PREMIÈRE MINISTRE

Liberté
Égalité
Fraternité

Instruction sur la politique de sécurité des systèmes d'information des services de la Première ministre (PSSI-SPM)

1er décembre 2022

Ce document ne s'applique qu'aux services de la Première ministre relevant de la chaîne fonctionnelle du haut fonctionnaire de défense et de sécurité placé auprès de la Première ministre. Elle s'adresse à l'ensemble des agents des entités relevant du haut fonctionnaire de défense et de sécurité de la Première ministre.

La présente PSSI-SPM n'a pas vocation à se substituer à la PSSI de l'Etat qui reste applicable dans son ensemble. La PSSI-SPM complète la PSSI-E pour le périmètre des services de la Première ministre au regard de leurs spécificités.

Table des matières

Table des matières 2
Introduction 5
Références 6
Première partie : instruction 7
Article 1. Champ d'application 7
Article 2. Date d'entrée en vigueur 7
Article 3. Pilotage et évolutions de la PSSI-SPM 7
Article 4. Mise en application de la PSSI-SPM 8
Article 5. Contrôle et suivi 8
Article 6. Traitement des incidents et gestion de crise 9
Deuxième partie : objectifs et règles 10
Gouvernance de la sécurité numérique des services de la Première ministre 10
Rôles liés à la gouvernance de la cybersécurité ministérielle 10
Comitologie de la cybersécurité au sein des services de la Première ministre 14
Organisation de la sous-traitance 15
Planifier : définir une cible de sécurité 16
Enjeux et objectifs de sécurité numérique 16
Feuille de route de la cybersécurité des SPM 17
Evaluer la sensibilité des données 17
Cartographie 19
Identifier les systèmes d'information critiques 19
Plan de continuité d'activité des systèmes d'information 19
Sensibiliser les agents au risque cyber 20
Protéger : garantir la confiance dans le temps 21
Gestion des risques et homologation de sécurité 21
Sécurité des développements logiciels et des services 22
Maintien en condition de sécurité des systèmes d'information 23
Gestion des vulnérabilités 24
Sécurité des services exposés sur Internet 24
Détecter 26

Contrôles 26
Dispositifs de détection techniques 27
Collecte des journaux 27
Répondre : faire face à la crise 28
Traitement des incidents 28
Processus de gestion des incidents de cybersécurité 29
Gestion de crise cyber 32
Astreintes 32
Dérogations 33
Annexe 1 : échelles des besoins de sécurité 34
Disponibilité 34
Intégrité 34
Confidentialité 34
Traçabilité 35

HISTORIQUE DES VERSIONS		
DATE	**VERSION**	**ÉVOLUTION DU DOCUMENT**
2022-12-01	3.0	*Mise en conformité de la Politique de sécurité des systèmes d'information des Services du Premier ministre compte tenu des nouveaux textes réglementaires ainsi que des évolutions en matière de protection des systèmes.*
2015-10-05	2.0	*Mise en conformité de la Politique de sécurité des systèmes d'information des Services du Premier ministre en déclinaison de la Politique de sécurité des systèmes d'information de l'État.*
2006-10-10	1.0	*Publication de la première Politique de sécurité des systèmes d'information des Services du Premier ministre*

Introduction

Cette PSSI des services de la Première ministre (PSSI-SPM), conformément à la circulaire du Premier ministre n°5725/SG du 17 juillet 2014 est une déclinaison de la PSSI de l'Etat (PSSIE).

La présente PSSI-SPM n'a pas vocation à se substituer à la PSSI-E qui reste applicable dans son ensemble. La PSSI-SPM complète la PSSI-E pour le périmètre des services de la Première ministre au regard de leurs spécificités.

Elle s'adresse à l'ensemble des agents des entités relevant du haut-fonctionnaire de défense et de sécurité de la Première ministre, et tout particulièrement :

- aux autorités hiérarchiques, qui sont responsables de la sécurité des informations traitées au sein de leurs services et plus particulièrement aux autorités qualifiées pour la sécurité des systèmes d'information (AQSSI) ainsi que leurs conseillers à la sécurité numérique (CSN) ;
- aux directeurs des systèmes d'information (DSI) ;
- aux personnes chargées de la sécurité et de l'exploitation des systèmes d'information.

Références

- Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (**RGPD** - Règlement général sur la protection des données) ;
- Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (**Directive NIS** - Network and Information System Security) ;
- Loi n° 1978-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité
- Code de la défense, notamment ses articles L. 2321-1, L. 1111-3, R.* 1132-1 à D. 1132-54 et R. 1143-1 à D. 1143-13; ;
- Décret n°2007-207 du 19 février 2007 relatif aux attributions des hauts fonctionnaires de défense et de sécurité (**HFDS**);
- Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (**Décret RGS**);
- Décret n°2012-383 du 20 mars 2012 relatif aux attributions du haut fonctionnaire de défense et de sécurité auprès du Premier ministre (**HFDS des SPM**);
- Décret n°2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique (**DINUM**) ;
- Décret n°2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics ;
- Arrêté du 4 avril 2022 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services du Premier ministre (**AQSSI**);
- Instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics (**IGI 1337**) ;
- Instruction générale interministérielle n°1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale (**IGI 1300**) ;
- Instruction interministérielle n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles **(II 901**) ;
- Circulaire n°5725/SG du 17 juillet 2014 relatif à la politique de sécurité des systèmes d'information de l'Etat (**PSSIE**) ;
- Circulaire n°6290/SG du 15 juillet 2021 relative aux actions à engager pour renforcer la cybersécurité de l'État ;

Première partie : instruction

Article 1. Champ d'application

La politique de sécurité des systèmes d'information des services de la Première ministre (PSSI-SPM)[1] s'applique à l'ensemble des services et entités relevant du champ de compétence du Haut fonctionnaire de défense et de sécurité auprès de la Première ministre (HFDS/PM)[2]. Elle s'impose à l'ensemble des personnes physiques ou morales utilisant ou intervenant sur les systèmes d'information, qu'il s'agisse des administrations de l'État et de leurs agents ou bien de tiers (prestataires ou sous-traitants) et de leurs employés.

La présente PSSI-SPM est déclinée par chacune des entités relevant du HFDS/PM.

La PSSI-SPM ne s'impose pas aux systèmes aptes à traiter des informations classifiées de défense, soumis à un corpus réglementaire spécifique.

Compte tenu de leur statut, les établissements publics, les autorités administratives indépendantes et les structures assimilées relevant de la Première ministre ne sont pas assujettis aux dispositions de la présente PSSI-SPM. Ces structures sont néanmoins encouragées à l'appliquer dans le cadre du déploiement de leur propre dispositif de cybersécurité.

Article 2. Date d'entrée en vigueur

Le présent document entre en vigueur le jour de sa diffusion.

Article 3. Pilotage et évolutions de la PSSI-SPM

La PSSI-SPM est amenée à évoluer dans le temps, notamment lors des évolutions de la politique de sécurité des systèmes d'information de l'Etat (PSSIE). Elle pourra notamment être revue afin de prendre en compte :

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

[1] PSSI issue de la déclinaison de la PSSIE et approuvée par le HFDS

[2] A l'exclusion cependant du SGDSN et des services qui lui sont rattachés.

