagers placent les systèmes d'information au cœur des activités. La présence d'intelligence embarquée, de l'extension des systèmes de pilotage centralisé de processus, du déploiement de services de mobilité et de la dématérialisation des procédures à l'attention des citoyens contribuent ainsi de manière structurante aux métiers essentiels des administrations de l'Etat (ministères, établissements publics sous tutelle d'un ministère, services déconcentrés et autorités administratives) et concourent à l'amélioration de la qualité de service rendu. Ils font partie intégrante de leur patrimoine informationnel.

Ces Systèmes d'Information (SI) sont exposés à de multiples menaces pouvant gravement porter atteinte au fonctionnement de ces structures. Par ailleurs, l'exposition et la complexité des SI ne font que croître, du fait de besoins d'ouverture, de mutualisation, d'harmonisation, de valorisation et de flexibilité toujours plus importants.

Ainsi, afin de prendre en compte ces évolutions et les risques associés, le Premier ministre a défini une politique de sécurité des systèmes d'information de l'Etat (PSSIE) qui fixe les règles de protection applicables aux systèmes d'information de l'Etat. Cette PSSIE affiche la volonté de l'Etat de se montrer exemplaire en matière de cybersécurité.

Pour garantir cette exigence, la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS), qui repose sur la PSSIE, définit le cadre régissant la mise en œuvre de la sécurité des systèmes d'information, avec comme objectif la protection des systèmes d'information et des infrastructures critiques pour l'ensemble des périmètres ministériels et permettre :

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

Les déclinaisons sectorielles (par exemple la PGSSI-S pour le secteur de la santé) ou d'organismes, doivent se conformer à la PSSI-MCAS ou à la PSSI-E.

La PSSI-MCAS s'adresse, sans exception, à l'ensemble des agents des MCAS et aux prestataires opérant au profit des ministères, et tout particulièrement :

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

La PSSI-MCAS reprend dans ses annexes les mesures techniques générales de la PSSI-E, qui constituent un socle minimal. Pour certaines applications, ce socle minimal ne devra pas être considéré comme suffisant. Chaque autorité qualifiée en sécurité des systèmes d'information s'appuie sur la PSSI-MCAS, sur les normes existantes et sur les guides techniques de l'ANSSI et du service du Haut fonctionnaire de défense et de sécurité des MCAS pour élaborer des mesures techniques détaillées.

Elle se décompose comme suit :

- ▶ Présentation des enjeux liés à la Sécurité des SI pour les MCAS, et des objectifs à atteindre pour obtenir un niveau de sécurité conforme à ces enjeux ;
- ▶ Définition des principes de gouvernance SSI au sein des MCAS;
- ▶ Définition d'une organisation de la Sécurité des SI, en détaillant les rôles et responsabilités des différents acteurs des MCAS;
- ▶ Formalisation des règles de sécurité à appliquer, permettant de garantir un niveau de protection adapté aux enjeux, contraintes et activités propres des Ministères Sociaux, de manière cohérente entre toutes les structures.

1. Objet du document

Le présent document définit la politique de sécurité des systèmes d'information des ministères chargés des affaires sociales (PSSI-MCAS). Cette politique repose sur la politique de sécurité des systèmes d'information de l'Etat du 17 juillet 2014 (PSSI-E) dont elle constitue la déclinaison sectorielle applicable aux MCAS.

La PSSI-MCAS s'articule en deux parties.

- La première partie, précise dans le contexte des MCAS l'organisation SSI prévue par la PSSI de l'Etat, en laissant la possibilité aux entités des MCAS de s'organiser à leur tour en leur sein.
- La seconde partie est un ensemble d'annexes :
 - L'annexe 1 indique schématiquement les actions à mettre en œuvre pour mettre en place une gouvernance de la sécurité des systèmes d'information.
 - L'annexe 2 reprend l'ensemble des mesures et règles techniques édictées par la PSSI-E pour les MCAS.
 - L'annexe 3 indique les procédures à mettre en place en cas d'incident/attaque.
 - L'annexe 4 concerne l'homologation obligatoire (simple ou suivant le référentiel général de sécurité) des systèmes d'information.
 - Enfin, un glossaire est mis en annexe 5

2. Champ d'application

2.1. Périmètre d'application

La politique de sécurité des systèmes d'information s'applique aux systèmes d'information contribuant à la mise en œuvre des missions confiées aux ministres :

- des affaires sociales, de la santé et des droits des femmes ;
- du travail, de l'emploi, de la formation professionnelle et du dialogue social ;
- de la ville, de la jeunesse et des sports.

Ils seront désignés ministères chargés des affaires sociales (MCAS) dans l'ensemble du document.

Elle concerne donc les directions, les services centraux, les services déconcentrés des MCAS, ainsi que les établissements placés sous leurs tutelles. Elle concerne également, par voie contractuelle ou conventionnelle, toute personne physique ou morale tierce intervenant dans un système d'information dont l'activité concourt aux missions des MCAS (fournisseurs, prestataires de services, sous-traitants, employés, agents...).

La politique ministérielle de sécurité des systèmes d'information des MCAS est un document à usage interne au ministère et externe (prestataires). Destiné à être connu, il ne fait pas l'objet de protection particulière et peut être communiqué en externe sans restriction.

2.2. Gestion des évolutions

La PSSI-MCAS devra être revue périodiquement pour prendre en compte :

- Les évolutions des directives et politiques de sécurité des Systèmes d'Information Ministérielles, par exemple la PSSI État, ou des orientations de l'ANSSI ;
- Les résultats d'analyses de risques, d'actions de contrôle ou d'inspection ;
- Les évolutions du contexte organisationnel et technologique des MCAS ;
- Les évolutions de périmètre des MCAS.

3. Enjeux et objectifs de la SSI

3.1. Enjeux en matière de SSI

Au-delà des systèmes informatiques, le terme « Systèmes d'Information » correspond à l'ensemble des ressources (les hommes, le matériel, les logiciels) organisées pour collecter, stocker, traiter et communiquer de l'information au sein même d'une organisation et dans ses relations avec l'extérieur.

L'indisponibilité, la modification et la divulgation non autorisées de ces ressources, essentielles au bon fonctionnement des MCAS, entraînerait des impacts forts sur ses activités : perte de marché public, perte de crédibilité, manquement grave aux obligations légales et réglementaires, atteinte au bon déroulement des activités, mise en danger de personnes, etc.

De ce fait, les Systèmes d'Information des MCAS portent des enjeux forts :

Des enjeux de continuité de service des activités de l'État

Une défaillance des Systèmes d'Information des MCAS pourrait nuire de façon importante à la continuité des services de l'État, notamment en ce qui concerne les services essentiels au fonctionnement du pays et à sa défense, et entraîner une non-conformité aux Directives Nationales de Sécurité.

Des enjeux d'image liés à une défaillance dans le service aux citoyens

La sécurisation des Systèmes d'Information des MCAS joue un rôle primordial dans le service aux citoyens ; une défaillance de ceux-ci pourrait en effet porter atteinte à l'image des MCAS et entraîner une perte de confiance de l'action ministérielle. Cela peut notamment se traduire par :

- Une perte de confiance des citoyens, en cas de défaillances dans le fonctionnement du système de protection sanitaire, social ou de solidarité ;
- Une perte de confiance des citoyens en cas de perte ou de divulgation d'informations à caractère personnel protégées par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- Une perte de confiance des citoyens et des professionnels du secteur, en cas de divulgation d'informations de santé publique, de sécurité nationale, financières ou sociales ;
- Une perte de confiance des fournisseurs en particulier dans le cas où les informations liées aux marchés public seraient divulguées ou compromises ;
- Une perte de confiance en cas d'usurpation ou de dénaturation d'informations ;

- Une perte de confiance en cas de mauvaise utilisation ou de détournement d'argent public ;
- Une perte de crédibilité sur la gestion ministérielle, en particulier dans l'hypothèse où les données opérationnelles, financières et statistiques ne seraient pas fiables ou produites à temps, etc.

Des enjeux d'organisation interne

Une défaillance de ces systèmes conduirait à une importante désorganisation dans la conduite des activités quotidiennes des Ministères et de leurs opérateurs. En effet, les processus étant très intégrés dans les SI, tout sinistre sur les SI (infrastructure bureautique, applications, etc.) a des conséquences directes sur les activités et peut ainsi ralentir les prises de décision et la mise en œuvre de traitements.

3.2. Objectifs en matière de SSI

Afin de répondre aux enjeux décrits ci-avant, il est donc nécessaire d'assurer :

■ La disponibilité des SI

La disponibilité des SI est au centre des préoccupations sécuritaires ministérielles, pour garantir la communication et le traitement des demandes des citoyens, des entreprises, des associations et des autres administrations.

Les SI doivent remplir leurs fonctions dans des conditions prédéfinies d'horaires, de délais et de performance.

■ L'intégrité des données et des traitements

Les SI doivent garantir que les informations opérationnelles sont inaltérables et certifier de leur exhaustivité, de leur validité et de leur cohérence.

■ La confidentialité des informations manipulées par les SI des MCAS

Les SI doivent garantir la confidentialité des informations sensibles, voire critiques du point de vue politique, économique, ou nominatif, en respectant notamment les obligations légales et réglementaires.

■ La traçabilité des événements sur le SI

Les SI doivent permettre la traçabilité des événements majeurs afin d'assurer notamment l'imputabilité des actions, le contrôle du bon déroulement des traitements, ou encore la maîtrise des accès au SI des MCAS.

Le respect de ces objectifs de sécurité de l'information implique notamment de :

■ Réaliser les analyses de risques pesant sur les SI

La sécurisation des SI passe en premier lieu par la réalisation de l'analyse des risques. Cela permet d'envisager les moyens organisationnels et techniques à mettre en place pour un juste niveau de sécurité au regard des enjeux et de concourir ainsi à la gestion des risques.

■ Mettre les SI en conformité avec les lois et réglementations.

Différentes obligations légales ou réglementaires doivent faire l'objet d'une prise en compte par les autorités (CNIL, RGS, eIDAS...) et de leur mise en conformité.

■ Sensibiliser et former le personnel

Les pratiques quotidiennes des utilisateurs et administrateurs des SI sont un élément clé de la SSI, et il est alors essentiel de leur faire prendre conscience et de les former aux enjeux de la sécurité de l'information.

■ Sécuriser les composants des SI et Maintenir les SI en condition de sécurité

La sécurisation des composants du SI concerne les **postes de travail, serveurs bureautiques et applicatifs, réseaux, applications etc.** ainsi que les éléments en périphérie des ressources informatiques tels que la sécurité physique des locaux.

La mise en place de SI demande, outre le maintien en condition opérationnel, de penser au maintien en condition de sécurité (mise à jour des correctifs de sécurité, vérification des comptes utilisateur...)

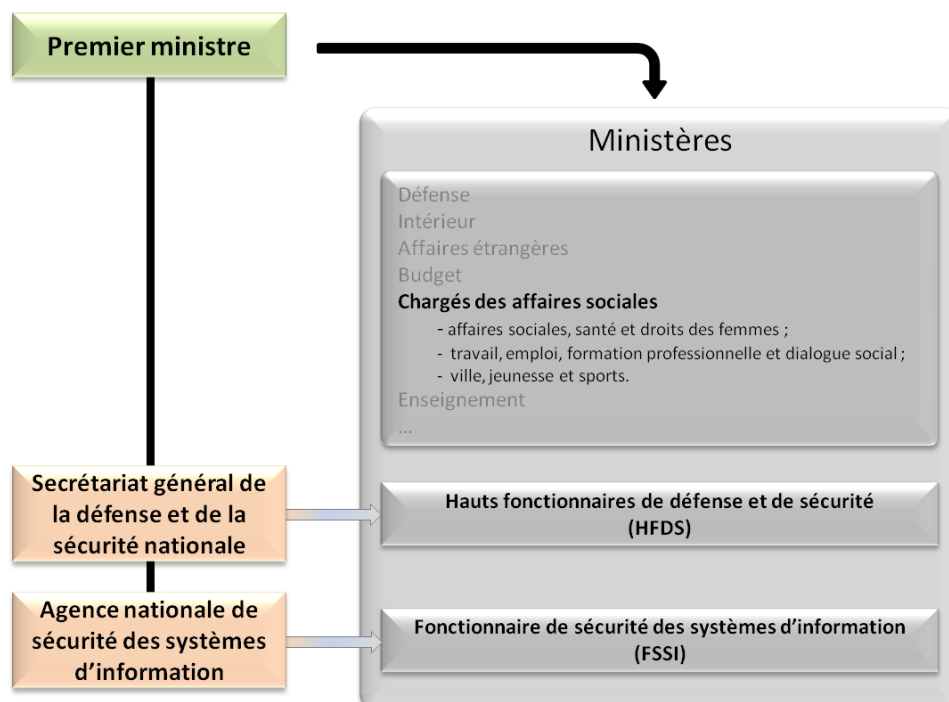
■ **Gestion efficace des incidents de sécurité, des crises et de la continuité d'activité ;**

La survenue d'un événement anormal affectant l'un des composants d'un système d'information et de communication doit être déclaré par tout agent auprès de son responsable informatique de proximité, de son responsable de la sécurité des systèmes d'information ou le cas échéant de l'AQSSI dont il dépend. En cas d'incident, sinistre ou piratage critique suspecté ou avéré, le service du Haut fonctionnaire de défense et de sécurité en est informé sans délai. Le FSSI peut être saisi directement (Cf. Annexe 3).

4. Organisation de la SSI pour les ministères chargés des affaires sociales

Comme le précise la loi n°2013-1168 du 18 décembre 2013, « le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité¹ nationale de sécurité des systèmes d'information », l'ANSSI, rattachée au secrétaire général de la défense et de la sécurité nationale.

La sécurité de l'information relève des responsabilités propres à chaque ministre dans le domaine dont il a la charge.



¹ Agence nationale de sécurité des systèmes d'information

4.1. Organisation de la cybersécurité (Sécurité des Systèmes d'Information)

Afin de répondre efficacement aux enjeux importants en matière de cybersécurité (ou sécurité des systèmes d'information), il est primordial de définir une organisation de la SSI qui soit adaptée aux besoins et spécificités des MCAS et suffisamment modulable pour s'appliquer à l'ensemble du périmètre des MCAS (l'administration centrale, services déconcentrés, opérateurs et établissements sous tutelle).

La sécurité des systèmes d'information ou cybersécurité, souvent abrégée « SSI » repose sur trois chaînes en coordination :

■ Une chaîne décisionnelle SSI.

