MINISTÈRE
DE LA JUSTICE

Liberté
Égalité
Fraternité

Politique Ministérielle de Sécurité Numérique

Version 2024-2025

Approuvée par Madame la secrétaire générale, haute fonctionnaire de défense et de sécurité NOR : JUST2417521A	

Table des modifications

Paragraphe	Nature de la modification
Annexe B-01	Le guide d'homologation est ajouté aux annexes de la PMSN dans la rubrique « **Démarche et homologation de sécurité** ».
document	Changement des appellations « chef/service du numérique » par « direction/directeur du numérique ».
3.1.1.3	Ajout du directeur du numérique dans la désignation des AQSSI.
3.1.1.4	La commission d'homologation des SI socle est organisée par le CSN de la direction du numérique et non le RCSSI.
3.1.2.1	Dans le cadre des incidents « très graves », le FSSI devient « le responsable du CSIRT » ministériel.
3.1.2.3	Les RCSSI sont les référents et les pilotes de la chaine opérationnelle de sécurité numérique et de cyberdéfense. Cette chaîne peut être de niveau : • Ministérielle (DNUM et DIT) ; • Directionnelle, uniquement pour les SI spécifiques non gérés par la DNUM (exemple GD et SI de sureté). Le paragraphe est retiré de la chaîne de pilotage et transféré dans la chaîne opérationnelle (3.1.3.1). Les informations spécifiques au RCSSI du SNUM sont supprimées. L'animation de la communauté des RSSI rattachés fonctionnellement est ajoutée aux missions des RCSSI. L'organisation des COTEC-SSI (ministériel ou directionnel) est ajoutée aux missions des RCSSI.
3.1.3.2	Le paragraphe « Le responsable du CSIRT ministériel » est supprimé de la chaîne opérationnelle. La fonction « responsable du CSIRT » et les missions afférentes au pilotage lors d'un incident « très grave » sont affectées au FSSI. Les missions de coordination, prévention, sensibilisation, suivi, veille et de traitement des injonctions ANSSI sont affectées au responsable de la « section coordination et prévention », nouvel acteur de la chaîne pilotage (cf. réorganisation du SG, création du département HFDS et du bureau de la sécurité numérique).

3.1.2.3	Ajout du responsable de la section maîtrise des risques numériques dans la chaîne de pilotage.
3.1.2.4	Ajout du responsable de la section prévention et coordination dans la chaîne de pilotage.
3.2.2	Le comité de pilotage de la sécurité numérique devient le comité de pilotage de la sécurité numérique de niveau ministériel. L'acronyme reste inchangé (COPIL-SN).
3.2.3	Un comité de pilotage de la sécurité numérique des établissements publics (COPIL-SN-EP) est créé.
4.1.1	Suppression des types de SI « systèmes et services informatifs » et « systèmes d'information de gestion courante ». Création du type de « SI non essentiel » (SINE).
Partie 5	Modifications textuelles sur l'ensemble du chapitre.

Table des matières

1. Avant-propos 5
2. Champ d'application 6
2.1. Cadre légal 6
2.2. Corpus de la sécurité numérique du ministère de la justice 6
2.3. Catégories thématiques des annexes 7
3. Organisation ministérielle de la gouvernance de la sécurité numérique 8
3.1. Chaînes, rôles et responsabilités 8
3.1.1. La chaîne décisionnelle de sécurité numérique 8
3.1.2. La chaîne fonctionnelle de sécurité numérique 10
3.1.3. La chaîne opérationnelle de sécurité numérique et de cyberdéfense 13
3.2. Les instances ministérielles 16
3.2.1. Le comité stratégique de la sécurité numérique 16
3.2.2. Le comité de pilotage de la sécurité numérique de niveau ministériel 17
3.2.3. Le comité de pilotage de la sécurité numérique des établissements publics 18
3.2.4. Le comité technique de la sécurité des systèmes d'informations 18
3.2.5. Le comité de gestion des risques numériques 19
4. Maîtrise du risque numérique 21
4.1. Typologie et criticité des systèmes d'information 21
4.1.1. Les systèmes d'information non essentiels (SINE) 21
4.1.2. Les systèmes d'information essentiels (SIE) 21
4.1.3. Les systèmes d'information d'importance vitale (SIIV) 22
4.2. Classification des informations et marquage des supports 22
4.3. Principes stratégiques de la maîtrise du risque numérique 22
4.3.1. Cartographies des risques numériques 22
4.3.2. Maîtrise des prestataires, fournisseurs et partenaires 23
4.3.3. Homologation de sécurité 23
5. La gestion des incidents de sécurité numérique 26
5.1. Définition 26
5.2. Qualification et pilotage d'un incident de sécurité numérique 26
5.3. Déclaration des incidents à la CNIL 27
6. Cas particulier des établissements publics de l'Etat 28
7. Glossaire 29
8. Références 30

1. Avant-propos

La transformation numérique, dans laquelle le ministère de la justice est pleinement impliqué, accroit notre exposition au numérique. Dans un contexte où les menaces cyber sont protéiformes et en augmentation constante, les institutions publiques sont des cibles particulièrement exposées. Les menaces s'affranchissent des frontières, profitent des interdépendances des systèmes d'information et sont susceptibles d'impacter toute une institution.

Aussi, la sécurité numérique est une condition fondamentale pour répondre aux enjeux de la transformation numérique et des missions du service public de la justice.

L'État répond à l'évolution des menaces et aux enjeux. Il déploie un dispositif d'ensemble qui se traduit notamment par une organisation de la gouvernance de la sécurité numérique, de la maîtrise du risque numérique et de la gestion des incidents de sécurité.

La présente politique ministérielle de sécurité du numérique décline pour le ministère de la justice les moyens mis en œuvre dans ce domaine.

2. Champ d'application

2.1. Cadre légal

Le présent document définit la politique ministérielle de sécurité numérique (PMSN) du ministère de la justice.

La PMSN vient décliner l'instruction générale interministérielle n°1337/SGDSN/ANSSI du 26 octobre 2022 portant sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics. Cette politique prend en compte les spécificités du ministère de la justice et son organisation.

La PMSN s'adresse à l'ensemble des services du ministère et des établissements publics placés sous sa tutelle.

La PMSN s'applique également, par voie contractuelle ou conventionnelle, aux gestions déléguées et aux services externalisés par le ministère de la justice (fournisseurs, prestataires de services, sous-traitants, etc.) ainsi qu'aux partenaires (organisations syndicales, mutuelles, associations, etc.) lorsqu'ils concourent aux missions du ministère ou qu'un accès aux informations du ministère leur a été accordé.

L'ensemble de ces acteurs proches est appelé « écosystème numérique » du ministère de la justice.

