MINISTÈRE
DE LA JUSTICE

Liberté
Égalité
Fraternité

Politique Ministérielle de Sécurité Numérique

Version 2026

Approuvée par la secrétaire générale, haute fonctionnaire de défense et de sécurité NOR : JUST2602389A	

Table des modifications

Paragraphe	Nature de la modification
2.1	La PMSN doit être mentionnée dans les contrats
2.3	Mise à jour de la liste des annexes : le guide d'homologation devient une politique (retrait du caractère facultatif)
3.1.1.3	- Mise en forme de la liste des AQSSI similaire à l'arrêté 13 juin 2024 ; - Ajout en référence de la Circulaire relative à l'organisation ministérielle de la gestion de crise du 13 juin 2025
3.1.1.4	Ajout pour le directeur du numérique de la possibilité d'adapter la démarche d'homologation pour le socle technique
3.1.2.1	Ajout pour le fonctionnaire SSI de s'assurer du respect des obligations réglementaires et des décisions interministérielles
3.1.2.2	Ajout pour les conseillers à la sécurité numérique de deux missions : - cartographier les risques numériques, les SI et les fournisseurs de service numériques ; - mettre en place un contrôle de la chaîne d'approvisionnement (cf. NISv2 et feuille de route interministérielles).
3.1.2.3	Ajout pour le responsable de la section maîtrise des risques : - Des missions de consolidation des cartographies au niveau ministériel ; - Reformulation des responsabilités pour l'annexe B-01
3.1.2.4	Ajout pour le responsable de la section coordination et prévention de la mission de pilotage des injonctions ministérielles
3.1.3	« La chaîne opérationnelle de sécurité numérique et de cyberdéfense » devient « La chaîne opérationnelle **et technique** de sécurité numérique et de cyberdéfense » du fait de la création du rôle d'expert SSI
3.1.3.1	Ajout de deux missions pour les RCSSI : - Formalisation d'une déclinaison opérationnel de la gestion des incidents ; - Traitement des injonctions. Ajout des instances directionnelles comme source des chantiers validés Assure la présidence des COTEC-SSI
3.1.3.3	Création du rôle et des responsabilités des administrateurs de la SSI
3.1.3.4	Création du rôle et des responsabilités des experts SSI
3.2.2	Pour les CR, ajout de l'exigence d'un relevé de décision indiquant les porteurs et les délais
3.2.3	Pour les CR, ajout de l'exigence d'un relevé de décision indiquant les porteurs et les délais
3.2.4	Présidence des COTEC-SSI modifiée (RCSSI) : - Pour les CR, ajout de l'exigence d'un relevé de décision indiquant les porteurs et les délais.

3.2.5	Pour les CR, ajout de l'exigence d'un relevé de décision indiquant les porteurs et les délais
4.1	Réécriture du paragraphe d'introduction de la maitrise des risques numérique
4.2	Le paragraphe « Classification des informations » est supprimé. Il fera l'objet d'une annexe dédiée.
5.2.	Prise en compte des remarques DPD sur la fonction « référents informatique et liberté » (RIL) Obligation de la formalisation d'un RETEX sur les incidents « grave » dans les 2 mois maximum
5.3	Refonte du paragraphe « violation de données » en regard des autorités de contrôle spécifiques au MJ et des responsabilités des RIL
7	Ajout dans le glossaire de la définition de « violation de données »
8 Références	Suppression de la référence au règlement (UE) 2016/679 (cf. DPD) Hiérarchie des actes administratifs

Table des matières

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 doit être mentionnée dans les contrats ou les conventions passées par le ministère de la Justice. Elle s'impose 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. 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 et annexes

Catégorie A : Organisation et gestion des incidents cyber

Porteur : DHFDS/BPSN : Responsable du CSIRT

A-01 : Politique de traitement des incidents de sécurité numérique

Catégorie B : Démarche et homologation de sécurité

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

B-01 : Politique de sécurité numérique : Démarche d'homologation

Catégorie C : Contrôle et audit de sécurité

Porteur : DHFDS/BPSN : 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, ministre de la Justice 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[4].

Sont désignés « autorités qualifiées en sécurité des systèmes d'information »[5] :

- pour les directions et services placés sous l'autorité du ministre :
  - pour le secrétariat général : le secrétaire général du ministère de la Justice, sous réserve de l'article 2 ;
  - pour les directions placées sous l'autorité directe du ministre : le directeur ;
  - pour l'inspection générale de la Justice : l'inspecteur général, chef de l'inspection générale ;
  - pour le Conseil d'Etat : le secrétaire général du Conseil d'Etat ;

[2] Article 4-2 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

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

[4] Circulaire du 13 juin 2025 relative à l'organisation ministérielle de la gestion de crise (NOR JUST2514726C)

[5] Articles 1, 2 et 3 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

- pour les services à compétence nationale rattachés directement au ministre ou à caractère interministériel : le directeur ou le chef de service.

- pour la direction du numérique rattachée au secrétariat général :
  - pour le socle technique : le directeur.

- pour les établissements publics nationaux placés sous la tutelle du ministre :
  - les responsables, quel que soit leur titre, des fonctions de direction générale des établissements publics.

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

3.1.1.4. Le directeur du numérique (DNUM)

Le **directeur du numérique** (DNUM)[6] 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 particuliers en adaptant autant que de besoin la démarche d'homologation.

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 du comité d'homologation organisé par le conseiller à la sécurité du numérique de la direction du numérique.

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

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.

3.1.2.1. Le fonctionnaire de sécurité des systèmes d'information

Le **fonctionnaire de sécurité des systèmes d'information** (FSSI)[7] [8] 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** de la sécurité numérique, du respect des obligations réglementaires et des décisions interministérielles ;
- **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 sur les dossiers d'homologation** 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.

[7] Article 4-1 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

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

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

Le **conseiller à la sécurité du numérique** (CSN)[9] 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 :

- Cartographier les risques numériques, les systèmes d'information placés sous la responsabilité de l'AQSSI et recenser les fournisseurs de service numériques nécessaires à leurs fonctionnements ;
- Mettre en place une politique de contrôle de la chaîne d'approvisionnement ;
- **Piloter la mise en œuvre des enjeux de sécurité** métier, en lien le responsable central de la sécurité des systèmes d'information (RCSSI) de la DNUM ou de la direction, 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 ;
- **Suivre les plans d'action** décidés en comité d'homologation ;
- Evaluer 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 son 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 et les chefs d'établissements publics sous tutelle, au développement de la maîtrise du risque numérique.

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

A ce titre, il réalise plusieurs missions :

- Consolider au niveau ministériel les cartographies des SI élaborées dans les directions ;
- Tenir à jour la liste des SIE homologués ;
- S'assurer que les systèmes d'information d'importance vitale (SIIV) et systèmes d'information essentiels (SIE) suivent une démarche de sécurité et que des plans de remédiation soient établis ; il prépare l'avis du FSSI sur les dossiers d'homologation de ces SI ;
- Identifier, évaluer et hiérarchiser les risques numériques du ministère ;
- Piloter les évolutions de l'annexe B-01 « Politique de sécurité numérique : Démarche d'homologation » conformément aux besoins de sécurité des projets, à la stratégie du FSSI et aux bonnes pratiques de l'ANSSI ;
- Piloter les évolution des référentiels de contrôle et d'audit ;
- 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[10], 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 injonctions ministérielles liées au traitement des vulnérabilités ;
- 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 ;

[10] Mandat CSIRT du 21/04/2023

- 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 et technique de sécurité numérique et de cyberdéfense

Pour mener à bien ses missions, le ministère s'appuie sur une **chaîne opérationnelle et technique** 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**. Dans ce cadre, ils travaillent en étroite collaboration avec le CSN.

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.
- Elaborer une déclinaison opérationnelle de la politique de traitement des incidents de sécurité numérique (annexe A-01) qui inclus :
  - L'information du responsable de la section coordination de tout incident ;
  - Le transfert au responsable du SOC ministériel des éléments techniques nécessaires au traitement et à la détection d'occurrence similaire ;

- La production et la transmission d'un rapport d'investigation validé par le CSN au responsable de la section coordination et au responsable du SOC ministériel ;

- Traiter les injonctions sur vulnérabilité et informer le responsable de la section coordination :
  - Pour la direction du numérique, l'ensemble des SI hébergés et soutenus ;
  - Pour les directions métier, l'ensemble des SI externalisés, en gestion déléguée et des établissements publics relevant de sa tutelle.
- Assurer la présidence des comités techniques de sécurité des systèmes d'information (COTEC-SSI) ;
- 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 et 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 RCSSI de la direction sur les aspects techniques, informe le conseiller à la sécurité du numérique de la direction de rattachement de l'avancement des travaux de la feuille de route et des risques numériques ;
- 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 et adressée au haut fonctionnaire de défense et de sécurité.