Elle décide, sur son périmètre de compétence, de l'organisation SSI et des mesures de protection des systèmes d'information à appliquer. Elle est composée comme suit :

- ▶ *les ministres ;*
- ▶ *le secrétaire général, haut fonctionnaire de défense et de sécurité ;*
- ▶ *le haut fonctionnaire de défense et de sécurité adjoint ;*
- ▶ *le fonctionnaire de sécurité des systèmes d'information (FSSI) ;*
- ▶ *les délégués sectoriels à la stratégie des systèmes d'information ;*
- ▶ *les autorités qualifiées en sécurité des systèmes d'information (AQSSI) ;*
- ▶ *les autorités d'homologation (AH) pour leur système d'information.*

■ Une chaîne fonctionnelle SSI.

Pour le compte des autorités hiérarchiques, elle :

- ▶ *fait appliquer les mesures de protection des SI et les textes réglementaires et en contrôle l'application ;*
- ▶ *conseille les autorités, les responsables de systèmes d'information, les directeurs de projet ;*
- ▶ *évalue le niveau de sécurité des SI, et exprime les risques portés par les systèmes d'information ;*
- ▶ *met en œuvre les systèmes d'information sécurisés gouvernementaux conçus par le SGDSN.*

Elle est composée comme suit :

- ▶ *le fonctionnaire de sécurité des systèmes d'information (FSSI) ;*
- ▶ *le cas échéant, l'autorité d'appui (AA), représentant de l'autorité qualifiée ;*
- ▶ *le responsable de la sécurité des systèmes d'information (RSSI²) placé auprès de l'AQSSI ;*
- ▶ *les maîtrises d'ouvrage (en tant que de besoin).*

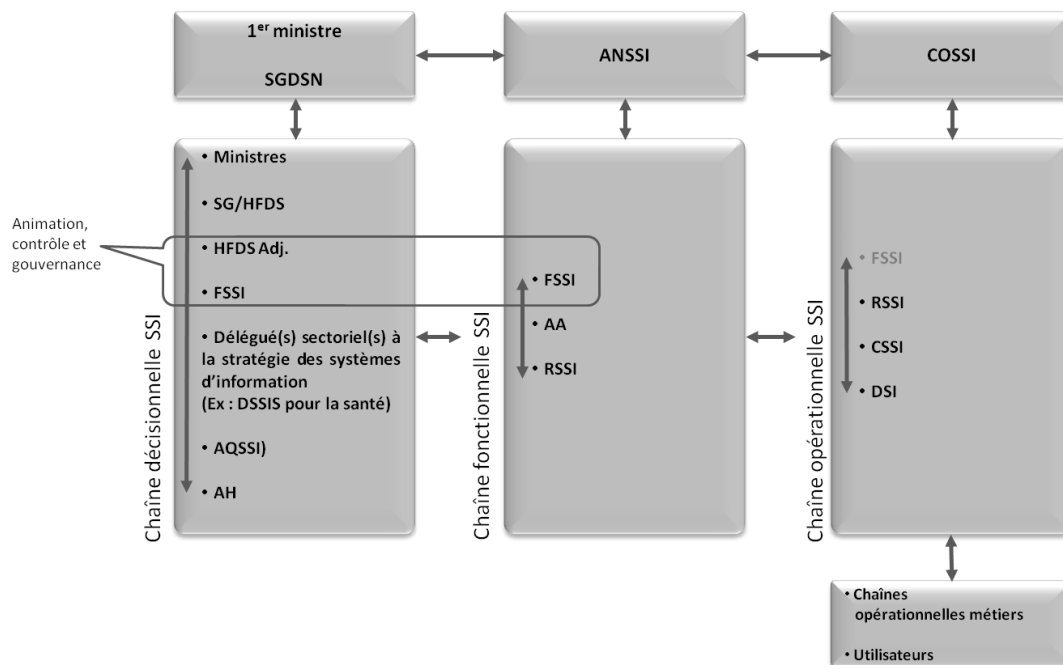
■ Une chaîne opérationnelle SSI.

Elle recherche les signaux précurseurs d'attaques, détecte les incidents de sécurité ou les attaques, exécute les actions d'urgence, et informe la chaîne fonctionnelle sur les menaces. Elle est composée comme suit :

- ▶ *le responsable de la sécurité des systèmes d'information (RSSI) placé auprès de l'AQSSI ;*
- ▶ *les directions ou services informatiques locaux ;*
- ▶ *les maîtrises d'œuvre (en tant que de besoin).*

▶ ² la dénomination varie en fonction des organismes (*responsable, officier, correspondant, conseiller, agent...* de la sécurité des systèmes d'information). Ils seront dénommé responsable de la sécurité des systèmes d'information dans la suite du document.

La gouvernance, l'animation et le contrôle de cet ensemble sont assurés par le service du haut fonctionnaire de défense et de sécurité. Afin d'assurer une cohérence entre les enjeux de sécurité et les enjeux de la gouvernance des systèmes d'information, le fonctionnaire de sécurité des systèmes d'information coordonne ses actions avec les directions, délégations ou services en charge de la stratégie et de la gouvernance des systèmes d'information des MCAS ou sectoriels.



4.1.1. Chaîne décisionnelle de cyberdéfense (SSI).

La sécurité de l'information relève des responsabilités propres à chaque ministre dans le domaine dont il a la charge.

Il est assisté par un haut fonctionnaire de défense et de sécurité (HFDS) dont les attributions sont fixées par le code de la défense. Le HFDS relève directement de ministres et dispose d'un service spécialisé.

Un fonctionnaire de sécurité des systèmes d'information (FSSI) est nommé par les ministre et placé sous l'autorité du HFDS. Il anime la politique de sécurité des systèmes d'information et en contrôle l'application.

Dans le respect des réglementations et des instructions interministérielles, les Ministres décident de l'organisation et des mesures de sécurité et de défense applicables aux systèmes d'information des MCAS, formalisées au sein de la politique de sécurité des systèmes d'information.

■ Le Haut Fonctionnaire de Défense et de Sécurité (HFDS)

Conformément aux missions édictées par l'article R1143-5 du Code de la Défense, en qualité de conseiller des ministres chargés des affaires sociales pour toutes les questions relatives à la défense et aux situations d'urgence affectant la défense, la sécurité et la vie de la nation, il doit notamment animer la politique de sécurité des systèmes d'information et contrôler l'application de celle-ci.

Pour exercer ses missions, il s'appuie sur le haut fonctionnaire de défense adjoint et le service qui lui est attaché.

En vue de garantir la sécurité globale des MCAS, le haut fonctionnaire de défense et de sécurité (HFDS) assisté du FSSI, anime, coordonne et contrôle l'application de la présente politique par les AQSSI.

■ Le Fonctionnaire de la Sécurité des Systèmes d'Information (FSSI)

Il est l'animateur de la Politique de Sécurité au sein pour les ministères chargés des affaires sociales et contrôle son application. Pour cela, il doit notamment :

- ▶ Assurer la mise en place et le bon fonctionnement, dans le cadre des directives du Secrétariat général de la défense et de la sécurité nationale (SGDSN), des moyens sécurisés de communication électronique gouvernementale en s'appuyant sur les services chargés de télécommunications ;
- ▶ Orienter la politique de sécurité des systèmes d'information, en s'appuyant sur les directions et services, et plus particulièrement sur les services chargés de l'informatique et des télécommunications. À ce titre, il lui incombe de constituer la voie fonctionnelle de sécurité des systèmes d'information ainsi que d'animer le réseau des Autorités Qualifiées de la Sécurité des Systèmes d'Information (AQSSI) ;
- ▶ Assurer la diffusion des directives et des recommandations de l'agence nationale de la sécurité des systèmes d'information (ANSSI) du secrétariat général de la défense et de la sécurité nationale (SGDSN) vers les directions et services et en vérifier l'application ;
- ▶ Mener auprès des opérateurs les actions de sensibilisation, d'incitation et de concertation nécessaires au renforcement de la sécurité de leurs systèmes d'information ;
- ▶ Faire procéder à la déclinaison ministérielle des plans gouvernementaux de vigilance, de prévention, de protection et de réaction ayant trait à la SSI à destination du centre opérationnel de sécurité des systèmes d'information (COSSI) de l'ANSSI ;
- ▶ Mettre en place les procédures nécessaires à la remontée des incidents et événements affectant la sécurité des systèmes d'information ainsi que la diffusion des alertes ;
- ▶ Participer aux travaux interministériels sur l'évolution des dispositions et des systèmes de protection en matière de SSI ;
- ▶ Définir les besoins de formation en matière de SSI et participer aux exercices de défense intéressant son domaine.

■ Les Autorités Qualifiées pour la Sécurité des Systèmes d'Information (AQSSI)

Pour toute entité des MCAS, est désignée une « autorité qualifiée pour la SSI (AQSSI)³ », qui est l'autorité hiérarchique qui possède la capacité d'arbitrage sur les moyens employés (organisationnels et techniques) pour que les systèmes d'information se rapprochent d'un état de sécurité jugé optimal. Elle est donc en charge de l'allocation et de l'emploi des moyens consacrés à la sécurité des systèmes d'information relevant de son domaine de compétence. Sa responsabilité ne peut être déléguée.

La désignation des AQSSI, est formalisée par arrêté, en distinguant les systèmes d'information propres à une entité des systèmes d'information transverses (mis en œuvre par un acteur au profit de plusieurs entités).

Elles sont juridiquement responsables de la sécurité des systèmes d'information sur leur périmètre (entité métier et/ou géographique) et doivent, dans leur périmètre de compétence :

- ▶ organiser la chaîne fonctionnelle SSI pour leur entité, composée des responsables de la sécurité des systèmes d'information ;
- ▶ définir, à partir des objectifs de sécurité fixés par le HFDS et la réglementation, une politique de sécurité des systèmes d'information adaptée à leur structure ;
- ▶ faire appliquer les directives, les instructions ministérielles et interministérielles, et les réglementations, diffusées, relayées ou transposées par le SHFDS ;
- ▶ s'assurer que les dispositions réglementaires et/ou contractuelles, sur la sécurité des systèmes d'information, sont appliquées, notamment au regard des systèmes traitant d'informations classifiées ou sensibles, et au regard des démarches d'homologation de sécurité des systèmes d'information ;

³ Directeurs d'administration centrale ; directeurs régionaux des entreprises, de la concurrence, de la consommation, du travail et de l'emploi ; directeurs régionaux de la jeunesse, des sports et de la cohésion sociale ; directeurs des agences sanitaires nationales et des agences régionales de santé ; directeurs des autres établissements publics et organismes placés sous la tutelle des ministres chargés des affaires sociales.

- ▶ *suivre la programmation et l'exécution des éventuelles actions correctives suite aux contrôles ou inspections portant sur la sécurité des systèmes d'information ;*
- ▶ *sensibiliser et former le personnel aux questions de sécurité ;*
- ▶ *rendre compte immédiatement au SHFDS, de tout incident et de tout phénomène suspect pouvant affecter la SSI avec, si besoin, un régime d'astreinte approprié.*
- ▶ *rendre compte annuellement, au Haut fonctionnaire de défense, de l'application des mesures prescrites en sécurité des systèmes d'information et de la gestion des incidents de sécurité et des cyberattaques.*

Bien que sa responsabilité ne puisse être déléguée, l'AQSSI peut désigner une Autorité d'Appui (AA) aux fins de la représenter, dans les différents organes de pilotage de la sécurité des systèmes d'information, sans en porter toutefois la responsabilité, et d'assurer la liaison fonctionnelle avec le FSSI.

Il existe également des systèmes d'information placés sous des responsabilités conjointes, parfois réparties sur plusieurs ministères. Ils relèvent alors simultanément de chacune des autorités qualifiées impliquées.

■ Les Autorités d'Homologation (AH)

L'homologation de sécurité est l'acte formel par lequel l'entité administrative en charge d'un système d'information atteste auprès des utilisateurs que son système d'information est protégé conformément aux enjeux de sécurité portés par le système.

L'autorité qualifiée pour la SSI peut prononcer l'homologation de sécurité pour les systèmes d'information relevant de son périmètre, mais plus fréquemment, elle désigne une autorité d'homologation à cet effet.

Le niveau de l'autorité d'homologation dans la hiérarchie de l'organisme doit correspondre au niveau stratégique du système d'information considéré. L'autorité d'homologation est une personne physique représentant l'autorité administrative. Elle est chargée de s'engager sur l'acceptabilité de la sécurité pour l'autorité administrative. Il est donc souhaitable que l'autorité d'homologation soit un décideur de la chaîne hiérarchique.

L'autorité prononçant l'homologation s'appuie sur l'avis émis par une commission d'homologation. Cette commission prononce un avis motivé sur la capacité du système à répondre ou non aux objectifs de sécurité assignés, et à s'assurer que l'ensemble des mesures techniques et organisationnelles permettant la sécurisation du système ont toutes été prises et sont correctement appliquées.

L'autorité prononçant l'homologation désigne les membres de la commission d'homologation, dans le respect des règles suivantes :

- ▶ *les représentants de la chaîne fonctionnelle SSI des différents acteurs du projet (notamment dans un contexte interministériel) sont membres de la commission ;*
- ▶ *le fonctionnaire de sécurité des systèmes d'information peut siéger ou participer aux commissions d'homologation.*

Prononcer l'homologation d'un système d'information est une décision d'autorité par laquelle l'administration valide l'utilisation d'un système pour exploiter des informations et/ou soutenir une activité dans des conditions d'emploi précises. Cette homologation fait l'objet d'un document formel indiquant le périmètre, la durée d'homologation et les risques résiduels acceptés. (Cf. Annexe 3)

L'autorité d'homologation transmet au SHFDS la décision d'homologation accompagnée du dossier ayant motivé cette décision.

4.1.2. Chaîne fonctionnelle de cyberdéfense (SSI)

Placée sous l'autorité fonctionnelle du fonctionnaire de sécurité des systèmes d'information (FSSI), la chaîne fonctionnelle SSI est un réseau de personnes (« acteurs SSI ») agissant de façon coordonnée, au profit des autorités hiérarchiques dont elles relèvent, pour :

- ▶ **conseiller** sur les mesures de sécurité et de défense des systèmes d'information à mettre en œuvre, notamment au moyen de l'expression des risques portés par les systèmes ;
- ▶ **contrôler** l'application effective des mesures de sécurité prescrites par la réglementation et des mesures de sécurité décidées par la chaîne décisionnelle ;
- ▶ **piloter** la chaîne de cyberdéfense en charge de la réponse aux incidents de sécurité des systèmes d'information, en lien direct avec l'ANSSI ;
- ▶ **mettre en œuvre** les systèmes d'information sécurisés gouvernementaux conçus par le SGDSN et gérer les « articles contrôlés de la SSI » qui s'y rapportent ;
- ▶ **rendre compte** à la chaîne décisionnelle, de l'application des mesures prescrites en sécurité des systèmes d'information et de la gestion des incidents de sécurité et des cyberattaques.