2.2. Corpus de la sécurité numérique du ministère de la justice

La PMSN est complétée par un corpus documentaire disponible en annexe. Le premier document recense l'ensemble des annexes et le plan de numérotation. Les annexes sont regroupées par catégories thématiques afin de faciliter la mise à jour du corpus, les recherches et l'appropriation par les différents acteurs. Tous les acteurs définis au paragraphe 3.1 de la PMSN peuvent proposer de nouveaux documents et des évolutions.

Pour le compte du haut fonctionnaire de défense et de sécurité (HFDS), le fonctionnaire de la sécurité des systèmes d'information (FSSI) maintient à jour la liste structurée des documents, de leurs porteurs, de leurs publications et leurs actualisations. Il assure également la communication auprès de chaque entité concernée.

Afin de maintenir le corpus de la PMSN à l'état de l'art, de mettre en œuvre la feuille de route ministérielle et de répondre aux risques conjoncturels, le comité de pilotage de la sécurité numérique (COPIL-SN) peut temporairement produire de nouvelles annexes et apporter des modifications aux documents existants.

Ces modifications ne peuvent en aucun cas porter atteinte au fonctionnement des services, modifier les modalités de gouvernance et les responsabilités des acteurs. Ces modifications doivent être approuvées par le comité stratégique de la sécurité numérique (COSTRA-SN) suivant.

2.3.Catégories thématiques des annexes

Catégorie A : Organisation et gestion des incidents cyber

Porteur : DHFDS/FSSI : Responsable du CSIRT

Catégorie B : Démarche et homologation de sécurité

Porteur : DHFDS/FSSI : Responsable de section de la maitrise des risques numériques

Catégorie C : Contrôle et audit de sécurité

Porteur : DHFDS/FSSI : Responsable de section de la maitrise des risques numériques

Catégorie D : Recrutement, formation et sensibilisation

Porteur : DHFDS/FSSI : Responsable du CSIRT

Catégorie E : Déclinaisons directionnelles ou spécifiques de la PMSN

Porteur : Tous les acteurs du COPIL-SN

Catégorie F : Directives techniques

Porteur : DNUM : Responsable Central de la Sécurité des Systèmes d'Information

3. Organisation ministérielle de la gouvernance de la sécurité numérique

3.1. Chaînes, rôles et responsabilités

3.1.1. La chaîne décisionnelle de sécurité numérique

Afin de mener à bien ses missions, le garde des sceaux, ministre de la justice, s'appuie sur une **chaîne décisionnelle** et sur des **instances de gouvernance** pour définir et contrôler la stratégie ministérielle de sécurité du numérique.

Cette stratégie a pour objectif d'accompagner le plan de transformation numérique et de renforcer la résilience du ministère face aux cyberattaques.

Les rôles et responsabilités présentés ici sont issus de l'arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics. Cette section décline ces rôles au sein du ministère de la justice.

3.1.1.1. Le garde des sceaux, ministre de la justice

Le **garde des sceaux est responsable de la sécurité numérique** des systèmes d'information et de communication du ministère et de ses établissements publics.

À ce titre, le ministre valide la politique ministérielle de sécurité numérique (PMSN), fixe les orientations stratégiques et s'assure que l'ensemble des systèmes d'information (SI) du ministère sont sous la responsabilité d'une autorité qualifiée en sécurité des systèmes d'information (AQSSI) en charge de la **maîtrise des risques numériques**.

Le ministre **préside le comité stratégique de la sécurité numérique** pendant lequel la feuille de route et les amendements de la politique ministérielle de sécurité numérique sont approuvés.

3.1.1.2. Le haut fonctionnaire de défense et de sécurité

Le **haut fonctionnaire de défense et de sécurité** (HFDS) conseille le ministre pour toutes les questions relatives à la sécurité du numérique.

À ce titre, le HFDS **propose au ministre la politique ministérielle de sécurité numérique** qu'il est chargé d'animer[1].

Le HFDS nomme un adjoint (HFDS-A) qui l'accompagne dans la réalisation de ses missions.

Le HFDS **préside le comité de pilotage de sécurité numérique**. À ce titre, le HFDS planifie et anime ce comité. Il peut décider de déléguer cette présidence au fonctionnaire de sécurité des systèmes d'information (FSSI).

[1] Article 4.2.2.1 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

3.1.1.3. Les autorités qualifiées en sécurité des systèmes d'information

L'**autorité qualifiée en sécurité des systèmes d'information** (AQSSI)[2] [3] est responsable de la sécurité des services numériques placés sous sa responsabilité et de leur homologation. Elle nomme, lorsqu'elle n'exerce pas elle-même cette fonction, des autorités d'homologation (AH) qui sont alors chargées de prononcer l'homologation après instruction du dossier d'homologation. Cette nomination ne décharge pas l'AQSSI de ses responsabilités.

L'AQSSI est en charge de :

- Garantir les ressources nécessaires pour mener à bien les projets de transformation numérique de son périmètre et **s'assurer que les risques numériques sont connus et maîtrisés** ;
- Réaliser et tenir à disposition du haut fonctionnaire de défense et de sécurité la **cartographie des risques numériques et des partenaires essentiels** à son activité ;
- **Contribuer à l'élaboration du rapport annuel de sécurité numérique** qui intègre l'évaluation du niveau de risque de chaque direction et la synthèse des incidents de sécurité numérique pour le ministère. Ce rapport est présenté en comité stratégique de la sécurité numérique ;
- **Participer à la résilience du ministère par l'élaboration et la mise en œuvre des plans de continuité d'activité** pour faire face à des incidents de sécurité numérique ;
- S'assurer, au travers d'exercices de la connaissance, de la **maîtrise des plans de reprise et de continuité d'activité, et de leur mise à jour**.

En cas d'incident numérique « très grave » pour le fonctionnement du ministère, les AQSSI sont intégrées à la cellule de crise ministérielle.

Sont désignés « autorités qualifiées en sécurité des systèmes d'information »[4] :

- Les directeurs des administrations centrales ;
- Le directeur du numérique ;
- Les chefs de service à compétence nationale rattachés directement au ministre ou à caractère interministériel ;
- Les directeurs des établissements publics de l'État.

L'AQSSI préside le comité de gestion des risques numériques de sa structure.

[2] Article 4.2 du décret n° 2019-1088 du 25 octobre 2019

[3] Article 4.2.3 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

[4] Articles 1 et 2 de l'arrêté du 13 juin 2024 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de la justice

3.1.1.4. Le directeur du numérique (DNUM)

Le **directeur du numérique** (DNUM)[5] définit la stratégie d'hébergement des services numériques et il s'assure de la prise en compte dans son service de la politique ministérielle de sécurité du numérique.

