Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

Arrêté du 19 juillet 2024 portant approbation de l'instruction ministérielle relative à la politique de gouvernance de la sécurité numérique (PGSN) de l'éducation nationale, de la jeunesse, des sports, de l'enseignement supérieur et de la recherche

NOR : *MENG2420767A*

La ministre de l'éducation nationale et de la jeunesse, la ministre des sports et des jeux Olympiques et Paralympiques et la ministre de l'enseignement supérieur et de la recherche,

Vu le code de la défense, notamment ses articles L. 1111-3, R.* 1132-1 à D. 1132-54 et R. 1143-1 à D. 1143-13 ;

Vu le code de l'éducation ;

Vu le code du sport ;

Vu le décret modifié 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 ;

Vu l'arrêté du 26 juin 2024 modifiant l'arrêté du 17 février 2014 modifié fixant l'organisation de l'administration centrale des ministères de l'éducation nationale, de la jeunesse et des sports et de l'enseignement supérieur et de la recherche ;

Vu l'instruction générale interministérielle n° 1337/SGDSN/ANSSI approuvé par arrêté du 26 octobre 2022 relatif à l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics,

Arrêtent :

Art. 1er. – L'instruction ministérielle sur la politique de gouvernance de la sécurité du numérique (PGSN) de l'éducation nationale, de la jeunesse, des sports, de l'enseignement supérieur et de la recherche, annexée au présent arrêté, est approuvée.

Art. 2. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 19 juillet 2024.

La ministre de l'éducation nationale
et de la jeunesse,
Pour la ministre et par délégation :
Le secrétaire général,
haut fonctionnaire de défense et de sécurité,
T. Le Goff

La ministre des sports
et des jeux Olympiques et Paralympiques,
Pour la ministre et par délégation :
Le secrétaire général,
haut fonctionnaire de défense et de sécurité,
T. Le Goff

La ministre de l'enseignement supérieur
et de la recherche,
Pour la ministre et par délégation :
Le secrétaire général,
haut fonctionnaire de défense et de sécurité,
T. Le Goff

ANNEXE

POLITIQUE DE GOUVERNANCE DE LA SÉCURITÉ NUMÉRIQUE (PGSN) DE L'ÉDUCATION NATIONALE, DE LA JEUNESSE, DES SPORTS, DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

1. **Préambule**

L'Etat a actualisé, par le décret n° 2022-513 du 8 avril 2022 et l'arrêté du 26 octobre 2022 n° 1337/SGDSN/ANSSI, les principes de l'organisation de la sécurité numérique de l'Etat et de ses établissements publics.

La présente politique en est la déclinaison pour les périmètres ministériels concernés.

2. **Périmètre d'application**

La présente instruction s'applique à l'ensemble des services centraux, des services déconcentrés et des établissements publics relevant du ministère de l'éducation nationale et de la jeunesse, du ministère de l'enseignement supérieur et de la recherche et du ministère des sports et des jeux olympiques et paralympiques.

3. **La chaîne fonctionnelle de la sécurité numérique**

Cette chaîne fonctionnelle est constituée :

– des ministres ;
– du haut fonctionnaire de défense et de sécurité (HFDS), secrétaire général des ministères, assisté du haut fonctionnaire adjoint de défense et de sécurité (HFaDS) ;
– du fonctionnaire de sécurité des systèmes d'information (FSSI), assisté de FSSI adjoints (FSSIa) ;
– des autorités qualifiées de la sécurité des systèmes d'information (AQSSI) ;
– des conseillers à la sécurité numérique (CSN) auprès des AQSSI ;
– des responsables de la sécurité des systèmes d'Information (RSSI) ;

– du directeur du numérique pour l'éducation (DNE), des directeurs régionaux académiques des SI (DRASI), des directeurs inter-académiques des SI (DIASI) et des directeurs des systèmes d'information en établissements publics (DSI) ;
– des centres de réponse à incident de sécurité des SI, constitués par le COSSIM et le CERT-RENATER ;
– de pôles nationaux d'appuis et de ressources pour la sécurité numérique.

Pour les établissements publics relevant de tutelles multiples, une chaine fonctionnelle de référence pour la sécurité numérique est déterminée par les hauts fonctionnaires de défense et de sécurité des périmètres ministériels concernés.