3.1.3.4. Les administrateurs de la sécurité des systèmes d'information

L'administrateur de solutions de sécurité installe, met en production, administre et exploite des solutions de sécurité (Active Directory, antivirus, EDR, sondes, firewalls, IAM, PKI/IGC, etc.). Il participe au bon fonctionnement des solutions de sécurité en garantissant le maintien en conditions opérationnelles et de sécurité.

Les administrateurs SSI réalisent plusieurs missions :

- S'assurer du fonctionnement optimal des solutions de sécurité dont ils ont la charge ;
- Configurer les solutions en conformité avec les normes et standards définis par les experts SSI,
- Effectuer des revues régulières des règles et paramétrages mis en place ;
- Définir et mettre en œuvre des procédures d'installation des correctifs de sécurité ;
- Mettre en place la collecte des logs et des alertes pour le service de détection d'incidents du SOC ;
- Gérer les droits d'accès aux solutions en fonction des profils ;
- Traiter les incidents opérationnels ou les anomalies ainsi que les exceptions.

3.1.3.5. Les experts de la sécurité des systèmes d'information

Les experts SSI possèdent une expertise sur la sécurité d'un domaine technique particulier (système, réseau, système de sureté ou industriel, Active Directory, Cloud, IAM, Intelligence Artificielle, etc.). Ils assurent un rôle de conseil, d'assistance, d'information, de formation, de qualification et d'alerte, et peuvent intervenir directement sur tout ce qui relève de leur domaine d'expertise, que ce soit dans les phases d'étude, de mise en œuvre, de maintien en conditions de sécurité ou d'investigation numérique.

Les experts SSI concourent à plusieurs missions :

- Conduire des études pour la sécurisation des composants et solutions de son domaine d'expertise ;
- Participer à l'élaboration des standards techniques de sécurité et de la documentation technique ;

- Analyser, recommander et valider les choix d'implémentation ;
- Contribuer au paramétrage efficace des solutions de sécurité ;
- Proposer des techniques de contrôle du respect des politiques de sécurité dans son domaine d'expertise, aider la constitution de tableaux de bord de contrôle ;
- Diagnostiquer les dysfonctionnements, contribuer à la remédiation, investiguer sur les causes d'un incident ou d'une cyberattaque ;
- Conduire des investigations numériques sur réquisition judiciaire ou administrative ;
- Intervenir dans le choix des fournisseurs.

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)[11].

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 ;

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

- 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.

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)[12].

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 (COSTRA-SN), les annexes de 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 ;

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

- 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. Il précise notamment les décisions prises, le ou les responsables des actions à mener ainsi que les délais pour les réaliser. Le cas échéant, il identifie le ou les risques pris en matière de sécurité numérique.

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 responsables de sécurité des systèmes d'informations des établissements publics ;
- Les conseillers à la sécurité numérique des directions de tutelle ou représentants ;
- 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. Il précise notamment les décisions prises, le ou les responsables des actions à mener ainsi que les délais pour les réaliser. Le cas échéant, il identifie le ou les risques pris en matière de sécurité numérique.

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

Le 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 et les instances de pilotage directionnelles.

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

- Le responsable central de la sécurité des systèmes d'information en tant que président ;
- 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. La réunion fait l'objet *a minima* d'un relevé de décisions qui précise notamment les décisions prises, le ou les responsables des actions à mener ainsi que les délais pour les réaliser. Le cas échéant, il identifie le ou les risques pris en matière de sécurité numérique.

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**).

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. La réunion fait l'objet *a minima* d'un relevé de décisions qui précise notamment les décisions prises, le ou les responsables des actions à mener ainsi que les délais pour les réaliser. Le cas échéant, il identifie le ou les risques pris en matière de sécurité numérique.

4. Maîtrise du risque numérique

4.1. Typologie et criticité des systèmes d'information

La maitrise des risques numériques vise à adapter les démarches de sécurité aux enjeux 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. La stratégie d'homologation formalise l'appréciation de la criticité des systèmes.

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 des missions régaliennes du 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'ils soient internes ou externes 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[13].

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.

[13] 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 »*[14].

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[15] 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[16] de l'arrêté sectoriel « Activités judiciaires »[17] 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. Principes stratégiques de la maîtrise du risque numérique

4.2.1. Cartographies des risques numériques

La cartographie est un outil de pilotage indispensable à la maîtrise des risques numériques[18].

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 relevant 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[19].

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.

---

[14] Conformément aux dispositions de l'article L. 1332-6-1 du code de la défense.

[15] 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.

[16] Annexe non publique en diffusion restreinte.

[17] 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 ».

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

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

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.

4.2.2. 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 modèle de 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.

4.2.3. 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[20].

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.

4.2.3.1. 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 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

[20] Article 3 du décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics

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.

Une politique d'homologation (Annexe B-01), disponible dans le corpus de la sécurité numérique détaille la manière dont doit être menée cette démarche.

4.2.3.2. Décision d'homologation

L'homologation est également la **décision formelle**[21] 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* »[22].

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 du comité d'homologation pour les systèmes d'information.

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.

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.

[21] Article 4-3 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

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

5. La gestion des incidents de sécurité numérique

5.1. Définition

Un incident de sécurité numérique est un événement qui perturbe ou altère le fonctionnement d'un système d'information et dont la gravité peut porter atteinte aux missions du ministère et au bon fonctionnement de la Justice. Le traitement des incidents a pour but de qualifier et de remédier ces incidents pour rétablir la continuité d'activité le plus rapidement possible ou se prémunir de risques d'aggravation de l'incident.

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 qualification des incidents est effectuée à l'aide de la matrice de qualification des incidents. En fonction de leur qualification, ces incidents sont traités par les RSSI, les RCSSI et le SOC. Lorsque le SOC escalade l'incident à la SCP, les CSN sont informés d'un incident sur leur périmètre et sont tenus d'assurer le suivi de cet incident. Les CSN sont également tenus d'informer immédiatement le référent informatique et libertés (RIL) de leur direction dès que l'incident de sécurité implique des données à caractère personnel. Dès lors que l'incident implique des impacts sur la continuité d'activité, le CSN est tenu de se rapprocher du DDS de sa direction afin d'anticiper les effets sur l'activité.

Dans le cas d'un incident nécessitant un passage en crise, la chaîne numérique se mobilise selon la procédure de gestion de crise[23]. Cette procédure doit être déclinée par les directions en s'appuyant sur la procédure de gestion des incidents, la procédure de gestion de crise d'origine cyber et l'instruction ministérielle.

[23] Instruction ministérielle de gestion de crise ; annexe de la circulaire du 13 juin 2025 relative à l'organisation ministérielle de la gestion de crise (NOR : JUST2514726C)

Tous les incidents de niveaux « **grave** » et « **très grave** » font l'objet d'un retour d'expérience (RETEX) dans un délai de deux mois maximum. 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. Il est adressé à l'ensemble des membres de la ligne hiérarchique chargée d'en tirer des enseignements. Le RETEX est également transmis au HFDS qui peut décider de contrôler dans un délai pertinent si les actions arrêtées à l'issue du RETEX ont bien été mises œuvre.

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. Gestion des incidents de sécurité entrainant une violation de données à caractère personnel

Lorsqu'un incident de sécurité, quelle que soit sa gravité, implique des données à caractère personnel, le référent informatique et libertés (RIL) de la direction concernée est immédiatement informé par le CSN. Ce signalement est circonstancié. La SCP informe également le délégué à la protection des données (DPD) de ces incidents.

Le RIL qualifie l'incident afin de savoir si une violation de données est constituée. Il analyse la nécessité de notifier cette violation à l'autorité de contrôle. En tout état de cause, il documente cette violation et conserve les éléments dans son registre des violations.

Lorsque la violation nécessite une notification à l'autorité de contrôle ou pour bénéficier d'un appui sur l'analyse de la violation, le RIL saisit le DPD.

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[24] [25] :

- **Le dirigeant exécutif est AQSSI sur son périmètre[26]**. 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[27].
- **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[28].

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.

[24] Article 4-4 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

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

[26] Article 3 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

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

[28] 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, …).

Violation de données : tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles (destruction, perte, altération, divulgation non autorisée).

8. Références

(1) 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.

(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) 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.

(4) 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.

MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

SG/HFDS/BPSN/SCP

Politique de sécurité numérique

-

Traitement des incidents

Annexe A-01

HISTORIQUE DES MODIFICATIONS

Version	Date	Auteur(s) - Entité	Description
V1.0	27/01/2025	Antonin GABION – DHFDS/BPSN/SCP	Politique de traitement des incidents de sécurité numérique.
V1.1	03/11/2025	Antonin GABION – DHFDS/BPSN/SCP	Actualisation et intégration de la chaîne I&L

VALIDATION DU DOCUMENT

Instance	Date
COPIL-SN	Continuation du 21/11/2025

APPROBATION DU DOCUMENT

Instance	Date
COSTRAT-SN	05/12/2025

Table des matières

INTRODUCTION

Ce document est une annexe de la Politique Ministérielle de Sécurité Numérique. Conformément à son paragraphe 2.3, ce document rentre dans la Catégorie A « Organisation et gestion des incidents cyber » et porte le numéro 1. Il est donc référencé **comme l'annexe A-01.**

Il concerne l'ensemble des services du ministère et des établissements publics placés sous sa tutelle[1] utilisant le SI ministériel.

Limitations : il ne concerne pas les situations de gestions déléguées ou de services externalisés (fournisseurs, sous-traitants, prestataires) ni les partenaires (organisations syndicales, mutuelles, associations, etc.) Une obligation de remontée d'incidents de sécurité numérique doit néanmoins être définie par voie contractuelle ou conventionnelle avec la direction concernée.

La procédure traite la gestion des incidents de sécurité numérique, face auxquels le ministère de la Justice doit développer et maintenir une capacité de réponse. Celle-ci s'appuie sur des moyens techniques mais aussi sur une organisation de la chaîne sécurité numérique. Elle passe par la coordination des différents acteurs à tous les niveaux de la chaîne sécurité numérique, de l'échelon local à l'échelon ministériel voire interministériel. Elle définit les acteurs, leurs rôles et leurs interactions à différentes phases du traitement :

- La distinction entre évènement et incident de sécurité
- La phase d'alerte et de qualification
- La phase de réponse à incident
- Le suivi post-incident

La procédure de traitement des incidents de sécurité numérique fait l'interface avec le plan ministériel de gestion des crises d'origine cyber, qui fait référence pour des situations de crise directionnelle ou ministérielle. Elle fait l'objet d'une revue au minimum une fois par an en fonction des besoins, avec l'objectif de garantir son effectivité.

Eléments définis par convention :

- **SOC :** Security Operational Center.
- **SCP :** Section coordination & prévention, rattachée au département HFDS.
- **DPD :** Délégué ministériel à la protection des données.
- **DIT :** Département Informatique et Télécommunications
- **CSN** : Conseiller à la sécurité numérique
- **RIL** : Responsable informatique et libertés
- **BPGC :** Bureau planification et gestion des crises du département HFDS.
- **EJ :** Etablissement Justice, soit un site du ministère de la Justice.
- **EP :** Etablissement Public
- **AAI :** Autorité administrative indépendante

[1] Certains établissements publics disposent de leur propre SI. Leur cas est évoqué dans le II de la partie 2.

PARTIE 1 : DE L'EVENEMENT A L'INCIDENT

I. Les évènements de sécurité

Les évènements de sécurité font partie du cycle de vie d'un système d'information. Si certains sont bénins en termes de sécurité numérique, d'autres sont susceptibles d'avoir des impacts sur le fonctionnement du SI et sur la continuité d'activité. Il est donc nécessaire de les superviser : un évènement de sécurité peut devenir un incident de sécurité.

a. Définition

Un évènement de sécurité est un comportement anormal ou inattendu rapporté provenant de l'intérieur ou de l'extérieur d'un SI et susceptible de mettre en cause sa sécurité. Il peut être rapporté par un système de surveillance ou un utilisateur. Il ne représente pas nécessairement une menace pour la sécurité informatique mais exige une analyse approfondie afin d'en vérifier l'origine et la nature. Un évènement de production touchant à la disponibilité est un évènement de sécurité qui nécessite d'être qualifié afin d'en déterminer la nature.

b. Le traitement des évènements de sécurité

Dans le cas d'un signalement provenant d'un utilisateur, le récipiendaire d'un évènement de sécurité est le Centre de Services National. Les signalements se font via un numéro de téléphone unique (01.70.22.88.36) ou une adresse de messagerie structurelle (support.csn@justice.gouv.fr).
Les évènements sont pré-qualifiés par le Centre de Support National à leur réception :

- Si l'évènement ne nécessite pas plus d'investigations, il est transmis aux équipes compétentes pour traitement.
- Dans le cas d'un évènement pré-qualifié d'incident de sécurité, il est soumis au SOC du ministère.
- Sur certains évènements, il peut être nécessaire d'effectuer une levée de doute, car l'évènement peut dégénérer en incident de sécurité numérique, avec des conséquences plus importantes. La levée de doute est effectuée par le SOC, qui peut alors requalifier l'évènement en incident.
- Certains évènements peuvent être d'abord qualifiés comme des incidents avant d'être requalifiés suite à des investigations ou de nouveaux éléments. Ils sont alors considérés comme des « faux positifs ».

Un signalement peut également aller vers un point de contact local qui transmet ensuite l'information au RSSI de son DIT puis au SOC. Tous ces évènements sont enregistrés par le SOC et associés à un numéro de RMJ (Référence Ministère de la Justice) pour assurer leur suivi.

II. Les incidents de sécurité numérique

a. Définition

Un incident de sécurité numérique est un événement qui perturbe ou altère le fonctionnement du système d'information et dont la gravité peut porter atteinte aux missions du ministère et au bon fonctionnement de la Justice. Le traitement des incidents a pour but de qualifier et de remédier ces incidents pour rétablir la continuité d'activité le plus rapidement possible ou se prémunir de risques d'aggravation de l'incident.

Dans le cas d'un incident grave affectant les infrastructures numériques et tant que la possibilité d'un incident cyber n'a pas été écartée, le SOC ministériel participe à la cellule de crise DNUM. Il détermine alors si des éléments pointent vers un incident de sécurité numérique et informe la SCP de son diagnostic.

b. Echelle de gravité

La prise de connaissance du signalement doit s'accompagner d'une évaluation de sa gravité. La qualification est essentielle car elle permet d'orienter les actions de remédiation ainsi que d'alerter et de mobiliser à bon escient. Conformément à la PMSN (paragraphe 5.2), la gravité d'un incident est évaluée sur une échelle de 1 à 4 :

- **1 : faible**. 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 ;
- **2 : modéré**. 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 ;
- **3 : grave**. Les services sont perturbés au niveau national ou en rupture au niveau local. Les structures locales rencontrent des difficultés sérieuses dans leur fonctionnement ;
- **4 : très grave**. 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).

c. La qualification des incidents

La qualification des incidents par niveau de gravité est réalisée conjointement par le SOC et la SCP lors de leur prise de connaissance du signalement. Elle se base sur une matrice d'engagement, disponible en annexe, qui croise l'effet de l'incident sur le ministère et le périmètre affecté pour déterminer le niveau de gravité de l'incident.

L'effet de l'incident est déterminé via des critères divers (impact technique, impact sur l'activité, impact réputationnel, etc.) qui sont propres à chaque typologie d'incident ou de comportement anormal. La qualification d'un incident n'est pas fixe : son niveau de gravité peut évoluer au fur et à mesure des investigations et des retours métier. Elle permet de faciliter et d'orienter la priorisation et l'affectation des ressources en cas d'incidents majeurs et/ou multiples.