Le directeur du numérique assure la **mise en œuvre et l'exploitation de services numériques et d'infrastructures du ministère**. A ce titre, pour les systèmes d'information dont il a la charge, il veille :

- A l'élaboration et au maintien à jour d'une cartographie des systèmes d'information sous sa responsabilité ;
- Au maintien en condition opérationnelle et de sécurité des systèmes d'information ;
- A la résilience numérique des services dont il a la charge ;
- A l'élaboration et la mise en œuvre des plans de continuité et de reprise informatique ;
- A la fourniture de moyens permettant de prévenir et de répondre aux incidents d'origine cyber.

Le directeur du numérique est **autorité qualifiée en sécurité des systèmes d'information (AQSSI) du socle technique**.

Ce socle est composé des briques d'infrastructure et des services mutualisés. A ce titre, il procède à l'homologation de sécurité de ces systèmes d'information.

Le fonctionnaire de sécurité des systèmes d'information (FSSI) et les conseillers à la sécurité du numérique (CSN) des directions utilisatrices de ces services mutualisés sont membres de droit de la commission d'homologation organisé par le conseiller à la sécurité du numérique de la direction du numérique.

3.1.2. La chaîne fonctionnelle de sécurité numérique

Afin de mener à bien ses missions, le ministère s'appuie sur une **chaîne fonctionnelle dédiée** et sur des **instances de pilotage** qui permettent de concilier les instances décisionnelles et les instances opérationnelles. Cette chaîne a la charge du **pilotage et du contrôle de la mise en œuvre opérationnelle** de la stratégie de sécurité numérique.

Les rôles et responsabilités présentés ici sont issus de l'arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics. Cette section décline ces rôles dans le cadre du ministère de la justice.

[5] Article 4.2.5 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

3.1.2.1. Le fonctionnaire de sécurité des systèmes d'information

Le **fonctionnaire de sécurité des systèmes d'information** (FSSI)[6] [7] pilote la mise en œuvre de la politique ministérielle permettant de maîtriser les risques de sécurité du numérique, de participer à la continuité des activités et la résilience du ministère. Il est consulté sur la bonne prise en compte de la sécurité du numérique dans les politiques publiques du ministère, la stratégie ministérielle du numérique et leurs déclinaisons au sein des directions.

Le FSSI réalise plusieurs missions :

- **Conseiller et accompagner** l'ensemble des acteurs du ministère ainsi que les établissements publics sur les questions relatives à la sécurité du numérique ;
- **S'assurer de la cohérence globale des mesures** en matière de sécurité numérique et de la prise en compte, au sein du ministère et des établissements publics, du respect des règles et des orientations politiques en matière de sécurité numérique ;
- **Contrôler** l'application des exigences de sécurité définies dans le présent document et ses annexes à l'aide d'audits, de contrôles et de bilans ;
- **Produire un avis formel sur les dossiers de sécurité** des systèmes d'information d'importance vitale (SIIV) et des systèmes d'information essentiels (SIE) dans le cadre de ses missions de conseil auprès des autorités qualifiées en sécurité des systèmes d'information.

Le **FSSI pilote la réponse aux incidents « très graves ».** À ce titre, il devient « le responsable du CSIRT » ministériel. Il informe l'Agence nationale de sécurité des systèmes d'information (ANSSI) des incidents de niveaux « **grave** » et « **très grave** » sur les systèmes d'information et de communication du ministère et des organismes placés sous sa tutelle.

Le FSSI est nommé par arrêté ministériel.

Le FSSI assure le secrétariat du comité de pilotage de la sécurité numérique. Par délégation du haut fonctionnaire de défense et de sécurité, il en assure également la présidence.

3.1.2.2. Les conseillers à la sécurité du numérique (CSN)

Le **conseiller à la sécurité du numérique** (CSN)[8] conseille et accompagne l'autorité qualifiée en sécurité des systèmes d'information dans l'exercice de ses responsabilités **pour la gestion des risques numériques**, les démarches d'homologation, l'évaluation fonctionnelle des incidents numériques, **l'anticipation et le traitement des crises d'origine cyber.**

Le CSN réalise plusieurs missions :

- **Piloter la mise en œuvre des enjeux de sécurité** métier dans le cadre de la feuille de route ministérielle ;
- **Conseiller l'autorité qualifiée ou l'autorité d'homologation** pour l'homologation des systèmes d'information ;

[6] Article 4-1 du décret n° 2019-1088 du 25 octobre 2019

[7] Article 4.2.2.2 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

[8] Article 4.2.4 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

- **Suivre les plans d'action** décidés en commission d'homologation ;
- Présenter le **niveau de sécurité** et les **risques liés à la sécurité numérique** des systèmes d'information de son entité ;
- **Informer** l'autorité qualifiée en sécurité des systèmes d'information lors du comité opérationnel de gestion des risques ;
- Participer à la gestion des incidents de niveaux « **grave** » et « **très grave** » pour **évaluer** les impacts métiers et **informer** sa chaîne décisionnelle.

Sans être un expert technique du domaine, il dispose d'une culture de la sécurité du numérique qui lui permet de traduire les enjeux en exigences de sécurité pour le compte de l'autorité qualifiée en sécurité des systèmes d'information.

Le CSN est nommé par note de service de l'autorité qualifiée en sécurité des systèmes d'information et adressée au haut fonctionnaire de défense et de sécurité.

Le CSN assure le secrétariat du comité de gestion des risques numériques de l'entité.

3.1.2.3. Le responsable de la section maitrise des risques numériques

Le responsable de la section maitrise des risques numériques assiste le fonctionnaire de sécurité des systèmes d'information (FSSI) dans le suivi des démarches de sécurité de système d'information du ministère.

Il est chargé d'accompagner les conseillers à la sécurité du numérique des directions métiers et les chefs d'établissements publics sous tutelle, au développement de la maîtrise du risque numérique.

A ce titre, il réalise plusieurs missions :

- Identifier, cartographier, évaluer et hiérarchiser les risques numériques du ministère ;
- Evaluer les dossiers de sécurité des systèmes d'information d'importance vitale (SIIV) et systèmes d'information essentiels (SIE) ;
- Proposer l'« avis formel » du FSSI ;
- Maintenir le guide d'homologation, annexe de la PMSN ;
- Former les maîtrises d'ouvrage et d'œuvre à la démarche de sécurité dans les projets ;
- Créer le référentiel d'audit et procéder à des contrôles ;
- Assurer la suppléance du FSSI pour les affaires courantes dans son domaine de compétences (gestion des risques numériques et démarche de sécurité).

Affecté au sein du bureau du FSSI, le responsable de la section maitrise des risques numériques est placé sous l'autorité hiérarchique directe du FSSI.

3.1.2.4. Le responsable de la section coordination et prévention

Dans le cadre de la stratégie CSIRT (*Computer Security Incident Response Team*) mise en œuvre par le ministère de la justice, les missions relevant du pilotage, de la coordination et de la prévention sont affectées à la section de coordination et prévention. Les missions techniques et d'expertises sont affectées au responsable du SOC (*Security operations center*) ministériel.