■ Les Responsables de Sécurité des Systèmes d'Information

L'essentiel de la chaîne fonctionnelle SSI est composée de conseillers dont les appellations varient. Ils sont désignés « responsables de la sécurité des systèmes d'information » (dénommés RSSI dans la suite du document).

Ils sont en charge des missions générales de la chaîne fonctionnelle SSI citées au début du présent chapitre.

Au sein de chaque entité des MCAS, les AQSSI décident de l'organisation de leur chaîne fonctionnelle SSI, dans le respect de la réglementation ainsi que de la présente politique.

La totalité du périmètre sous responsabilité de l'AQSSI doit être couvert par la chaîne fonctionnelle SSI (informatique et communication générale, technique, d'infrastructure, bâtiminaire, etc.).

Le document décrivant cette organisation doit être validé par l'AQSSI (« note d'organisation », « politique SSI... »).

Même en l'absence d'une telle organisation formelle, l'AQSSI est tenue de désigner au moins un représentant de sa chaîne fonctionnelle SSI. Le fonctionnaire de sécurité des systèmes d'information est informé de cette désignation ainsi que des coordonnées du RSSI.

- ▶ Le RSSI est désigné par l'autorité hiérarchique correspondant au périmètre pour lequel il exerce. La désignation est transmise au FSSI pour information, sous couvert de l'AQSSI. Le cas échéant, la quotité en équivalent-temps-plein consacrée à cette fonction SSI est mentionnée lors de la désignation.
- ▶ **Dans la mesure du possible**, Le RSSI est sans lien de subordination avec la direction, service ou le bureau des systèmes d'information et de communication. Le cas échéant, un rattachement direct au plus haut responsable en charge des systèmes d'information doit être envisagé. Dans ce cas, le lien de subordination ne doit pas s'exercer vis-à-vis des missions de la chaîne fonctionnelle de cybersécurité (sécurité des systèmes d'information). En effet, pour l'exercice de ses fonctions le RSSI rend compte directement à l'autorité qui l'a désigné, ainsi qu'à sa chaîne fonctionnelle SSI.
- ▶ Conseiller de l'autorité en matière de SSI, il dispose de l'autorité et du statut nécessaire pour assurer ses missions au sein de sa structure, notamment par rapport aux services en charge des moyens s'appuyant sur des systèmes d'information (ex : informatique, téléphonie, bâtiment, biomédical, technique...).
- ▶ réalise au moins deux entretiens annuels avec l'autorité qui l'a désigné, permettant notamment d'effectuer le bilan annuel de la SSI, des incidents, et des risques ;

La fonction SSI doit être correctement dimensionnée et identifiée. L'importance de la chaîne fonctionnelle doit être adaptée aux enjeux, à la taille, et à la dispersion géographique des services. Si l'ampleur de la tâche ou la situation géographique le justifie, Le RSSI pourra être secondé par un adjoint et/ou disposer d'un réseau de correspondants locaux de sécurité des systèmes d'information. Ainsi, au RSSI d'un grand opérateur pourrait être mis en place les services d'un adjoint et d'autant de correspondants qu'il existe de directions.

Dans le cas d'un réseau SSI d'organisme, afin de garantir synergie et réactivité, le RSSI doit mettre en place et assurer une communication et une transparence permanente auprès de toutes les personnes impliquées, en termes d'incidents, d'actions en cours, des constats associés et mesures prises.

Le RSSI doit particulièrement :

- ▶ *Conduire des actions de sensibilisation et de formation à la SSI ;*
- ▶ *Établir un inventaire des SI et évaluer la sensibilité de tous les éléments représentant de la valeur pour l'organisation (actifs⁴) ;*
- ▶ *Conduire des analyses de risques pour tout nouveau système d'information sensible et pour toute évolution majeure de système d'information sensible existant ;*
- ▶ *Mettre en application les dispositions de sécurité édictées par les maîtres d'ouvrage des SI ;*
- ▶ *Conduire des actions régulières de contrôle du niveau de sécurité des SI et mettre en œuvre les actions correctives nécessaires ;*
- ▶ *Définir et mettre en place les modalités permettant de faire face aux alertes, aux incidents de sécurité et aux situations d'urgence concernant la sécurité des SI ;*
- ▶ *Demander et/ou allouer les moyens nécessaires à la mise en œuvre des actions relatives à la sécurité des SI.*

Le RSSI pourra s'appuyer sur des relais techniques dans les différentes entités (métier / géographique) afin de mettre en œuvre les dispositions de la PSSI-MCAS.

4.1.3. Chaîne opérationnelle de cyberdéfense (SSI)

Le Haut fonctionnaire de défense des MCAS s'assure de l'existence continue au sein des MCAS d'une chaîne opérationnelle de cyberdéfense.

Dans l'immédiat, cette chaîne opérationnelle est articulée autour du FSSI qui, à ce titre, exerce principalement les activités :

- ▶ *de veille et alerte sur les cyberattaques et de pilotage ministériel de la réponse aux incidents de sécurité significatifs ;*
- ▶ *d'appui aux corps d'inspections, aux autorités judiciaires et plus largement aux autorités hiérarchiques en matière cybersécurité ;*
- ▶ *de suivi dans la durée des actions de prévention et de protection à mener afin que les incidents les plus significatifs ne se reproduisent pas ;*
- ▶ *de communication interne régulière, au profit de tous les agents, des hautes autorités, ou des instances techniques, aux fins de prévention et de sensibilisation au regard des cyberattaques effectivement constatées ;*
- ▶ *de gestion de la communauté des acteurs SSI (informations, formations, soutien en matière d'expertise et de conseil) ;*

⁴ Par 'actif', l'on comprend un bien ou un service ayant une certaine valeur pour l'entreprise. Les actifs sont sujets à différentes vulnérabilités, susceptibles d'être exploitées par des menaces qui auront des impacts au niveau de l'entreprise. Pour protéger ses actifs, une entreprise mettra en place des mesures de sécurité. La sélection de ces mesures se fait lors de la phase de gestion des risques. Il y a deux types d'actifs :

- actifs primaires: processus et informations
- actifs de support: tous les autres actifs comme notamment les personnes, machines, ...

Le FSSI pilote la chaîne opérationnelle SSI, qui l'informe des événements, incidents ou attaques SSI. A défaut d'organisation locale plus précise, c'est le FSSI qui réceptionne les signalements relatifs à de tels événements de la part de l'ensemble des services et agents du ministère, ainsi que des partenaires extérieurs.

Le FSSI est le point de contact des MCAS pour l'agence nationale de sécurité des systèmes d'information (ANSSI). Il assure notamment la liaison avec le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) armé par le Centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI.

5. Pilotage de la cybersécurité

La cybersécurité et la défense des systèmes d'information reposent sur trois piliers :

- ▶ *la gestion des risques SSI (évaluation, traitement, communication...) ;*
- ▶ *les contrôles SSI (audits de vulnérabilités des SI) ;*
- ▶ *la gestion des incidents SSI.*

Pour les MCAS, un niveau de pilotage de la SSI est défini. En outre, des groupes de travail sectoriels précisent les mesures de sécurité génériques concernant leur périmètre et élaborent les documents d'application (guides, recommandations, exceptions...).

■ Le comité stratégique de la sécurité des systèmes d'information

Le pilotage de la sécurité des systèmes d'information et de communication est placé sous l'autorité du haut fonctionnaire de défense. Il préside annuellement le comité stratégique de la sécurité des systèmes d'information. Y participent :

- ▶ *le haut fonctionnaire de défense et son adjoint ;*
- ▶ *le fonctionnaire de sécurité des systèmes d'information ;*
- ▶ *le directeur des systèmes d'information des MCAS ;*
- ▶ *le(s) délégué(s) sectoriel (s) à la stratégie des systèmes d'information ou leur représentant ;*
- ▶ *les autorités qualifiées en sécurité des systèmes d'information ou leurs représentants ;*

Ses principales missions sont de :

- ▶ *veiller à l'application de la présente instruction et à la progression du niveau de conformité des MCAS à la PSSI de l'Etat ;*
- ▶ *exploiter le bilan des incidents significatifs, et l'état des lieux des cybermenaces susceptibles d'affecter les MCAS ;*
- ▶ *exploiter les résultats des contrôles SSI menés sur les SI jugés essentiels et les actions qui en découlent ;*
- ▶ *Arbitrer les priorités globales des MCAS en matière de cybersécurité et de défense des systèmes d'information, au regard de la gestion des risques.*

■ Les groupes de travail sectoriels ou techniques en sécurité des systèmes d'information

Des groupes de travail sectoriels ou techniques placés sous le pilotage des AQSSI ou de délégué(s) sectoriel(s) à la stratégie des systèmes d'information ou de leur représentant. Ils se réunissent autant que de besoin.

Des groupes de travail peuvent être déclinés aux échelons territoriaux.

Un groupe est composé des représentants de la chaîne fonctionnelle SSI et de la chaîne opérationnelle SSI.

A l'échelon central, il comprend principalement :

- ▶ *le Fonctionnaire SSI ;*

- ▶ le responsable de la sécurité des systèmes d'information des MCAS
- ▶ les conseillers SSI auprès des AQSSI et ceux au sein des acteurs des systèmes d'information et de communication ;
- ▶ les représentants des chaînes opérationnelles SSI des acteurs des systèmes d'information et de communication.

Ses principales missions sont de :

- ▶ diffuser et transposer en interne les réglementations, guides et recommandations de l'ANSSI ;
- ▶ élaborer, diffuser et tenir à jour les documents d'application de la PSSI-MCAS et les recommandations SSI à vocation ministérielle ;
- ▶ élaborer et proposer à la validation du Haut fonctionnaire de défense adjoint les instructions et directives SSI à vocation ministérielle ;
- ▶ proposer au Haut fonctionnaire de défense adjoint les dérogations à la PSSI-MCAS.

6. Mesures particulières pour les MCAS

La prise en compte, sur l'ensemble des acteurs du périmètre des MCAS, du niveau de sécurité et des moyens dédiés, nécessite un ajustement de certaines règles de la PSSIE.

Les règles indiquées en annexe 2 sont la déclinaison pour le périmètre des MCAS. Elles déclinent le socle minimal à respecter.

Conformément à la PSSIE, il est possible, sur autorisation du Haut fonctionnaire de défense et de sécurité de déroger à certaines règles.

Pour ne pas baisser le niveau minimal de sécurité admissible, toute demande de dérogation, doit être accompagnée systématiquement d'une analyse de risques, validée par le SHFDS.

Concernant particulièrement certains travaux SSI sectoriels pour l'établissement de règles ou recommandations, le SHFDS participant à l'ensemble de ces travaux, les documents validés et publiés sont applicables sur le secteur qu'ils adressent (par exemple la PGSSI-S).

ANNEXE 1 Cybersécurité – Mise en œuvre simplifiée

Mettre en œuvre la cybersécurité (ou sécurité des systèmes d'information) de façon performante et peu coûteuse ... c'est possible.

Si, dans un premier temps, les normes et les technologies de sécurité des systèmes d'information semblent souvent contraignantes et bien loin des impératifs métiers, il convient de revenir à l'essentiel, c'est-à-dire d'identifier la nature du périmètre à sécuriser, de protéger « l'ADN de l'organisme » regroupant tout à la fois : savoir-faire, informations (données métier, données privées, données de fonctionnement...) ainsi que les systèmes concourant à l'élaboration, au traitement, au stockage, à la diffusion de ces informations.

Les mesures de protection adaptées sont déjà bien souvent présentes : il suffit de les identifier et de les organiser afin d'assurer et de pérenniser un niveau de sécurité conforme à ses besoins.

La meilleure façon de protéger un organisme consiste à adopter un processus de gestion des risques dans une démarche d'amélioration continue, en prenant en considération les vrais besoins en matière de sécurité. Cette approche nécessite un peu de temps, mais elle sera mieux adaptée aux besoins réels - elle est plus efficace et moins chère.

De façon générale, la sécurité vise à réduire le nombre ainsi que l'envergure des impacts :

- ▶ juridiques
- ▶ sur la réputation
- ▶ sur le temps (perdu)
- ▶ sur le savoir-faire
- ▶ sur la santé
- ▶ financiers
- ▶ ...

Concernant l'impact financier, il est à noter que tout incident de sécurité sur un système d'information induit obligatoirement des surcoûts directs ou indirects très supérieurs aux investissements qui auraient pu être mis en place pour sécuriser les systèmes d'information.

Le risque peut se définir par le calcul suivant : $\text{risque} = \text{vulnérabilité} \times \text{menace} \times \text{impact}$. Il est composé d'un facteur 'probabilité' (provenant de la menace) et d'un facteur 'dégât' (provenant de la valeur de l'actif⁵ compromis et de la valeur du dommage indirect subi). La vulnérabilité utilisée dans cette fonction prend compte des mesures de sécurité mise en place.

⁵ Bien ou un service ayant une certaine valeur pour l'entreprise. Les actifs sont sujets à différentes vulnérabilités, susceptibles d'être exploitées par des menaces qui auront des impacts au niveau de l'entreprise. Pour protéger ses actifs, une entreprise mettra en place des mesures de sécurité. La sélection de ces mesures se fait lors de la phase de gestion des risques. Il y a deux types d'actifs :

- actifs primaires: processus et informations
- actifs de support: tous les autres actifs comme notamment les personnes, machines, ...

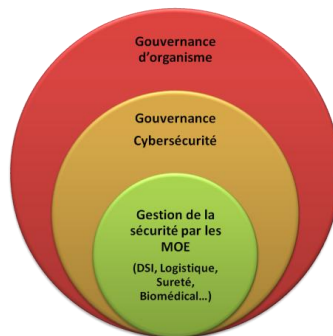
Il est pratiquement impossible de prévenir un risque en voulant agir sur les menaces existantes. Par contre, on peut agir sur le risque en réduisant les facteurs 'vulnérabilité' et 'impact' :

- réduire le facteur 'vulnérabilité', par la mise en place de mesures de sécurité ciblées ;
- réduire l'impact potentiel, par la mise en place d'un plan de continuité des systèmes d'information (inclus dans le plan de continuité de l'organisme) – par exemple mise en place de systèmes de redondances des données et d'un plan de reprise des systèmes d'information (inclus dans le plan de reprise d'activité).

De la mise en place d'une gouvernance de la sécurité des systèmes d'information : Une approche graduelle

Il s'agit d'établir et de maintenir un pilotage structuré de la cybersécurité afin de s'assurer que les stratégies de sécurité de l'organisation sont conformes aux objectifs de l'activité et compatibles avec les lois et les réglementations qui lui sont applicables.