Article 4. Mise en application de la PSSI-SPM

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

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

Dans ce but, chaque entité :

- met en place une organisation en application de la PSSI-SPM ;
- établit un inventaire de ses systèmes d'information et en évalue la sensibilité; conduit une analyse de risques pour ses systèmes d'information et met en place les mesures de sécurité nécessaires ;
- conduit des actions de motivation : sensibilisation et formation à la sécurité des systèmes d'information, communication claire sur les sanctions encourues (par exemple, dans les chartes d'usage des SI) ;
- conduit des actions régulières de contrôle du niveau de sécurité de ses systèmes d'information et met en œuvre les actions correctives nécessaires ;
- met en place les processus lui permettant de faire face aux alertes, aux incidents de sécurité et aux situations d'urgence.

Il peut être nécessaire, dans certains cas, de déroger aux règles énoncées par la PSSI-SPM. Il appartient alors à l'autorité de l'entité concernée de leur substituer formellement des règles spécifiques. Pour chacune de ces règles, la dérogation, motivée et justifiée, doit être expressément accordée par le HFDS/PM pour une durée déterminée. La décision de dérogation, accompagnée de la justification, est tenue à la disposition de l'ANSSI.

Article 5. Contrôle et suivi

Le respect de la PSSI-SPM fait l'objet de contrôles réguliers à différents niveaux, sous la responsabilité de la chaîne fonctionnelle SSI avec compte rendu au FSSI des services de la Première ministre (FSSI/PM). Le HFDS/PM désigne les organismes compétents pour la réalisation de ces contrôles.

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

Les actions de contrôle relatives au niveau de sécurité des systèmes d'informations, ainsi que les incidents de sécurité, font l'objet d'échanges réguliers entre le délégué à la protection des données (DPD) et le FSSI placés auprès de la Première ministre.

Article 6. Traitement des incidents et gestion de crise

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

L'ensemble des acteurs (utilisateurs, responsables d'applications, des réseaux et des centres serveurs …) doit remonter tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des systèmes d'information d'une entité. Ces incidents de sécurité doivent être signalés sans délai à la chaîne opérationnelle SSI qui informe la chaîne fonctionnelle. Les incidents jugés significatifs sont remontés à l'ANSSI sous la responsabilité du HFDS/PM. Le responsable de traitement assisté par le DPD/PM veillera à traiter l'incident conformément aux textes relatifs à la protection des données personnelles le cas échéant.

Une alerte est une action d'information sur des situations ou des faits nécessitant un traitement et une vérification des mesures prises. Leur prise en compte au sein de chaque entité est organisée sous la responsabilité du HFDS/PM.

Une situation d'urgence SSI impose une forte réactivité et une coordination planifiée des différents acteurs concernés. Chaque entité prend en compte la SSI dans l'organisation de gestion de crise et des plans de continuité et de reprise d'activité. Ces actions doivent être menées en cohérence avec la planification interministérielle de gestion de crise.

Deuxième partie : objectifs et règles

Gouvernance de la sécurité numérique des services de la Première ministre

Rôles liés à la gouvernance de la cybersécurité ministérielle

Une organisation dédiée à la sécurité du numérique est déployée au sein de chaque entité suivant les principes de l'IGI 1300 et du Décret n°2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics[3].

Le HFDS/PM

Cette organisation, établie selon les directives du haut fonctionnaire de défense et de sécurité auprès de la Première ministre (HFDS/PM), définit les responsabilités internes et à l'égard des tiers, les modalités de coordination avec les autorités externes, et définit la politique de sécurité ministérielle. Le HFDS/PM conseille le cabinet de la Première ministre sur toute question relative à la sécurité du numérique de son périmètre de compétence.

Le FSSI/PM

Le fonctionnaire de sécurité des systèmes d'information auprès de la Première ministre (FSSI/PM) définit la politique des SPM permettant de maîtriser les risques de sécurité du numérique et de garantir la continuité des activités. Il est consulté sur la bonne prise en compte de la sécurité du numérique dans les politiques publiques du ministère et la stratégie ministérielle du numérique.

Il conseille et accompagne l'ensemble des acteurs et des entités relevant du HFDS/PM sur les questions relatives à la sécurité du numérique.

Dans le cas particulier des SPM, le FSSI/PM est également le « conseiller cybersécurité » de la secrétaire générale du Gouvernement (SGG).

Le FSSI/PM s'assure de la cohérence des mesures en matière de sécurité numérique et de la prise en compte, par les entités relevant du HFDS/PM, du respect des règles et des orientations en matière de sécurité numérique. Il contrôle l'application des exigences de sécurité définies dans le présent document à l'aide d'audits, de contrôles et de bilans.

Il pilote la réponse aux incidents majeurs de sécurité du numérique.

[3] Le système d'information et de communication de l'Etat et de ses établissements publics comprend les infrastructures et services logiciels informatiques qui composent le système d'information et de communication de l'Etat mentionné à l'article 1er du présent décret font l'objet, préalablement à leur mise en œuvre, d'une homologation de sécurité.

Le FSSI/PM est l'interlocuteur privilégié de l'Agence nationale de sécurité des systèmes d'information (ANSSI). Il l'informe des incidents majeurs sur les systèmes d'information et de communication de son périmètre de compétence.

Nommé par la Première ministre, le FSSI/PM est placé sous l'autorité hiérarchique du HFDS/PM.

L'AQSSI

L'autorité qualifiée en sécurité des systèmes d'information (AQSSI) est responsable de la sécurité des services numériques qui contribuent à l'exécution des missions dont elle a la charge. La liste des AQSSI des services de la Première ministre est définit par arrêté[4].

L'AQSSI ne peut déléguer cette responsabilité. À ce titre, elle est responsable sur son périmètre, en particulier, de :

- l'élaboration et le maintien à jour d'une cartographie de ses services ;
- maintenir en condition opérationnelle et de sécurité ses services ;
- planifier des audits de sécurité de ses services ;
- l'allocation les ressources nécessaires pour mener à bien les projets de transformation numérique, en veillant à la prise en compte de la sécurité numérique ;
- s'assurer de la bonne prise en compte du risque numérique dans la cartographie des risques de son entité ;
- contrôler l'application des exigences de sécurité du numérique auxquelles elle est soumise ;
- remettre annuellement au haut fonctionnaire de défense et de sécurité un rapport de sécurité dans lequel elle intègre l'évaluation du niveau de sécurité du numérique et une synthèse des incidents de sécurité numérique ayant impactés ses missions ;
- s'assurer de l'élaboration, de la mise en œuvre et du maintien, notamment au travers d'exercices, des plans de continuité et de reprise des activités relevant de son domaine de responsabilité face à des incidents de sécurité numérique.

La SGG définit, sur son domaine de responsabilités, les modalités de nomination des AQSSI.

L'AQSSI est l'autorité d'homologation, par défaut, de chaque service numérique et infrastructure dont elle est responsable.

Pour l'assister dans l'exercice de ses responsabilités, l'AQSSI nomme, auprès d'elle, au moins un conseiller à la sécurité du numérique (CSN).

[4] Arrêté du 4 avril 2022 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services du Premier ministre (AQSSI);

L'AQSSI est membre du comité de pilotage de la cybersécurité des SPM. Elle contribue à la chaîne fonctionnelle de la sécurité des systèmes d'information.