Lors d'un incident « grave » et « très grave », ces deux composantes constituent le CSIRT ministériel dont le fonctionnaire de sécurité des systèmes d'information (FSSI) est le responsable pour garantir une réponse efficace.

Le responsable de la section coordination et prévention réalise plusieurs missions :

- Animer la chaîne de réponse à incident avec le responsable du SOC ministériel ;
- Informer les membres du comité de pilotage en cas d'incident et en particulier le délégué à la protection des données ;
- Piloter les incidents de niveau « **grave** » si aucune cellule de crise n'est armée ;
- Assurer la montée et le maintien en compétence des acteurs en charge de la réponse à incident ;
- Organiser des exercices cyber pour tester les procédures de gestion des incidents ;
- Sensibiliser les acteurs du ministère à la sécurité numérique ;
- Suivre et proposer la réponse aux injonctions de l'ANSSI ;
- Organiser la veille stratégique ;
- Assurer la suppléance du FSSI pour les affaires courantes dans son domaine de compétences (gestion des incidents de sécurité numérique).

Affecté au sein du bureau du FSSI, le responsable de la section coordination et prévention est placé sous l'autorité hiérarchique directe du FSSI.

3.1.3. La chaîne opérationnelle de sécurité numérique et de cyberdéfense

Pour mener à bien ses missions, le ministère s'appuie sur une **chaîne opérationnelle dédiée** et sur des **instances de suivi** qui permettent de décliner de manière concrète et pragmatique la stratégie ministérielle de sécurité numérique en recherchant l'efficience.

En cas de difficulté, elle informe la chaîne fonctionnelle avant toute mise en œuvre ou modification des actions validées en comité technique de la sécurité des systèmes d'information (COTEC-SSI), comité de pilotage de la sécurité numérique de niveau ministériel (COPIL-SN) ou cellule de crise ministérielle.

3.1.3.1. Les responsables centraux de la sécurité des systèmes d'information (RCSSI)

Les **responsables centraux de la sécurité des systèmes d'information** (RCSSI) sont les responsables de la sécurité des systèmes d'information (RSSI) du **service numérique ministériel et des directions d'administration centrale**.

Les RCSSI réalisent plusieurs missions :

- **Garantir la mise en œuvre des moyens et des procédures techniques** en termes de sécurité numérique qui visent à répondre :
  - au plan de transformation numérique ministériel ;
  - à la feuille de route ministérielle en matière de sécurité numérique ;
  - aux enjeux de sécurité métier issus des analyses de risque.
- **Animer la communauté des responsables de la sécurité des systèmes d'information rattachés fonctionnellement**, qu'ils soient affectés au sein de la direction centrale, en services déconcentrés ou dans des services à compétence nationale ;
- Piloter les incidents de niveaux « faible » à « modéré » dans le cadre d'un processus standard, maîtrisé et partagé, et informer le responsable du CSIRT qui décide de partager les informations techniques afin d'anticiper les risques de propagation ou de latéralisation ;
- Assurer le secrétariat des comités techniques de sécurité des systèmes d'information (COTEC-SSI) pour les chaînes numériques ministérielle et directionnelle ;
- Piloter et contrôler la réalisation des actions décidées en COTEC-SSI.

Les RCSSI sont nommés par note de service des autorités qualifiées en sécurité des systèmes d'information, adressée au haut fonctionnaire de défense et de sécurité.

3.1.3.2. Le responsable SOC ministériel

Le **responsable du SOC ministériel** est responsable de la gestion technique des incidents de sécurité numérique.

Le responsable du SOC ministériel réalise plusieurs missions :

- Détecter, analyser et qualifier les évènements de sécurité numérique ;
- Effectuer et organiser la veille sur vulnérabilités auprès des éditeurs de logiciel ;
- **Assurer la gestion des incidents** des évènements de sécurité ayant un impact de niveaux **« faible »** à **« modéré »** ;
- **Appuyer le CSIRT** dans le cas d'un **incident « grave »** ou **« très grave »** survenant dans l'écosystème numérique du ministère.

Le responsable du SOC ministériel est nommé par note de service du directeur du numérique.

3.1.3.3. Les responsables de la sécurité des systèmes d'information (RSSI)

Les **responsables de la sécurité des systèmes d'information (RSSI)** sont des **experts techniques** qui peuvent être affectés auprès :

- D'un conseiller à la sécurité du numérique pour l'appuyer dans les domaines techniques propres à sa direction métier ;
- D'un service à compétence nationale afin de traiter les spécificités de l'entité. Dans ce cadre, il rend compte au conseiller à la sécurité du numérique de la

direction de rattachement de l'avancement des travaux de la feuille de route ministérielle, et transmet les indicateurs de pilotage ;

- D'une direction de programme afin de traiter les spécificités du projet. Dans ce cadre, il rend compte au conseiller à la sécurité du numérique de la direction de rattachement de l'avancement des travaux de la feuille de route ministérielle, et transmet les indicateurs de pilotage ;
- D'une structure numérique afin de maintenir, superviser, contrôler les systèmes locaux, piloter les actions validées en comité technique de sécurité des systèmes d'information (COTEC-SSI), opérer les actions d'endiguement et de remédiation en cas d'incident cyber.

Dans le cadre de la gestion des incidents, il réalise ou s'assure de l'exécution des prescriptions techniques du responsable du SOC ministériel. Il participe à la récupération et à l'analyse des traces, et informe les autorités de sa structure et son conseiller à la sécurité du numérique de rattachement.

Les RSSI sont nommés par note de service du responsable de l'entité, adressée au haut fonctionnaire de défense et de sécurité.

3.2. Les instances ministérielles

Pour mener à bien ses missions, le ministère s'appuie sur une comitologie à trois niveaux : **stratégique** pour la gouvernance, **pilotage** pour le suivi et **technique** pour la mise en œuvre opérationnelle. Chacune de ces instances est composée comme suit :

- Un président, dont le rôle est de convoquer et d'animer le comité, et de valider le compte rendu proposé par le secrétaire ;
- Un secrétaire, dont le rôle est de formaliser le compte rendu du comité et de transmettre au président pour approbation avant diffusion à l'ensemble des parties prenantes ;
- Un ensemble d'acteurs, en fonction du comité ou de l'ordre du jour associé.

3.2.1. Le comité stratégique de la sécurité numérique

Le **comité stratégique de la sécurité numérique (COSTRA-SN)** valide les orientations stratégiques du ministère de la justice en matière de sécurité numérique. Il prend en compte les orientations du comité stratégique interministériel de la sécurité numérique (COSINUS). Les membres du COSTRA-SN valident la feuille de route ministérielle pour répondre aux enjeux du ministère et aux décisions des réunions interministérielles cybersécurité (RIM cyber et COSINUS)[9].