Le pilotage de la sécurité par les risques est une approche « stratégique » car elle permet d'acquérir une vision globale de la sécurité à travers les activités métiers de l'organisme. Elle facilite ainsi à la fois la mise en place immédiate de solutions de sécurité « curatives » sans pour autant perdre le lien avec les besoins de sécurité de l'entreprise mais permet surtout de mettre en place des moyens « préventifs » et ainsi réduire les surfaces de vulnérabilités ou d'attaque.



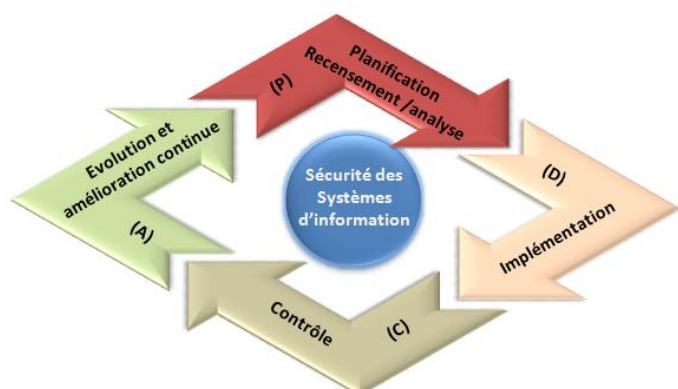
Organisation :

Dans le cadre de la sécurité des systèmes d'informations, toutes les responsabilités doivent être clairement définies dans l'organisation. La direction désigne les responsables ainsi que leurs champs de compétences.

Cartographie : Savoir ce que l'on possède et ce que l'on veut protéger

Il faut identifier les données et actifs indispensables à l'organisme et au bon accomplissement de ses missions (ex : *informatique générale, gestion technique centralisée (ascenseurs, ventilations, climatisation contrôles d'accès...), systèmes d'information hospitalier, systèmes de communication, informatique embarquée ou associée à des dispositifs médicaux....*).

L'organisation de la sécurité des systèmes d'information au sein d'un organisme suit une démarche cyclique (roue de Deming). La mise en œuvre de ce cycle implique la définition d'une gouvernance de la cybersécurité qui sera adaptée à la nature de l'activité et aura pour mission de démarrer et d'entretenir le cycle.



Analyser des risques

Pour pouvoir protéger les données et actifs importants et vitaux, il faut d'abord identifier les risques par une analyse, identifier les menaces et la probabilité que celles-ci risquent de survenir, identifier l'ampleur des vulnérabilités humaines et techniques et quantifier les impacts potentiels.

Le recensement des besoins de sécurité sera réalisé en répondant notamment aux questions suivantes :

- ▶ Quelles sont les activités critiques de mon organisation ?
- ▶ Quels sont les systèmes qui concourent au bon fonctionnement de ces activités ?
- ▶ Quelles sont les contraintes légales et réglementaires que l'on doit respecter ?
- ▶ Quelle est la disponibilité souhaitée de mes systèmes d'information ?
- ▶ Quelle résistance à l'altération des données et des traitements dois-je mettre en œuvre ?
- ▶ Quel est le niveau de confidentialité à prendre en compte pour les données et les traitements ?
- ▶ Faut-il conserver des traces des transactions numériques ?

Protéger

- ▶ procéder à la protection des données et des systèmes permettant leur traitement. Une fois classifiées, il faut mettre en place les moyens visant à assurer leur protection par des sauvegardes, lors de leur transport ou encore lors de leur transmission. Il convient également de prévoir leur destruction sécurisée.
- ▶ Mettre en place des mesures préventives et protectrices pour les matériels (ordinateurs, ordinateurs portables, serveurs, informatique embarquée ou adjointe) et pour les réseaux (téléphoniques, informatiques...)
- ▶ Mettre en place des mesures de type « réaction sur incidents ».

Sensibiliser et former la totalité des personnels

L'adoption des bonnes mesures comportementales par l'ensemble du personnel est une mesure extrêmement importante. Il importe donc de promouvoir une culture de la sécurité des systèmes d'information au travers de bonnes pratiques accessibles aux utilisateurs, maîtrises d'ouvrage et maîtrises d'œuvre.

Les utilisateurs doivent appliquer et respecter les règles de sécurité définies. Une charte d'utilisation des systèmes d'information doit être mise en place. Cette charte doit être opposable en cas d'incident ou de litige.

Cette approche n'est efficace que si elle est bien comprise par l'ensemble des différents acteurs. Cette démarche se doit d'intégrer bonnes pratiques de sécurité permettant de garantir le niveau de protection existant et/ou attendu.

Il est donc essentiel de propager une culture « sécurité » via une communication adaptée aux différents acteurs.

ANNEXE 2 Règles

Politique, organisation, gouvernance

Organisation de la sécurité des systèmes d'information

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

Organisation SSI

ORG-SSI : organisation SSI.

Une organisation dédiée à la SSI est déployée dans toutes les directions, services déconcentrés, agences régionales de santé, établissements publics et opérateurs du périmètre des MCAS. Cette organisation, établie selon les directives du haut fonctionnaire de défense et de sécurité (HFDS), définit les responsabilités internes et à l'égard des tiers, les modalités de coordination avec les autorités externes, ainsi que les modalités d'application des mesures de protection. Des procédures d'applications sont écrites et portées à la connaissance de tous.

Acteurs SSI

ORG-ACT-SSI : identification des acteurs SSI.

L'organisation SSI des MCAS s'appuie sur des acteurs SSI clairement identifiés, à tous ses niveaux d'organisation. Les acteurs responsables en matière de SSI sont chargés de la mise en application générale de la PSSI-MCAS. Ils sont référencés dans un annuaire ministériel. Cette chaîne fonctionnelle s'appuie sur le service du haut fonctionnaire de défense et de sécurité, notamment sur le fonctionnaire de sécurité des systèmes d'information (FSSI) pour les MCAS.

Responsabilités internes

ORG-RSSI : désignation du responsable SSI.

Chaque autorité qualifiée en sécurité des systèmes d'information (AQSSI) s'appuie sur un ou plusieurs responsables de la sécurité des systèmes d'information (RSSI), chargé(s) de l'assister dans le pilotage et la gestion de la SSI. Des correspondants locaux SSI (CLSSI) 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-MCAS par l'AQSSI et veille à leur application. Des dénominations alternatives des fonctions citées ci-dessus peuvent être utilisées si nécessaire.

ORG-RESP : formalisation des responsabilités.

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

Responsabilités vis-à-vis des tiers

ORG-TIERS : gestion contractuelle des tiers.

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

PSSI ministérielle

ORG-PIL-PMSSI : définition et pilotage de la PSSI ministérielle.

La PSSI-MCAS est placée sous la responsabilité du HFDS. Elle reprend le socle commun établi par la PSSI. Une structure de pilotage de la PSSI ministérielle est définie : le Comité Stratégique de la Sécurité des Systèmes d'Information (CosStratSSI). Cette structure est chargée de sa mise en place, de son évolution, de son suivi et de son contrôle.

Application des mesures de sécurité au sein de l'entité

ORG-APP-INSTR : application de l'instruction dans l'entité.

Le RSSI planifie les actions de mise en application de la PSSI-MCAS. Il rend compte régulièrement de la mise en application des mesures de sécurité à son autorité qualifiée et, le cas échéant au FSSI.

ORG-APP-DOCS : formalisation de documents d'application.

Le RSSI formalise et tient à jour les documents d'application, approuvés par l'autorité qualifiée, permettant la mise en œuvre des mesures de la PSSI-MCAS sur son périmètre.

Ressources humaines

Objectif 2 : ressources humaines. Faire des personnes les maillons forts des SI sur le périmètre des MCAS.

Utilisateurs

RH-SSI : charte d'application SSI.

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

Personnel permanent

RH-MOTIV : choix et sensibilisation des personnes tenant les postes clés de la SSI.

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

RH-CONF : personnels de confiance.

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

RH-UTIL : sensibilisation des utilisateurs des systèmes d'information.

Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant, et motivé à leur respect. Il doit être formé à l'utilisation des outils de travail conformément aux règles SSI.

Mouvement de personnel

RH-MOUV : gestion des arrivées, des mutations et des départs.

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

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

Personnel non permanent

RH-NPERM : gestion du personnel non permanent (stagiaires, intérimaires, prestataires ...).

Les règles de la PSSI-MCAS s'appliquent à tout personnel non permanent utilisateur d'un SI des MCAS. Les dispositions contractuelles préexistantes régissant l'emploi de ce personnel sont amendées si nécessaire. Pour tout personnel non permanent, un tutorat par un agent permanent est mis en place, afin de l'informer de ces règles et d'en contrôler l'application.

Gestion des biens

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

GDB-INVENT : inventaire des ressources informatiques.

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

GDB-CARTO : cartographie.

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

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

Concernant les MCAS la qualification de l'information en fonction du besoin de confidentialité est la suivante :

- ▶ Publique : Ce niveau concerne les informations réputées publiques et notamment celles publiées en ligne ou via un autre moyen de diffusion.
- ▶ Interne : Ce niveau traduit que la diffusion n'est pas possible vers des membres externes à un organisme.
- ▶ Limitée : Informations destinées à être diffusées uniquement à une liste spécifiée et restreinte de destinataires.

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.

Les informations sensibles reçoivent une mention rappelant leur sensibilité en considération de la gravité des conséquences qu'aurait une divulgation et apposer une mention telle que « confidentiel » sur les documents sensibles ainsi que dans les courriers ou courriels qui les accompagnent. A titre d'exemple, on pourra utiliser les mentions suivantes :

- ▶ Confidentiel médical
- ▶ Confidentiel personnel
- ▶ ...

Cette mention peut être complétée d'un marquage spécifiant l'usage restrictif qui doit être fait par son destinataire (diffusion interne, diffusion limitée)

GDB-PROT-IS : protection des informations.

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

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

Gestion des risques et homologation de sécurité

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

INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d'information.

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

Maintien en condition de sécurité des systèmes d'information

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

INT-SSI : intégration de la sécurité dans les projets.

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

INT-QUOT-SSI : mise en œuvre au quotidien de la SSI.

La sécurité des systèmes d'information se traite au quotidien par des pratiques d'hygiène informatique. Des procédures écrites définissent les actes élémentaires du maintien en condition de sécurité lors des phases de conception, évolution ou retrait d'un système. Tout système d'information doit faire l'objet, outre le maintien en condition opérationnelle, d'un maintien en condition de sécurité.

INT-TDB : créer un tableau de bord SSI.

Un tableau de bord SSI est mis en place et tenu à jour. Il fournit au RSSI et aux autorités une vision générale du niveau de sécurité et de son évolution, rendant ainsi plus efficace le pilotage de la SSI. Au niveau stratégique, le tableau de bord SSI permet de suivre l'application de la politique de sécurité et de disposer d'éléments propres à qualifier les ressources devant être allouées à la SSI.

Au niveau du pilotage, la mise en place de ce tableau de bord permet de contrôler la réalisation d'objectifs opérationnels, d'améliorer la qualité de service et de détecter au plus tôt les retards dans la réalisation de certains objectifs de sécurité.

Produits et services labellisés

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

INT-AQ-PSL : acquisition de produits et services de confiance.

Il est recommandé d'utiliser, lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI.

Dans le cadre d'un marché, un critère de choix, dont la notation est clairement définie, sur l'existence d'un label ANSSI est indiqué.

L'ordre de choix peut être le suivant (avec une quotation adaptée) :

- ▶ Qualification renforcée de l'(ANSSI) ;
- ▶ Qualification standard de l'ANSSI ;
- ▶ Reconnaissance SOG-IS⁶ ;
- ▶ Reconnaissance critères communs⁷ ;
- ▶ Certification de sécurité de premier niveau de l'ANSSI
- ▶ En cours de labellisation auprès de l'ANSSI (sans présomption du résultat mais dans ce cas avec l'obligation pour le soumissionnaire de fournir le récépissé du dépôt de la demande réalisée auprès de l'ANSSI) ;
- ▶ Reconnaissance autre ;
- ▶ Pas de labellisation.

La labellisation est réalisée suivant une cible de sécurité définie. En cas de plusieurs solutions labellisées proposées, une attention particulière doit donc être portée sur la cible de sécurité ayant permis leur labellisation (périmètre total ou partiel de la solution).

Gestion des prestataires

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

INT-PRES-CS : clauses de sécurité.

Toute prestation dans le domaine des SI doit être encadrée par des clauses de sécurité (plan d'assurance sécurité). Ces clauses spécifient les mesures SSI que le prestataire doit respecter dans le cadre de ses activités.

INT-PRES-CNTRL : suivi et contrôle des prestations fournies.

Le maintien d'un niveau de sécurité au cours du temps nécessite un double contrôle :

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

⁶ L'accord européen de reconnaissance mutuelle du SOG-IS permet la reconnaissance entre les États signataires de l'accord, des certificats délivrés par leur autorité de certification.

⁷ Critères Communs : la reconnaissance mutuelle par les signataires d'un accord d'acceptation des certificats de sécurité des technologies de l'information émis par l'un des pays signataires. Le produit certifié en toute impartialité par une autorité compétente, peut être utilisé sans nécessiter une évaluation plus poussée.

INT-REX-AR : analyse de risques.

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

INT-REX-HB : hébergement.

L'hébergement de données sensibles sur le territoire national est fortement recommandé. En outre, l'hébergement concernant certaines données doit répondre aux exigences légales et réglementaires (données nominatives, données de santé...).

INT-REX-HS : hébergement et clauses de sécurité.

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

Sécurité physique

Sécurité physique des locaux abritant les SI

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

PHY-ZONES : découpage des sites en zones de sécurité.

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

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

PHY-PUBL : accès réseau en zone d'accueil du public.

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

PHY-SENS : protection des informations sensibles au sein des zones d'accueil.

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

Règles de sécurité complémentaires s'appliquant aux locaux techniques

PHY-TECH : sécurité physique des locaux techniques.

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

PHY-TELECOM : protection des câbles électriques et de télécommunications.

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

PHY-CTRL : contrôles anti-piégeages.

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

Sécurité physique des centres informatiques

Le terme de centre peut désigner différents modèles (Service informatique, local informatique...) Il convient d'adapter au contexte de l'entité.

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

Règles générales

PHY-CI-LOC : découpage des locaux en zones de sécurité.

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

PHY-CI-HEBERG : convention de service en cas d'hébergement tiers.

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

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

PHY-CI-CTRLACC : contrôle d'accès physique.

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

PHY-CI-MOYENS : délivrance des moyens d'accès physique.

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

PHY-CI-TRACE : traçabilité des accès.

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

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

PHY-CI-ENERGIE : local énergie.

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

PHY-CI-CLIM : climatisation.

Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique doit être installé. Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement.

Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

PHY-CI-INC : lutte contre l'incendie.

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

PHY CI-EAU : lutte contre les voies d'eau.

