



MINISTÈRE DE L'INTÉRIEUR

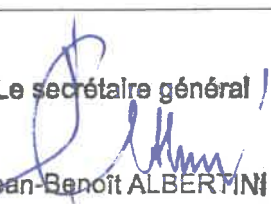
*Liberté
Égalité
Fraternité*

Politique générale de sécurité numérique du ministère de l'Intérieur

Approuvée par le préfet, secrétaire général,
haut fonctionnaire de défense

N°NOR : INTA2202748J

Le secrétaire général


Jean-Benoît ALBERTINI

Avant-propos

Les réformes successives de l'État ont modifié en profondeur son organisation et ses missions, en l'engageant dans une transformation numérique profonde.

La sécurité numérique représente un critère essentiel de réussite de cette transformation notamment en ce qui concerne le ministère de l'Intérieur compte tenu de la criticité de ses missions régaliennes et de la sensibilité des données qu'il est amené à traiter.

Cette exigence de sécurité est d'autant plus nécessaire dans un contexte où la cybermenace est croissante, renforcée par la prolifération d'outils malveillants. Les modes opératoires utilisés par les attaquants, leurs motivations et les moyens dont ils disposent, représentent un éventail très large, allant des tentatives d'accès les plus anodines jusqu'aux attaques les plus sophistiquées.

Objectifs stratégiques

Les objectifs stratégiques de cette politique générale de sécurité numérique sont les suivants :

- S1. Éviter la déstabilisation des missions du ministère, en se préparant aux attaques ciblées et sophistiquées dont il fait l'objet.** En effet, des groupes organisés, disposant de moyens importants, prennent pour cible les missions les plus essentielles du ministère. Celui-ci doit donc bâtir un système de protection et de défense adaptées.
- S2. Rendre indolores les très nombreuses cyberattaques d'intensité moyenne contre le ministère et son écosystème numérique.** La consolidation d'un socle de sécurité doit permettre de réduire la fréquence des incidents et l'impact des attaques les plus courantes, sur le périmètre du ministère de l'Intérieur et son écosystème numérique.
- S3. S'attacher à intégrer le risque numérique dans l'organisation et les procédures internes du ministère, en particulier dans la gestion de crise.** La dimension numérique ne doit plus être considérée comme un volet juxtaposé aux autres, mais comme un facteur transverse et naturel.

Le présent document présente l'organisation décisionnelle, fonctionnelle et opérationnelle dont le ministère de l'Intérieur se dote pour atteindre ces objectifs.

Instruction relative à la sécurité numérique du ministère de l'Intérieur

Table des matières

Préambule.....	5
Article 1. Corpus de la sécurité numérique du ministère de l'Intérieur.....	5
Article 2. Champ d'application.....	5
Article 3. Cadre obligatoire de la PGSN-MI	6
Article 4. Date d'effet et révision	6
Article 5. Terminologie utilisée	6
TITRE I : Organisation ministérielle de la sécurité numérique.....	8
<u>Chapitre 1 : La chaîne décisionnelle de sécurité numérique.....</u>	<u>8</u>
Article 6. Composition de la chaîne décisionnelle	8
Article 7. Le haut fonctionnaire de défense.....	8
Article 8. Les autorités qualifiées en sécurité des systèmes d'information	8
Article 9. Les préfets de zone de défense et de sécurité	9
<u>Chapitre 2 – La chaîne fonctionnelle de sécurité numérique</u>	<u>9</u>
Article 10. Composition de la chaîne fonctionnelle	9
Article 11. Le fonctionnaire de sécurité des systèmes d'information	10
Article 12. Les conseillers à la sécurité du numérique.....	10
Article 13. Les assistants locaux à la sécurité du numérique.....	10
Article 14. Les délégués zonaux à la sécurité du numérique.....	11
<u>Chapitre 3 – La chaîne opérationnelle de sécurité numérique et de cyberdéfense</u>	<u>11</u>
Article 15. Composition de la chaîne opérationnelle.....	11
Article 16. Centre de cyberdéfense du ministère de l'Intérieur.....	12
Article 17. Les services opérationnels numériques	12
Article 18. Les responsables de la sécurité des systèmes d'information	12
Article 19. Les assistants locaux à la sécurité des systèmes d'information	13
TITRE II : La gouvernance ministérielle de la sécurité numérique.....	14
Article 20. Système de gouvernance de la sécurité numérique.....	14
Article 21. Tour de table des comités de gouvernance	14
Article 22. Le comité stratégique de la sécurité numérique.....	14
Article 23. Le comité de pilotage de la sécurité numérique	15
Article 24. Le comité de suivi de la sécurité numérique.....	15
Article 25. Rapports annuels de la sécurité numérique.....	15

TITRE III : La maîtrise du risque numérique.....	17
Article 26. Principes stratégiques de la maîtrise du risque numérique	17
Article 27. Politique d’audit de sécurité.....	17
Article 28. Cartographie des SI	17
Article 29. Cartographie des risques numériques	18
Article 30. Intégration de la sécurité dans les projets.....	18
Article 31. Maîtrise des prestataires, fournisseurs et partenaires	19
Article 32. Homologation de sécurité	19
Article 33. Systèmes d’information essentiels.....	19
Article 34. Systèmes d’information d’importance vitale.....	20
TITRE IV : La résilience des activités	21
Article 35. Principes stratégiques de la cyber-résilience	21
Article 36. Gestion de crise.....	21
Article 37. Plan de continuité d’activité.....	21
TITRE V : Dispositions opérationnelles.....	22
Article 38. Enjeux de la prévention	22
Article 39. Enjeux de la protection	22
Article 40. Enjeux de la détection des événements suspects.....	23
Article 41. Enjeux de la réponse aux attaques	23

Préambule

Le présent document définit la politique générale de sécurité numérique du ministère de l'Intérieur (PGSN-MI).

Cette politique s'inscrit dans le cadre de la politique de sécurité des systèmes d'information de l'État (PSSI-E), approuvée par la circulaire du Premier ministre n°5725/SG du 17 juillet 2014. Elle expose les principes stratégiques structurant l'action ministérielle en matière de sécurité numérique ; elle précise l'organisation et les structures de gouvernance ministérielles ; elle présente les dispositions générales permettant d'assurer la protection et la défense des systèmes d'information.