Le comité stratégique de la sécurité numérique réalise plusieurs missions :

- Valider, amender et suivre l'avancement de la feuille de route ministérielle de sécurité numérique ;
- Valider la politique ministérielle de sécurité numérique et ses annexes en s'appuyant sur les comptes rendus des comités de pilotage de la sécurité numérique ;
- Valider la synthèse annuelle des incidents de sécurité qui sera transmise à l'ANSSI.

Le comité stratégique de la sécurité numérique est composé comme suit :

- Le ministre, en tant que président ;
- Le haut fonctionnaire de défense et de sécurité (HFDS) ;
- Le haut fonctionnaire de défense et de sécurité adjoint (HFDS-A) en tant que secrétaire ;
- L'ensemble des autorités qualifiées en sécurité des systèmes d'information du ministère (AQSSI) ;
- Le fonctionnaire de sécurité des systèmes d'information (FSSI) ;
- Toute personne ou expert nécessaire en fonction de l'ordre du jour.

Le comité stratégique de la sécurité numérique se réunit au moins une fois par an sur convocation de son président.

[9] Articles 3.3.1 et 3.3.2 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

3.2.2. Le comité de pilotage de la sécurité numérique de niveau ministériel

Le **comité de pilotage de la sécurité numérique de niveau ministériel (COPIL-SN)** a pour objectif de piloter les activités relatives à la sécurité numérique et d'assurer le suivi de la feuille de route validée au cours du comité stratégique de la sécurité numérique**.** Il intègre les éléments du comité interministériel de pilotage de la sécurité numérique (CINUS)[10].

Le comité de pilotage sécurité du numérique réalise plusieurs missions :

- Piloter la feuille de route ministérielle de sécurité numérique ;
- Valider, amender jusqu'au prochain comité stratégique (COSTRAT), les annexes à la PMSN permettant la mise en œuvre de la feuille de route ;
- Prendre les décisions nécessaires au traitement des risques numériques sans remettre en cause le fonctionnement des activités essentielles et vitales du ministère ;
- Décider des actions de contrôle en cas de constatation de dysfonctionnement, de non-respect de la PMSN ou de la feuille de route ;
- Elaborer la synthèse des incidents de sécurité collectés auprès du comité technique de sécurité des systèmes d'information (COTEC-SSI) ;
- Préparer et proposer la feuille de route ministérielle ;
- Alerter et sensibiliser la chaîne décisionnelle en cas de changement de l'état de la menace et de risques conjoncturels ;
- Fixer les objectifs et priorités du COTEC-SSI.

Le comité de pilotage sécurité du numérique est composé comme suit :

- Le haut fonctionnaire de défense et de sécurité ou son adjoint en tant que président, représentés par le fonctionnaire de sécurité des systèmes d'information ;
- Le fonctionnaire de sécurité des systèmes d'information en tant que secrétaire ;
- Les conseillers à la sécurité du numérique ou représentants ;
- Le délégué à la protection des données ;
- Les responsables centraux à la sécurité des systèmes d'informations sur validation du conseiller à la sécurité du numérique de direction ;
- Toute personne ou expert nécessaire en fonction de l'ordre du jour.

Le comité de pilotage sécurité numérique se réunit au minimum une fois tous les deux mois sur convocation de son président ou son représentant.

Les COPIL-SN font l'objet d'un compte rendu formel adressé à la chaîne décisionnelle.

[10] Article 3.3.3 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

3.2.3. Le comité de pilotage de la sécurité numérique des établissements publics

Le **comité de pilotage de la sécurité numérique des établissement publics (COPIL-SN-EP)** a pour objectif d'accompagner et d'assurer un suivi des activités relatives à la sécurité numérique des établissements publics.

Le COPIL-SN-EP réalise plusieurs missions :

- Etablir et suivre une **feuille de route de sécurité numérique réaliste** pour les établissements publics ;
- Suivre les démarches d'homologation des systèmes d'information des établissements publics ;
- Informer le COPIL-SN ministériel des travaux au sein des établissements publics.

Le comité de pilotage sécurité du numérique des EP est composé comme suit :

- Le haut fonctionnaire de défense et de sécurité ou son adjoint en tant que président, représentés par le fonctionnaire de sécurité des systèmes d'information ;
- Le fonctionnaire de sécurité des systèmes d'information en tant que secrétaire ;
- Les conseillers à la sécurité numérique des directions de tutelle ou représentants ;
- Les responsables de sécurité des systèmes d'informations des établissements publics ;
- Toute personne ou expert nécessaire en fonction de l'ordre du jour.

Le comité de pilotage sécurité numérique des établissements publics se réunit au minimum une fois par semestre.

Les COPIL-SN-EP font l'objet d'un compte rendu formel adressé au haut fonctionnaire de défense et de sécurité, aux directeurs des administrations centrales de tutelle et aux responsables des fonctions de direction générale des établissements publics.

3.2.4. Le comité technique de la sécurité des systèmes d'informations

L**e comité technique de la sécurité des systèmes d'information (COTEC-SSI)** veille à la mise en œuvre des activités et chantiers relatifs à la sécurité numérique, à la continuité d'activité et à la protection des données personnelles.

Il peut être :

- Ministériel dans le cadre des services numériques mis en œuvre par la direction du numérique ;
- Directionnel dans le cadre des spécificités numériques propres à une direction et non mis en œuvre par la direction du numérique (gestion déléguée, systèmes d'information de sureté ou industriel, etc.).

Le comité technique de la sécurité des systèmes d'information réalise plusieurs missions :

- Fixer les règles de sécurité et identifier les mesures techniques à mettre en œuvre pour les atteindre ;
- Piloter les plans d'actions ;
- Suivre les chantiers validés par le comité de pilotage de la sécurité numérique.

Le comité technique de la sécurité des systèmes d'information est composé comme suit :

- Pour le COTEC-SSI **ministériel** :
  - Le fonctionnaire de sécurité des systèmes d'information en tant que président ;
  - Le responsable central de la sécurité des systèmes d'information de la direction du numérique, en tant qu'organisateur et secrétaire ;
  - Toute personne ou expert nécessaire en fonction de l'ordre du jour.
- Pour les COTEC-SSI **directionnel :**
  - Le conseiller à la sécurité numérique en tant que président ;
  - Le responsable central de la sécurité des systèmes d'information en tant qu'organisateur et secrétaire ;
  - Toute personne ou expert nécessaire en fonction de l'ordre du jour.

Le comité technique de la sécurité des systèmes d'information se réunit au minimum une fois par trimestre sur convocation du secrétaire.

3.2.5. Le comité de gestion des risques numériques

Chaque entité placée sous la responsabilité d'une autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) organise un **comité de gestion des risques numériques** (**COGER**). Ce comité pilote la mise en œuvre des chantiers de sécurisation des systèmes d'information de l'entité qui concourent à ses missions.