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

SI de sûreté

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

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

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

PHY-SI-SUR : sécurisation du SI de sûreté.

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

Sécurité des réseaux

Sécurité des réseaux nationaux

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

RES-MAITRISE : systèmes autorisés sur le réseau.

Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'une entité.

RES-INTERCO : interconnexion avec des réseaux externes.

Toute interconnexion entre les réseaux locaux d'une entité et un réseau externe (réseau d'un tiers, Internet, etc.) doit être, pour les organismes éligibles, réalisée via les infrastructures nationales (réseau interministériel de l'Etat, RENATER). Pour les autres il convient de maîtriser les interconnexions (connaissance des fournisseurs d'accès, réversibilité de la solution, maintien en condition de sécurité)

RES-ENTSOR : mettre en place un filtrage réseau pour les flux sortants et entrants.

Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées.

RES-PROT : protection des informations.

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

Sécurité des réseaux locaux

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

RES-CLOIS : cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes.

Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.

RES-INTERCOGEO : interconnexion des sites géographiques locaux d'une entité.

L'interconnexion au niveau local de réseaux locaux d'une entité n'est possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions dédiées à cet effet, et de passerelles sécurisées et homologuées par l'AQSSI et validée par le HFDS.

RES-RESS : cloisonnement des ressources en cas de partage de locaux.

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

Accès spécifiques

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

RES-INTERNET-SPECIFIQUE : cas particulier des accès spécifiques dans une entité.

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

Sécurité des réseaux sans fil

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

RES-SSFIL : mise en place de réseaux sans fil.

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

Sécurisation des mécanismes de commutation et de routage

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

RES-COUCHBAS : implanter des mécanismes de protection contre les attaques sur les couches basses.

Une attention particulière doit être apportée à l'implantation des protocoles de couches basses, de façon à se prémunir des attaques usuelles.

RES-ROUTDYN : surveiller les annonces de routage.

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

RES-ROUTDYN-IGP : configurer le protocole IGP⁸ 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 être réalisée suivant les préconisations de l'Agence nationale de sécurité des systèmes d'information.

RES-ROUTDYN-EGP : sécuriser les sessions EGP⁹.

Lors de la mise en place d'une session EGP avec un pair extérieur sur un média partagé, cette session doit être réalisée suivant les préconisations de l'Agence nationale de sécurité des systèmes d'information.

RES-SECRET : modifier systématiquement les éléments d'authentification par défaut des équipements et services.

Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.

RES-DURCI : durcir les configurations des équipements de réseaux.

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

Cartographie réseau

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

RES-CARTO : élaborer les documents d'architecture technique et fonctionnelle.

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

Architecture des SI

Architecture des centres informatiques

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

ARCHI-HEBERG : principes d'architecture de la zone d'hébergement.

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

⁸ Interior Gateway Protocol

⁹ Exterior Gateway Protocol

ARCHI-STOCKCI : architecture de stockage et de sauvegarde.

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

ARCHI-PASS : passerelle Internet.

Les interconnexions Internet passent obligatoirement par des passerelles homologuées.

Exploitation des SI

Protection des informations sensibles

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

EXP-PROT-INF : protection des informations sensibles en confidentialité et en intégrité.

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

Sécurité des ressources informatiques

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

EXP-TRAC : traçabilité des interventions sur le système.

Les interventions de maintenance sur les ressources informatiques de l'entité doivent être tracées par le service informatique, et ces traces doivent être accessibles au RSSI local durant au moins un an.

EXP-CONFIG : configuration des ressources informatiques.

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

EXP-DOC-CONFIG : documentation des configurations.

La configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.

Gestion des autorisations et contrôle d'accès logique aux ressources

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

Contrôle des accès logiques

EXP-ID-AUTH : identification, authentification et contrôle d'accès logique.

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

EXP-DROITS : droits d'accès aux ressources.

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

EXP-PROFILS : gestion des profils d'accès aux applications.

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

Processus d'autorisation

EXP-PROC-AUTH : autorisations d'accès des utilisateurs.

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

EXP-REVUE-AUTH : revue des autorisations d'accès.

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

Gestion des authentifiants

EXP-CONF-AUTH : confidentialité des informations d'authentification.

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

EXP-GEST-PASS : gestion des mots de passe.

Les utilisateurs ne doivent pas stocker leurs mots de passe en clair (par exemple dans un fichier) sur leur poste de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.

EXP-INIT-PASS : initialisation des mots de passe.

Chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique. Si les circonstances l'imposent, un mot de passe plus simple mais à usage unique peut être envisagé.

EXP-POL-PASS : politiques de mots de passe.

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

EXP-CERTIFS : utilisation de certificats électroniques.

L'utilisation de certificats électroniques doit respecter les règles édictées par le RGS.

EXP-QUAL-PASS : contrôle systématique de la qualité des mots de passe.

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

Gestion des authentifiants d'administration

EXP-SEQ-ADMIN : séquestre des authentifiants « administrateur ».

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

EXP-POL-ADMIN : politique de mots de passe « administrateurs ».

Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.

EXP-DEP-ADMIN : gestion du départ d'un administrateur des SI.

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

Exploitation sécurisée des ressources informatiques

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

Administration des systèmes

EXP-RESTR-DROITS : restriction des droits.

Sauf exception dûment motivée et validée par le RSSI, les utilisateurs, quelque soit leur statut, n'ont pas de droits d'administration (domaine, local). Dans le cas d'une exception, elle doit être tracée et doit être renouvelée tous les ans. A défaut de renouvellement, les privilèges d'administration doivent être supprimés.

EXP-PROT-ADMIN : protection des accès aux outils d'administration.

L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès.

EXP-HABILIT-ADMIN : habilitation des administrateurs.

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

EXP-GEST-ADMIN : gestion des actions d'administration.

Les opérations d'administration doivent être tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration.

EXP-SEC-FLUXADMIN : sécurisation des flux d'administration.

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

EXP-CENTRAL : centraliser la gestion du système d'information.

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

EXP-SECX-DIST : sécurisation des outils de prise de main à distance.

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

Administration des domaines

EXP-DOM-POL : définir une politique de gestion des comptes du domaine.

Une politique explicite de gestion des comptes du domaine doit être documentée.

EXP-DOM-PASS : configurer la stratégie des mots de passe des domaines.

La politique de gestion des mots de passe doit être conçue de façon à protéger contre les attaques par essais successifs de mots de passe. Une complexité minimale dans le choix des mots de passe doit être imposée aux utilisateurs.

EXP-DOM-NOMENCLAT : définir et appliquer une nomenclature des comptes du domaine.

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

EXP-DOM-RESTADMIN : restreindre au maximum l'appartenance aux groupes d'administration du domaine.

L'appartenance aux groupes du domaine ADMINISTRATEURS et ADMINISTRATEURS DU DOMAINE n'est nécessaire que dans de très rares cas. Les opérations les plus courantes doivent être effectuées avec des comptes du domaine membres des groupes locaux d'administration des ordinateurs ou ayant une délégation d'administration.

EXP-DOM-SERV : maîtriser l'utilisation des comptes de service.

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

EXP-DOM-LIMITSERV : limiter les droits des comptes de service.

Les comptes de service doivent faire l'objet d'une restriction des droits, en suivant le principe du moindre privilège.

EXP-DOM-OBSOLET : désactiver les comptes du domaine obsolètes.

Il est nécessaire de désactiver immédiatement, voire de supprimer, les comptes obsolètes, que ce soient des comptes d'utilisateur (administrateur, de service ou utilisateur standard) ou des comptes de machine.

EXP-DOM-ADMINLOC : améliorer la gestion des comptes d'administrateur locaux.

Afin d'empêcher la réutilisation des empreintes d'un compte utilisateur local d'une machine à une autre, il faut soit utiliser des mots de passe différents pour les comptes locaux d'administration, soit interdire la connexion à distance via ces comptes.

Envoi en maintenance et mise au rebut

EXP-MAINT-EXT : maintenance externe.

Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique. Pour les équipements contenant des données sensibles, il doit être mis en place des mesures de rétention des supports d'information.

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 ou le support d'information détruit.

L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.

Lutte contre les codes malveillants

EXP-PROT-MALV : protection contre les codes malveillants.

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

EXP-GES-ANTIVIR : gestion des événements de sécurité de l'antivirus.

Les événements de sécurité de l'antivirus doivent être remontés sur un serveur central 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 directions, bureaux ou services informatiques, validé par le RSSI.

EXP-NAVIG : configuration du navigateur Internet.

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

Mise à jour des systèmes et des logiciels

EXP-POL-COR : définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité.

Le maintien dans le temps du niveau de sécurité d'un système d'information impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à chaque système ou applicatif doit être défini, et adapté suivant les contraintes et le niveau d'exposition du système.

EXP-COR-SEC : déploiement des correctifs de sécurité.

Les correctifs de sécurité des ressources informatiques locales doivent être déployés par l'équipe locale chargée des SI en s'appuyant sur les préconisations et outils proposés par les directions, bureaux ou services informatiques.

EXP-OBSOLET : assurer la migration des systèmes obsolètes.

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

EXP-ISOL : isoler les systèmes obsolètes restants.

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

Journalisation

EXP-JOUR-SUR : journalisation des alertes.

Chaque système doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité. Ces traces doivent être conservées de manière sûre.

EXP-POL-JOUR : définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces.

Une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie par le RSSI, validée par l'autorité qualifiée, et mise en œuvre. Le niveau de sécurité d'un système d'information dépend en grande partie de la capacité de ses exploitants et administrateurs à détecter les erreurs, dysfonctionnements et tentatives d'accès illicites survenant sur les éléments qui le composent.

EXP-CONS-JOUR : conservation des journaux.

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

Défense des systèmes d'information

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

EXP-GES-DYN : gestion dynamique de la sécurité.

Les personnes en charge de la SSI doivent procéder, notamment via l'analyse des journaux, à la surveillance des comportements anormaux au sein du système d'information, et à la surveillance des flux d'entrée et de sortie du système d'information.

Gestion des matériels informatiques fournis à l'utilisateur

EXP-MAIT-MAT : maîtrise des matériels.

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

EXP-PROT-VOL : rappel des mesures de protection contre le vol.

Les postes fixes bénéficient des mesures de protection physique offertes au titre de la directive de sécurité physique de la présente PSSI-MCAS. 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-REAFPECT : réaffectation de matériels informatiques.

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

Nomadisme

EXP-NOMAD-SENS : déclaration des équipements nomades aptes à traiter des informations sensibles.

L'autorité d'homologation du SI valide les usages possibles des équipements nomades vis-à-vis du traitement des informations sensibles ; les usages non explicitement autorisés sont interdits.

EXP-ACC-DIST : accès à distance au système d'information de l'organisme.

Les utilisateurs distants doivent s'authentifier sur le réseau de l'entité en utilisant une authentification forte.

Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles

EXP-IMP-SENS : impression des informations sensibles.

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

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

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

Exploitation des centres informatiques

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

Sécurité des ressources informatiques

EXP-CI-OS : systèmes d'exploitation.

Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque.

Une attention particulière doit être apportée aux comptes administrateurs.

EXP-CI-LTP : logiciels en Tiers Présentation.

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

EXP-CI-LTA : logiciels en Tiers Application.

Des règles de développement sécurisé, et les configurations des logiciels en Tiers Application doivent être fixées et appliquées.

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...).

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) d'une part, les flux d'administration des applications métier (réservés à la direction métier) d'autre part. L'attribution des droits d'administration doit respecter cette différenciation, et les 2 types de flux d'administration doivent être dans la mesure du possible cloisonnés.

EXP-CI-DNS : service de noms de domaine – DNS technique.

Dans le cas du déploiement d'un serveur de noms de domaines pour les besoins techniques internes au centre informatique, il sera utilisé de préférence les extensions sécurisées DNSSEC.

EXP-CI-EFFAC : effacement de support.

Le reconditionnement et la réutilisation des disques durs pour un autre usage (ex : réattribution d'une machine/serveur) ne sont autorisés qu'après une opération d'effacement sécurisé des données.

EXP-CI-DESTR : destruction de support.

La fin de vie d'un support ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur...) doit s'accompagner d'une opération de destruction avant remise au rebut.

EXP-CI-TRAC : traçabilité / imputabilité.

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

EXP-CI-SUPERVIS : supervision.

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

EXP-CI-AMOV : accès aux périphériques amovibles.

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

EXP-CI-ACCRES : accès aux réseaux.

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

EXP-CI-AUDIT : audit/contrôle.

Le RSSI pilote des audits réguliers du système d'information relevant de sa responsabilité.

Sécurité du poste de travail

Sécurisation des postes de travail

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

Mise à disposition du poste

PDT-GEST : fourniture et gestion des postes de travail.

Les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par l'équipe locale chargée des SI.

Si un poste est mis à disposition par une autre voie, sa connexion au réseau est soumise à l'autorisation du RSSI.

PDT-CONFIG : formalisation de la configuration des postes de travail.

Une procédure formalisée de configuration des postes de travail est établie par chaque entité.

Sécurité physique des postes de travail

PDT-VEROUIL-FIXE : verrouillage de l'unité centrale des postes fixes.

Lorsque l'unité centrale d'un poste fixe est peu volumineuse, donc susceptible d'être facilement emportée, elle doit être protégée contre le vol par un système d'attache (par exemple un câble antivol).

PDT-VEROUIL-PORT : verrouillage des postes portables.

Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation.

Réaffectation du poste et récupération d'informations

PDT-REAFECT : réaffectation du poste de travail.

Une procédure SSI définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.

Gestion des privilèges sur les postes de travail

PDT-PRIVIL : privilèges des utilisateurs sur les postes de travail.

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

PDT-PRIV : utilisation des privilèges d'accès « administrateur ».

Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.

PDT-ADM-LOCAL : gestion du compte « administrateur local ».

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

Protection des informations

PDT-STOCK : stockage des informations.

Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des entités.

PDT-SAUV-LOC : sauvegarde / synchronisation des données locales.

Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs.

PDT-PART-FIC : partage de fichiers.

Le partage de répertoires ou de données hébergées localement sur les postes de travail est à proscrire

PDT-SUPPR-PART : suppression des données sur les postes partagés.

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

PDT-CHIFF-SENS : chiffrement des données sensibles.

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

PDT-AMOV : fourniture de supports de stockage amovibles.

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

Nomadisme

PDT-NOMAD-ACCESS : accès à distance aux Systèmes d'Information de l'entité.

Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent être réalisés via des infrastructures homologuées. L'usage de réseaux privés virtuels (VPN) de confiance est nécessaire.

PDT-NOMAD-PAREFEU : pare-feu local.

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

PDT-NOMAD-STOCK : stockage local d'information sur les postes nomades.

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

PDT-NOMAD-FILT : filtre de confidentialité.