La PGSN-MI est disponible sur l'intranet du ministère de l'Intérieur à l'adresse :

<http://ssi.minint.fr/index.php/politique-de-securite/pgsn-mi>

Article 1. Corpus de la sécurité numérique du ministère de l'Intérieur

La PGSN-MI est complétée par un corpus documentaire disponible à la même adresse. Il précise la manière dont les principes sont mis en œuvre de manière opérationnelle. Il indique également comment les règles de la PSSI-E sont adaptées au contexte du ministère de l'Intérieur.

Pour chaque document constitutif du corpus de la sécurité numérique du ministère de l'intérieur, une entité est désignée pour son élaboration et son maintien à jour. Toute entité peut proposer des nouveaux documents ou des évolutions sur ceux existants.

Pour le compte du haut fonctionnaire de défense (HFD), le fonctionnaire de sécurité des systèmes d'information (FSSI) assure la maîtrise des documents publiés, relevant d'un caractère normatif pour le ministère. Il maintient à jour la liste structurée des documents, de leur responsable, de leur publication et de leurs mises à jour. Il assure également la notification auprès de chaque entité concernée.

Article 2. Champ d'application

La PGSN-MI s'applique à l'ensemble du ministère de l'Intérieur et du ministère des outre-mer : les directions générales, les directions, les services centraux, les services déconcentrés du ministère de l'Intérieur, ainsi que les établissements publics et offices placés sous leur tutelle. Par convention, l'ensemble de ces entités est regroupé sous le terme « ministère de l'Intérieur ».

La PGSN-MI s'applique également aux préfetures, directions départementales interministérielles (DDI) et secrétariats généraux communs départementaux (SGC), regroupés sous le terme « Administration territoriale de l'Etat » (ATE) dans la PGSN et son corpus.

La PGSN-MI s'applique également, par voie contractuelle ou conventionnelle, aux services externalisés par le ministère de l'Intérieur (fournisseurs, prestataires de services, sous-traitants...) ainsi qu'aux partenaires (organisations syndicales, mutuelles, associations...) lorsqu'ils concourent aux missions du ministère ou qu'ils ont accès à des informations sensibles du ministère. L'ensemble de ces acteurs proches est appelé « écosystème numérique » du ministère de l'Intérieur.

Les règles de la PGSN-MI s'appliquent à tous les systèmes d'information du ministère de l'Intérieur, intégrant l'ensemble des systèmes de téléphonie. Pour les systèmes aptes à traiter des informations classifiées de défense, il appartient à chaque autorité qualifiée, en lien avec

leur conseiller à la sécurité numérique (CSN¹), d'appliquer la réglementation spécifique (IGI 1300) et d'assurer une cohérence avec les exigences de la PGSN-MI.

Tous les « systèmes d'information de sûreté » entrent également dans le périmètre de la présente PGSN-MI : systèmes de contrôle d'accès physique et de détection d'intrusion, systèmes de sécurité incendie, systèmes de gestion technique de bâtiment, systèmes de vidéosurveillance, etc.

Article 3. Cadre obligatoire de la PGSN-MI

La PGSN-MI constitue le cadre obligatoire dans lequel toute entité entrant dans le champ d'application de l'article 2, inscrit ses actions liées à la sécurité numérique.

Chaque autorité qualifiée en SSI (AQSSI²) publie sa propre politique de sécurité numérique en conformité avec la présente PGSN-MI, précisant la manière dont elle organise et pilote, sur son périmètre, les processus liés à la sécurité numérique.

En cas d'impossibilité de mise en application de la PGSN-MI sur un périmètre donné, une demande de dérogation doit être formalisée par l'autorité qualifiée en sécurité des systèmes d'information et transmise pour approbation au haut fonctionnaire de défense (HFD).

Article 4. Date d'effet et révision

La mise en œuvre de la PGSN-MI est engagée dès sa publication et abroge la PSSI-MI du 10 mars 2015. Cette mise en œuvre est suivie annuellement par le comité stratégique de la sécurité numérique (COSTRAT SECNUM³), grâce à un tableau de bord et un plan annuel de sécurité numérique.

Toute demande d'évolution ou d'adaptation de la PGSN-MI est soumise au COSTRAT SECNUM pour instruction. Le besoin de réviser la PGSN-MI est étudié au plus tard tous les cinq ans, ainsi que lors de la publication d'un texte normatif interministériel relatif à la sécurité numérique.

Article 5. Terminologie utilisée

La transformation numérique favorise l'évolution des concepts et des techniques. Des travaux interministériels poussent à la traduction de cette évolution dans la terminologie employée. À titre d'exemple, le terme « sécurité des systèmes d'information » (SSI) est progressivement remplacé par le terme « sécurité numérique » (SN).

Par rapport aux documents précédents de politique de sécurité, plusieurs termes évoluent :

- Le responsable de la sécurité des systèmes d'information (RSSI) devient, suivant les cas :
 - o le conseiller à la sécurité du numérique (CSN) s'il est placé auprès d'une autorité qualifiée en SSI ou d'une autorité ayant délégation ;
 - o il conserve le titre de RSSI s'il est placé auprès du responsable d'une structure en charge du numérique⁴.
- Le responsable zonal de la sécurité des systèmes d'information (RZSSI), devient délégué zonal à la sécurité du numérique (DZSN).

¹ Voir article 12

² Voir article 8

³ Voir article 22

⁴ Directeur du numérique, chef du service des technologies et des systèmes d'information de la sécurité intérieure, chef de service interministériel départemental des systèmes d'information et de communication, etc.

- L'assistant local de la sécurité des systèmes d'information (ALSSI) et le correspondant local de la sécurité des systèmes d'information (CLSSI) deviennent, suivant les cas :
 - o l'assistant local à la sécurité du numérique (ALSN) quand il est rattaché à un CSN ;
 - o l'assistant local à la sécurité des systèmes d'information (ALSSI) quand il est dans une structure en charge du numérique, rattaché à un RSSI.

TITRE I : Organisation ministérielle de la sécurité numérique

Chapitre 1 : La chaîne décisionnelle de sécurité numérique

Article 6. Composition de la chaîne décisionnelle

Conformément au premier principe stratégique évoqué en introduction, les processus liés à la sécurité numérique s'intègrent dans les processus habituels. Les décisions portant sur des enjeux de sécurité numérique sont prises par les autorités de niveau adéquat, qui composent la structure de commandement du ministère. Les décisions sont prises avec l'objectif de garder le risque en dessous d'un niveau jugé acceptable.