Le comité de gestion des risques numériques réalise plusieurs missions :

- Fournir à l'AQSSI une vision consolidée des risques numériques ;
- Rendre compte de l'avancement des démarches de sécurité des systèmes d'information ;
- Vérifier la bonne exécution des plans d'action sur lesquels l'AQSSI s'est engagée ;
- Solliciter l'AQSSI en cas de difficultés dans l'exécution des plans d'action et des démarches d'homologation.

Le comité de gestion des risques est composé comme suit :

- L'autorité qualifiée pour la sécurité des systèmes d'information en tant que président ;
- Le conseiller à la sécurité du numérique en tant que secrétaire ;
- L'ensemble des autorités d'homologation désignées ;
- Les directions projets ;

- Toute personne ou expert jugée nécessaire au bon déroulement de l'ordre du jour.

Le comité de gestion des risques numériques se réunit au minimum deux fois par an sur convocation de son président ou du conseiller à la sécurité du numérique par délégation.

4. Maîtrise du risque numérique

4.1. Typologie et criticité des systèmes d'information

La maitrise des risques numériques doit être adaptée aux enjeux de sécurité d'un système, notamment en fonction de sa criticité et de la nature des informations qu'il traite.

Afin de faciliter l'appréciation de la criticité et de la nature des informations traitées, le ministère de la justice met en œuvre les typologies définies plus bas.

Les systèmes d'information du ministère de la justice sont repartis en trois catégories, de la criticité la plus faible à la plus forte. Une note d'orientation, disponible dans le corpus de la sécurité numérique, permet d'apprécier la criticité des systèmes.

La prochaine version du guide précisera les spécificités d'homologation des systèmes d'information de types industriel, bâtimentaire et de sûreté.

4.1.1. Les systèmes d'information non essentiels (SINE)

Les systèmes d'information non essentiels (SINE) sont définis dans les cas suivants :

- Ils ne concourent pas directement au fonctionnement ou à l'accomplissement de ses missions par le ministère. Une atteinte portée à ces systèmes et services aurait un impact faible sur le fonctionnement et sur l'accomplissement de ses missions par le ministère. Ils ne génèrent pas d'échanges de flux de données entrant ou sortant avec le ministère. Les besoins de sécurité de ces systèmes et services sont faibles.

  Exemples : systèmes et services informatifs uniquement destinés à informer et à communiquer avec le public, qu'il soit interne ou externe au ministère.

- Ils concourent de manière accessoire au fonctionnement et à l'accomplissement de ses missions par le ministère. Une atteinte portée à un tel système d'information aurait un impact modéré sur le fonctionnement et sur l'accomplissement de ses missions par le ministère. Les besoins de sécurité de ces systèmes sont modérés.

  Exemples : systèmes d'information bureautiques et systèmes d'information (industriels ou pas) de gestion courante des services.

4.1.2. Les systèmes d'information essentiels (SIE)

Les systèmes d'information essentiels (SIE) sont identifiés par le ministère comme étant essentiels à son fonctionnement et à l'accomplissement de ses missions. Certains systèmes d'information industriels peuvent être considérés comme essentiels. Une atteinte portée à un tel système aurait un impact grave sur le fonctionnement et sur l'accomplissement de ses missions par le ministère. Les besoins de sécurité de ces systèmes sont importants.

Afin de répondre à ces besoins de sécurité importants, ces systèmes doivent être conformes aux exigences de sécurité de la transposition en droit national de la directive NIS v2[11].

De plus, tout sous-système mutualisé utilisé par un système d'information d'importance vitale (SIIV), strictement nécessaire à son fonctionnement ou à sa sécurité, est identifié comme un système d'information essentiel.

[11] 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.

4.1.3. Les systèmes d'information d'importance vitale (SIIV)

Les systèmes d'information d'importance vitale (SIIV) sont indispensables au fonctionnement et à l'accomplissement de ses missions par le ministère.

Une atteinte au fonctionnement ou la sécurité de ces systèmes aurait un impact très grave sur le fonctionnement et sur l'accomplissement de ses missions par le ministère et *« risquerait de diminuer d'une façon importante […] la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population »*[12].

Les besoins de sécurité des systèmes d'information d'importance vitale sont très importants.

Ces systèmes sont soumis aux dispositions du code de la défense, créées et modifiées par les lois de programmation militaire[13] et doivent, à ce titre, faire l'objet de mesures de sécurité spécifiques.

Ces systèmes doivent correspondre à l'un des types prévus à l'annexe 3[14] de l'arrêté sectoriel « Activités judiciaires »[15] et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.

La liste de ces systèmes est communiquée annuellement à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et est protégée par le secret de la défense nationale.

4.2. Classification des informations et marquage des supports

[La catégorisation des informations au sein du ministère de la justice sera précisée dans la prochaine version de cette politique de sécurité numérique.]

4.3. Principes stratégiques de la maîtrise du risque numérique

4.3.1. Cartographies des risques numériques

La cartographie est un outil de pilotage indispensable à la maîtrise des risques numériques[16].

Le haut fonctionnaire de défense et de sécurité doit disposer d'une cartographie actualisée des risques numériques pesant sur le ministère.

A cette fin, chaque entité relavant d'une autorité qualifiée en sécurité des systèmes d'information doit maintenir à jour un **inventaire des risques numériques et des partenaires essentiels** à son activité. L'autorité qualifiée en sécurité des systèmes d'information est responsable de l'élaboration et du maintien à jour de la cartographie des risques numériques pesant sur son périmètre[17].

---

[12] Conformément aux dispositions de l'article L1332-6-1 du Code de la défense.

[13] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale et LOI n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025.

[14] Annexe non publique en diffusion restreinte.

[15] Arrêté du 23 décembre 2021 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Activités judiciaires ».

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

[17] Article 4.2.3 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

L'élaboration et le maintien à jour de la cartographie des risques numériques d'une entité est pilotée par le conseiller à la sécurité numérique de l'entité.

La cartographie des risques numériques de chaque entité est alimentée par les éléments remontés par les responsables de projets, les systèmes d'information et de communication (SIC), et les audits réalisés.

Le conseiller à la sécurité numérique rend compte à l'autorité qualifiée en sécurité des systèmes d'information des risques importants pesant sur son entité au moins une fois par an et en cas de nouveaux risques jugés majeurs. Il informe systématiquement le fonctionnaire de sécurité des systèmes d'information des risques critiques impactant les systèmes d'information essentiels et les systèmes d'information d'importance vitale.

La cartographie des risques numériques de chaque entité alimente le rapport annuel sur la sécurité numérique du ministère.

4.3.2. Maîtrise des prestataires, fournisseurs et partenaires

Les autorités qualifiées en sécurité des systèmes d'information s'assurent du traitement des risques que les activités des tiers (prestataires, fournisseurs ou partenaires) font peser sur le ministère. Lorsque les prestations intellectuelles ou techniques relèvent de différents services ou directions, une matrice validée par le donneur d'ordre doit être établie dans le but de définir les rôles et responsabilités des différentes parties prenantes.