PARTIE 2 : LE PROCESSUS D'ALERTE

I. Objectifs de l'alerte

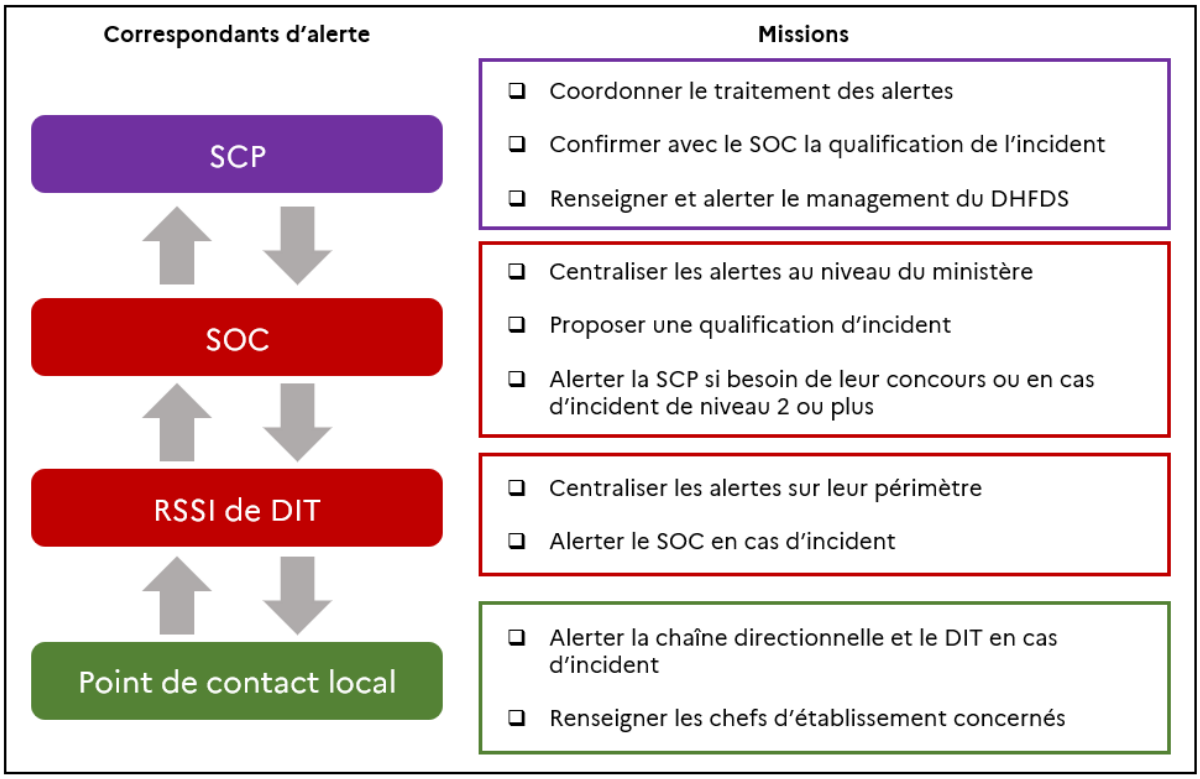
L'alerte a pour but principal de partager la prise de connaissance des éléments constitutifs de l'incident et de sa qualification initiale par le SOC. En heures non-ouvrables, en fonction du niveau de qualification, le processus d'alerte peut être amené à déclencher l'astreinte SCP.

La SCP est responsable de la constitution et de l'entretien d'un annuaire qui contient tous les contacts utiles au traitement des incidents et à la gestion des crises d'origine cyber. A ce titre, un modèle d'annuaire est fourni en annexe. Cet annuaire à jour est transmis chaque vendredi au HFDS-A, aux chefs de bureau du département du HFDS, au SOC, aux membres des COPIL-SN et au chef du bureau du cabinet.

L'alerte peut circuler dans deux sens : soit elle est initiée par le niveau local et remonte vers les échelons centraux (alerte montante), soit l'alerte est diffusée par l'administration centrale vers les échelons locaux (alerte descendante). Les interactions entre les différents acteurs de la chaîne sécurité numérique sont définies au paragraphe 2 – II.
Les objectifs du dispositif d'alerte sont les suivants :

- Être permanent et effectif
- Recueillir les faits liés à l'évènement
- Qualifier les impacts connus à ce stade
- Informer les échelons hiérarchiques supérieurs et subordonnés

La chaîne de traitement des incidents s'appuie sur la chaîne opérationnelle de sécurité numérique telle que définie dans la PMSN. Le schéma d'alerte ci-dessous ne représente pas la chaîne d'alerte propre à chaque direction.



II. La chaîne de traitement des incidents

La chaîne de traitement des incidents est composée d'une chaîne opérationnelle et d'une chaîne de pilotage. Au niveau central, le traitement des incidents est une des missions du SOC du ministère de la Justice, en relation avec la SCP du département HFDS :

- Le SOC est en charge de la supervision et de la détection. Il est également chargé de l'analyse et de la qualification technique des incidents. Il est l'interlocuteur privilégié des RSSI de DIT et auprès des différents services de la DNUM.
- La SCP a un rôle de coordination et de pilotage. Elle prend en compte la qualification technique et aide à évaluer les impacts métier en relation avec les conseillers à la sécurité numérique des directions et les responsables SSI des établissements publics. Elle échange avec le FSSI pour évaluer les impacts à l'échelle du ministère. Elle est l'interlocutrice privilégiée de la DICOM et du DPD.

Le SOC et la SCP échangent continuellement et s'appuient sur la chaîne de traitement des incidents du ministère de la Justice. Dans le cadre d'un incident grave ou très grave, ces deux entités forment le CSIRT (Equipe de réponse à incident de sécurité numérique) ministériel, dirigé par le FSSI.

Ces deux entités sont joignables par mail via leurs boites structurelles :

- **soc@justice.gouv.fr pour le SOC**
- **csirt@justice.gouv.fr pour la SCP.**

En HNO (heures non ouvrées), elles tiennent chacun une permanence :

- La permanence SOC est l'interlocutrice de la chaîne technique et de l'ANSSI en cas d'incident. Elle est joignable au **06.13.66.60.47.**
- La permanence SCP est déclenchée en cas de crise et/ou d'incident grave et très grave. Elle est à destination des CSN et des autorités et est joignable au **06.23.06.63.55.**

Les réseaux directionnels de la sécurité numérique sont pilotés par les conseillers à la sécurité numérique (CSN) de chaque direction. En lien avec leurs points de contact locaux, ils sont informés de signalements ou d'incidents de sécurité numérique qu'ils transmettent à la SCP. Dès qu'ils ont connaissance d'un incident de sécurité impliquant des données à caractère personnel, ils informent le RIL de leur direction.

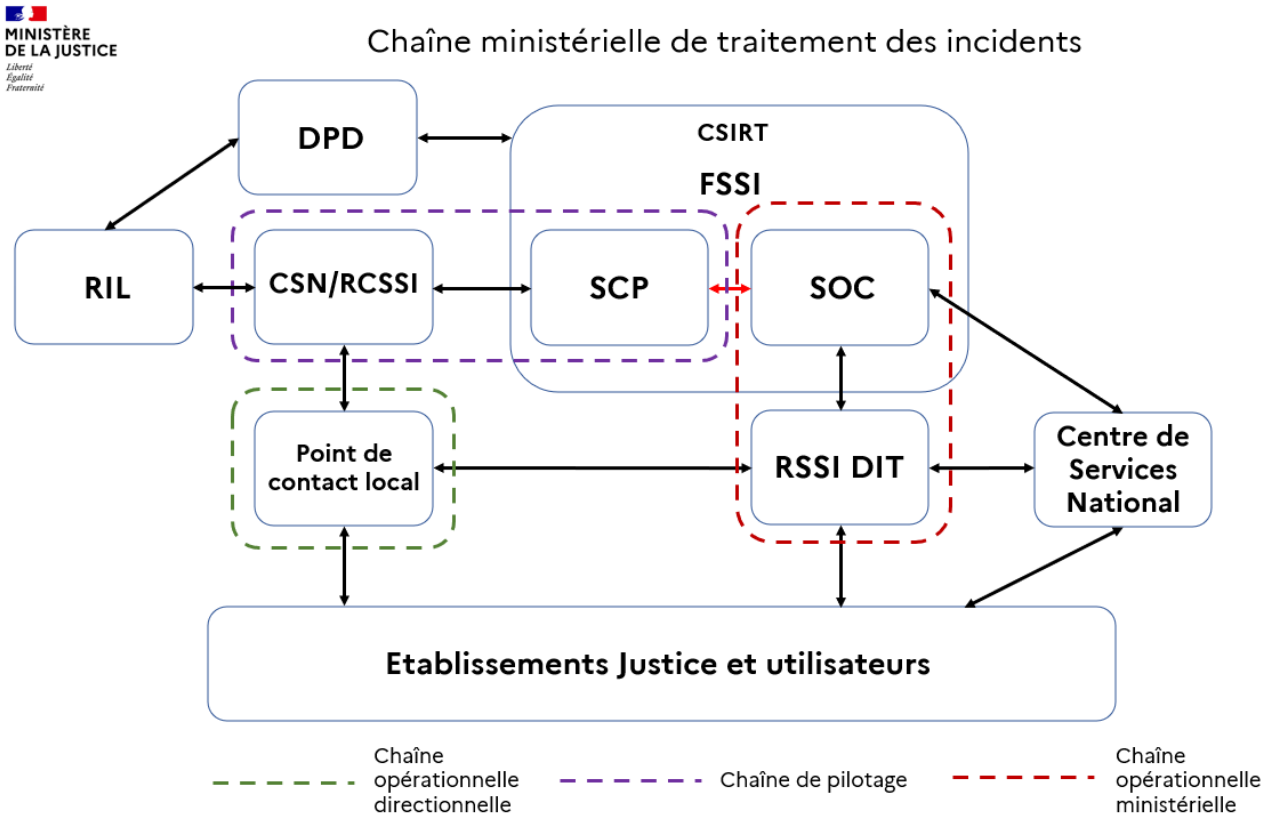
Les points de contact locaux des directions doivent participer à la réponse à incident sur leur périmètre en lien avec les RSSI des DIT. Selon les directions, l'organisation et les titres de ces correspondants varient.