La chaîne décisionnelle est chargée du pilotage de la mise en œuvre de la politique de sécurité et du contrôle de son application. Le cas échéant, elle organise les modalités d'arbitrage sur les décisions concernant les mesures de sécurité.

Les principales autorités qui composent la chaîne décisionnelle de sécurité numérique sont :

- les ministres ;
- le secrétaire général, haut fonctionnaire de défense ;
- les directeurs généraux, les directeurs centraux, les directeurs d'établissement ou chefs de service ;
- les préfets de zone de défense et de sécurité, les préfets délégués de défense et de sécurité, les préfets de département.

Article 7. Le haut fonctionnaire de défense

Conformément aux missions édictées par l'article R1143-5 du Code de la Défense et l'IGI 1300, le haut fonctionnaire de défense anime la politique de sécurité et contrôle son application. Pour le ministère de l'Intérieur, le secrétaire général est désigné haut fonctionnaire de défense (HFD).

En vue de garantir la sécurité globale du ministère, le haut fonctionnaire de défense anime, coordonne et contrôle l'application de la présente politique par les autorités qualifiées en sécurité des systèmes d'information.

Le HFD fixe également les éléments constitutifs du corpus de la sécurité numérique du ministère, listé dans le document intitulé « *Organisation du corpus de la sécurité numérique* ».

Pour exercer ses missions, il s'appuie sur le haut fonctionnaire de défense adjoint (HFDA) et sur le service qui lui est attaché à l'échelon central. A l'échelon territorial, il s'appuie sur les préfets de zones de défense et de sécurité et les autorités qualifiées en sécurité des systèmes d'information.

Article 8. Les autorités qualifiées en sécurité des systèmes d'information

Chaque entité du ministère est placée sous la responsabilité d'une autorité qualifiée en sécurité des systèmes d'information (AQSSI). La responsabilité d'une AQSSI ne peut pas être déléguée.

L'AQSSI possède le pouvoir hiérarchique et la capacité d'arbitrage sur les moyens, budgétaires et humains, employés pour que la sécurité numérique de l'entité se rapproche d'un état jugé optimal.

Les attributions et la mention du périmètre de compétence des AQSSI sont fixées par arrêté ministériel. Au niveau départemental, le préfet est AQSSI sur le périmètre des services de l'administration territoriale de l'État sous sa responsabilité et relevant du ministère de l'Intérieur.

Pour une entité donnée, l'AQSSI est en principe unique. Lorsqu'une entité du ministère est pilotée par une tutelle multiple, les AQSSI concernées s'accordent pour désigner formellement la seule autorité compétente dans le domaine de la sécurité numérique et de la gestion de crise cyber.

Article 9. Les préfets de zone de défense et de sécurité

Sans se substituer aux AQSSI, le préfet de zone de défense et de sécurité a en charge la coordination des moyens liés la sécurité numérique pour l'ensemble des services de sa zone relevant du ministère de l'Intérieur.

En lien avec les AQSSI et les préfets de département, le préfet de zone a pour missions :

- de préparer les mesures concourant à la sécurité nationale, notamment en matière de sécurité numérique et de gestion de crise cyber ;
- d'établir un état des lieux du niveau de résilience opérationnelle des services du ministère de sa zone face à la cybermenace et d'en communiquer régulièrement les résultats au HFD.
- de procéder, sur le périmètre de sa zone, à la demande du HFD ou des AQSSI, à des audits de sécurité des services du ministère de l'Intérieur. Ces audits sont réalisés sous la coordination des AQSSI concernées, ou leur représentant.

Le préfet de zone diligente des contrôles sur l'application zonale de la présente politique, en coordination avec les AQSSI. Il est assisté dans ses missions par le préfet délégué pour la défense et la sécurité (PDDS).

Chapitre 2 – La chaîne fonctionnelle de sécurité numérique

Article 10. Composition de la chaîne fonctionnelle

La chaîne fonctionnelle de sécurité numérique est chargée de faire appliquer sur son périmètre, les mesures de sécurité numérique, d'en contrôler l'exécution et de conseiller la chaîne décisionnelle. Elle est constituée des acteurs placés auprès des membres de la chaîne décisionnelle :

- auprès des ministres : le haut fonctionnaire de défense et son adjoint, assistés du fonctionnaire de sécurité des systèmes d'information ;
- auprès des autorités qualifiées en sécurité des systèmes d'information : le conseiller à la sécurité du numérique . Il peut lui-même être conseillé par un responsable de la sécurité des systèmes d'information ;
- auprès des préfets de zone et des préfets délégués pour la défense et la sécurité : le délégué zonal de la sécurité numérique, tenant un rôle particulier dans la chaîne, en appui du HFD.

Article 11. Le fonctionnaire de sécurité des systèmes d'information

Placé sous l'autorité du haut fonctionnaire de défense adjoint et désigné par le haut fonctionnaire de défense, le fonctionnaire de sécurité des systèmes d'information (FSSI) anime la chaîne fonctionnelle de sécurité numérique du ministère pour l'ensemble des activités qui lui sont dévolues.

En particulier, le FSSI est chargé de consolider la vision globale des risques de sécurité numérique sur l'ensemble du périmètre ministériel.

Il est également chargé du plan de contrôle de l'application de la politique générale de sécurité numérique. Il pilote la chaîne de cyberdéfense, au moyen du centre de cyberdéfense du ministère de l'Intérieur (C2MI).

Le rôle et les missions du FSSI sont décrits dans le document intitulé « Missions des acteurs de la sécurité numérique », inclus dans le corpus de la sécurité numérique du ministère de l'Intérieur.

Article 12. Les conseillers à la sécurité du numérique

Placé auprès d'une autorité qualifiée en sécurité des systèmes d'information ou d'une autorité ayant une large délégation en matière de sécurité numérique, le conseiller à la sécurité du numérique (CSN) anime la chaîne fonctionnelle relevant du périmètre de son autorité. Il assure des fonctions de conseil, de contrôle, de pilotage des risques et des processus d'homologation.

Au sein de l'entité dans laquelle il exerce, le CSN est placé dans une position organique lui permettant d'assurer ses missions et notamment celles de conseil et de contrôle. En particulier, en dehors des entités à vocation numérique, le rôle de CSN est positionné en dehors d'un service opérationnel numérique.

Le CSN participe au comité de direction en tant que de besoin pour présenter régulièrement à l'autorité un état des lieux du niveau de sécurité numérique de l'entité ou lui faire part d'un point en particulier.