Chaque AQSSI s'appuie sur le(s) CSN, chargé(s) de l'assister respectivement dans la gestion des risques numériques et dans la mise en œuvre opérationnelle de la sécurité du numérique. Par leur rattachement hiérarchique, le positionnement du CSN doit lui permettre d'accomplir en toute indépendance ses fonctions d'alerte et de conseil auprès de son AQSSI et des autorités d'homologation.

Le CSN

Le conseiller à la sécurité du numérique (CSN) conseille et accompagne l'AQSSI dans l'exercice de ses responsabilités pour la gestion des risques numériques. Il assiste notamment l'autorité qualifiée et les autorités d'homologation pour l'homologation des systèmes d'information.

Le CSN dispose d'une culture de la sécurité du numérique, et le cas échéant de compétences techniques lui permettant d'en traduire les enjeux pour le compte de son AQSSI.

Membre du comité de direction, le conseiller à la sécurité du numérique est nommé par l'AQSSI.

Le RSSI

Le responsable de la sécurité des systèmes d'information (RSSI) contrôle la mise en application de la PSSI-SPM ainsi que la documentation qui participe à sa mise en œuvre. Il rend compte régulièrement de la mise en application des mesures de sécurité auprès du CSN. Le RSSI dispose d'une expertise technique en matière de sécurité numérique.

Il contribue à la chaîne fonctionnelle de sécurité des systèmes d'information et est membre de l'instance ministérielle de pilotage de la sécurité numérique.

Des « correspondants locaux SSI » peuvent être désignés en complément, afin de constituer un relais du RSSI. Le RSSI d'une entité fait valider les mesures d'application de la PSSI-SPM par l'autorité qualifiée et veille à leur application.

Nota : Compte tenu des spécificités de l'organisation de certains services relevant de la Première ministre, le cumul des rôles de CSN et RSSI est possible de manière transitoire.

DSI ou entités mettant en œuvre des systèmes d'information

Les DSI (divisions, sous-directions, bureaux et autres structures mettant en œuvre des SI) assurent la mise en œuvre et l'exploitation de services numériques et d'infrastructures. Ils veillent, notamment dans le cadre des démarches d'homologation, à l'élaboration et au maintien à jour d'une cartographie des systèmes d'information sous leur responsabilité, à leur maintien en condition opérationnelle et

de sécurité, à la réalisation d'audits de sécurité, à l'élaboration des plans de continuité et de reprise informatique ainsi qu'à la fourniture de moyens permettant de répondre à des crises liées à sécurité du numérique. Les schémas directeurs, les plans de transformation numérique et les comités stratégiques relatifs aux enjeux numériques des SPM sont soumis à l'avis du FSSI/PM.

Les DSI ne dépendent pas de la chaîne fonctionnelle SSI des SPM mais sont responsables de la bonne application des prérogatives édictées par celle-ci.

Gestion de crise cyber & annuaire de crise cyber

Un dispositif de gestion de crise cyber est mis en œuvre au sein des SPM. Ce dispositif prévoit une astreinte hebdomadaire et une gouvernance spécifique adaptée à la gestion de crise dans le contexte des SPM, s'agissant notamment des intervenants, de la chaîne décisionnelle, des critères d'activations de la cellule de crise cyber et des processus de traitement d'une telle crise.

Un annuaire de crise cyber est institué au sein du service du HFDS/PM. Cet annuaire comporte l'ensemble des coordonnées des acteurs de la cybersécurité énoncés ci-dessus. Il est tenu et mis à jour par le service du HFDS/PM, à partir des données que lui transmettent les services.

Cas particulier des fonctions liées à la protection du secret

En matière de protection du secret, les acteurs sont désignés dans l'IGI 1300, et les agents chargés de les assister dans cette mission, sont responsables de la mise en application générale de la politique SSI de l'État. Ils sont référencés dans un annuaire interministériel. Cette chaîne fonctionnelle s'appuie sur le HFDS/PM, assisté par le FSSI/PM.

Cas particulier de la direction interministérielle du numérique

La direction interministérielle du numérique (DINUM) propose à la Première ministre et met en œuvre la stratégie numérique de l'État[5]. Elle s'assure de la bonne prise en compte de la politique de sécurité du numérique de l'État dans cette stratégie ainsi que dans les différents projets qui lui sont soumis au titre de cette stratégie et de ses attributions[6].

Pour les sujets relatifs à la sécurité du numérique des services interministériels dont elle a la charge, la DINUM s'inscrit dans la chaîne fonctionnelle de la sécurité des systèmes d'information des services du Premier ministre.

[5] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique, art. 6, 1°
[6] Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique, art. 3

Le/La directeur/rice interministériel(le) du numérique est autorité qualifiée en sécurité des systèmes d'information des services numériques et des infrastructures transverses dont il a la responsabilité. À ce titre, il assume les responsabilités décrites supra.

La DINUM établit et maintient à jour un catalogue des services qu'elle propose et le communique aux administrations de l'État afin de les accompagner dans leurs projets de transformation numérique. Pour chaque service, ce catalogue précise le niveau de sécurité, le périmètre et les conditions d'emploi validés par l'autorité d'homologation.

Le/La directeur/rice interministériel(le) du numérique est membre du comité stratégique interministériel de la sécurité du numérique (cf 3.3.2 de l'IGI1337).

Cas particulier des établissements publics, des autorités administratives indépendantes et structures assimilées

Les établissements publics, les autorités administratives indépendantes, les autorités publiques indépendantes, nomment un référent auprès de leur dirigeant exécutif, président ou tout autre forme de responsable de structure, pour tous les sujets relatifs à la sécurité numérique.

Ce référent est le correspondant privilégié du FSSI/PM et de l'ANSSI pour tout sujet relatif à la sécurité numérique de sa structure.

Le dirigeant exécutif, président ou tout autre forme de responsable de structure s'assure que les informations de contact de ce référent sont communiquées au HFDS/PM et à l'ANSSI.

Les incidents de sécurité affectant le système d'information et de communication de la structure sont déclarés auprès du FSSI/PM et sont également déclarés à l'ANSSI.

Comitologie de la cybersécurité au sein des services de la Première ministre

En sus de la comitologie interministérielle décrite au sein de l'IGI 1337, une comitologie relative à la cybersécurité est déployée dans les services relevant du HFDS/PM. Celle-ci se décline comme suit :

Comité stratégique pour la cybersécurité des SPM

Un comité stratégique pour la cybersécurité est institué. Son secrétariat est assuré par le service du HFDS/PM. Présidé par le directeur de cabinet de la Première ministre, le comité stratégique est composé de la SGG (HFDS/PM), du HFDS adjoint/PM, du FSSI/PM et le cas échéant, des AQSSI.

Cette instance a pour objectif de présenter l'état de la menace, le niveau de sécurité des SI ainsi que de définir les orientations stratégiques des SPM en matière de sécurité du numérique.

Le directeur général de l'ANSSI y est convié afin de présenter l'état de la menace.

Le FSSI/PM y siège es-qualité et comme conseiller cybersécurité de la SGG.

Il se réunit annuellement *a minima*.

Comité de pilotage pour la cybersécurité des SPM

Un comité de pilotage pour la cybersécurité est institué, présidé par la SGG et dont le secrétariat est assuré par le FSSI/PM. Cette instance vise à suivre le niveau de sécurité des SI ainsi que de piloter l'avancement de la feuille de route définie par le comité stratégique.

Présidé par le SGG (HFDS/PM), ou en son absence par le HFDSa/PM, le comité de pilotage est composé du HFDS adjoint, du FSSI/PM, des CSN et des représentants des AQSSI. Le DPD peut également y être convié.