Dans les services déconcentrés, les points de contact transverses pour le traitement des incidents sur le SI ministériel sont les RSSI des DIT (Département Informatique et Télécommunications). Ils sont informés des incidents par les points de contact locaux des directions. Ils interviennent dans le cadre de la réponse à incident sur leur zone territoriale, en lien avec le SOC.

Pour les établissements publics, le référent ou RSSI nommé par le dirigeant de l'établissement public intervient dans le cadre de la réponse à incident. Au titre de la tutelle, il peut être amené à échanger avec le CSN de la direction concernée.

Remarque : certains établissements publics ou autorités administratives indépendantes disposent de leur propre système d'information, distinct du SI Justice. En cas d'incident touchant ces entités, elles alertent le FSSI.

Toutefois, ces entités font partie du « périmètre 2 » défini dans le mandat du CSIRT ministériel. A ce titre, elles peuvent bénéficier sur demande d'une assistance du SOC et de la SCP mais le pilotage opérationnel de l'incident n'est pas assuré par le CSIRT ministériel



Au-delà du processus d'alerte basé sur les signalements au Centre de Services National, d'autres vecteurs et chaînes d'alerte existent. Ces alertes se font par des moyens classiques (messagerie, téléphone, Tchap) et peuvent provenir de deux types de sources :

- Des alertes provenant de sources internes comme les outils de détection (sondes, anti-virus, EDR, etc.) du SOC ou des RSSI de DIT, les remontées des chaînes métier via les CSN et le BPGC, ou la chaîne Informatique & Libertés.

- Des alertes provenant de sources externes, comme le CERT-FR de l'ANSSI ou d'autres CSIRT ministériels.

PARTIE 3 : LA REPONSE A INCIDENT

I. Rôles et responsabilités

Pour organiser la réponse à incident, le SOC et la SCP s'appuient sur des procédures internes. Celles-ci définissent les agents en charge du traitement de l'incident ainsi que la façon de l'organiser. Le SOC construit et partage des procédures avec les RSSI de DIT afin d'adapter leurs actions aux différentes typologies d'incidents. La SCP détaille dans ses procédures les points d'attention pour chaque incident et les acteurs à informer.

a. Incidents de niveau 1

Les incidents de niveau 1 sont pilotés par les RSSI de DIT ou le SOC selon le périmètre et la typologie de l'incident. Le responsable du pilotage est défini dans leurs procédures communes. Ils se tiennent informés de la situation et des mesures prises, et s'appuient sur les points de contacts locaux du périmètre concerné. Ils mènent les actions d'investigation et de remédiation si nécessaire.

b. Incidents de niveau 2

Les responsabilités sont les mêmes pour les incidents de niveau 2. Cependant, le SOC informe régulièrement la SCP de l'évolution de l'incident. Il peut demander validation pour la réalisation de certaines actions via la SCP et les CSN.

La SCP reste en lien avec le SOC pendant le processus de traitement de l'incident. Elle tient informé de l'évolution de la situation le FSSI ainsi que les CSN des directions concernées. Selon la nature de l'incident, elle peut également communiquer avec différents interlocuteurs :

- Si la situation l'exige, la SCP peut informer le HFDS-A de l'incident et de son évolution. La SCP, en lien avec le FSSI, peut déposer plainte au nom du ministère de la Justice auprès du parquet de Paris (section J3).

- Le CERT-FR de l'ANSSI peut également être informé d'un incident et de son évolution. Si l'incident touche un SIIV cette information est une obligation, conformément au Code de la défense.

- S'il y a un risque de médiatisation de l'incident (médias, réseaux sociaux, etc.), la délégation à l'information et la communication (DICOM) peut être informée pour s'y préparer.

Lorsqu'un incident de sécurité, quelle que soit sa gravité, implique des données à caractère personnel, le CSN informe immédiatement le RIL de sa direction. Ce signalement est circonstancié. La SCP informe également la DPD de ces incidents.
Le RIL qualifie l'incident afin de savoir si une violation de données est constituée. Il analyse la nécessité de notifier cette violation à l'autorité de contrôle. En tout état de cause, il documente cette violation et conserve les éléments dans son registre des violations.
Lorsque la violation nécessite une notification à l'autorité de contrôle ou pour bénéficier d'un appui sur l'analyse de la violation, le RIL saisit le DPD.

c. Incidents de niveau 3 ou 4 et requalification

Un incident de niveau 1 ou 2 est susceptible d'être requalifié :

- Par le SOC en fonction des éléments techniques recueillis au cours de ses investigations.
- Par le(s) CSN du fait de l'évolution des impacts fonctionnels sur l'activité de la direction.
- Par le BPGC du fait des impacts au niveau ministériel (continuité d'activité, médiatisation, juridiques, humains).

Dans le cas d'une requalification ou d'un incident qualifié de niveau 3 ou 4, la SCP informe le CO Vendôme ainsi que le HFDS-A de la situation pour un potentiel passage à l'état de crise. Cette information se fait par un appel téléphonique doublé d'un mail. Dans le cadre d'une situation de crise, le CSIRT est instancié en tant que structure et convoque une cellule opérationnelle cyber.

Celle-ci est dirigée et mise en œuvre par le FSSI pour piloter la réponse sur incident, rechercher des solutions avec les différents acteurs techniques et informer la cellule de crise. Les rôles et responsabilités du CSIRT, de la cellule opérationnelle cyber, ainsi que des différents acteurs dans cette situation particulière sont définis par l'annexe A-02 de la PMSN « Plan de gestion des crises d'origine cyber ».

II. Suivi et clôture de l'incident

Pendant la période où un incident est considéré comme « en cours », la SCP et le SOC assurent un suivi régulier de son évolution et des actions en cours. Ce suivi est répertorié dans un outil de ticketing commun au SOC et à la SCP. Le traitement des incidents est évoqué régulièrement dans les points bihebdomadaires entre les deux équipes.

Pour qu'un incident de niveau 1 ou 2 puisse être clôturé, un de ces trois critères doit être rempli :
- La fin des actions de remédiation immédiates et leur effectivité.
- Le retour à un niveau de risque acceptable sur le périmètre de l'incident.
- L'incident a été pris en charge par l'acteur externe impacté dont c'est la responsabilité.

Le SOC et la SCP s'assurent qu'un de ces critères est bien rempli et de la bonne information de toutes les parties prenantes à la résolution de l'incident. La fin de l'incident peut alors être entérinée par une décision conjointe entre la SCP et le SOC.

III. Le suivi post-incident

Après la clôture de l'incident, il appartient à la chaîne sécurité numérique de réaliser un suivi pour s'assurer que le retour à une activité normale est durable :
- Le SOC garde un niveau de vigilance adapté sur le SI récemment affecté par un incident.
- La SCP communique la clôture de l'incident au métier.
- Si l'incident a mené à l'élaboration d'un plan d'actions (montée de version, refonte ou décommissionnement d'une solution, etc.), le suivi de ce plan d'actions est à la charge du CSN ou du RSSI de la direction concernée. La section Maîtrise des risques numériques du département HFDS peut également être impliquée dans le suivi et l'implémentation du plan d'actions.
- En fonction de l'incident et de sa gravité, la SCP et le SOC peuvent être amenés à formuler un rapport sur l'incident et son traitement dans un objectif d'amélioration continue.

Remarque : Pour les incidents de niveau 3 ou 4, l'organisation du retour d'expérience est définie par l'annexe A-02 de la PMSN « Plan de gestion des crises d'origine cyber ».