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

PDT-NOMAD-CONNEX : configuration des interfaces de connexion sans fil.

La configuration des interfaces de connexion sans fil doit interdire les usages dangereux de ces interfaces.

PDT-NOMAD-DESACTIV : désactivation des interfaces de connexion sans fil.

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

Sécurisation des imprimantes et copieurs multifonctions

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

PDT-MUL-DURCISS : durcissement des imprimantes et copieurs multifonctions.

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

PDT-MUL-SECNUM : sécurisation de la fonction de numérisation.

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

Sécurisation de la téléphonie

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

PDT-TEL-MINIM : sécuriser la configuration des autocommutateurs.

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

PDT-TEL-CODES : codes d'accès téléphoniques.

Il est nécessaire de sensibiliser les utilisateurs au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.

PDT-TEL-DECT : limiter l'utilisation du DECT.

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

Contrôles de conformité

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

PDT-CONF-VERIF : utiliser des outils de vérification automatique de la conformité.

Un outil de vérification régulière de la conformité des éléments de configuration des postes de travail doit être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration.

Développement des systèmes

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

DEV-INTEGR-SECLOC : intégrer la sécurité dans les développements locaux.

Toute initiative locale de développement informatique doit respecter les exigences SSI, concernant la prise en compte de la sécurité dans les projets et les développements informatiques (notamment la réalisation d'une analyse de risques). Le service à l'origine du projet se porte garant d'une démarche d'homologation du système de l'application et le cas échéant de l'application du référentiel général de sécurité.

DEV-SOUS-TRAIT : intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique.

Lors de l'écriture d'un contrat de sous-traitance de développement, plusieurs clauses relatives à la SSI doivent être intégrées :

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

Développements logiciels et sécurité

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

DEV-FUITES : limiter les fuites d'information.

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

DEV-LOG-ADHER : réduire l'adhérence des applications à des produits ou technologies spécifiques.

Le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. En phases de conception et de spécification technique, il est nécessaire de s'assurer que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent. En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent. En plus du maintien en condition de sécurité propre à l'application, il est donc nécessaire de pouvoir faire évoluer son environnement pour garantir sa sécurité dans la durée.

DEV-LOG-CRIT : instaurer des critères de développement sécurisé.

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

DEV-LOG-CYCLE : intégrer la sécurité dans le cycle de vie logiciel.

La sécurité doit être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

DEV-LOG-WEB : améliorer la prise en compte de la sécurité dans les développements Web.

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

DEV-LOG-PASS : calculer les empreintes de mots de passe de manière sécurisée.

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

Applications à risques

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

DEV-FILT-APPL : mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque.

Devant les applications à risques, il est recommandé de faire usage d'une solution tierce de filtrage applicatif.

Traitement des incidents

Chaînes opérationnelles

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

TI-OPS-SSI : chaînes opérationnelles SSI.

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

Traitement des alertes de sécurité émises par les instances nationales (FSSI / 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 (Cf. Annexe 3)

TI-QUAL-TRAIT : qualification et traitement des incidents.

La chaîne fonctionnelle SSI est informée par la chaîne opérationnelle de tout incident de sécurité, et contribue si nécessaire à la qualification de l'incident et au pilotage de son traitement.

TI-INC-REM : remontée des incidents.

Tout incident de sécurité, même apparemment mineur, dont l'impact dépasse ou est susceptible de dépasser le SI d'une entité ou des MCAS, fait l'objet d'un compte-rendu, via la chaîne SSI, au FSSI qui, le cas échéant, alerte le Centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI.

La remontée d'incidents par la chaîne opérationnelle ministérielle participe à la posture permanente de vigilance. Cette remontée est immédiate pour les incidents dont la portée est susceptible de dépasser à court terme le périmètre de l'entité ou des MCAS, 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. En fonction de la situation, le HFDS peut prescrire un rythme hebdomadaire ou journalier de ces remontés.

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

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

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

Continuité d'activité

Gestion de la continuité d'activité des SI

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

PCA-MINIS : définition du plan ministériel de continuité d'activité des Systèmes d'Information.

Les MCAS définissent un plan de continuité d'activité ministériel des systèmes d'information permettant d'assurer, en cas de sinistre, la continuité d'activité des systèmes d'information.

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

PCA-LOCAL : définition du plan local de continuité d'activité des systèmes d'information.

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

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

PCA-SUIVILocal : suivi de la mise en œuvre du plan de continuité d'activité local des Système d'Information (PCA des SI).

Le RSSI d'une entité s'assure de la bonne mise en œuvre des dispositions prévues dans le plan de continuité d'activité des systèmes d'information.

PCA-PROC : mise en œuvre des dispositifs techniques et des procédures opérationnelles.

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

PCA-SAUVE : protection de la disponibilité des sauvegardes.

Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées.

PCA-PROT : protection de la confidentialité des sauvegardes.

Les sauvegardes doivent être traitées de manière à garantir leur confidentialité et leur intégrité.

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

PCA-EXERC : exercice régulier du plan local de continuité d'activité des systèmes d'information.

Le RSSI d'une entité organise des exercices réguliers, afin de tester le plan local de continuité d'activité des systèmes d'information.

PCA-MISAJOUR : mise à jour du plan local de continuité d'activité des systèmes d'information.

Le RSSI d'une entité assure le maintien à jour du plan local de continuité d'activité des Systèmes d'Information.

Conformité, audit, inspection, contrôle

Contrôles

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

CONTR-SSI : contrôles locaux.

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

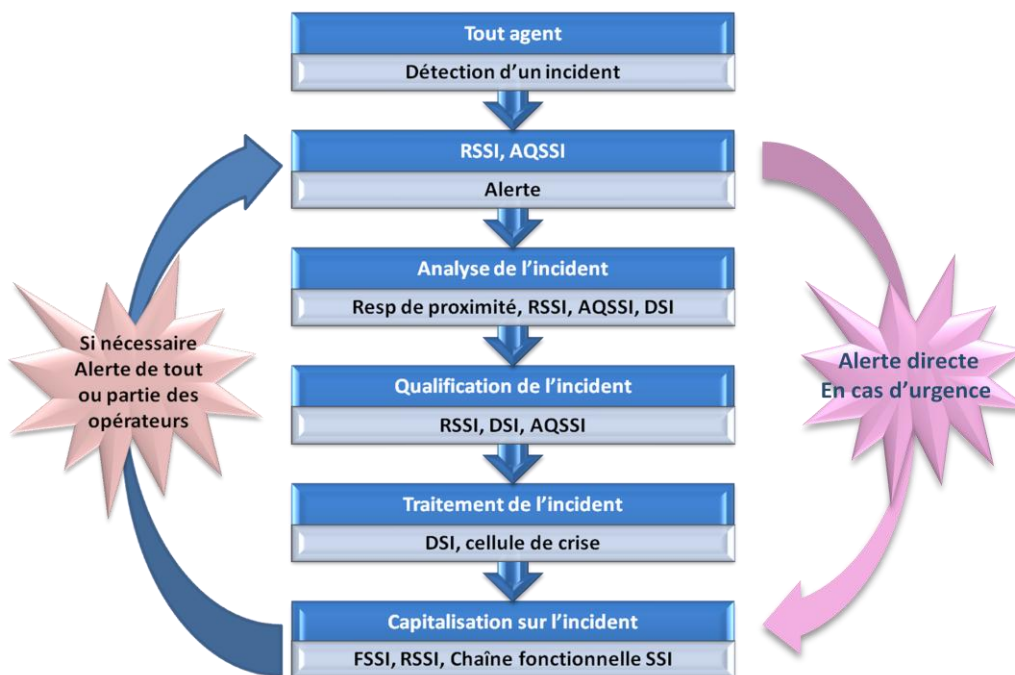
CONTR-BILAN-SSI : bilan annuel.

Les ministères chargés des affaires sociales établissent un bilan annuel mesurant sa maturité SSI globale, qu'il transmet à l'ANSSI.

ANNEXE 3 gestion des incidents liés à la sécurité de l'information¹⁰

La survenue d'un événement anormal affectant l'un des composants d'un SI doit être déclaré par tout agent le constatant auprès de sa chaîne SSI ou le cas échéant de l'AQSSI dont il dépend.

Le circuit de gestion d'un incident doit suivre le processus suivant



Après sa détection, l'incident est analysé par l'entité qui est alertée – RSSI, responsable de proximité, AQSSI, etc. - avec l'appui du service en charge de la sécurité opérationnelle. Ce dernier réalise une analyse technique permettant de définir la nature de l'incident et sa portée.

En cas d'incident critique suspecté, le FSSI pourra être saisi directement à l'adresse :

ssi@sq.social.gouv.fr (Cf. modèle de formulaire incident ci-dessous)

La qualification précise de l'incident requiert la mise en œuvre d'une matrice d'indice de gravité des incidents de sécurité basée sur 3 axes :

1. Les catégories d'incidents¹¹ :

- ▶ Accès, modification, collecte non autorisés de données,
- ▶ Divulgence d'information,
- ▶ Intrusion / prise de contrôle,
- ▶ Comportements anormaux (usages frauduleux, usages abusifs, comportements déviants,...),

¹⁰ La norme ISO 27035 sur la gestion des incidents

¹¹ La classification des incidents en catégorie peut être effectuée en s'appuyant sur EBIOS

- ▶ Présence de fichiers malveillants (malware),
 - ▶ Dysfonctionnements (dénier de service, par exemple : indisponibilité de service non expliquée),
 - ▶ Vulnérabilités critiques.
2. Le niveau de sensibilité des actifs impactés (services, applications ou données).
 3. L'ampleur de l'incident (nombre d'actifs impactés, niveau de contagion).

Dans le cadre de la gestion des incidents de sécurité, il est nécessaire de connaître les bons interlocuteurs avec qui échanger et communiquer les bonnes informations. Cela est indispensable afin d'éviter tout manquement qui nuirait à une réponse efficace face aux incidents.

En effet, les informations doivent circuler le plus rapidement possible au sein de l'organisation afin que les décisions prises le soient en ayant recueilli le maximum de renseignements.

Des personnes comme le responsable de la production, le responsable du plan de continuité d'activité, de la sécurité physique ou de la sécurité des systèmes d'informations ou encore la direction des risques constituent des interlocuteurs privilégiés dans le cadre de la gestion des incidents de sécurité. De nombreux acteurs peuvent être sollicités en fonction de la réaction à apporter (service juridique, service des ressources humaines...).

En fonction d'une première estimation de sa gravité, l'incident est porté immédiatement ou dès que possible à la connaissance de la DSI (ou du service en charge des systèmes d'information). Une première analyse, confirme ou infirme la catégorisation « incident de sécurité ». Les incidents non confirmés « incident de sécurité » sont transmis aux équipes support pour traitement.

Il est procédé si nécessaire à des investigations complémentaires pour qualifier l'événement. Pour bénéficier des dispositifs de mobilisation et d'escalade déjà en place, l'échelle des indices de gravité des incidents de sécurité doit être calquée sur celle des indices de gravité des incidents de production et doit intégrer le principe d'escalade dans la durée (plus l'incident dure sans résolution, plus son indice de gravité augmente).

Lorsque le traitement d'un incident de sécurité requiert des échanges avec les équipes métier, l'utilisation de la matrice d'indices de gravité des incidents de sécurité n'est pas toujours adaptée. C'est pourquoi une matrice des impacts métier sera privilégiée pour une meilleure communication sur l'incident en cours auprès des équipes métier. Cette matrice est classiquement basée sur une catégorie et un niveau d'impact métier :

- ▶ Perte financière,
- ▶ Atteinte à la réputation / image de marque,
- ▶ Réglementation / Juridique,
- ▶ Insatisfaction clients,
- ▶ Disponibilité des services.

L'ensemble des matrices de qualification de la gravité des incidents de sécurité doit être élaboré avec les acteurs de l'organisation (directions métier, équipes opérationnelles) pour une meilleure adhésion au dispositif, facteur clé de succès. Typiquement ces critères sont issus de l'analyse de risque.

Il est nécessaire de tenir un journal de bord horodaté et précis des événements et actions dès sollicitation de l'équipe.

Il convient de prendre certaines précautions en fonction de l'incident (ex piratage) et de préserver le contexte de preuve (copie de disques, sauvegardes, logs...) avant toute remédiation. L'analyse peut, dans certains cas modifier, voire effacer, les traces du passage d'un « attaquant ». En effet, le travail d'analyse génère lui-même des traces qui se confondent ensuite avec les traces laissées par l'agresseur. De fait, il est nécessaire de sauvegarder (par exemple via une copie intégrale, de type bit à bit) les informations avant d'entreprendre toute action susceptible de nuire à l'intégrité des données sur le support d'origine.

Si une copie des disques n'est pas réalisable ou l'est difficilement, il faut au moins conserver une copie des logs (journaux de connexions au système).

La cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication ou ciblant ces mêmes réseaux. En cas d'attaque (virale, du fait d'un pirate...) Un dépôt de plainte doit être effectué.

Les retours d'expérience sur les incidents de cybersécurité doivent permettre de réévaluer régulièrement la pertinence de ces matrices et sont l'occasion d'expliquer et de communiquer sur le niveau de gravité de l'incident. Par ailleurs, dans un souci d'amélioration continue, des exercices de crise de sécurité peuvent être réalisés périodiquement en se basant sur différents types de scénarios :

- ▶ le plus probable,
- ▶ celui qui présente le plus fort impact technique,
- ▶ le plus transverse (impactant le plus de directions techniques et métier),
- ▶ celui qui est couplé avec un exercice de PCA/PRA (par exemple, le scénario de déclenchement du PCA ou PRA en réponse à une attaque informatique massive de type déni de service).

Formulaire de déclaration d'incident/piratage

Informations générales *(Cette partie peut être renseignée à l'avance par les organismes)*

Date* <div style="border: 1px solid black; width: 100px; height: 20px; margin: 5px 0;"></div> (jj/mm/aa)	Type de déclaration* <input type="checkbox"/> Déclaration initiale (à effectuer dès la constatation de l'incident) <input type="checkbox"/> Déclaration complémentaire (à effectuer au fur et à mesure de l'analyse de l'incident)
Dénomination de l'opérateur *	

Personne déclarant l'incident

Nom et prénom*			Service et fonction*		
Adresse postale			<div style="border: 1px solid black; width: 100px; height: 20px; margin: 5px 0;"></div> Code postal	Ville	
Tél.*	<div style="border: 1px solid black; width: 100%; height: 20px;"></div>				
Adresse électronique*			@*		

Personne à contacter pour obtenir des informations complémentaires *(Cette partie peut être renseignée à l'avance par les organismes)*

Nom et prénom*			Service et fonction*		
Adresse postale			<div style="border: 1px solid black; width: 100px; height: 20px; margin: 5px 0;"></div> Code postal	Ville	
Tél.*	<div style="border: 1px solid black; width: 100%; height: 20px;"></div>				
Adresse électronique*			@*		
Contact HNO¹² (si différent)	Nom et prénom ou service d'astreinte			Service et fonction	
	Tél.	<div style="border: 1px solid black; width: 100%; height: 20px;"></div>			
	Tél. / Adresse électronique			@	

Description de l'incident

a. Système d'information concerné

Nom ou identifiant du système d'information Description du système d'information*

b. Incident constaté

Date de détection¹³* <div style="border: 1px solid black; width: 100px; height: 20px; margin: 5px 0;"></div> (jj/mm/aa)

¹² Contact en heures non ouvrées.