Il se réunit quatre fois par an, dont, *a minima* une fois sous la présidence du HFDS/PM.

Comité de sécurité

Des comités de sécurité peuvent être organisés selon les besoins des services. Ces comités visent à évaluer l'intégration de la sécurité dans les projets et de traiter toute question relative au maintien en condition de sécurité des systèmes (politique de gestion des mises à jour, états des lieux des évènements et incidents de sécurité, traitement des risques résiduels issus des homologations etc.)

Les CSN veilleront à ce que les systèmes ou projets représentant un risque pour leur périmètre soient suivis *a minima* trois fois par an lors d'un comité de sécurité. En tant que de besoin, le FSSI/PM et l'autorité d'homologation y assistent.

Ces réunions du comité de sécurité donneront lieu à la production d'un compte rendu communiqué au FSSI/PM.

Organisation de la sous-traitance

Clauses de sécurité

Tout contrat élaboré par les services achats des SPM détaille les dispositions mises en œuvre pour prendre en compte la cybersécurité. Ce sont notamment les mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace. Des clauses types sont mises à disposition des entités sur sollicitation du FSSI/PM.

Le CSN s'assure de 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. Ces clauses doivent permettre à l'administration de faire respecter la présente PSSI par le prestataire en charge de la livraison des produits et services. Ces

clauses spécifient les mesures SSI que le prestataire doit respecter dans le cadre de ses activités.

Le CSN, en lien avec le correspondant RGPD de l'entité, s'assure également de l'intégration des clauses liées au respect du RGPD, notamment en ses articles 13, 28, 32, 35 et 44 dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques impliquant des données personnelles.

Suivi et contrôle des prestations fournies

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

- l'un, effectué par l'équipe de la maîtrise d'œuvre encadrant la prestation, qui porte sur les actions du sous-traitant et la conformité au cahier des charges ;
- l'autre, effectué par la maîtrise d'ouvrage, qui veille au niveau de sécurité global obtenu en production, en s'appuyant notamment sur la chaîne fonctionnelle SSI.

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.

Plus largement, la défaillance, la compromission ou le rachat du sous-traitant doivent être pris en compte dans l'analyse de risque du SI et plus globalement de l'entité.

Une liste complète des fournisseurs intervenant sur les périmètres et systèmes les plus critiques doit être tenue à jour. Elle comporte *a minima* la criticité et les exigences de sécurité (DICT) du système ainsi que les exigences du contrat en cours. Il est vivement recommandé qu'une telle liste soit étendue à l'ensemble du périmètre numérique, y compris concernant les actifs moins critiques.

Une politique d'externalisation doit être définie par l'entité afin d'identifier quels cas d'usages peuvent faire l'objet d'une externalisation ou d'une sous-traitance, et d'identifier quelles fonctions, services et activités ne peuvent en bénéficier. La décision d'externaliser un produit ou un service doit toutefois permettre au système d'information de demeurer conforme à la démarche d'homologation.

Planifier : définir une cible de sécurité

Enjeux et objectifs de sécurité numérique

Les efforts en matière de sécurité numérique des SPM doivent d'abord se concentrer sur les actifs les plus stratégiques et essentiels.

Chaque AQSSI veille à définir en priorité les besoins en confidentialité et résilience de ses SI conformément à l'analyse de risque de son entité, et en veillant tout particulièrement aux impacts sur les missions du Gouvernement ou sur les citoyens.

Feuille de route de la cybersécurité des SPM

Les SPM se dotent d'une feuille de route détaillant le plan d'actions nécessaire à la mise en conformité à la présente instruction. Les axes stratégiques de cette feuille de route sont validés au comité stratégique pour la cybersécurité des SPM, et soumis pour approbation et déclinaison dans les services au comité de pilotage pour la cybersécurité des SPM.

Evaluer la sensibilité des données

La sensibilité (besoin en confidentialité, disponibilité, intégrité et traçabilité) de toute information doit être évaluée. Les documents doivent être marqués pour indiquer le niveau de sensibilité. Une échelle de sensibilité des données est établie suivant la grille d'évaluation suivante, basée sur une liste d'exemples non-exhaustive :

Niveau de sensibilité	Exemples
Classifié	Données pouvant porter atteinte aux intérêts de la nation et relevant du secret de la défense nationale (IGI1300) Attention : ces données ne peuvent être traitées que sur des systèmes d'information spécifiquement dédiés à cet usage.
Sensible	Données identifiées « Diffusion restreinte » (ne peuvent être traitées que dans des SI homologués au niveau « Diffusion restreinte ») Données à caractère personnel d'une sensibilité particulière tel que l'article 9 (données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques…), ou 10 du RGPD, le NIR, la copie d'une CNI… Données révélant des informations liées à l'exploitation des systèmes d'information (procédures d'exploitation, rapports d'audit) Notes administratives couvertes par le secret des délibérations du Gouvernement
Interne administration	Productions et échanges internes Données personnelles hors articles 9 et 10 du RGPD Tout document de travail
Public	Données publiées sur internet ou dans le cadre d'une démarche open data

Chaque agent 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 l'élaboration jusqu'à la destruction. À ces fins, des moyens adaptés au niveau de sensibilité sont mis à disposition pour chaque étape du cycle de vie des informations.

Les données ne peuvent être hébergées que sur des systèmes d'information bénéficiant d'une homologation pour un niveau de sensibilité adapté.

Cartographie

Chaque entité établit et maintient à jour un inventaire des systèmes d'information sous sa responsabilité.

Il comprend notamment, pour chaque SI :

- les données traitées, le niveau de sécurité et de résilience ;
- le dossier d'homologation ;
- la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes ;
- une base de données de configuration, maintenue à jour ;
- une cartographie précise des centres informatiques ;
- les architectures des réseaux (sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées).

L'AQSSI s'assure qu'un inventaire est tenu à disposition du CSN, du RSSI, ainsi que du FSSI/PM et de l'ANSSI en cas de besoin de coordination opérationnelle.

Ces informations sont indispensables en cas de crise cyber et doivent être accessibles depuis une sauvegarde « hors ligne »

Identifier les systèmes d'information critiques

Chaque service doit communiquer au FSSI/PM l'état de son patrimoine de SI critiques :

- SIIV – systèmes d'information d'importance vitale ;
- SIE – systèmes d'information essentiels ;
- tous ceux qui ne sont pas déclarés en tant que tels mais dont la criticité ou l'importance sont évidentes au regard des missions métier portées par le système.

Les SIIV et SIE doivent faire l'objet d'une déclaration formelle auprès du FSSI/PM et de l'ANSSI, en plus d'une déclaration formelle au ministère en charge du suivi du domaine d'activité considéré [7]. Ils doivent impérativement faire l'objet d'une démarche d'homologation formalisée précisant la criticité du système et les mesures attendues afin de le protéger.

Plan de continuité d'activité des systèmes d'information

Chaque entité définit, en cohérence avec son analyse des risques majeurs, un plan de continuité d'activité des systèmes d'information permettant d'assurer, en cas de sinistre, la continuité d'activité des systèmes d'information.