4. **Rôles et responsabilités des acteurs de la sécurité numérique**

Les rôles et responsabilités, issus de l'instruction générale interministérielle n° 1337 du 26 octobre 2022, sont précisés en annexe de la présente instruction.

4.1. *Les autorités qualifiées de la sécurité des systèmes d'information (AQSSI)*

L'autorité qualifiée de la sécurité des systèmes d'information (AQSSI) est responsable de la sécurité des systèmes d'information et de communication qui contribuent à l'exécution des missions et du périmètre dont elle a la charge. L'AQSSI ne peut déléguer cette responsabilité.

Le HFDS tient à jour un registre ministériel des autorités qualifiées de la sécurité des systèmes d'information.

Sont désignés AQSSI en administration centrale :

– les directeurs et délégués d'administration centrale ;
– les chefs de service rattachés au secrétaire général ;
– le directeur du numérique pour l'éducation, pour les services numériques transverses à portée nationale ou ne relevant pas des attributions d'autres directions métiers ;
– le secrétaire général, pour le numérique spécifique aux équipes internes du secrétariat général ;
– la cheffe de service de l'inspection générale de l'éducation, du sport et de la recherche, pour le numérique spécifique à l'inspection générale ;
– le chef du bureau des cabinets, pour le numérique spécifique aux cabinets ;
– chaque directeur de service à compétence nationale.

Sont désignés AQSSI en services déconcentrés :

– les recteurs de région académique, pour le numérique en responsabilité directe de la région académique et les éventuels services de région académique ;
– les recteurs d'académie, pour le numérique de portée académique et les éventuels services inter-académiques sous leurs responsabilités.

Sont désignés AQSSI en établissements publics relevant de la tutelle ministérielle :

– les dirigeants exécutifs d'établissement public de l'Etat, pour leur périmètre de missions. Il s'agit notamment des présidents ou directeurs généraux des :
  – établissements publics à caractère scientifique, culturel et professionnel (EPSCP) ;
  – établissements publics scientifiques et techniques (EPST) ;
  – établissements publics administratifs (EPA) ;
  – établissements publics à caractère industriel et commercial (EPIC) ;
  – établissements publics locaux de formation (EPLF) du secteur sport.

Concernant les établissements publics locaux d'enseignement (EPLE) :

En application des dispositions de la loi d'orientation et de programmation pour la refondation de l'Ecole de la République du 8 juillet 2013 (1), la maintenance et l'équipement informatique des établissements publics locaux d'enseignement (EPLE) sont à la charge des collectivités territoriales, à l'exception des services numériques contractualisés directement par le chef d'établissement. Le contrôle de l'application des référentiels de sécurité ainsi que le traitement des incidents de niveau majeur relèvent d'un traitement conjoint entre les RSSI académiques, qui sont en charge du signalement des incidents de sécurité numérique auprès du centre opérationnel de la sécurité des systèmes d'information du ministère (COSSIM), et les RSSI des collectivités territoriales.

Chaque chef d'établissement, sans être AQSSI, constitue le point de contact de la sécurité numérique pour les services déconcentrés de l'éducation nationale, notamment en cas d'incident de sécurité du numérique qui impacte fortement les activités de son établissement.

Chaque académie maintient un annuaire des points de contacts en EPLE.

4.2. *Les conseillers à la sécurité numérique (CSN)*

Le conseiller à la sécurité numérique conseille et accompagne l'autorité qualifiée dans l'exercice de ses responsabilités pour la maitrise des risques numériques.

Le CSN assiste l'AQSSI pour l'homologation des systèmes d'information, il dispose de la connaissance des enjeux métiers et des politiques publiques en responsabilité. Sans être un expert de la sécurité numérique, le CSN

dispose d'une culture générale du numérique lui permettant de traduire et contextualiser les enjeux pour le compte de son AQSSI. Il contribue à l'animation de la sécurité numérique dans le périmètre de responsabilité de son AQSSI. Une description type des missions d'un conseiller à la sécurité numérique est précisée en annexe.