Le CSN est désigné par l'autorité hiérarchique auprès de laquelle il exerce. La désignation précise le rattachement hiérarchique de l'agent. Elle est transmise au SHFD pour validation et prise en compte.

Le CSN assiste, sur son périmètre, les autorités de la chaîne décisionnelle SN dans la désignation de leurs adjoints et des assistants locaux à la sécurité du numérique (ALSN). En particulier, il définit précisément les attributions des ALSN placés auprès de lui.

Chaque AQSSI est libre d'établir dans la politique de sécurité numérique de son entité, l'organisation de la chaîne fonctionnelle de ses CSN.

Le rôle et les missions des conseillers à la sécurité du numérique sont détaillés dans le document intitulé « Missions des acteurs de la sécurité numérique », inclus dans le corpus de la sécurité numérique du ministère de l'Intérieur.

Article 13. Les assistants locaux à la sécurité du numérique

Placé auprès d'un CSN, l'assistant local à la sécurité du numérique (ALSN) assure une mission de soutien dans l'accomplissement de leurs missions. L'ALSN est désigné par l'autorité hiérarchique du CSN auprès duquel il exerce. La désignation précise le CSN de rattachement de l'agent et est transmise au SHFD pour validation et prise en compte.

L'ALSN possède les connaissances fonctionnelles des problématiques métiers de son entité, nécessaires à l'accomplissement des missions attribuées par son CSN de rattachement.

Le rôle et les missions des assistants locaux à la sécurité du numérique sont détaillés dans le document intitulé « Missions des acteurs de la sécurité numérique », inclus dans le corpus de la sécurité numérique du ministère de l'Intérieur.

Article 14. Les délégués zonaux à la sécurité du numérique

A l'échelon territorial, le HFD s'appuie sur les services des préfets de zone. Pour ce qui relève de la sécurité numérique, ils proposent au HFD un délégué zonal à la sécurité du numérique (DZSN). Celui-ci est le délégué du FSSI pour la zone de défense et de sécurité de son périmètre.

Sous l'autorité du PDDS et au profit des services du ministère de l'intérieur, le DZSN élabore annuellement, en liaison avec les CSN concernés, un état des lieux permettant de mesurer l'adéquation des moyens déployés en zone vis-à-vis des enjeux de sécurité numérique et de gestion de crise. Le DZSN transmet ce document au PDDS de sa zone.

Le DZSN contrôle, en lien avec le CSN, le niveau de maturité de sa zone d'exercice concernant l'application des processus d'homologation. A ce titre :

- il est membre de droit des commissions d'homologation des systèmes d'information de sa zone et assiste le SHFD dans la rédaction des avis conformément à la démarche d'intégration de la sécurité des systèmes d'information dans les projets du ministère.
- il assiste le FSSI dans la réalisation de la cartographie des risques numériques de sa zone et dans la consolidation du patrimoine applicatif ministériel.
- il apporte soutien et conseil aux CSN et RSSI de sa zone dans la conduite des démarches d'homologation.

Le DZSN procède, à la demande des AQSSI ou du FSSI, à des audits sur l'application des mesures et politiques de sécurité numérique sur sa zone. Il propose annuellement au FSSI un programme d'audit annuel sur le périmètre de sa zone. La réalisation de ces audits est coordonnée par l'AQSSI de l'entité auditée, ou son représentant.

Le rôle et les missions des délégués zonaux à la sécurité du numérique sont détaillés dans le document intitulé « Missions des acteurs de la sécurité numérique », inclus dans le corpus de la sécurité numérique du ministère de l'Intérieur.

Chapitre 3 – La chaîne opérationnelle de sécurité numérique et de cyberdéfense

Article 15. Composition de la chaîne opérationnelle

La chaîne opérationnelle de sécurité numérique et de cyberdéfense est chargée de mettre en œuvre les mesures opérationnelles de sécurité, notamment en cas d'incident et de vigilance renforcée.

Elle agit en appui direct de la chaîne fonctionnelle de sécurité numérique. Elle comprend en outre les services opérationnels numériques chargés de la mise en œuvre, de l'exploitation et de l'administration des systèmes d'information et de communication.

La chaîne opérationnelle de sécurité numérique et de cyberdéfense est articulée autour du centre de cyberdéfense du ministère de l'Intérieur placé sous l'autorité du FSSI.

Article 16. Centre de cyberdéfense du ministère de l'Intérieur

En matière de défense des systèmes d'information du ministère, le centre de cyberdéfense du ministère de l'Intérieur (C2MI) a comme missions principales :

- la supervision de sécurité des infrastructures transverses, des passerelles d'interconnexion du ministère ;
- la détection des cyberattaques sur les systèmes d'information essentiels ;
- la coordination ministérielle de la réponse aux incidents de sécurité numérique ;
- la veille technologique sur les vulnérabilités et l'analyse de la menace pesant sur le ministère ;
- des activités de communication et de sensibilisation des agents du ministère et des acteurs de la chaîne fonctionnelle de sécurité numérique ;
- la diffusion des instructions ministérielles relatives à la gestion des incidents de sécurité numérique ;
- la transmission aux AQSSI ou leur représentant, des informations relatives aux événements et incidents SSI relevant de leur périmètre.

Le C2MI est le point de contact ministériel vis-à-vis de ses équivalents au sein des partenaires : CERT (Computer Emergency Response Team), SOC (Security Operational Center).

Les échanges avec les partenaires des secteurs publics et privés (gestion de crise, réponse aux incidents, offres de services, ...) font l'objet de protocoles formalisés.

Le C2MI assure notamment la liaison opérationnelle avec les équipes de l'ANSSI, protocolisée dans un document qui garantit la totale complémentarité entre les deux structures.

Article 17. Les services opérationnels numériques

Opérateurs techniques, les services opérationnels numériques sont responsables de la conception, de l'administration, de l'exploitation et de la sûreté de fonctionnement des systèmes d'information et de communication nécessaires à l'activité du ministère et à la réalisation de ses missions de service public.

Les services opérationnels numériques assurent le maintien en condition opérationnelle, le maintien en condition de sécurité et interviennent dans la résolution des incidents de sécurité numérique.

En amont, ils élaborent et déploient des architectures résilientes, formalisent et implémentent les mesures techniques permettant de répondre aux exigences réglementaires, aux objectifs de sécurité approuvés par les autorités d'homologation, aux recommandations de l'ANSSI et à la stratégie ministérielle de la sécurité numérique.