Le CSN s'assure, pour le compte de l'AQSSI, de la bonne mise en œuvre des dispositions prévues dans le plan de continuité d'activité des systèmes d'information

[7] A titre d'exemple, le ministère de l'Intérieur et des outre-mer est en charge du domaine « activités civiles de l'Etat ».

de son entité. Le plan de continuité doit être testé et éprouvé régulièrement afin de s'assurer de son efficacité.

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.

Les sauvegardes de données constituent un élément essentiel du dispositif de continuité d'activité. Les entités doivent assurer une capacité à conserver des sauvegardes hors-ligne de leurs actifs stratégiques afin de faciliter la reprise d'activité en cas de sinistre. Les sauvegardes doivent être traitées de manière à garantir leur confidentialité et leur intégrité.

Chaque entité assure le maintien à jour du plan de continuité d'activité des systèmes d'information, notamment en prenant en compte les retours d'expériences des exercices de crise ou de toute activation du plan de continuité d'activité en conditions réelles.

Sensibiliser les agents au risque cyber

Les agents sont les premiers piliers de la cybersécurité. Leur vigilance individuelle et leur capacité à rendre compte est indispensable et représente la première défense en cybersécurité.

Formation des agents au risque cyber

Les agents intégrant les SPM doivent faire l'objet d'une session de sensibilisation aux risques cyber. Cette sensibilisation peut prendre la forme d'une formation collective, individuelle, ou d'un MOOC en ligne.

Exercice de sensibilisation à l'attention des agents

Les services du HFDS/PM ou les CSN/RSSI peuvent conduire des exercices de sensibilisation à l'attention des agents relevant de leur périmètre. Ces exercices peuvent prendre la forme notamment de campagnes d'hameçonnage fictives.

Charte de l'utilisateur informatique

La présente PSSI-SPM est déclinée dans chaque entité relevant du HFDS/PM. Une charte d'application de cette déclinaison, 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 systèmes d'information de l'entité des SPM au sein de laquelle il est amené à intervenir.

Charte de l'administrateur informatique ou administrateur fonctionnel

Pour assurer le fonctionnement des systèmes informatiques, des agents employés spécifiquement (dénommés « administrateurs » ou « administrateurs fonctionnels ») sont amenés à effectuer diverses opérations techniques ou fonctionnelles pour fournir un service de qualité aux utilisateurs.

Les règles et procédures de sécurité sont indiquées dans une charte et s'imposent à toutes personnes chargées de l'exploitation, de la maintenance, du suivi de l'utilisation des ressources informatiques et télécommunications, de la mise en œuvre des logiciels que ce soit sur site ou à distance (ex. astreintes).

Protéger : garantir la confiance dans le temps

Gestion des risques et homologation de sécurité

Toutes les infrastructures et services logiciels informatiques qui composent le système d'information et de communication de l'Etat doivent faire l'objet, préalablement à leur mise en œuvre, d'une homologation de sécurité.

Analyse des risques

Préalablement à toute démarche d'homologation, le système, le service ou le projet doit faire l'objet d'une démarche d'évaluation des risques. La méthode EBIOS-RM est préconisée, bien qu'une démarche allégée puisse être utilisée selon la stratégie ou le référentiel d'homologation défini par l'entité.

Evaluation de la menace

L'homologation de sécurité doit préciser le niveau de menace auquel le SI doit faire face. A minima, cette évaluation doit prendre en compte trois niveaux de menaces qu'il conviendra de retenir ou d'écarter dans la démarche d'homologation :

- Menace **étatique** : attaques sophistiquées, menées ou financées par un État, le plus généralement à des fins d'espionnage ou de sabotage;
- Menace **criminelle** : attaques menées par un groupe criminel, ou le grand banditisme, à des fins lucratives (rançongiciel, etc.), de chantages ou d'actes de malveillance;
- Menace **hacktiviste** ou de faible intensité: attaques menées par un individu isolé et/ou via des outils automatisés peu sophistiqués.

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 sa durée de validité ainsi que les conditions d'emploi. Les services se dotent d'une stratégie d'homologation adaptée aux enjeux de sécurité. Cette stratégie peut prévoir plusieurs dispositifs pour attester du niveau de sécurité actuel du système en fonction de la sensibilité portée par celui-ci :

- audit par un prestataire qualifié PASSI, en cas de systèmes présentant une sensibilité particulière ou un enjeu spécifique ;
- audit par un prestataire non qualifié PASSI, ou en cours de qualification ;
- *bug bounty* ;
- analyse interne.

En outre, un dispositif de maintien en condition de sécurité y est systématiquement intégré : il permet de garantir la confiance durant la période d'homologation quant au niveau de sécurité du système. Le FSSI/PM est systématiquement informé de toute décision d'homologation.

Sécurité des développements logiciels et des services

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.

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, le développement et les phases de recette. Toute mise en production de code, binaire ou autre librairie doit faire l'objet d'un examen adapté aux enjeux de sécurité du SI (contrôle manuel par l'administration, analyse de code automatisée ou audit dédié).

Dans le cadre de projets faisant appel à des méthodes de développement de type agile, l'entité veille à l'intégration[8] de la démarche de développement sécurisé[9] dans les différentes étapes des sprints de développement (par exemple grâce à l'intégration d'une revue de sécurité du code, la réalisation de rapports automatisés, la tenue d'ateliers d'analyse de risque réguliers, la réévaluation du périmètre d'homologation en fonction des *user-stories* livrées etc).

[8] Une bonne pratique consiste à mettre en place un cycle de développement sécurisé (SDLC ou *Software developement life cycle*) adapté à la méthodologie de projet retenue. Cette méthodologie peut prévoir une analyse régulière des besoins de sécurité, des scénarios de risques et peut intégrer dans les phases de test des sprints des « evil user » à même de tester le niveau de sécurité de chaque livraison.

[9] Se référer au guide de l'ANSSI prévu à cet effet : https://www.ssi.gouv.fr/guide/agilite-et-securite-numeriques-methode-et-outils-a-lusage-des-equipes-projet/

Il convient d'assurer une détection des vulnérabilités le plus en amont possible dans la chaîne de développement (et tout particulièrement avant la mise en production) par exemple en s'appuyant sur des outils d'analyse de code statique (SAST) durant la phase de développement ou dynamique (DAST) durant la phase de recette. L'objectif d'une telle démarche est de réduire le temps de détection des vulnérabilités issues des phases de conception.

Dans ce cadre, une vigilance particulière doit être portée à l'intégration de bibliothèques de développement ou de dépendances (paquets NPM, JS, ou PIP par exemple), notamment en ce qui concerne les vulnérabilités qu'elles peuvent incorporer dans la *supply chain*, ainsi que le nécessaire suivi des mises à jour qu'elles imposent.

Une application ne doit pas être mise en production sur un environnement de développement ou de qualification. Inversement, un environnement de production ne doit pas être utilisé à des fins de développement ou de qualification. Aucune donnée de production ne doit être utilisée sur des environnements hors-production (à l'exception des données qui font l'objet d'une catégorisation « données publiques » cf chapitre planification).

Les développements Web font l'objet de problèmes de sécurité récurrents qui ont conduit à la constitution de référentiels de sécurité. Ces référentiels[10] ont pour objectif de fixer des règles 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.). Il convient en particulier de prendre en compte le top 10 des vulnérabilités de l'OWASP[11] tout au long des développements et évolutions du système.

L'ensemble des dispositifs décrits ci-dessus fait partie intégrante du dossier d'homologation.