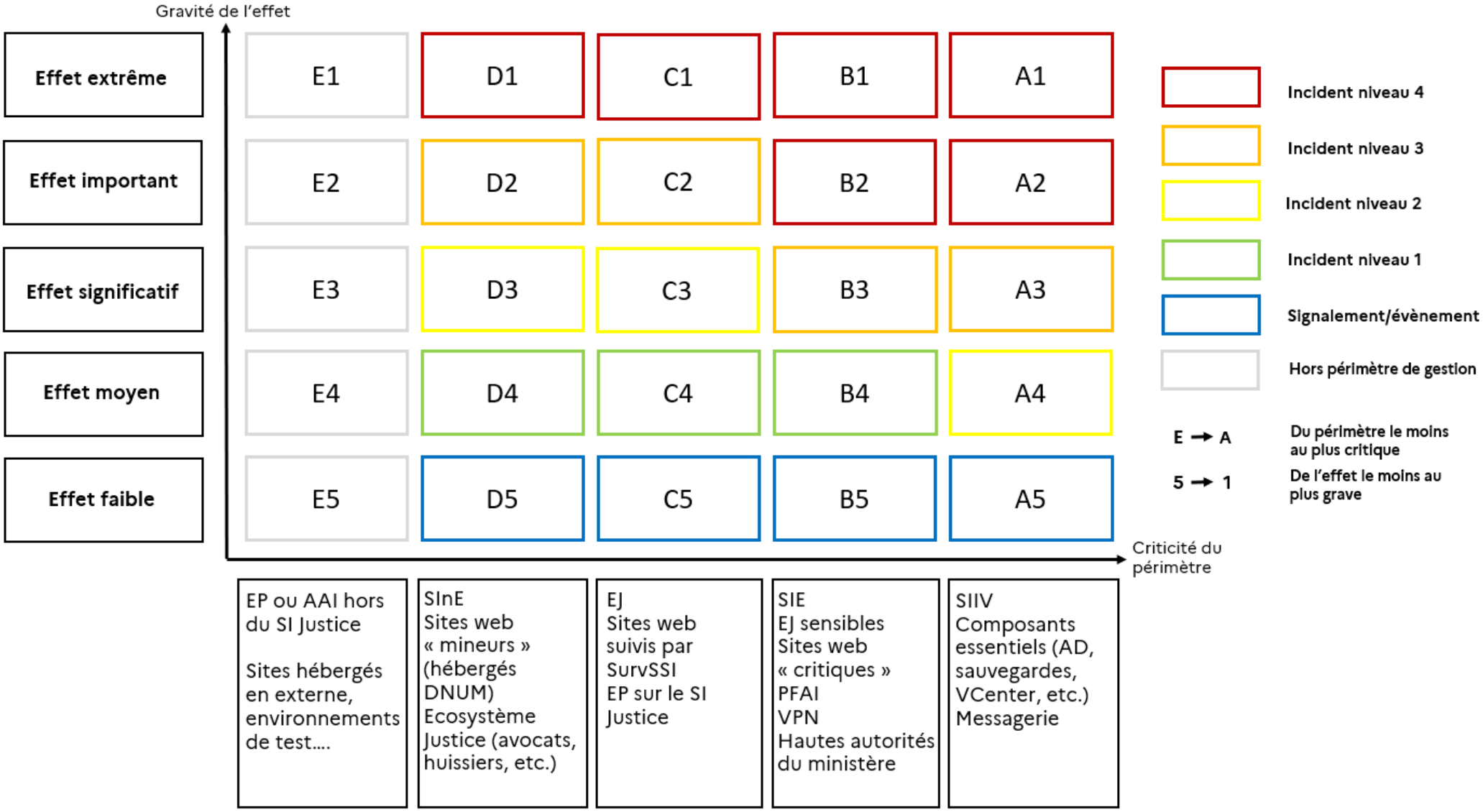
ANNEXES

Annexe 1 : modèle d'annuaire

Annuaire de gestion des incidents de sécurité numérique

DIRECTION OU ETABLISSEMENT PUBLIC					
NOM	Prénom	Fonction	Mobile	Fixe	Mail
Bureau ou sous-division de l'entité					
Bureau ou sous-division de l'entité					

Annexe 2 : matrice de qualification des incidents



MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

SG/DHFDS/BPSN/SMR

Politique de sécurité

-

Démarche d'homologation de sécurité

Annexe B-01 de la PMSN

HISTORIQUE DES MODIFICATIONS

Version	Date	Suivi des modifications
V 0.9	01.09.2025	Initialisation du document par le bureau du pilotage de la sécurité numérique
V 1	21.11.2025	Validation FSSI après prise en compte des remarques des CSN

VALIDATION DU DOCUMENT

Instance	Date
COPIL-SN	Continuation du 21/11/2025

APPROBATION DU DOCUMENT

Instance	Date
COSTRAT-SN	05/12/2025

TABLE DES MATIERES

AVANT PROPOS : LA NOUVELLE DEMARCHE D'HOMOLOGATION

Ce document définit la démarche d'homologation, en s'appuyant sur le dernier guide de l'homologation de sécurité des systèmes d'information produit par l'agence nationale de sécurité des systèmes d'information (ANSSI), dont il embrasse la majorité des mesures en les adaptant au contexte ministériel.

Il s'applique à tous les systèmes d'information (SI) sauf :

- Les systèmes industriels et de sûreté qui font l'objet d'une démarche particulière ;
- Les SI d'infrastructure placés sous l'autorité du directeur du numérique en tant qu'autorité qualifiée (AQSSI). La direction du numérique (DNUM) propose une démarche à la validation des directions utilisatrices de ces SI.

1.1 OBJECTIFS DE LA DEMARCHE D'HOMOLOGATION

Le présent document vise à **simplifier et accélérer** la démarche d'homologation. Pour y contribuer, il intègre une démarche en **trois niveaux** de sécurité (simplifié, intermédiaire et renforcé).

L'attention du lecteur est portée sur **la stratégie d'homologation**, un des livrables clé de cette nouvelle démarche. Elle inclut ses objectifs macro, une estimation du niveau de risque et la planification des ressources nécessaires à l'homologation.

Le document offre la possibilité :

- D'organiser les comités d'homologation dématérialisés et aux AQSSI de signer les décisions via un parapheur électronique ;
- D'homologuer les systèmes non essentiels à l'aide de l'outil *Mon Service Sécurisé* (https://monservicesecurise.cyber.gouv.fr/).

1.2 MESURES TRANSITOIRES

Tout système d'information non homologué devrait, en principe, être mis hors service conformément aux recommandations du guide de l'ANSSI.

- A titre dérogatoire, la présentation d'un plan d'actions correctif accompagné d'un rapport de test d'intrusion peut justifier une homologation de courte durée, le temps de constituer un dossier complet, conforme aux exigences ministérielles.
- Même les systèmes dont le décommissionnement est prévu doivent faire l'objet d'une homologation. Le plan d'actions prévoit des mesures conservatoires et de décommissionnement. La décision d'homologation indique alors la date prévisionnelle de décommissionnement du SI. Il est conseillé d'avoir une date d'homologation de 3 à 6 mois au-delà de la date de décommissionnement.

Cette démarche ne traite pas des systèmes classifiés de défense et soumis à l'IGI 1300.

LA DEMARCHE D'HOMOLOGATION

L'emploi d'un système d'information peut entraîner des risques ayant des impacts graves pour une activité. Afin d'en garantir une maîtrise raisonnée, il convient de définir ce qu'est une homologation de sécurité.

2.1 DEFINITION D'UNE HOMOLOGATION

L'homologation de sécurité est une démarche formalisée permettant à une autorité de décider, en connaissance de cause, de l'exploitation d'un système d'information. Elle repose sur une analyse structurée et documentée des menaces pesant sur le système, des mesures mises en œuvre et des risques résiduels.

Elle se conclut par une décision formelle de l'autorité d'homologation (AH), par laquelle celle-ci atteste que les risques sont connus et acceptés et que les mesures de sécurité sont adaptées aux besoins de sécurité du SI.

Un système d'information peut être homologué, même si certains risques demeurent non traités, dès lors qu'ils sont jugés acceptables par l'autorité et que les actions de remédiation sont programmées.

2.2 PRINCIPES DE L'HOMOLOGATION

La démarche d'homologation permet l'intégration de la sécurité numérique **tout au long du projet** et de l'exploitation du SI et doit être renouvelée périodiquement jusqu'à son décommissionnement.

L'homologation vise à :

- Intégrer la sécurité dès la conception du projet ;
- Adapter les mesures aux enjeux du système (usages, données, contexte) ;
- Garantir la connaissance et l'acceptation des risques.

Elle doit être engagée dès le lancement du projet et associer, en cas de traitement de données à caractère personnel, le référent informatique et libertés (RIL). Elle vise également à démontrer le respect des obligations de sécurité prévues par la réglementation en matière de protection des données (RGPD et loi du 6 janvier 1978 relative à l'informatique et aux libertés).

L'homologation n'est ni une certification, ni un audit technique. Elle formalise un engagement de responsabilité.

2.3 CADRE REGLEMENTAIRE

Conformément à la PMSN-MJ, tout système d'information du ministère doit être homologué.

L'homologation est en outre rendue obligatoire par différents textes, et en particulier le 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.