Pour cela, les AQSSI veillent à insérer ou à faire insérer dans les contrats ou les conventions de service, des clauses de sécurité permettant l'engagement des tiers à répondre aux exigences de sécurité numérique du ministère. Ces exigences de sécurité se matérialisent par l'intégration d'un plan d'assurance sécurité (PAS) au dispositif contractuel et doivent garantir la bonne exécution des prestations pendant la durée du marché.

Ces clauses doivent notamment prévoir la faculté pour l'autorité qualifiée en sécurité des systèmes d'information, ou toute personne désignée par elle, de contrôler régulièrement le respect de ces exigences de sécurité.

Afin d'aider les entités du ministère à construire leurs exigences contractuelles, un modèle de PAS est proposé dans le corpus de la sécurité numérique.

4.3.3. Homologation de sécurité

Les infrastructures et services logiciels informatiques qui composent le système d'information et de communication de l'Etat, doivent faire l'objet de l'homologation de sécurité[18].

Une homologation de sécurité est **obligatoire** pour tous les systèmes d'information et est un prérequis indispensable à leur mise en service. L'homologation recouvre deux aspects :

- d'une part, une **démarche** de maitrise des risques numériques ;
- d'autre part, la **décision** formelle prise par l'autorité d'homologation à l'issue de la mise en œuvre de la démarche d'homologation de sécurité.

[18] Article 3 du décret n° 2022-513 du 8 avril 2022

4.3.3.1. Démarche d'homologation

La **démarche** d'homologation est la démarche de maitrise des risques numériques, destinée à identifier, évaluer et traiter les risques liés à l'exploitation d'un système d'information.

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

La démarche d'homologation doit être initiée dès la phase de lancement du projet, et menée tout au long de son développement. Elle doit permettre le pilotage des risques numériques liés au système d'information dès sa mise en production et jusqu'au retrait de son service ou son décommissionnement.

Dès le lancement du projet, la démarche d'homologation doit permettre de définir le périmètre, le cadre réglementaire applicable, les acteurs du projet ainsi que ses besoins de sécurité et la typologie du système d'information concerné par l'homologation.

Tout au long du projet, la démarche d'homologation doit permettre de constituer un dossier de sécurité regroupant tous les documents qui permettront d'identifier, d'évaluer et de traiter les risques pesant sur le système d'information, ainsi que les mesures prises pour traiter ces risques, et tout autre document attestant de la bonne prise en compte des exigences de sécurité dans le développement du projet. Ce dossier doit notamment comporter une analyse de risques, les besoins de sécurité du système d'information, les rapports d'audits réalisés, les risques résiduels et le plan d'action qui en résulte.

Durant tout le cycle de vie du système et jusqu'au retrait de son service, la démarche doit permettre de s'assurer du bon pilotage du plan d'action et du déploiement des mesures de traitement des risques. Ce pilotage est effectué par un comité de gestion des risques directionnel, piloté par le conseiller à la sécurité du numérique et présenté à minima annuellement à l'autorité qualifiée en sécurité des systèmes d'information de l'entité.

Un guide de l'homologation, disponible dans le corpus de la sécurité numérique détaille la manière dont doit être menée une démarche d'homologation.

4.3.3.2. Décision d'homologation

L'homologation est également la **décision formelle**[19] par laquelle l'autorité d'homologation (AH) « *atteste que les risques pesant sur le système d'information ont été identifiés, que les mesures nécessaires pour le protéger sont mises en œuvre et que les risques résiduels ont été identifiés et acceptés* »[20].

L'autorité qualifiée pour la sécurité des systèmes d'information, ou toute autorité d'homologation qu'elle désigne, prononce la décision d'homologation après avis de la commission d'homologation et du fonctionnaire de sécurité des systèmes d'information pour les systèmes d'information essentiels (SIE) et les systèmes d'information d'importance vitale (SIIV).

Cette décision fait l'objet d'une attestation formelle indiquant notamment le périmètre et la durée de l'homologation, les autorisations spécifiques liées au télétravail ou au nomadisme, ainsi que les éventuelles réserves. Cette décision est transmise au haut fonctionnaire de défense et de sécurité.

---

[19] Article 4-3 du décret n° 2019-1088 du 25 octobre 2019

[20] Arrêté sectoriel AJ, Annexe 1 ; 2. Règle relative à l'homologation.

Dans le cas d'une responsabilité partagée entre plusieurs autorités qualifiées pour la sécurité des systèmes d'information, ces dernières s'accordent pour désigner une autorité d'homologation commune qui peut être l'une des autorités qualifiées pour la sécurité des systèmes d'information.

5. La gestion des incidents de sécurité numérique

5.1. Définition

Un **incident de sécurité numérique** est un événement qualifié qui perturbe ou altère le fonctionnement d'un système d'information ou d'une application et dont la gravité peut porter atteinte aux missions du ministère et au bon fonctionnement de la justice. Le niveau de qualification de l'incident varie de « faible » à « très grave », et peut nécessiter l'activation d'une cellule de crise.

La gestion des incidents a pour but de qualifier et de traiter les incidents, ainsi que de juguler leurs effets afin de rétablir le service le plus rapidement possible et de manière sécurisée.

Les enseignements tirés de la gestion d'un incident doivent assurer qu'il ne se reproduise pas.

5.2. Qualification et pilotage d'un incident de sécurité numérique

La qualification des incidents de sécurité numérique qui affectent le ministère de la justice est réalisée par le SOC et confirmée ou modifiée par la section coordination et prévention (SCP). Quatre niveaux de qualification sont retenus en prenant en compte l'impact technique, l'impact sur les activités, l'impact médiatique et l'impact sur les agents :

- **Faible (incident de niveau 1)** : les services sont légèrement perturbés (incident perceptible, localisé), mais sans réel impact pour les activités du ministère, le fonctionnement d'une structure ou d'un établissement ;
- **Modéré (incident de niveau 2)** : le fonctionnement d'un service est perturbé (incident constaté, gêne dans le fonctionnement), mais les impacts sont limités ou localisés. Ils ne portent pas atteinte de manière significative au bon fonctionnement de la structure ou de l'établissement ;
- **Grave (incident de niveau 3)** : les services sont perturbés au niveau national ou en rupture au niveau local. Les structures locales rencontrent des difficultés sérieuses dans leur fonctionnement ;
- **Très grave (incident de niveau 4)** : la conjonction de plusieurs incidents graves ou d'un incident majeur altère le fonctionnement des activités judiciaires, d'une zone de défense, d'un nombre important d'établissements, de l'ensemble des services d'une direction, d'un système d'information d'importance vitale (SIIV).