Article 18. Les responsables de la sécurité des systèmes d'information

Placé auprès du responsable d'un service opérationnel numérique, le responsable de la sécurité des systèmes d'information (RSSI) conseille et accompagne leur autorité et les CSN dans la mise en œuvre opérationnelle de la sécurité du numérique.

Le RSSI est désigné par l'autorité hiérarchique auprès de laquelle il exerce. La désignation précise le rattachement hiérarchique de l'agent. Elle est transmise au SHFD pour validation et prise en compte.

Le RSSI assiste les AQSSI, en lien avec les CSN, à l'élaboration du rapport annuel de la sécurité numérique.

Le rôle et les missions des responsables de la sécurité des systèmes d'information sont détaillés dans le document intitulé « Missions des acteurs de la sécurité numérique », inclus dans le corpus de la sécurité numérique du ministère de l'Intérieur.

Article 19. Les assistants locaux à la sécurité des systèmes d'information

Placé auprès d'un RSSI, l'assistant local à la sécurité des systèmes d'information (ALSSI) assure une mission de soutien dans l'accomplissement de leurs missions. L'ALSSI est désigné par l'autorité hiérarchique du RSSI auprès duquel il exerce. La désignation précise le RSSI de rattachement de l'agent et est transmise au SHFD pour validation et prise en compte.

L'ALSSI possède les connaissances techniques nécessaire à l'accomplissement des missions attribuées par son RSSI de rattachement.

Le rôle et les missions des assistants locaux à la sécurité des systèmes d'information sont détaillés dans le document intitulé « Missions des acteurs de la sécurité numérique », inclus dans le corpus de la sécurité numérique du ministère de l'Intérieur.

TITRE II : La gouvernance ministérielle de la sécurité numérique

Article 20. Système de gouvernance de la sécurité numérique

Le système de gouvernance ministérielle de la sécurité numérique permet d'animer les processus de décision, de pilotage et d'amélioration continue de la sécurité numérique. Il définit les règles et les priorités. Il permet la mise en œuvre cohérente et coordonnée de mesures spécifiques, fondées sur des capacités techniques et opérationnelles de prévention, de protection, de détection et de réponse aux cyberattaques :

- pour être efficaces, les mesures de prévention et de protection doivent être comprises, acceptées, effectivement déployées, maintenues dans le temps et contrôlées.
- pour être efficaces, les mesures de détection et de réponse doivent être formalisées, régulièrement testées et faire l'objet d'un processus d'amélioration continue.

Article 21. Tour de table des comités de gouvernance

Deux niveaux de gouvernance ministérielle sont définis : un niveau stratégique présidé par le HFD et un niveau de pilotage présidé par le HFDA. En outre, des comités de suivi présidés par le FSSI peuvent se réunir en tant que de besoin, afin de préparer les décisions du comité stratégique et du comité de pilotage.

Au sein de ces comités, les autorités suivantes sont représentées :

- le haut fonctionnaire de défense ;
- les autorités qualifiées en sécurité des systèmes d'information ;
- les directions du secrétariat général du ministère ;
- le chef du service des technologies et des systèmes d'informations de la sécurité intérieure ;
- les préfets délégués à la défense et à la sécurité.

Article 22. Le comité stratégique de la sécurité numérique

Le haut fonctionnaire de défense décide des orientations stratégiques de la sécurité numérique. Il préside annuellement le comité stratégique de la sécurité numérique (COSTRAT SECNUM).

Ses principales missions sont de :

- définir et arbitrer les orientations stratégiques relatives à la sécurité numérique et à la cyberdéfense du ministère de l'Intérieur ;
- présenter une synthèse des menaces pesant sur les systèmes d'information du ministère ;
- veiller à l'application de la présente instruction et à la progression du niveau de conformité du ministère à la PSSI-E. Il examine la PGSN-MI et la fait évoluer régulièrement pour l'actualiser selon les besoins ;
- exploiter le bilan des incidents significatifs, et l'état des lieux des cybermenaces susceptibles d'affecter le ministère ;
- présenter une synthèse du niveau de sécurité des SI essentiels ;
- identifier les systèmes d'information essentiels à inscrire dans le programme annuel d'audit du ministère.

Article 23. Le comité de pilotage de la sécurité numérique

Le comité de pilotage de la sécurité numérique (COFIL SECNUM) est présidé par le haut fonctionnaire de défense adjoint et se réunit au moins deux fois par an.

Les principaux objectifs du COFIL sécurité numérique sont de :

- préparer les éléments d'arbitrage du COSTRAT SECNUM ;
- actualiser l'inventaire des SIE au regard des risques stratégiques du ministère ;
- assurer le suivi des incidents de sécurité numérique et de l'état de la menace cyber pesant sur les SI du ministère ;
- arbitrer les orientations techniques en matière de sécurité numérique et de cyberdéfense du ministère ;
- arbitrer si nécessaire les dérogations aux exigences de la PSSI-E au regard des risques de sécurité numérique ;
- suivre l'état d'avancement des audits inscrits au programme annuel d'audit du ministère ;
- suivre la mise en œuvre des plans d'action découlant des audits.

Article 24. Le comité de suivi de la sécurité numérique

Le Fonctionnaire de sécurité des systèmes d'information peut réunir en tant que de besoin le comité de suivi de la sécurité numérique.

Ce comité peut se réunir notamment pour :

- transposer en interne les réglementations, guides et recommandations de l'ANSSI ;
- élaborer, diffuser et tenir à jour les doctrines d'emploi en déclinaison de la PGSN-MI ;
- élaborer et proposer à la validation du haut fonctionnaire de défense adjoint les instructions et directives de sécurité numérique à vocation ministérielle ;
- proposer au haut fonctionnaire de défense adjoint les dérogations à la PSSI-E jugées nécessaires.

Article 25. Rapports annuels de la sécurité numérique

Chaque AQSSI fournit un rapport annuel de la sécurité numérique au haut fonctionnaire de défense. Ce rapport, protégé par les mentions « Diffusion Restreinte » et « Spécial France », est transmis avant la fin du premier trimestre de l'année civile suivante.

Un modèle de rapport annuel est inclus dans le corpus de la sécurité numérique du ministère de l'Intérieur. Il comprend au moins les éléments et indicateurs suivants :

- les incidents significatifs et autres événements remarquables :
 - Indicateur 1. Nombre d'incidents de sécurité subis au cours de l'année ;
 - Indicateur 2. Délai moyen de remontée des informations au C2MI une fois l'incident déclaré ;
 - Indicateur 3. Délai moyen de déploiement d'une mise à jour (ou mesure de contournement) une fois la vulnérabilité découverte ;
 - Indicateur 4. Pourcentage des incidents de sécurité ayant fait l'objet d'un dépôt de plainte.