L'obligation réglementaire de désignation de CSN varie selon le type d'organisation :

En administration centrale :

– chaque AQSSI désigne un CSN pour son périmètre de missions et en informe le HFDS qui maintient un registre des CSN ;
– le CSN est nécessairement un acteur du pilotage et de la gouvernance du périmètre. A ce titre, il fait partie du comité de direction du périmètre.

En services déconcentrés :

– en accord avec les recteurs d'académie du périmètre, le recteur de région académique peut désigner un CSN de région académique (CSN-RA) agissant pour l'ensemble des académies ;
– à défaut de CSN de région académique, chaque recteur d'académie désigne un CSN (CSN-A) ;
– le CSN est nécessairement un acteur du pilotage et de la gouvernance du périmètre. A ce titre, il fait partie du comité de direction du périmètre ;
– le recteur de région académique informe le HFDS de l'organisation choisie et désigne le ou les CSN au HFDS, qui en tient compte dans le registre ministériel des CSN.

En établissement public, la nomination d'un conseiller à la sécurité numérique n'est pas attendue.

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

Le responsable de la sécurité des systèmes d'information (RSSI) est l'acteur clé de la sécurité opérationnelle d'un périmètre d'activité. Il dispose d'une lettre de mission ou d'une fiche de poste signée par l'AQSSI ou le dirigeant.

En administration centrale :

– le secrétaire général désigne un RSSI ministériel (RSSI-M) dont le mandat comprend le numérique ministériel et des missions nationales. Le RSSI ministériel dispose de RSSI ministériels adjoints (RSSIa-M), chacun disposant d'un mandat précisant son périmètre. Il anime le réseau des RSSI académiques et des correspondants à la SSI (CSSI) en administration centrale, en lien avec le FSSI. Les RSSI ministériels adjoints contribuent à la continuité des missions de RSSI ministériel ;
– les AQSSI, autres que le DNE, agissant en maitres d'œuvre (conception, développement, maintenance) de systèmes d'information, disposent nécessairement d'un responsable de la sécurité des systèmes d'information. Ce RSSI est affecté à la DNE dans le service en charge de la sécurité numérique. Néanmoins, en accord avec le secrétaire général, l'AQSSI peut désigner un RSSI, nécessairement dédié à cette fonction, affecté dans son service. A défaut, l'AQSSI désigne un correspondant à la sécurité des SI (CSSI) ;
– la liste des RSSI et des CSSI des ministères est maintenue par le HFDS ;
– l'AQSSI s'assure que le RSSI ministériel dispose de la visibilité complète sur les SI et les projets numériques du périmètre.

En services déconcentrés, selon l'un des schémas d'organisation suivants :

– première modalité d'organisation :
  – un RSSI de région académique (RSSI-RA), occupant ces missions à temps plein, nommé par le recteur de région et les recteurs d'académie. Le RSSI-RA pilote et coordonne les acteurs de la SSI de l'ensemble régional ;
  – associé à un RSSI adjoint par académie (RSSIa-A), agissant au moins 50 % de son temps pour les missions de sécurité numérique ;
  – le RSSI-RA et le(s) RSSIa-A participent à la continuité des missions de RSSI pour la plaque territoriale ;
– la seconde modalité d'organisation est réservée aux régions mono-académiques :
  – un RSSI d'académie (RSSI-A) agissant à temps plein sur la sécurité numérique est nommé par le recteur d'académie ;
  – associé, *a minima*, à un RSSI adjoint d'académie (RSSIa-A) agissant à minima à 30 % de son temps pour la sécurité numérique ;
  – le RSSIa-A participe à la continuité des missions du RSSI-A.

Il est recommandé que les RSSI de région académique et d'académie s'appuient sur des correspondants pour la sécurité des SI (CSSI) dans les directions des services départementaux de l'éducation nationale (DSDEN).

Dans les établissements publics :

Du fait de la diversité des structures, il est déterminé deux profils de RSSI :

Pour les établissements publics à portée nationale, disposant de réseaux de délégations ou directions territoriales (opérateurs nationaux de la recherche ou de l'enseignement) :

- le dirigeant désigne un RSSI national (RSSI-N) disposant du mandat pour l'ensemble de l'établissement public et de ses implantations ;
- le RSSI-N constitue le point de contact pour la sécurité numérique de l'établissement. A ce titre, il est nommé par le dirigeant, au sein de l'établissement et dispose d'un lien fonctionnel avec lui ;
- il est recommandé que le RSSI national dispose d'au moins un RSSI national adjoint (RSSIa-N) ;
- les RSSI-N et RSSIa-N s'appuient sur un réseau identifié et formalisé de correspondants à la SSI (CSSI), par exemple dans chaque centre, campus ou site, laboratoire de recherche, etc.