La gestion des incidents est pilotée à trois niveaux, en fonction de la gravité de l'incident :

- « **Faible** » et « **Modéré** » (incident contenu) : pour les incidents d'intensité « faible » à « modéré », les RSSI en pilotent la gestion dans le cadre d'un processus standard et maîtrisé. Pour ce faire, ils s'appuient sur le responsable du SOC ministériel pour les systèmes d'information gérés par la direction du numérique ou sur des procédures de sécurité prévues dans les marchés pour les systèmes d'information en gestion déléguée ou les systèmes d'information externalisés. Pour les incidents « modérés », le SOC informe la section coordination et prévention qui communiquera sur l'incident, en tant que de besoin au fonctionnaire de sécurité des systèmes d'information et aux conseillers à la sécurité du numérique.
- « **Grave** » : l'incident technique est piloté par le CSIRT. Le conseiller à la sécurité du numérique (CSN) et/ou le responsable central de la sécurité des systèmes d'information (RCSSI) concerné s'appuie sur les évènements remontés par le responsable du CSIRT

pour analyser, évaluer les impacts fonctionnels et anticiper l'évolution de la situation. Il informe le délégué à la défense et à la sécurité (DDS) et conseille l'autorité qualifiée en sécurité des systèmes d'information (AQSSI) qui décide, dans le cadre de la continuité d'activité, d'activer une cellule de crise directionnelle conformément à la politique de gestion de crise ministérielle.

- « **Très grave** » : assisté du CSIRT, le fonctionnaire de sécurité des systèmes d'information (FSSI) pilote la gestion technique de l'incident. Il agit telle une cellule « ***situation*** » dédiée au numérique. Les CSN et les RCSSI participent aux points de situation et à l'élaboration des mesures qui seront proposées en cellule « **décision** » (direction de crise). La gestion des incidents « **très graves** » s'inscrit dans le processus de gestion de crise ministérielle qui est défini dans la politique dédiée.

Tous les incidents de niveaux « **grave** » et « **très grave** » font l'objet d'un retour d'expérience (RETEX). Ce RETEX comprend un rappel des faits, l'évaluation des origines, des impacts, ainsi que le traitement de l'incident. Il intègre des recommandations et un plan d'action afin de prévenir la survenance d'un incident similaire où d'en améliorer la gestion.

L'ensemble du corpus regroupant les doctrines de traitement des incidents et de gestion de crise d'origine cyber se trouve dans l'annexe « Catégorie A ».

5.3. Déclaration des incidents à la CNIL

Un incident, quelle que soit la gravité, et faisant craindre une fuite ou violation de données, fait l'objet d'un signalement circonstancié et détaillé au délégué à la protection des données (DPD) du ministère. Ce signalement est initié par le responsable du CSIRT et complété par les conseillers à la sécurité du numérique des entités affectées.

Seuls le DPD et ses équipes sont en capacité d'estimer la nécessité de déclarer l'incident à la Commission nationale de l'informatique et des libertés (CNIL) et d'opérer cette déclaration[21].

[21] Article 33 du règlement (UE) 2016/679 dit « RGPD »

6. Cas particulier des établissements publics de l'Etat

Les établissements publics de l'État disposent d'une autonomie administrative et financière afin de remplir une mission d'intérêt général, précisément définie, sous le contrôle de l'État.

Le dirigeant exécutif de l'établissement est responsable, sur son périmètre, de la sécurité numérique. Cette responsabilité se traduit par les exigences suivantes[22] [23] :

- **Le dirigeant exécutif est AQSSI sur son périmètre[24]**. À ce titre, il est responsable de la sécurité numérique de l'ensemble de ses systèmes d'information et de l'homologation des systèmes d'information de son périmètre. Afin de mettre en place cette sécurité, le dirigeant exécutif de l'établissement peut se rapprocher du CSIRT ministériel.
- Le dirigeant exécutif doit **désigner un point de contact direct pour le fonctionnaire de sécurité des systèmes d'information (FSSI)** et **le responsable du CSIRT ministériel.** Celui-ci peut être le responsable de la sécurité des systèmes d'information (RSSI) ou à défaut le directeur des systèmes d'information (DSI) de l'établissement[25].
- **Le dirigeant exécutif contribue à l'élaboration d'un rapport annuel de sécurité** intégrant l'évaluation du niveau de sécurité du numérique et une synthèse des incidents de sécurité numérique. Ce rapport est transmis au FSSI annuellement[26].

Les incidents de sécurité affectant le système d'information et de communication de l'établissement doivent être déclarés auprès du FSSI du ministère, ainsi qu'à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) conformément à l'instruction générale interministérielle susmentionnée.

[22] Article 4-4 du décret n° 2019-1088 du 25 octobre 2019

[23] Article 5 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

[24] Article 2 de l'arrêté du 17 février 2020 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de la justice

[25] Article 5.2 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

[26] Article 5.3 de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI

7. Glossaire

Autorité d'homologation : personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du système d'information et de communication, c'est-à-dire, prend la décision d'accepter les risques résiduels identifiés sur le système.

Incident de sécurité : événement qui perturbe le fonctionnement d'un service et altère l'activité. En fonction de son niveau de gravité et de son risque sur l'organisation, il peut être catégorisé de « faible » à « très grave » et nécessiter l'activation de la cellule de crise.

Plan de transformation numérique : document qui définit les orientations en matière de transformation numérique d'un ministère ou d'un établissement.

Politique de sécurité numérique : document qui définit les orientations en matière de sécurité numérique d'un ministère ou d'un établissement.

Résilience numérique : capacité d'une organisation à mettre en place les moyens opérationnels adaptés aux menaces et les déployer pour, en cas de crise, être en mesure de maintenir et rétablir les services rendus par les systèmes d'information et de communication concourant à la réalisation des activités critiques de l'organisation, qu'ils soient internes ou externes.

Sécurité numérique : ensemble d'activités organisationnelles, techniques ou juridiques visant à protéger et défendre les systèmes d'information et de communication, ainsi que les informations qu'ils manipulent, contre d'éventuels incidents de sécurité de nature accidentelle ou intentionnelle, et à assurer la résilience numérique des entités concernées.

Système d'information et de communication de l'Etat : défini à l'article 1er du 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, « [l]e système d'information et de communication de l'Etat est composé de l'ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker sous forme numérique les données qui concourent aux missions des services de l'Etat et des organismes placés sous sa tutelle. »

Système d'information et de communication : sous-ensemble du système d'information et de communication de l'Etat mis en œuvre par une direction ou un service d'un ministère ou par un établissement public de l'Etat pour la réalisation de ses missions.

Système d'information industriel : système d'information visant à piloter des installations ou équipements physiques (caméras, gestion des énergies, automates, portes, …).

8. Références

(1) 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 (règlement général sur la protection des données.

(2) 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) 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.

(4) Arrêté du 14 juin 2024 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de la justice.

(5) Arrêté du 26 octobre 2022 portant approbation de l'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.