Maintien en condition de sécurité des systèmes d'information

Le maintien en condition de sécurité des SI vise à garantir un niveau de sécurité cible, identifié au cours du processus d'homologation, durant l'ensemble de la durée de vie du projet ou du système. Dispositif essentiel de la sécurité des systèmes d'information, le processus de MCS doit permettre d'assurer le suivi des vulnérabilités des différentes briques composant le système (systèmes d'exploitation, applicatifs, plugins, librairies et autres composants techniques) ainsi que de la bonne application des correctifs de sécurité. Le MCS doit assurer la prise en compte des actions correctrices (mises à jour

[10] Notamment les guides :
- https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-securisation-des-sites-web/
- https://www.ssi.gouv.fr/guide/regles-de-programmation-pour-le-developpement-securise-de-logiciels-en-langage-c/

[11] https://owasp.org/Top10/fr/

dans les temps), de contournement (extinction ou isolement du système par exemple) ou d'acceptation.

Ce dispositif doit aussi assurer la sécurité du système dans le cadre de ses évolutions. A titre d'exemple, la livraison de nouvelles fonctionnalités développées dans de nouvelles portions de code doit faire l'objet d'une évaluation de son niveau de sécurité afin d'identifier les potentielles vulnérabilités importées par ces évolutions.

En outre, le processus de MCS doit assurer le suivi des réserves et des risques résiduels actés au cours du processus d'homologation afin d'atteindre la cible du niveau de sécurité décidé, dans le temps imparti.

Gestion des vulnérabilités

Les services se dotent d'un processus de gestion des vulnérabilités. Celui-ci doit prévoir la capacité à remédier à une vulnérabilité (application d'un correctif de sécurité, d'une mesure de contournement ou d'une extinction du système) sous un délai explicité dans le dossier d'homologation contraint par les enjeux de sécurité portés par le système. Ce processus participe à la réponse aux injonctions de l'ANSSI.

Sécurité des services exposés sur Internet

L'exploitation de services exposés sur internet nécessite la mise en œuvre de moyens spécifiques et une grande réactivité. Ces services peuvent être exploités directement par l'administration, sur ses infrastructures propres ou dans des infrastructures publiques (hébergeur, *cloud*) ou entièrement externalisées auprès de prestataires extérieurs (*software as a service*).

Certificats

Les services exposés sur internet, et tous systèmes d'information en environnement de production, doivent utiliser des certificats de confiance conformément au décret RGS. L'utilisation de certificats non RGS dans des environnements de production ou identifiés comme sensibles, est proscrite.

Noms de domaine

La création ou la refonte de tout téléservice ou site web à vocation publique doit être réalisée sous un nom de domaine « .gouv.fr » afin de permettre d'identifier l'authenticité de celui-ci. En outre, et quel que soit son extension (.gouv.fr, .fr, etc), sa mise en ligne devra faire l'objet d'une demande d'agrément du Service d'Information du Gouvernement (SIG).

Surveillance des noms de domaine et marques associées

Tout site web ou application exposée sur internet présentant une marque distinctive (« legifrance », « franceconnect » ou autre) doit faire l'objet d'une surveillance

particulière afin d'éviter tout effet de *typosquatting* visant à usurper l'identité de l'administration dans le but de tromper les visiteurs.

A ce titre, il est recommandé de communiquer au FSSI/PM les noms de domaines et marques correspondantes afin d'intégrer leur surveillance au sein d'un outil dédié.

Hébergement

Les choix d'hébergement retenus doivent être conformes aux règlementations en vigueur (données de santé, RGPD…) et en cohérence avec la doctrine Cloud de l'Etat.

La disponibilité et le niveau de cybersécurité proposé par la solution d'hébergement font partie du périmètre d'homologation (une application nécessitant un besoin de disponibilité de 4h sera incompatible avec un hébergement proposant une garantie de temps de rétablissement de 12h sans mesure compensatoire).

Utilisation des équipements personnels

Il est interdit de :

- traiter des données professionnelles sur des équipements non maîtrisés par l'administration ;
- connecter un équipement non maîtrisé par l'administration sur des équipements professionnels (par exemple, connexion d'une clef USB personnelle sur un équipement professionnel, connexion d'un terminal personnel sur le réseau professionnel de l'administration non prévu à cet effet).

Dans le cadre d'une dérogation, l'AQSSI détermine si le risque lié à l'usage d'équipements non maîtrisés par l'administration est acceptable. Cette autorisation dérogatoire doit être effectuée dans un cadre d'emploi strict et communiqué aux agents, en adéquation avec les enjeux de sécurité portés par le SI ou par les données traitées dans le cadre des missions de chaque agent, après avoir réalisé une analyse de risque adéquate et mis en place des mesures garantissant la sécurité des échanges et des terminaux. Le cadre d'emploi doit être défini en fonction de l'usage ciblé et du niveau de menace retenu dans la démarche d'analyse de risque.

Nomadisme (PC, téléphone, tablette)

La sécurité du SI s'entend de manière globale et donc au travers de tous les accès matériels et logiciels (WebMail, service de télétravail exposé sur internet…) au-delà du seul ordinateur professionnel.

Les accès à distance au système d'information de l'entité s'ils sont autorisés, doivent être réalisés via un réseau privé virtuel (VPN) de confiance.

Le stockage local d'information sur le terminal doit être limité au strict nécessaire. Le disque de stockage du terminal doit être intégralement chiffré.

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.

Tous les terminaux se connectant au réseau de l'entité doivent faire l'objet d'une gestion centralisée permettant, entre autres, d'assurer le maintien en conditions de sécurité du parc.

L'ensemble de la présente partie « Nomadisme (PC, téléphone, tablette) » ne peut s'appliquer dans un environnement dont la menace étatique aurait été retenue durant l'analyse de risque.

Détecter

Contrôles

La conformité à la présente PSSI est vérifiée par des contrôles réguliers donnant lieu, si nécessaire, à des plans d'actions d'améliorations et de corrections. Le CSN en transmettra un bilan annuel au FSSI.

Les CSN de chaque entité organisent des actions d'évaluation de la conformité et contribuent à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en œuvre. Ces audits sont suivis d'un plan d'actions d'amélioration et de correction. Dans ce cadre, les RSSI sont associés aux travaux de mise en œuvre.

Des contrôles réguliers du niveau de sécurité et de l'efficacité des mesures de protection mises en œuvre sur le périmètre des systèmes en production doivent être réalisés afin de mettre en évidence le plus rapidement possible les anomalies et incidents, et conduire à la mise en œuvre des mesures correctrices appropriées. Des audits non planifiés peuvent être décidés à l'initiative du FSSI/PM, du CSN ou d'une autorité compétente.

Afin de garantir un niveau de résilience suffisant des infrastructures exposées, des outils de l'ANSSI sont mis à disposition des services afin d'évaluer leur niveau de sécurité et les actions correctrices à mettre en œuvre.

Les services exploitant un système d'information qui comprend une brique d'annuaire de type « Active Directory » intègrent systématiquement une évaluation régulière de son niveau de sécurité grâce à l'utilisation de l'outil mis à disposition par l'ANSSI (**ADS**).

De la même manière, les entités exploitant un ou plusieurs systèmes d'information exposés sur internet intègrent systématiquement une évaluation régulière de leur niveau de sécurité grâce à l'utilisation de l'outil mis à disposition par l'ANSSI (**SILENE**).