- les éléments de cartographie :
Indicateur 5. Date de mise à jour des éléments d'inventaire et de cartographie.
- la liste des systèmes d'information homologués :
Indicateur 6. Pourcentage de systèmes d'information de l'entité faisant l'objet d'une décision d'homologation valide.
- les différents audits de sécurité réalisés :
Indicateur 7. Nombre d'audits réalisés dans l'année ;
Indicateur 8. Nombre de systèmes d'information ayant fait l'objet d'un audit de moins de 2 ans.
- les ressources affectées à la sécurité numérique, ainsi que les formations et les actions de sensibilisation :
Indicateur 9. Pourcentage du budget annuel de l'entité alloué à la sécurité numérique ;
Indicateur 10. Pourcentage du budget annuel de l'entité dépensé dans la sécurité numérique ;
Indicateur 11. Nombre de formations réalisées dans l'année ;
Indicateur 12. Nombre d'actions de sensibilisation réalisées dans l'année ;
Indicateur 13. Nombre de personnels affectés à la sécurité numérique.

Sur la base des rapports annuels des AQSSI, le HFD produit un rapport annuel de sécurité numérique pour le périmètre ministériel et le transmet aux ministres.

TITRE III : La maîtrise du risque numérique

Article 26. Principes stratégiques de la maîtrise du risque numérique

L'évolution du risque numérique dans l'action de l'État engage la responsabilité des autorités. Cette responsabilité est accentuée par l'émergence ou l'évolution de la réglementation (Règlement général sur la protection des données, dispositif sur la sécurité des secteurs d'activités d'importance vitale, protection du secret de la défense nationale, etc.).

Devant l'accroissement du risque numérique et sa propension à gagner toutes les activités du ministère de l'Intérieur, les autorités doivent définir, sur leur périmètre de responsabilité de nouveaux seuils d'acceptabilité du risque. Ces risques ne sont pas limités au strict périmètre ministériel, mais concernent également l'écosystème numérique du ministère, formé des prestataires, fournisseurs, sous-traitants, associations partenaires, organisations syndicales, mutuelles, etc.

Cet écosystème numérique participe directement ou indirectement aux missions du ministère. La vulnérabilité de cet écosystème doit être prise en compte dans la maîtrise du risque numérique.

L'hébergement des données doit être maîtrisé. Les informations sensibles du ministère doivent être hébergées dans des centres d'hébergement maîtrisés, dont les procédures de sécurité sont connues et homologuées.

Article 27. Politique d'audit de sécurité

Chaque AQSSI doit s'assurer que le niveau des risques auquel sont exposés ses systèmes d'information, reste en permanence à un seuil acceptable. A ce titre, les audits de sécurité ont pour objectif de permettre :

- la visualisation concrète du niveau de maturité d'un SI en matière de sécurité numérique ;
- l'évaluation de l'efficacité des mécanismes de sécurité d'un SI ;
- l'évaluation de la conformité aux exigences des référentiels applicables du domaine de la sécurité numérique ;
- l'alimentation du plan d'action sécuritaire du SI et d'en suivre l'évolution dans le temps, notamment lors du renouvellement des campagnes d'audit et des homologations ;
- l'investigation sur les traces d'une attaque en vue d'en établir ses impacts réels.

Le haut fonctionnaire de défense définit, en liaison avec les AQSSI, un programme annuel d'audit du ministère. Un audit peut concerner un système d'information en particulier, un processus métier, une entité ou une emprise géographique.

Le haut fonctionnaire de défense s'appuie également sur les moyens à dispositions des préfets de zone pour permettre aux AQSSI d'effectuer des audits sur l'ensemble du territoire.

Article 28. Cartographie des SI

Les systèmes d'information sont de plus en plus complexes et interconnectés. La cartographie des SI est un outil stratégique, nécessaire à la maîtrise du système d'information.

Une cartographie maintenue à jour permet :

- de disposer d'une vision commune et partagée du système d'information ; elle facilite la capitalisation et la prise de décision, permet d'assurer le maintien en condition de sécurité et d'améliorer le niveau de maturité ;
- d'identifier les systèmes les plus essentiels et les plus exposés, d'anticiper les chemins d'attaque et de mettre en place les mesures adéquates ;
- de réagir plus efficacement en cas d'incident ou d'attaque, de qualifier les impacts et de prévoir les conséquences des actions défensives ;
- d'identifier les activités clés et de définir un plan de continuité d'activité.

Le CSN doit s'assurer que l'inventaire et la cartographie sont réalisés et maintenus à jour. Il peut s'appuyer sur les services des SIC opérationnels.

L'AQSSI s'assure que cette cartographie est mise à jour au moins annuellement et en fait état dans son rapport annuel, conformément à l'Article 25. Rapports annuels de la sécurité numérique Cette cartographie doit être tenue à disposition du FSSI.

Article 29. Cartographie des risques numériques

La cartographie est un outil de pilotage indispensable à la maîtrise des risques numériques⁵. Le FSSI doit maintenir à jour une cartographie des risques pour le ministère.

La cartographie des risques d'une entité est pilotée par le CSN de l'entité. Elle est alimentée par les éléments remontés par les responsables de projets, les SIC et les audits réalisés. Le CSN la maintient à jour et rend compte à l'AQSSI des risques persistants pour son entité au moins une fois par an et en cas de nouveaux risques jugés majeurs. Il informe systématiquement le FSSI des risques impactant les SIE.

L'AQSSI alimente le rapport annuel par les éléments de cartographie des risques fournis par les CSN.

Article 30. Intégration de la sécurité dans les projets

Dès le début des études préliminaires et jusqu'à leur décommissionnement, l'intégration de la sécurité dans les projets est placée sous la responsabilité de l'AQSSI, qui peut s'appuyer sur un chef de projet de son entité pour la mise en pratique la démarche d'intégration de la sécurité des systèmes d'information dans les projets (DISSIP) du ministère de l'Intérieur.