Il revient à la maîtrise d'ouvrage, avec l'appui du conseiller à la sécurité numérique (CSN), d'identifier les textes applicables dans la stratégie d'homologation.

LES ETAPES DE LA DEMARCHE D'HOMOLOGATION

3.1 CADRAGE DE LA DEMARCHE

3.1.1 IDENTIFIER LE NIVEAU DE LA DEMARCHE

L'identification du niveau de démarche d'homologation repose sur une double évaluation prenant en compte la criticité du système d'information et son exposition aux sources de risque numérique. **L'objectif est de rester pragmatique et d'éviter les surcoûts.**

Elle correspond aux deux premières étapes du guide de l'ANSSI[1]. Elle suppose une appréciation fine des **impacts potentiels pour l'organisation** en cas d'incident, ainsi que des vecteurs d'attaque possibles selon l'utilisation du système.

Trois niveaux de démarche, découlant de cette analyse, sont proposés : une démarche **simplifiée** pour les systèmes non essentiels (SInE), une démarche **intermédiaire** pour les systèmes essentiels (SIE), une démarche **renforcée** pour les systèmes d'importance vitale (SIIV) et les systèmes d'information à diffusion restreinte (SI DR).

Le responsable fonctionnel et le CSN planifient et préparent la réunion de lancement ; ils identifient les contributeurs (parties prenantes) du projet, cadrent le périmètre, présentent la démarche, les attendus pour chacun des participants, établissent la stratégie et formalisent les jalons initiaux.

Si le modèle de stratégie d'homologation est à la discrétion de chaque CSN, l'emploi d'un scoring est en revanche obligatoire. Cette étape inclut également la constitution du comité d'homologation.

3.1.2 LIVRABLE : STRATEGIE D'HOMOLOGATION

La réunion de lancement doit permettre de renseigner la stratégie d'homologation. Cette dernière cote numériquement la criticité et les besoins de sécurité du système afin de déterminer la démarche la plus adaptée. Cette étape est indispensable pour identifier les livrables inclus dans le dossier d'homologation. Le CSN sélectionne les audits à engager en tenant compte du projet, des risques identifiés et des résultats des précédents audits.

Sa validation est à la charge des responsables métiers, qui fixe les objectifs de sécurité ; il est recommandé qu'elle soit réalisée de manière conjointe avec le chef de projet de la maîtrise d'œuvre (MOE), le RSSI de la MOE, le CSN et le RIL de la direction concernée.

Le niveau retenu doit faire l'objet d'un consensus du comité d'homologation et peut évoluer dans le temps en fonction des changements du système ou de son environnement.

La direction de projet ou le CSN peuvent proposer de mener une démarche de niveau supérieur. L'AH statue alors définitivement sur le niveau retenu.

Lorsque la stratégie d'homologation concerne des SI non essentiels et recommande une démarche simplifiée, celle-ci peut être menée avec l'outil MonServiceSécurisé[1]. Pour les SI non essentiels, le CSN peut être désigné AH.

[1] Cf. § 3.2.1 à 3.2.3 du guide L'homologation de sécurité des systèmes d'information | ANSSI

Sélection du niveau de la démarche d'homologation de la sécurité			
	Exposition faible	Exposition importante	Exposition totale
SIIV	Renforcé	Renforcé	Renforcé
SIE	Intermédiaire	Intermédiaire	Renforcé
SInE	Simplifié	Simplifié	Intermédiaire

Exposition faible : SI ouvert uniquement sur des réseaux maîtrisés (ex : intranet).
Exposition importante : SI indirectement ouvert sur des réseaux non maîtrisés (par exemple à l'aide d'interconnexion de SI avec tunnel TLS). L'accès est possible au seul personnel habilité par l'entité et n'autorise pas les accès nomades.
Exposition totale : SI directement ouvert sur Internet pour tous les types d'utilisateurs et d'équipements.

3.2 CONSTITUER LE DOSSIER D'HOMOLOGATION

Le dossier d'homologation regroupe l'ensemble des documents permettant au comité d'homologation de donner un avis et de conseiller l'autorité d'homologation (AH) pour prendre une décision éclairée[2].

3.2.1 LIVRABLES CYBER

- **Stratégie d'homologation**

Définit les enjeux de sécurité, le niveau de démarche, précise le socle de conformité aux référentiels (ex : un SIIV doit se conformer à l'II 901, à la LPM ...) et les livrables requis.

- **Déclaration d'applicabilité (DdA)**

Contient les moyens de maîtrise de risque nécessaires, leur justification de leur inclusion et leur statut de mise en œuvre. Une priorisation (*must / should / may*) peut être indiquée.

- **Analyse de risques**

Etablie de préférence selon la méthode EBIOS RM, identifie les menaces, les vulnérabilités, les impacts et les risques résiduels. Pour simplifier la lecture et la compréhension des enjeux du SI, une

[2] Cf. chapitre 3.2.4 du *guide de l'homologation de sécurité des systèmes d'information* de l'ANSSI.

synthèse managériale peut être fournie. Les homologations effectuées avec MSS ne comportent pas d'analyse de risques.

- **Procédures d'exploitation de sécurité**

Décrivent les actions liées à la sécurité opérationnelle. : gestion des comptes, sauvegarde, maintien en condition opérationnelle (MCO) et en sécurité (MCS), etc.

- **Rapports techniques et d'expertise**

  - Audit d'**architecture** : conformité aux bonnes pratiques d'urbanisation des SI.
  - Audit de **configuration** : vérification des équipements (OS, serveurs, logiciels…).
  - Audit de **code source** : recherche de failles (ex. stockage de mots de passe).
  - Test d'**intrusion** (ou *pen test*) : évaluation de la robustesse face à une attaque.

Les prestataires d'audits qualifiés PASSI intègrent l'ensemble des audits et tests d'intrusions mentionnés dans ce point.

  - **Campagnes de *bug bounty*** : tentative d'intrusion par des hackers éthiques, recherches de vulnérabilités en échange de récompenses proportionnées à la gravité des failles signalées.

- **Procédure de gestion des incidents de sécurité numérique**

Déclinaison opérationnelle de la politique de traitement des incidents de sécurité numérique ministérielle (annexe A-01 de la PMSN-MJ) ; à défaut d'une déclinaison au sein de la direction, elle doit être réalisée au niveau du projet.

- **Convention de service de supervision de sécurité**

Accord avec un prestataire en détection d'incident de sécurité (PDIS), interne ou externe, précisant les modalités de détection des incidents.

- **Plan de traitement des risques**

Synthèse des actions issues de l'analyse de risques et des audits, incluant les mesures, responsables, échéances et statuts.

- **Support de présentation du comité d'homologation**

Document synthétique présenté au comité d'homologation. Il comporte à titre informatif une planche sur l'état de la conformité IL (validée par le DPD) si le SI traite des données à caractère personnel et une planche mentionnant l'avis du FSSI[3].

- **Décision d'homologation**

Signée par l'AH, exprimant l'acceptation totale ou sous réserves ou le refus des risques résiduels.

[3] Les modèles sont proposés en annexe. La planche présentant l'avis du FSSI, conformément à la PMSN-MJ au paragraphe 31-21, constitue son avis formel.

- **Audit organisationnel et physique**

L'audit organisationnel et physique[4] consiste à évaluer le niveau de conformité et/ou de sécurité de la gouvernance, des politiques et procédures de sécurité mises en œuvre pour assurer le maintien en conditions de sécurité du système d'information audité. L'audit organisationnel et physique peut couvrir l'évaluation de la protection des ressources physiques du système d'information audité comme par exemple les systèmes de contrôle d'accès physique, de détection d'intrusions physiques, de vidéoprotection, de prévention des risques naturels (incendie, inondations, etc.).
Cet audit n'est requis que pour l'homologation d'un SIIV.

La conformité de la sécurité physique relève de la responsabilité de l'officier de sécurité (OS). L'OS et le responsable du site confirment la capacité des infrastructures physiques à héberger un SIIV mais ne communiquent pas les rapports d'audit physique.

3.2.2 LIVRABLE PROJET

- **Dossier d'architecture**

Document détaillant l'architecture fonctionnelle (DAF), applicative et technique (DAT) du SI faisant l'objet de la démarche d'homologation. Ils concourent au dossier mais ils ne sont pas produits par les acteurs de la sécurité numérique.

[4] Source : référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information version 2.2 (2024).