Dispositifs de détection techniques

Les services mettent en œuvre des dispositifs de détection (réseaux, systèmes, applicatifs qui peuvent se traduire par des dispositifs techniques de type SIEM, SOC, EDR, SONDES, IDS, IPS, Proxy) permettant d'assurer un niveau de sécurité adapté aux enjeux portés par le système d'information. Ces dispositifs doivent permettre de détecter les tentatives d'attaques sur les différentes briques du système : périmétrique, serveur, postes de travail et autres terminaux.

Ces dispositifs doivent être opérés et surveillés, soit en interne soit par un prestataire de confiance [12] (PDIS : prestataire de détection d'incidents de sécurité) si le SI concerné présente une sensibilité particulière.

Pour les SI présentant une sensibilité moindre, l'externalisation de la fonction de détection peut être déléguée à un prestataire non qualifié ou en cours de qualification. Le risque induit par cette externalisation devra être évalué par l'autorité d'homologation au cours du processus d'homologation.

Collecte des journaux

Afin de garantir une capacité de détection efficace, les services doivent mettre en œuvre des systèmes de collecte et éventuellement d'analyse des journaux techniques afin de pouvoir :

- détecter des tentatives d'intrusion ou de compromission ;
- corréler des évènements de sécurité en vue d'anticiper des tentatives d'attaques ;
- réaliser des analyses en cas de soupçon d'intrusion et procéder à des analyses post-mortem en cas d'intrusion avérée.

Ces dispositifs peuvent être déployés en interne ou opérés par un prestataire de confiance selon le niveau de sensibilité retenu pour le SI dans la démarche d'homologation retenue.

Ces données sont mises à disposition du FSSI/PM en cas de besoin.

Une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie par le RSSI en lien avec le CSN, validée par l'autorité qualifiée, et mise en œuvre par le RSSI en lien avec le service numérique compétent. 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.

[12] https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-detection-dincidents-de-securite-pdis/
Le prestataire de confiance peut également être une autre entité ministérielle.

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.

Répondre : faire face à la crise

Traitement des incidents

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

En cas d'alerte de sécurité identifiée au niveau national, le CSN de chaque entité s'assure de la bonne application des exigences formulées ci-dessous, dans les meilleurs délais.

En cas d'alerte de sécurité ayant un caractère d'injonction, identifiée au niveau interministériel ou bien relative à un système d'information spécifiquement identifié, les services se mettent en capacité de répondre sous le délai spécifié par le HFDS/PM.

Remontée des incidents de sécurité

Tout utilisateur constatant un incident ou une anomalie susceptible d'affecter la sécurité des SI doit la signaler selon une procédure adaptée. Il s'agit *a minima* de prévenir immédiatement sa hiérarchie, qui informera elle-même la chaîne SSI de l'entité. En aucun cas, un agent ne doit diffuser ces informations.

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

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

Réponse à incident de sécurité

En cas d'indisponibilité de ressources internes aptes à traiter la réponse à incident de sécurité, les services victimes d'un incident de sécurité sur un ou plusieurs de leurs systèmes d'information font appel à un prestataire certifié (PRIS), ou en cours de certification, afin d'identifier les sources de compromission et d'orienter les mesures de remédiation à mettre en œuvre. Les conclusions de cette prestation sont communiquées au FSSI/PM.

En cas d'impossibilité de recourir à une société certifiée PRIS ou en cours de certification PRIS, une demande de dérogation dûment justifiée peut être demandée auprès du HFDS/PM.

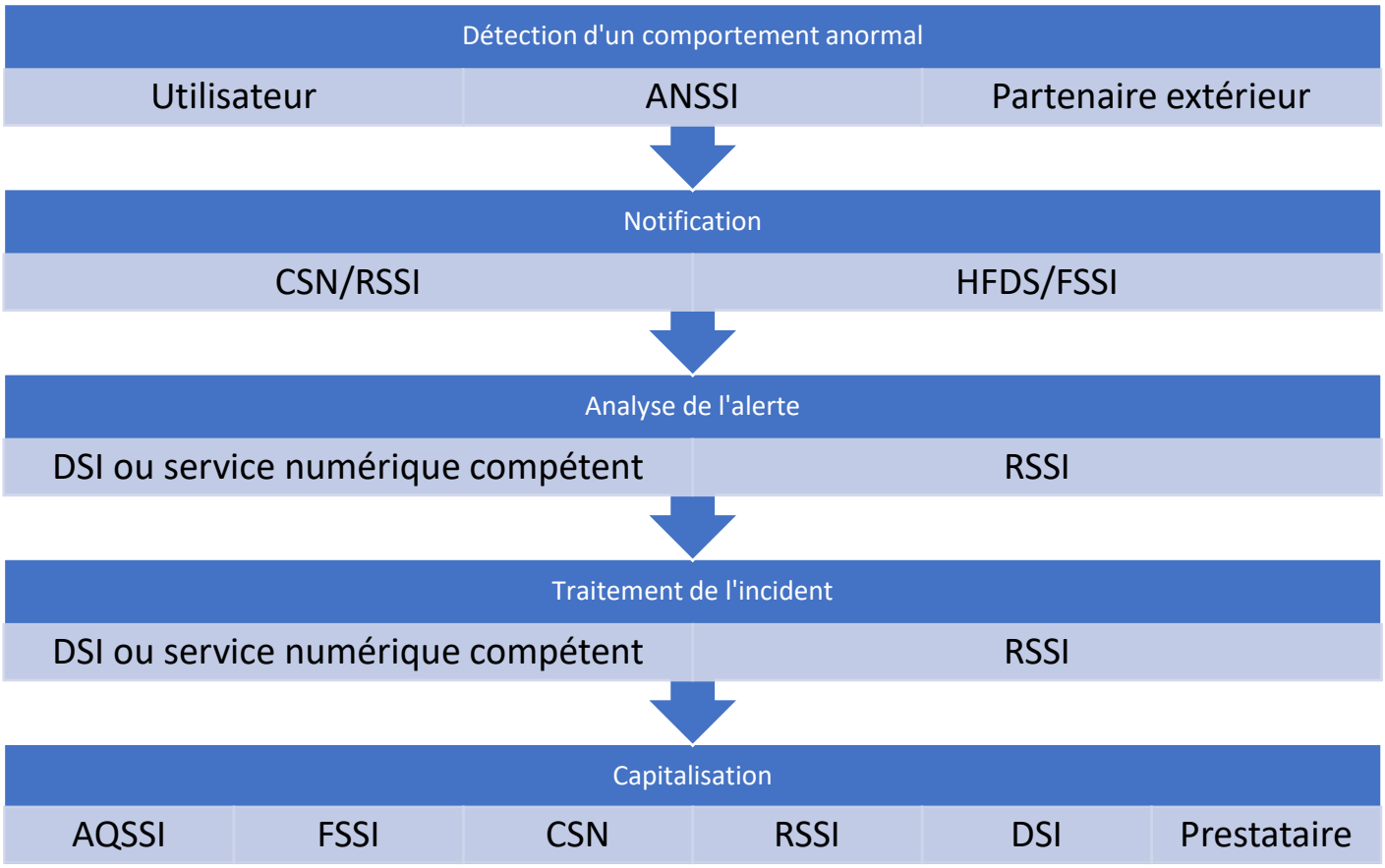
Tout incident de sécurité avéré doit faire l'objet d'une capitalisation par les services afin de mettre en œuvre des mesures correctrices, préventives ou structurantes dans la survenue d'incidents similaires. Un retour d'expérience peut être demandé par le FSSI/PM.