L'intégration de la sécurité dans un projet doit impliquer plusieurs points de vue dont en particulier :

- la maîtrise d'ouvrage du projet qui doit exprimer ses enjeux de sécurité relatifs au projet.
- le chef de projet qui peut demander au CSN auquel il est rattaché des avis et conseils pour assurer un traitement des risques adapté et cohérent.
- le CSN qui contrôle pour son périmètre que tous les projets ont intégré une réflexion sécurité pour eux même et pour l'écosystème. Le CSN doit alerter l'AQSSI s'il considère que les risques résiduels ne sont pas suffisamment traités par le projet et peuvent avoir un impact significatif sur le ministère ou son écosystème.

⁵ Se référer au guide pour la cartographie du système d'information, disponible sur le site de l'ANSSI.

Article 31. Maîtrise des prestataires, fournisseurs et partenaires

Les AQSSI s'assurent du traitement des risques que les activités des tiers (prestataires, fournisseurs ou partenaires) font peser sur le ministère.

Pour cela, ils veillent à insérer dans les contrats ou conventions de services, les clauses de sécurité permettant l'engagement des tiers à répondre aux objectifs de sécurité des projets. Pour maintenir un niveau de confiance suffisant des dispositions prises par les tiers, il est essentiel de procéder à des revues régulières de l'application de ces clauses.

Des clauses contractuelles types de sécurité sont proposées dans le corpus de la sécurité numérique.

Article 32. Homologation de sécurité

La décision d'homologation est prononcée par l'autorité d'homologation⁶ (AH), après avis de la commission d'homologation. Cette décision fait l'objet d'une attestation formelle indiquant le périmètre, la durée d'homologation, les autorisations spécifiques liées au télétravail et les éventuelles réserves. Cette attestation est transmise au haut fonctionnaire de défense. Tout au long du cycle de vie du système, le processus d'homologation permet de maintenir le risque de sécurité numérique à niveau adapté et accepté.

Pour un système d'information, l'autorité d'homologation est formellement désignée par l'AQSSI de l'entité qui assure la maîtrise d'ouvrage du système. Dans le cas d'une responsabilité partagée entre plusieurs AQSSI, c'est celle désignée comme compétente sur le domaine de la sécurité numérique qui désigne l'AH. A défaut, les AQSSI s'accordent pour désigner une autorité d'homologation commune. Les AH sont directement subordonnées aux AQSSI compétentes et sont responsables de la conduite des missions pour lesquelles le système est créé.

Le processus d'homologation est détaillé dans le corpus documentaire du ministère de l'Intérieur, dans la démarche d'intégration de la SSI dans les projets (DISSIP).

Pour tous les systèmes d'information, l'homologation de sécurité est obligatoire. Pour les nouveaux systèmes d'information, elle doit conditionner la mise en production.

Les risques pesant sur un SI doivent être périodiquement réévalués dans une démarche d'amélioration continue et d'adaptation permanente à l'évolution de la menace. A ce titre, une homologation a nécessairement une durée limitée dans le temps et un périmètre d'analyse précis, conformément à la démarche ministérielle d'intégration de la sécurité des systèmes d'information dans les projets.

Article 33. Systèmes d'information essentiels

Au sein du patrimoine applicatif du ministère de l'Intérieur, certains systèmes d'information sont désignés « système d'information essentiel » (SIE)⁷.

Un système d'information essentiel est un système pour lequel une atteinte à la disponibilité, l'intégrité ou la confidentialité aurait un impact critique⁸ pour le ministère de l'Intérieur. Ces SI sont donc assujettis à des exigences supplémentaires détaillées dans le corpus de la sécurité numérique.

⁶ Personne désignée à un niveau hiérarchique suffisant pour assumer les responsabilités liées à l'acceptation des risques résiduels identifiés sur le SI cible. Elle est généralement membre de la direction de l'entité.

⁷ La notion de système d'information essentiel est propre au ministère de l'Intérieur et est à différencier de celle issue de la directive NIS.

⁸ Se référer au document détaillant les métriques de la DISSIP, disponible sur le site <http://ssi.minint.fr>

Lors du processus d'homologation d'un SIE, le SHFD formalise sa position sur le fond du dossier d'homologation et la pertinence des éléments d'aide à la décision proposés à l'autorité d'homologation. Dans le cas où un SIE présente des vulnérabilités pouvant nuire gravement au ministère, le SHFD peut exceptionnellement prononcer un refus catégorique de sa mise en service et ainsi bloquer son homologation par l'autorité compétente.

Un système d'information essentiel est désigné par l'AQSSI concernée, en concertation avec le haut fonctionnaire de défense. La désignation engage l'AQSSI dans le respect des exigences spécifiques du corpus de la sécurité numérique. A ce titre, un système d'information désigné comme essentiel peut perdre ce statut en l'absence, dans des délais raisonnables, des garanties suffisantes sur sa maîtrise des risques.

Article 34. Systèmes d'information d'importance vitale

L'arrêté du 29 mai 2019 fixe les règles de sécurité et les modalités de déclaration des SIIV et des incidents de sécurité relatives au secteur d'activités d'importance « Activités civiles de l'État » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.

Afin de clarifier les liens entre ces les SIIV et les SIE, il convient de considérer les points suivants :

- un SIIV est nécessairement un SIE ;
- un SIIV est l'unique porteur de l'impact des incidents de fonctionnement ou de sécurité touchant des sous-systèmes mutualisés⁹. Tout sous-système mutualisé utilisé par SIIV, strictement nécessaire à son fonctionnement ou sa sécurité, est désigné comme un SIE.

⁹ À titre d'exemple, un sous-système mutualisé peut-être : Chaîne de services (pare-feu, routeur...), annuaires, passerelles SSO, plateformes d'échanges, de supervision, d'exploitation ou d'administration.

TITRE IV : La résilience des activités

Article 35. Principes stratégiques de la cyber-résilience

Le risque zéro n'existe pas en matière de sécurité numérique. Même si des mesures de prévention et de protection sont mises en œuvre pour limiter la survenue d'incidents de sécurité, une cyberattaque sophistiquée ou de forte intensité peut impacter gravement le ministère.

Chaque AQSSI doit donc s'assurer, sur son périmètre de responsabilité, de sa capacité à surmonter les très forts impacts induits par la réalisation d'un scénario de risque cyber, à en limiter les effets directs sur ses objectifs et à assurer la continuité d'activité malgré la perte de ressources critiques.

Article 36. Gestion de crise

La gestion de crise est une activité primordiale au sein du ministère de l'Intérieur. L'émergence du numérique dans les missions du ministère implique que l'organisation et les procédures internes de gestion de crise doivent être adaptées pour y incorporer la dimension numérique.