¹³ Date à laquelle l'incident a été constaté.

Date et heure estimées du début de l'incident

--	--	--	--	--	--	--	--	--	--

(jj/mm/aa)

Heure :

Localisation géographique des équipements impactés*

c. Qualification de l'incident

Nature de l'incident*

État de la qualification*

Incident en cours de qualification ☐

Incident en cours de remédiation ☐

Incident résolu ☐

Description de l'origine connue ou présumée – ou – Méthode de l'attaquant¹⁴ si action malveillante.

Indicateurs techniques de compromission informatique¹⁵

Joindre à ce formulaire les indicateurs de compromission connus

Références des documents joints

État supposé de l'attaque*

Activités préparatoires avant attaque ☐

Tentative d'attaque non aboutie ☐

Attaque aboutie ☐

Type d'impact constaté ou pressenti*

Disponibilité ☐

Confidentialité ☐

Intégrité ☐

Impacts métier¹⁶

d. Mesures prises ou prévues

Actions et traitements réalisés

Dépôt de plainte

Non envisagé ☐

Envisagé ☐

Réalisé ☐

Observations complémentaires

Signature manuscrite (si envoi par courrier postal)

¹⁴ Se référer au guide situé en annexes. Au besoin, annexer les résultats d'analyse en pièces jointes.

¹⁵ Se référer au guide situé en annexes.

¹⁶ Risques associés à l'incident (exfiltration, destruction, etc.), nature des éléments affectés ou exfiltrés, systèmes piégés ou détruits.

Pour transmettre le formulaire ou pour toute question :

Adresse postale	Ministères chargés des affaires sociales 14 avenue Duquesne 75007 paris	
Contact H24	Messagerie Internet	ssi@sg.social.gouv.fr
	Téléphone	01 40 56 63 36
	Téléphone de secours	01 40 56 48 49 / 06 33 31 16 88

Guide de remplissage du paragraphe 3.c

« Méthode de l'attaquant »

Les éléments de caractérisation connus dans la liste suivante peuvent être renseignés :

Eléments de synthèse :

- ▶ motivation présumée de l'attaquant (chantage, sabotage, vol d'information, etc.) ;
- ▶ présence éventuelle de l'attaquant dans le système d'information (constatation d'exfiltrations, d'altérations de fonctionnement de machines) ;
- ▶ niveau de complexité de l'attaque (attaque ciblée ou non).

Détails techniques :

- ▶ chronologie générale des activités de l'attaquant (p.ex. reconnaissance, infiltration initiale, interaction avec le contrôle commande, contamination d'autres machines, exfiltration, etc.) ;
- ▶ périmètre de la compromission :
 - ▶ niveau de privilège obtenu par l'attaquant ;
 - ▶ nombre et types de machines compromises, comptes et domaines d'administration usurpés ;
 - ▶ modifications internes sur le système d'information (ACL, fichiers, base de registre etc.).
- ▶ vulnérabilités exploitées, outils et techniques utilisés pour :
 - ▶ la compromission initiale ;
 - ▶ l'escalade de privilège sur le système d'information (le cas échéant) ;
 - ▶ l'exfiltration de données (le cas échéant) ;
 - ▶ la persistance éventuelle sur le système (le cas échéant) ;
 - ▶ l'exécution de commandes à distance sur des ressources internes (le cas échéant).

« Indicateurs de compromission »

Les indicateurs de compromission à joindre sont les informations techniques représentatives d'une manifestation de compromission, qui peuvent être identifiées à partir de l'analyse d'un système, d'un code malveillant ou de traces réseau.

Exemples : adresses IP, noms de domaine, URL, empreintes cryptographiques ou noms de fichiers ou de codes malveillants, chaînes spécifiques contenues dans des codes malveillants, informations sur un processus ou un service, entrées dans la base de registre Windows, etc.

ANNEXE 4 Homologation

En matière de système d'information, l'homologation permet à un responsable, en s'appuyant sur l'avis des experts, de s'informer et d'attester aux utilisateurs du système que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés. L'homologation est d'autant plus nécessaire, aujourd'hui, que les systèmes d'information sont de plus en plus complexes et que les impacts potentiels d'un incident sont de plus en plus graves. La démarche d'homologation d'un système d'information est un préalable à l'instauration de la confiance dans les systèmes d'information et dans leur exploitation.

Il s'agit d'un processus d'information et de responsabilisation qui aboutit à une décision, prise par le responsable de l'organisation. Cette décision constitue un acte formel par lequel il :

- ▶ *atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;*
- ▶ *accepte les risques qui demeurent (risques résiduels).*

La démarche d'homologation peut être décomposée en neuf étapes, dont la mise en œuvre est directement liée à la complexité du système à homologuer. Les questions posées lors de ces neuf étapes permettent de constituer un dossier, sur lequel l'autorité d'homologation s'appuie pour prendre sa décision.

La démarche d'homologation doit être adaptée aux enjeux de sécurité du système, notamment au contexte d'emploi, à la nature des données contenues, ainsi qu'aux utilisateurs.

Options qui s'offrent à l'autorité d'homologation ?

L'autorité d'homologation décide, après avoir pris l'avis des membres de la commission d'homologation, d'attester formellement de la prise en compte dans la sécurité dans un système d'information.

Après analyse, trois options se présentent à elle :

- ▶ *la sécurité du système est satisfaisante et celui-ci est homologué pour une durée définie dans le périmètre nominal.*
- ▶ *la sécurité du système est acceptable mais des mesures sont encore à prendre pour atteindre la couverture des risques recherchée. Le système est homologué temporairement (pour une durée courte de l'ordre de six mois) et/ou sur un périmètre restreint. Dans ces conditions, un plan d'action est dressé et la commission d'homologation est convoquée au terme de cette période pour réévaluer cette homologation.*
- ▶ *la sécurité du système n'est pas acceptable. L'homologation est reportée. Le système n'est pas mis en service. Les travaux complémentaires à réaliser sur le système sont identifiés pour qu'il soit de nouveau présenté à l'homologation.*

Définition de la stratégie d'homologation

Étape n° 1 : Quel système d'information dois-je homologuer et pourquoi ?

- ▶ *Définir le référentiel réglementaire applicable et délimiter le périmètre du système à homologuer.*

Étape n° 2 : Quel type de démarche dois-je mettre en œuvre ?

- ▶ *Estimer les enjeux de sécurité du système et en déduire la profondeur nécessaire de la démarche à mettre en œuvre.*

Étape n° 3 : Qui contribue à la démarche ?

- ▶ *Identifier les acteurs de l'homologation et leur rôle (décisionnaire, assistance, expertise technique, etc.).*

Étape n° 4 : Comment s'organise-t-on pour recueillir et présenter les informations ?

- ▶ *Détailler le contenu du dossier d'homologation et définir le planning.*

Maîtrise des risques

Étape n° 5 : Quels sont les risques pesant sur le système ?

- ▶ *Analyser les risques pesant sur le système en fonction du contexte et de la nature de l'organisme et fixer les objectifs de sécurité.*

Étape n° 6 : La réalité correspond-elle à l'analyse ?

- ▶ *Mesurer l'écart entre les objectifs et la réalité.*

Étape n° 7 : Quelles sont les mesures de sécurité supplémentaires à mettre en œuvre pour couvrir ces risques ?

- ▶ *Analyser et mettre en œuvre les mesures nécessaires à la réduction des risques pesant sur le système d'information. Identifier les risques résiduels.*

Prise de décision

Étape n° 8 : Comment réaliser la décision d'homologation ?

- ▶ *Accepter les risques résiduels : l'autorité d'homologation signe une attestation formelle autorisant la mise en service du système d'information, du point de vue de la sécurité.*

Suivi a posteriori

Étape n° 9 : Qu'est-il prévu pour maintenir la sécurité et continuer de l'améliorer ?

- ▶ *Mettre en place une procédure de révision périodique de l'homologation et un plan d'action pour traiter les risques résiduels et les nouveaux risques qui apparaîtraient.*

La MOA (ou le RSSI formalise l'organisation de l'homologation dans un document de synthèse validé par l'autorité d'homologation. Cette stratégie d'homologation précise l'ensemble des parties prenantes à l'homologation ainsi que :

- ▶ *le cadre réglementaire applicable (règles de protection des informations confidentielles, règles sectorielles, etc.);*
- ▶ *l'organisation (acteurs, missions, etc.);*
- ▶ *la démarche ;*
- ▶ *le périmètre et le cycle de vie du SI à homologuer;*
- ▶ *le calendrier;*
- ▶ *la criticité des informations utilisées dans le cadre de l'homologation;*
- ▶ *les pièces constitutives du dossier d'homologation.*

Exemple de document de stratégie :

Document de stratégie d'homologation du système XXXXX¹⁷

OBJECTIF DU DOCUMENT

Ce document a pour objet de définir la stratégie d'homologation du système d'information XXXXX. *(Il est possible de rajouter : dans le cadre des exigences du Référentiel Général de Sécurité (RGS) si c'est le cas).*

L'homologation de sécurité, prononcée par l'autorité qualifiée après avis d'une commission ad hoc, atteste de la capacité d'un système à traiter des informations sensibles au vu des mesures qu'il met en œuvre pour les protéger. Elle traduit l'acceptation d'un niveau quantifié de risques résiduels pour la confidentialité, l'intégrité et la disponibilité.

La présente stratégie d'homologation a pour objectif de présenter les étapes et les éléments nécessaires à l'homologation du « Système d'Informations XXXXX ». Elle comporte notamment :

- ▶ *la définition du périmètre faisant l'objet de l'évaluation,*
- ▶ *les méthodes et référentiels retenus,*
- ▶ *la liste des documents de sécurité (dossier d'homologation) et outils qui permettront d'analyser et de maîtriser les risques de sécurité.*

PRESENTATION DU SYSTEME D'INFORMATIONS XXXXX

Par <référence de la décision de création du SI>, il a été décidé la création d'un traitement de données dénommé « Système d'Information XXXXX », dont la finalité est d'assurer XXXXX.

Ce système d'information dédiée est permet de partager les informations entre XXXXX et XXXXX.

¹⁷ Remplacer les XXXXX par les informations correspondantes (structure, SI, nom...).

(Description des publics concernés et les éventuels pré-requis.)

Contexte général

Le « Système d'Informations XXXXX » a pour vocation de XXXXX.

Ont directement accès à l'application, à raison de leurs attributions respectives et dans la limite du besoin d'en connaître :

- XXXXX ;
- XXXXX.

Les informations transitent au moyen du réseau (RIE, dédié, Internet).

Ainsi le « Système d'Informations XXXXX » est composé (*description technique*)

Logiciel / Type de Serveur	Nom	Version	Ressources système

Les rôles, responsabilités et interactions entre les parties prenantes sont détaillés dans une note organisationnelle (cf. pièce n° 6 Note organisationnelle).

Identification des parties prenantes

Les parties prenantes identifiées dans le cadre de la mise en œuvre du système XXXXX sont

Acteurs : il s'agit XXXXX

- ▶ **Direction des systèmes d'information**: représentée par XXXXX

La DSI a pour mission :

- ▶ **RSSI**: Les missions relatives à la sécurité du SI XXXXX sont exercées par XXXXX.

Le responsable de la sécurité des systèmes d'information (RSSI) conduit les missions suivantes (expliquer les missions) :

- ▶ **Fournisseurs**

- ▶ **Prestataires**

- ▶ **Utilisateurs** : il s'agit des utilisateurs du SI XXXXX

- ▶ **Administrations** : ex : il s'agit du ministère chargé des affaires sociales, d'établissements publics, citoyens ... - Limites du périmètre d'homologation

L'homologation concerne XXXXX (*description*), ainsi que les processus nécessaires au fonctionnement de l'application, à savoir : exploitation, administration, supervision, gestion de la sécurité, gestion administrative et contractuelle, évolution technique et gouvernance.

Le périmètre fonctionnel à considérer couvre donc l'ensemble XXXXX

Le périmètre de chaque service est précisé dans l'analyse de risques (cf. pièce n°2 : analyse de risques).

Les futurs services additionnels, non fournis actuellement, feront l'objet d'une homologation propre et d'une révision éventuelle de l'homologation du SI XXXXX (cf. révision de l'homologation).

ACTEURS ET RESPONSABILITÉS

Autorité d'homologation

L'autorité responsable de l'homologation du SI XXXXX est XXXXX (*nom de l'autorité d'homologation*). L'autorité est chargée d'approuver la démarche d'homologation et le dossier d'homologation fondé notamment sur :

- la prise en compte des exigences de sécurité et des risques résiduels identifiés (cf. Pièce n°2 : Analyse de risques) ;
- le suivi et la validation du dossier d'homologation (cf. Suivi de l'homologation).

Elle s'appuie sur la commission d'homologation, dont elle fixe la composition. La désignation de ces membres pourra être subordonnée, si besoin, à leur habilitation préalable au niveau nécessaire.

Elle veille à ce que tous les acteurs concourant à la sécurité du système d'information soient identifiés et désignés et, si besoin, habilités.

Ces missions incluent en particulier :

- examiner et approuver les rapports d'homologation ;
- approuver la décision d'homologation du SI XXXXX ;
- émettre le certificat d'homologation du SI XXXXX.

Selon les résultats de l'analyse de risques effectuée dans le cadre de la démarche d'homologation, l'autorité d'homologation pourra prononcer :

- une homologation provisoire, ou autorisation provisoire d'emploi, assortie de réserves et d'un délai de mise en conformité des défauts de sécurité rencontrés ;
- une homologation pour une durée déterminée ;
- un refus d'homologation, si les risques résiduels sont jugés inacceptables.

Autorité d'emploi

L'autorité d'emploi du système est XXXXX, (qui assure également les fonctions de maîtrise d'ouvrage (MOA) et de direction de l'exploitation [à ajouter si cela est le cas]). Elle est chargée de :

- s'assurer du fonctionnement du SI XXXXXX ;
- gérer la bonne utilisation des moyens nécessaires à son fonctionnement ;
- contrôler l'application des mesures de sécurité préconisées ;
- proposer les évolutions nécessaires au regard des contraintes d'emploi ou de l'évolution fonctionnelle des besoins ;
- diligenter au besoin les audits de sécurité.