Processus de gestion des incidents de cybersécurité

Tout événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien lié à un système d'information doit faire l'objet d'une déclaration auprès de la chaîne d'alerte.

Plusieurs catégories d'incident sont définies, telles que :

- intrusion ou tentative de prise de contrôle d'un système ;
- réception et/ou activation d'un lien de phishing ou autre email malveillant ;
- réception et/ou exécution d'un fichier malveillant (malware, virus, trojan, worm) ;
- indisponibilité liée à une attaque par déni de service (DoS, DDoS) ;
- usurpation d'identité d'une administration (typosquatting) ou d'un agent de l'Etat (phishing) ;
- divulgation de données non maitrisées (fuite, exposition, suppression, perte de clé USB etc) ;
- perte d'un matériel informatique de l'administration (ordinateur, smartphone, tablette et tout autre moyen de communication) ;
- perte d'un document ou d'une information relatifs à un SI identifié comme critique.



En cas d'incident critique suspecté, le FSSI/PM peut être saisi directement : à l'adresse suivante : fssi[@]pm[.]gouv[.]fr par téléphone : au **01 42 75 80 00 en demandant l'astreinte du HFDS**

Déclaration à la CNIL

Il est indispensable d'identifier, en cas de suspicion d'une compromission ou d'une compromission avérée, si le système assurait le traitement de données personnelles (collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction). Le cas échéant, en cas de compromission avérée, il convient de prendre en compte le délai légal de notification de l'incident à l'autorité compétente (CNIL).

Retour d'expérience

Tout incident de sécurité avéré doit faire l'objet d'une capitalisation par les services afin de mettre en œuvre des mesures correctrices, préventives ou structurantes dans

la survenue d'incidents similaires. Un retour d'expérience peut être demandé par le FSSI/PM.

Partage d'informations sur la menace

Les services doivent systématiquement communiquer au FSSI/PM les éléments de preuves permettant de qualifier la menace : indicateurs de compromission (adresse IP, nom de domaine, hash et nom de fichier) et le mode d'action utilisé par l'attaquant.

Gestion de crise cyber

Les entités relevant du HFDS/PM disposent d'un dispositif de gestion de crise cyber visant à répondre à toute crise majeure d'origine cyber ou ayant des impacts sur les activités cyber. Ce dispositif est partagé avec l'ensemble des acteurs de la gestion de crise cyber du périmètre.

Tout incident de cybersécurité peut donner lieu à un déclenchement d'une cellule de crise cyber conformément au plan de gestion des crises des SPM.

Chaque entité doit se doter d'un dispositif local de gestion de crise adapté à l'éventualité d'une crise d'origine cyber. Ce dispositif doit prévoir la chaîne de décision, les acteurs et ressources clés ainsi que les procédures adéquates.

Ce dispositif de gestion de crise cyber doit a *minima* permettre de :

- connaître et maîtriser ses systèmes d'information ;
- mettre en place un socle de capacités opérationnelles garantissant un niveau adapté de résilience numérique ;
- formaliser une stratégie de communication de crise cyber ;
- adapter son organisation de crise au scénario cyber ;
- préparer ses capacités de réponse à incident ;
- s'entraîner pour pratiquer et s'améliorer.

Astreintes

Afin de faire face à tout incident de sécurité pouvant survenir en dehors des horaires de travail, un dispositif d'astreinte dédié à la cybersécurité est mis en place dans les services du Premier ministre. Ce dispositif sollicite l'ensemble des acteurs de la chaîne fonctionnelle de sécurité des systèmes d'information. Le standard de Matignon (01 42 75 80 00) est chargé de recueillir les alertes de cybersécurité, en heures ouvrables et non ouvrables, et de mobiliser l'astreinte.

Le bon fonctionnement du dispositif de traitement des incidents de cybersécurité suppose que les services soient pleinement impliqués. Le standard de Matignon doit ainsi disposer à tout moment des coordonnées du cadre référent, responsable de la gestion des incidents informatiques affectant l'application, le site Web ou plus largement tout SI de l'entité. Ce cadre référent est susceptible d'être mis en contact avec celui de l'astreinte de cybersécurité et de répondre à ses demandes. Il doit également être en mesure de prendre ou d'obtenir directement et rapidement de l'autorité une décision concernant les mesures conservatoires nécessaires en cas de cyberattaque (par exemple, l'interruption du service web attaqué ou la fermeture d'une application compromise).

Dérogations

Toute dérogation à une règle de la PSSI-SPM doit obtenir l'accord exprès du HFDS/PM. La demande, transmise par l'intermédiaire du CSN doit comporter les motivations, la durée souhaitée, ainsi que l'analyse des risques et les mesures de mitigation associées. La décision, signée par le HFDS/PM, est tenue à la disposition de l'ANSSI.

Une revue de toutes les dérogations est effectuée annuellement par la chaîne SSI.

Le haut fonctionnaire
de défense et de sécurité

Claire LANDAIS

Annexe 1 : échelles des besoins de sécurité

Chaque critère de sécurité est évalué selon une échelle de besoin à plusieurs niveaux. La signification de chaque niveau est explicitée pour chaque critère dans les tableaux ci-dessous. Un besoin évalué à 0 est plus faible qu'un besoin évalué à 2.

Disponibilité

La disponibilité est l'aptitude d'un processus à rendre le service attendu en temps voulu et dans les conditions d'usage prévues. Il reflète le besoin de continuité de fonctionnement.

Elle est exprimée en heure en précisant s'il s'agit d'heures ouvrées ou non ouvrées, de jours fériés et de weekend.

Intégrité

L'intégrité est la propriété permettant de s'assurer qu'une information n'est modifiée ou détruite que par les utilisateurs habilités ou les processus réalisés dans les conditions initialement prévues. C'est la garantie de fiabilité et d'exhaustivité de l'information.

Échelle		Expression du besoin d'Intégrité
3	Très élevé	Aucune altération n'est acceptable.
2	Élevé	La détection d'une altération doit être automatique et doit entraîner la correction.
1	Normal	La détection doit être automatique.
0	Faible	Les données sont altérables.

Confidentialité

La confidentialité est la propriété permettant de s'assurer que seuls les utilisateurs habilités dans les conditions normales prévues ont accès aux informations.

Échelle		Expression du besoin de Confidentialité
3	Très sensible	La divulgation d'information a des conséquences inacceptables.
2	Sensible	La divulgation d'information a des conséquences **très importantes.**
1	Interne	La divulgation d'information a des conséquences **dommageables**.
0	Public	La divulgation d'information n'a **aucune conséquence**.

Traçabilité

La traçabilité est la propriété qui garantit la conservation des enchaînements d'opérations (par exemple la création d'un document, les personnes qui y ont eu accès et l'historique des modifications…).

Échelle		Expression du besoin de Traçabilité
3	Impérative	Aucune contestation n'est possible (preuve opposable).
2	Forte	La traçabilité est assurée, l'identification des auteurs est résistante à la répudiation des actions (preuve opposable).
1	Effective	La traçabilité est assurée sur les fonctions majeures, mais l'identification des auteurs n'a pas à être résistante à la répudiation.
0	Faible	Des traces peuvent être générées mais l'identification des acteurs n'est pas requise.