Les acteurs de la gestion de crise ne doivent plus considérer la dimension numérique comme un volet juxtaposé aux autres, mais comme un facteur transverse et naturel.

Le plan gestion de crise du ministère et ses déclinaisons opérationnelles, sont des éléments du corpus de la sécurité numérique.

L'AQSSI doit se préparer pour son entité à la gestion d'incidents de sécurité numérique. En particulier, des réponses aux scénarios de cyberattaques critiques doivent être préparées et s'appuyer sur un plan de continuité d'activité (PCA).

Article 37. Plan de continuité d'activité

Le plan de continuité d'activité (PCA) constitue un chapitre essentiel de la politique de sécurité d'une entité. Il doit pleinement intégrer le risque numérique. Il doit être revu, testé, et enrichi à intervalles réguliers pour rester efficace.

L'AQSSI définit la stratégie de PCA pour son entité et engage les moyens numériques pour sa mise en œuvre. Ils peuvent nommer des responsables des PCA qui assurent, en lien avec le CSN de leur entité, la bonne mise en œuvre des dispositions prévues dans celui-ci et veillent également à son maintien en condition opérationnelle.

Les CSN doivent s'assurer que les SIC sont en mesure d'assurer le fonctionnement des moyens numériques du PCA. Les SIC mettent en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la continuité du SI, en assurent la supervision au quotidien et la maintenance dans le temps.

Tout projet dès lors qu'il dispose d'enjeux forts de disponibilité ou d'intégrité doit être inscrit au PCA de l'entité. Les dispositions garantissant la continuité de service doivent être établies avec les maîtrises d'ouvrage concernées.

TITRE V : Dispositions opérationnelles

Les dispositions opérationnelles reposent sur les 4 objectifs suivants : prévenir, protéger, détecter et réagir aux cyberattaques.

Article 38. Enjeux de la prévention

La plupart des attaques informatiques utilisent successivement plusieurs techniques de propagation.

La prévention permet de limiter la survenue des incidents de sécurité en réduisant la probabilité qu'une erreur humaine permette au scénario de risque de se dérouler entièrement.

Le dispositif de prévention mis en œuvre par le ministère repose principalement sur :

- la sensibilisation des personnes, tant internes qu'externes, à leurs responsabilités en matière de sécurité,
- la communication régulière des bonnes pratiques à respecter au quotidien ;
- la diffusion et publication d'une charte des bons usages des moyens numériques du ministère.

Les CSN et RSSI s'assurent que l'ensemble des ALSN et des ALSSI a les compétences requises pour remplir les fonctions qui lui sont confiées ou est en mesure de les acquérir. L'ensemble des acteurs SN met en place les actions de communications appropriées (information, sensibilisation ou formation du personnel à la sécurité du SI).

Des dispositions opérationnelles relatives à la prévention sont décrites au sein du corpus de la sécurité numérique.

Article 39. Enjeux de la protection

Protéger les activités métier et les SIC passe par la mise en œuvre de mesures de protection, numériques et physiques. Cette protection repose sur la maîtrise des identités numériques, la gestion des accès et des droits aux SI, sur la capacité des infrastructures tant logique que physique à résister aux attaques, mais également sur la maîtrise des engagements juridiques, réglementaires et contractuels impactant la sécurité numérique.

La protection vise ainsi à limiter l'impact direct des attaques de sécurité et freiner leur propagation au sein du système d'information. A ce titre, plusieurs principes élémentaires permettent de répondre à cet objectif :

- principe de durcissement de la protection : Un SI doit être considéré en prenant en compte l'ensemble de son écosystème (ex : briques d'infrastructure) et non restreint aux seuls services métiers qu'il serait amené à rendre ;
- principe de frugalité numérique :
 - o tout système d'information doit limiter son exposition au strict nécessaire ;
 - o seules les données strictement nécessaires à l'accomplissement de la mission sont collectées et traitées.
- principe d'autorisation limitée : les habilitations et autorisations liées aux missions de chacun sont personnelles, incessibles et limitées dans le temps ;
- principe du besoin d'en connaître : l'accès à des ressources sensibles est limité aux utilisateurs qui en ont strictement la nécessité pour accomplir leurs missions ;

- principe du moindre privilège : une tâche ne doit bénéficier que de privilèges strictement nécessaires pour mener à bien ses fonctionnalités. En particulier, un administrateur doit toujours utiliser son compte utilisateur normal lorsqu'il n'a pas besoin d'utiliser ses privilèges d'administrateur ;
- principe de cloisonnement : des ressources étant couvertes par des besoins de sécurité différents ne doivent pas être mutualisées.

Des dispositions opérationnelles relatives à la protection sont décrites au sein du corpus de la sécurité numérique.

Article 40. Enjeux de la détection des événements suspects

La détection rapide, assurant la qualification d'un incident en vue d'une réponse adaptée, permet d'en limiter son impact. Il s'agit d'optimiser les moyens et les outils, en les orientant vers les chemins et les méthodes empruntés par les attaquants.

Le ministère s'est ainsi doté d'un centre de cyberdéfense au service des AQSSI pour assurer une surveillance des systèmes d'information contre les cyberattaques.

Dès lors qu'un projet présente de forts besoins de sécurité, il doit être intégré au dispositif de surveillance.

Des dispositions opérationnelles relatives à la détection sont décrites au sein du corpus de la sécurité numérique.

Article 41. Enjeux de la réponse aux attaques

La réponse aux attaques est coordonnée par le C2MI, en lien avec les acteurs métiers du ministère et l'ANSSI.

Une réponse adaptée aux attaques comprend non seulement la gestion technique assurée par les services opérationnels numériques, mais également la continuité des activités des équipes métiers, la relation avec les autorités et la communication avec les parties prenantes et les instances judiciaires.

Les dispositifs dont se dote le ministère pour répondre à ces enjeux reposent sur des procédures de gestion d'incident et de crise élaborées et maintenues par chaque entité, avec l'assistance du SHFD. Ces procédures abordent les aspects essentiels pour une gestion des incidents et de crise efficace :

- des priorités de cloisonnement et de reprise ;
- une stratégie de communication adaptée et partagée ;
- des exercices réguliers de crise, impliquant les autorités et entraînant les personnels.

Des dispositions opérationnelles relatives à la réponse aux attaques sont décrites au sein du corpus de la sécurité numérique.

FIN DU DOCUMENT