3.2.3 SYNTHESE DES LIVRABLES

Livrable	Simplifié	Intermédiaire	Renforcé
Stratégie d'homologation	✓	✓	✓
Déclaration d'applicabilité		✓	✓
Analyse de risques	✓ *	✓ **	✓
Procédures d'exploitation de sécurité		✓	✓
Rapports techniques et d'expertises			✓
Procédure de gestion des incidents de sécurité numérique			✓
Convention de service de supervision de sécurité			✓
Plan de traitement des risques	✓	✓	✓
Support de présentation du comité d'homologation		✓	✓
Décision d'homologation	✓	✓	✓
Dossier d'architecture technique	✓	✓	✓

* Afin de faciliter la démarche, il est recommandé de passer par Mon Service Sécurisé
** Dans le cadre d'une analyse de risque EBIOS RM, tous les ateliers ne sont pas nécessaires (à minima les ateliers 1 et 5 doivent être effectués).

3.2.4 MATRICE DE RESPONSABILITE PAR LIVRABLE

La matrice, issue de la comitologie projet, est transcrite dans la stratégie d'homologation. La matrice présentée peut être adaptée selon les spécificités du projet et de la direction.

Livrables cyber	Exploitation	Maître d'œuvre	Resp. cyber du projet	Fonctionnel	CSN	AQSSI	FSSI	DPD
Stratégie d'homologation		C	C	R	R	A	C	I
Déclaration d'applicabilité		R	R	C	A		C	I
Analyse de risques		R	R	R	A		C	I
Procédures d'exploitation de sécurité	R	R	A	C	C		I	I
Rapports techniques et d'expertise	R	R	A	C	C		I	I
Procédure de gestion des incidents de SN		C	R	C	A		I	I
Convention de service de supervision de sécurité		R	A	R	C		I	I
Plan de traitement des risques		R	R	C	C	A	I	I
Support de présentation de la commission d'homologation		C	R	R	A	I	C	C
Décision d'homologation	I	C	C	C	R	A	C	C
Livrable projet								
Dossier d'architecture technique			C		I		I	I

Légende : Réalisateur, Approbateur, Consulté, Informé.

Responsable cyber du projet : acteur responsable des travaux d'homologation de sécurité qui prenne en compte l'ensemble des aspects cyber techniques et organisationnels et qui peut être dans la MOA, la MOE, le CSN ou le RSSI.

3.3 HOMOLOGUER LE SYSTEME D'INFORMATION

3.3.1 PRE-COMITE D'HOMOLOGATION

Le pré-comité vise à anticiper les débats et à lever toute ambiguïté avant le comité formel. **Il est obligatoire pour les SIIV et fortement recommandé pour les SIE.**

Le dossier d'homologation complet chiffré doit être transmis au bureau du FSSI dès que possible et au moins une semaine avant l'échéance. L'avis du FSSI est préparé avant le comité afin de garantir une instruction fluide. Il est recommandé de composer le pré-comité comme suit :

Composition du pré-comité d'homologation

Membres permanents

- CSN
- Chef de projet MOA
- Chef de projet MOE
- Représentant FSSI
- Représentant DPD
- RCSSI MOA
- RSSI MOE

Membres invités

- Experts
- Partenaires et prestataires

Cette composition peut toutefois être adaptée en fonction des spécifiés d'un projet particulier.

3.3.2 COMITE D'HOMOLOGATION

Le comité d'homologation, présidée par l'AQSSI ou l'AH, est organisé par la direction de projet, avec l'appui du CSN. Le FSSI et le DPD y participent de droit.

Le chef d'un service à compétence national peut être désigné autorité d'homologation pour tout système d'information outillant son activité, y compris un système d'information d'importance vitale.

Le CSN évalue la pertinence de faire intervenir des prestataires externes ou des partenaires institutionnels en lien avec le FSSI.

Le comité d'homologation n'est pas l'instance de débats ou de décisions techniques : le support et les échanges doivent être axés sur le métier. Ce faisant, le comité d'homologation ne doit pas excéder une heure.

Composition du comité d'homologation				
Démarche simplifiée	Démarche intermédiaire		Démarche renforcée	
	Membres permanents	**Membres facultatifs**	**Membres permanents**	**Membres facultatifs**
La procédure étant dématérialisée, la composition de la commission d'homologation intègre, a minima, le CSN.	- AQSSI / AH - CSN - Chef de projet MOA - Chef de projet MOE - R(C)SSI métier - RCSSI DNUM - FSSI - DPD	- Partenaires institutionnels - Experts techniques	- AQSSI / AH - CSN - Chef de projet MOA - Chef de projet MOE - R(C)SSI métier - RCSSI DNUM - DNUM - FSSI - DPD	- ANSSI - Partenaires institutionnels - Experts techniques

3.4 DECISION D'HOMOLOGATION

L'AH prononce une décision formelle[5]. Si l'homologation est acceptée, elle fixe :

- La durée de validité de l'homologation (maximum 3 ans) ;
- La fréquence minimale du comité de suivi des risques numériques, au moins semestrielle pour un SI essentiel ou vital ;
- Eventuellement, les conditions ou réserves assorties à l'homologation.

En cas de refus, l'autorité fixe les objectifs à atteindre pour réévaluer le dossier.

Toute décision de refus d'homologation est accompagnée, soit d'une décision de maintien en production du système d'information, soit d'une décision d'arrêt.

[5] Deux modèles de décision – refus ou acceptation - sont proposés en annexe.

POST HOMOLOGATION

4.1 SUIVI DE L'HOMOLOGATION

Le plan de traitement des risques doit être suivi via un comité dédié. Sa fréquence est fixée dans la décision d'homologation.
Ce comité vise à :

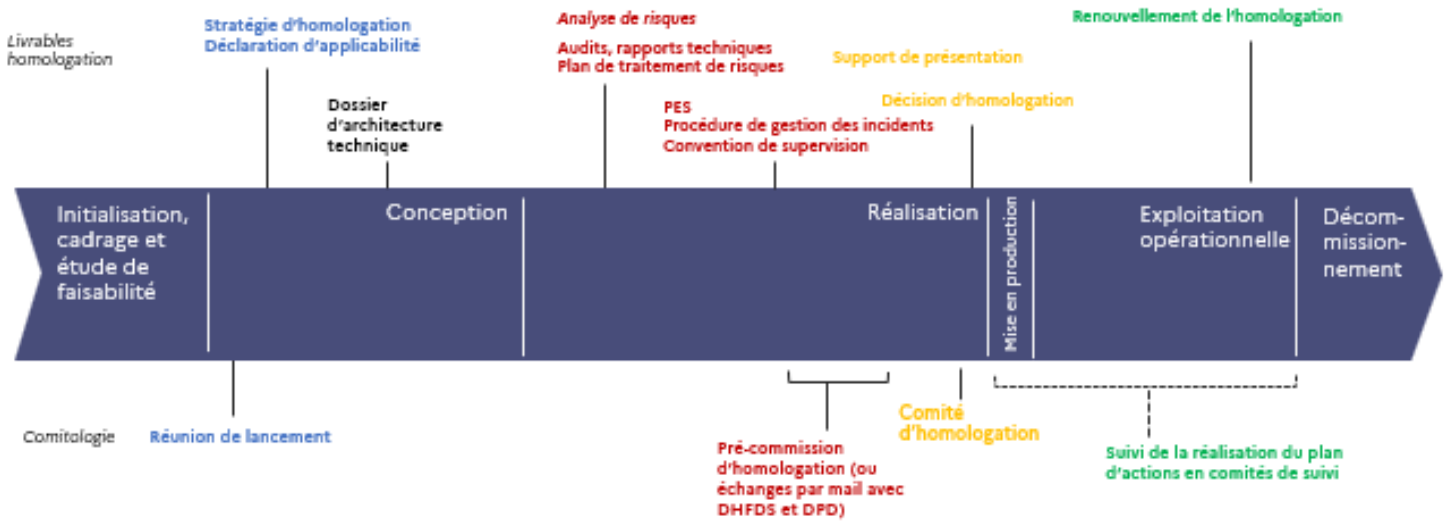
- Suivre l'avancement des actions correctives et préventives ;
- Evaluer l'impact des évolutions du SI (techniques, fonctionnelles) sur la sécurité numérique ;
- Assurer le lien avec les instances ministérielles (CoGeR, DPD).

Conformément à la PMSN-MJ, chaque direction met en œuvre un comité de gestion de risque. Si le projet est un SIIV, il est impérativement suivi semestriellement en CoGeR.

4.2 CADUCITE DE L'HOMOLOGATION

Toute modification majeure (architecture, traitement, exposition) du SI rend l'homologation caduque. Une mise à jour du dossier et une nouvelle décision d'homologation sont alors nécessaires.

4.3 SYNCHRONISATION DES LIVRABLES CYBER DANS LA CONDUITE DE PROJET



Signé
électroniquement :
MICHEL Samuel
Le 03/02/2026 UTC(OP)