Commission d'homologation

Pour mener à bien sa mission, l'autorité d'homologation s'appuie sur l'avis organisationnel et technique fourni par la commission d'homologation. Elle est donc chargée de fournir un avis motivé sur la capacité du système à répondre ou non aux objectifs de sécurité assignés, de s'assurer que l'ensemble des mesures techniques et organisationnelles permettant la sécurisation du système ont toutes été prises et sont correctement appliquées.

Pour cela, elle est chargée de :

- rédiger, revoir et maintenir la stratégie d'homologation du SI XXXXX (cf. Suivi de l'homologation) ;
- suivre la constitution du dossier d'homologation ;
- examiner et analyser toutes les preuves de sécurité requises pour l'homologation ;
- diligenter au besoin les audits de sécurité ;
- examiner et proposer le besoin en termes de post-homologation et ré-homologation.

La commission d'homologation est présidée par **l'autorité d'homologation ou il désigne un président de commission.**

Le secrétariat et l'organisation sont confiés à XXXXX. L'autorité d'homologation prend les décisions après consultation et avis des membres de la commission d'homologation ;

La commission d'homologation de sécurité est composée comme suit :

■ **Membres permanents :**

- ▶ la ou le XXXXX, autorité d'homologation ;
- ▶ le président de la commission ;
- ▶ la ou le responsable du pilotage du projet ;
- ▶ la ou le chef de projet MOA ;
- ▶ la ou le chef de la DSI en charge de l'exploitation de l'application ou du service ou son représentant ;
- ▶ le responsable de la sécurité des systèmes d'information.

■ **Invités (si nécessaire) :**

- ▶ Le fonctionnaire de sécurité des systèmes d'information (FSSI) des ministères chargés des affaires sociales ;

- ▶ le représentant de XXXXX ;
- ▶ représentants « métier »;
- ▶ auditeurs et/ou experts techniques, notamment dans le domaine de la SSI.

Groupe de travail SSI

Ce groupe instruit l'ensemble des questions relatives à la sécurité du système. Il élabore un ensemble de propositions qu'il transmet à la commission d'homologation. Il a notamment pour mission de réaliser ou faire réaliser :

- les analyses de risques ;
- les audits de sécurité ;
- le suivi des plans d'action ;
- la composition du dossier de sécurité.

Ce groupe est constitué comme suit :

■ **Membres permanents :**

- ▶ le responsable du pilotage du projet ;
- ▶ le chef de projet MOA ;
- ▶ le DSI ou son représentant ;
- ▶ le RSSI.

■ **Invités** (si nécessaire) :

- ▶ auditeurs et/ou experts techniques, notamment dans le domaine de la SSI ;

Le groupe de travail SSI se réunira autant que de besoin, et a minima XXXXX, pour réaliser les tâches qui lui incombent.

Responsables de la SSI du système

Le responsable de la sécurité pour le « XXXXX » est le RSSI de XXXXX.

En lien avec XXXXX, il s'assure du respect de l'application des mesures de sécurité sur l'ensemble du périmètre d'homologation. (cf. Pièce n°6 : Note organisationnelle).

Qualification et audit

Un audit de sécurité du SI a été mené par XXXXX en date du :

Le compte-rendu d'audit est versé au dossier d'homologation.

Le RSSI peut, de sa propre initiative ou sur demande, diligenter ou faire diligenter à tout moment des audits de sécurité. Ces audits seront régulièrement menés afin de vérifier la bonne application de règles de sécurité sur l'ensemble du périmètre d'homologation. Un audit de sécurité sera par ailleurs systématiquement effectué après tout incident révélant une défaillance dans l'application des règles de sécurité.

Un audit de sécurité fera systématiquement l'objet d'un compte rendu, pouvant être assorti de mesures correctives à appliquer et d'un calendrier de mise en conformité. Un audit de vérification pourra être effectué pour vérifier cette mise en conformité.

DOSSIER D'HOMOLOGATION

Le dossier d'homologation comporte les pièces suivantes :

- la stratégie d'homologation ;
- l'analyse de risques;
- la politique de sécurité du système d'information (si existant) ;
- le dossier d'architecture technique (si existant) ;
- les procédures d'exploitation de la sécurité ;
- la gestion des risques résiduels ;
- les résultats des tests et des audits menés pour vérifier la conformité du système à la politique de sécurité et aux procédures d'exploitation ;
- une note organisationnelle désignant sans ambiguïté les responsabilités et rôle de chaque acteur en matière de SSI.

Pièce n°1 : Stratégie d'homologation

Il s'agit du présent document.

Pièce n°2 : Analyse de risques¹⁸

Une fiche d'expression rationnelle des objectifs de sécurité (FEROS) a été établie en s'appuyant sur la méthodologie XXXXXX (EBIOS). Elle décrit formellement les objectifs de sécurité du réseau et de ses composantes en matière de disponibilité, d'intégrité, de confidentialité et de traçabilité dans le contexte d'un ensemble de menaces identifiées. Elle décline par ailleurs les exigences de sécurité qui doivent être prises en compte par le projet.

Pièce n°3 : Politique de sécurité du système d'information

La politique de sécurité du « Système d'Informations XXXXX » décrit l'ensemble de mesures de sécurité à mettre en œuvre pour respecter les conditions d'emploi du réseau au maintien de son niveau de sécurité.

Tout aménagement à cette politique doit faire l'objet d'une étude d'impact en termes de sécurité et l'acceptation doit faire l'objet d'un accord explicite de XXXXX, à la condition que cet aménagement ne remette pas en cause l'homologation du SIXXXX. Si tel était le cas une nouvelle homologation est à effectuer (cf. Révision de l'homologation).

Pièce n°5 : Procédures d'exploitation de la sécurité

Ce document expose les procédures d'exploitation de sécurité du SI XXXXX. Ce document est la déclinaison opérationnelle des mesures établies dans la PSSI (cf. Pièce n°2 : Analyse de risques).

Pièce n°6 : Note organisationnelle

Ce document présente l'organisation mise en place pour la gestion de la sécurité pour le SI XXXXX. Elle identifie l'ensemble des acteurs prenant part à la sécurité de l'application, précise sans ambiguïté les rôles et responsabilités de chaque acteur et formalise les relations entre chacun d'eux.

Pièce n°7 : Compte-rendu des audits de sécurité

PROCESSUS D'HOMOLOGATION

Principe général

Dans le cas d'une homologation RGS : Conformément à l'article 14 de 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, les autorités administratives doivent mettre leurs systèmes d'information existants à la date de publication du RGS en conformité avec ce référentiel dans un délai de trois ans à compter de sa publication. Les systèmes créés dans les six mois qui suivent la publication du RGS doivent être mis en conformité dans un délai de 12 mois. Cette conformité est un préalable à la mise en service opérationnelle de tout système d'information. Par ailleurs, le Référentiel Général de Sécurité (RGS) impose aux autorités administratives d'homologuer les systèmes d'informations permettant l'échange d'informations entre autorités différentes. En tant qu'infrastructure interministérielle, le réseau interministériel de l'Etat relève du RGS et doit donc être homologué.

L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise par l'autorité d'homologation (désignée par l'autorité qualifiée) après avis, le cas échéant, de la commission d'homologation. Cette décision précise les conditions d'emploi du système d'information considéré.

Durée de l'homologation

L'homologation initiale est demandée pour une durée de 3 ans. Durant cette période, l'homologation pourra être revue selon les modalités et principes exposés ci-après.

Révision de l'homologation

Une révision de l'homologation est nécessaire à l'issue de cette période ou si un fait significatif de nature à remettre en cause l'homologation en cours, dont le périmètre du système a été précisé, est constaté. La liste ci-après énumère un certain nombre d'événements qui impliquent le renouvellement de l'homologation :

- modifications majeures de l'architecture du réseau ou introduction d'une interconnexion non prévue ;
- modifications majeures des composants du réseau (matériels, configuration logicielle, etc.) ;
- modification du niveau de menace portant sur le système considéré ;
- changement de classification de l'information traitée ;
- incident de sécurité qui remet manifestement en cause l'homologation en cours ;

¹⁸ Cela est un exemple, d'autres méthodes d'analyses de risques peuvent être utilisées.

- résultats non satisfaisants d'une inspection, contrôle ou audit de sécurité ;
- fin de la période initiale d'homologation ;
- plus généralement, sur décision de l'autorité d'homologation.

Suivi de l'homologation

L'homologation d'un système d'information est non seulement l'un des objectifs à atteindre avant sa mise en service, mais également l'attestation d'un état de protection dont il faudra garantir le maintien jusqu'à la décision du retrait de service. La procédure mise en œuvre pour l'homologation d'un système doit donc revêtir un caractère itératif tout au long du cycle de vie de ce système.

Afin d'avoir une vision dans le temps du niveau de sécurité des systèmes et applications homologués, la commission d'homologation se réunit a minima une fois par an afin d'examiner les points suivants :

- suivi des indicateurs de sécurité du réseau, pouvant inclure des indicateurs d'exploitation. Ces indicateurs de niveau stratégique, pilotage et opérationnel seront définis par le groupe de travail SSI, validés par la commission d'homologation et inscrits dans la PSSI (cf. Pièce n°3 : Politique de sécurité du système d'information) ;
- analyse des retours sur incidents SSI éventuels ;
- information sur les évolutions du réseau ou des systèmes d'information ministériels pouvant impacter sur l'homologation ;
- réévaluation éventuelle de la menace ou des objectifs de sécurité induisant une mise à jour de l'analyse de risques et des mesures de sécurité mises en œuvre.

La commission d'homologation peut se réunir de manière exceptionnelle ou à une fréquence plus régulière sur demande justifiée au Président de la commission de l'un de ses membres ou du groupe de travail SSI. La révision de l'homologation, pour l'un des motifs précédemment citée (cf. révision de l'homologation), ou un risque SSI particulier peuvent justifier d'une réunion exceptionnelle.

Textes applicables

La démarche d'homologation répond aux exigences réglementaires suivantes :

- Politique des systèmes d'information de l'Etat du 17 juillet 2014
- Référentiel Général de sécurité version 2.0 du 13 juin 2014.

Exemple de décision d'homologation

En application de (PMSSI-MCAS ou du Référentiel général de sécurité), M./Mme PRENOM NOM, FONCTION/QUALITE agissant par délégation du ministre / directeur général de l'organisme ORGANISME prononce l'homologation de sécurité du système (libellé du système d'information, de l'application ou de la téléprocédure).

Cette homologation atteste des moyens mis en œuvre pour que le système puisse élaborer, traiter, stocker, acheminer ou présenter l'information sont en cohérence avec la cible de sécurité définie. Elle est liée au respect strict du périmètre et des règles définies dans le dossier de sécurité qui a été approuvé. Elle est valable du DATE DE DEBUT au DATE DE FIN.

ANNEXE 5 GLOSSAIRE

Sigle	Définition
AA	Autorité d'appui
Actif	Tout élément représentant de la valeur pour l'organisation / l'entreprise.
AH	Autorité d'homologation
ALSSI	Agent local de sécurité des systèmes d'information Cf. RSSI
ANSSI	Agence nationale de la sécurité des systèmes d'information.
AQSSI	Autorité qualifiée de sécurité des systèmes d'information
ASSI	Agent de sécurité des systèmes d'information Cf. RSSI
CERT-FR	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
CIL	Correspondant informatique et liberté
CLSSI	Correspondant local de sécurité des systèmes d'information
CNIL	Commission nationale informatique et liberté
COSSI	Centre opérationnel de la sécurité des systèmes d'information (tél H24 : 01 71 75 84 68)
CYBERSECURITE	Recouvre l'ensemble des mesures de sécurité susceptibles d'être prises pour se défendre contre des incidents ou attaques.
DSI	Direction des systèmes d'information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité – Méthode d'analyse de risques
EGP	Exterior Gateway Protocol : Protocole de routage dans Internet. EGP est aussi utilisé pour désigner, de façon générale, les protocoles de routage extérieur, c'est-à-dire entre deux systèmes autonomes différents, et par opposition aux protocoles de routage interne.
IGP	Interior Gateway Protocol : Protocole de routage utilisé dans les systèmes autonomes.
eIDAS	Electronic Identification and Signature. Règlement européen qui permet d'établir une fédération des identités sur le sol européen
FSSI	Fonctionnaire de sécurité des systèmes d'information
HFDS	Haut fonctionnaire de défense et de sécurité
Impact :	Conséquence négative qui survient lorsqu'une menace exploite une vulnérabilité d'un actif.
MCAS	Ministères chargés des affaires sociales
OSSI	Officier de sécurité des systèmes d'information Cf. RSSI
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PSSI	Politique de sécurité des systèmes d'information
PSSIE	Politique de sécurité des systèmes d'information de l'Etat
PSSI-MCAS	Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales
RGS	Référentiel général de sécurité http://www.ssi.gouv.fr/entreprise/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs/
RSI	Responsable de sécurité informatique

RSSI	<i>Responsable de sécurité des systèmes d'information</i>
SGDSN	<i>Secrétariat général de la défense et de la sécurité nationale</i>
SHFDS	<i>Service du Haut fonctionnaire de défense et de sécurité</i>
SI ou SIC	<i>Système d'information (ou système d'information et de communication): ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information</i>

Définitions

- **Besoin de sécurité** : Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité...).
- **Bien essentiel** : Information ou processus jugé comme important pour l'organisme. On appréciera ses besoins de sécurité mais pas ses vulnérabilités.
- **Bien support** : Bien sur lequel reposent des biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux. On appréciera ses vulnérabilités mais pas ses besoins de sécurité.
- **Confidentialité** : Propriété des biens essentiels de n'être accessibles qu'aux personnes autorisées
- **Disponibilité** : Propriété d'accessibilité au moment voulu des biens essentiels par les personnes autorisées
- **Intégrité** : Propriété d'exactitude et de complétude des biens essentiels
- **Menace** : Moyen type utilisé par une source de menace
- **Mesure de sécurité** : Moyen de traiter un risque de sécurité de l'information. La nature et le niveau de détail de la description d'une mesure de sécurité peuvent être très variables
- **Objectif de sécurité** : Expression de la décision de traiter un risque selon des modalités prescrites. On distingue notamment la réduction, le transfert (partage des pertes), le refus (changements structurels pour éviter une situation à risque) et la prise de risque
- **Organisme** : Ensemble d'installations et de personnes avec des responsabilités, pouvoirs et relations
- **Réduction de risque** : Choix de traitement consistant à appliquer des mesures de sécurité destinées à réduire les risques
- **Risque résiduel** : Risque subsistant après le traitement du risque
- **Vulnérabilité** : Caractéristique d'un bien support qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information