Pour tous les autres établissements publics :

- le dirigeant désigne un RSSI disposant de l'ensemble du mandat pour l'ensemble de l'établissement ;
- le RSSI constitue le point de contact pour la sécurité numérique de l'établissement. A ce titre, il est nommé par le dirigeant parmi les personnels de l'établissement. Quelle que soit son affectation dans la structure, il dispose d'un lien fonctionnel avec le dirigeant de l'établissement ;
- le RSSI d'établissement s'appuie sur des RSSI suppléants ou adjoints afin d'assurer la continuité des missions du RSSI et d'être en mesure de couvrir l'ensemble du périmètre de l'établissement et de ses composantes ;
- si cela est adapté au contexte de l'établissement, le RSSI s'appuie sur un réseau identifié et formalisé de correspondants à la SSI (CSSI).

4.4. *Les centres de réponse à incident de sécurité du numérique*

Les centres de réponse à incident de sécurité du numérique reçoivent et traitent les déclarations d'incidents des entités relevant de leurs mandats. Ils réalisent l'assistance à leurs bénéficiaires dans l'analyse des symptômes, le diagnostic, le traitement et la réaction aux incidents. Ils se coordonnent avec d'autres centres de réponse à incidents, en lien avec le centre national de réponse aux incidents (ANSSI/CERT-Fr). Ils diffusent des alertes et des recommandations. Ils sont susceptibles de prendre des mesures de mise en protection immédiate face à une menace majeure confirmée et imminente.

Le centre opérationnel de la sécurité des systèmes d'information ministériels (COSSIM) est le centre ministériel de référence pour l'assistance et le suivi des incidents de sécurité numérique des services centraux et déconcentrés et des établissements publics relevant du périmètre ministériel. Le COSSIM est positionné à la DNE, dans la sous-direction du socle numérique et dispose d'un lien fonctionnel avec le HFDS.

Pour les EPLE, le COSSIM s'appuie sur les RSSI de région académique et d'académie qui assistent les EPLE, en lien avec les collectivités territoriales. Les RSSI académiques signalent les incidents significatifs (2) des EPLE au COSSIM.

Pour les établissements de l'enseignement supérieur et de la recherche, le COSSIM s'appuie sur le CERT-RENATER qui prend en compte les signalisations initiales de ce périmètre, qualifie et assiste les établissements.

Le CERT (3)**-RENATER** est le centre de signalisation et d'expertises réseaux pour les incidents de sécurité du numérique :

- des établissements publics relevant de la tutelle du ministère de l'enseignement supérieur et de la recherche et raccordés à RENATER ;
- de toute autre entité raccordée au réseau RENATER, à l'exclusion et sans préjudice de dispositions spécifiques existantes pour les établissements publics relevant de tutelles ministérielles autres que celle de l'enseignement supérieur et de la recherche.

Le CERT-RENATER partage avec le COSSIM et le FSSI tous les incidents significatifs (2) affectant des établissements relevant de la tutelle du ministère de l'enseignement supérieur et de la recherche.

Le CERT-RENATER peut, avec l'accord du FSSI ou à défaut du COSSIM, mettre en œuvre des actions de mise en protection immédiate d'un établissement raccordé dans le cas d'une menace majeure confirmée et imminente, en particulier lorsque ni le RSSI ni l'AQSSI de l'établissement n'ont pu être contactés.

Le CERT-RENATER peut demander l'appui du COSSIM pour la remédiation d'établissements relevant de l'enseignement supérieur et de la recherche.

Le CERT-RENATER peut inviter le RSSI d'un établissement relevant de l'enseignement supérieur et de la recherche à solliciter le COSSIM pour bénéficier d'un appui à la remédiation d'incidents. Tous les incidents dont la gravité estimée est supérieure ou égale à « 3 – important » doivent faire l'objet d'une assistance conjointe avec le COSSIM.

Le FSSI dispose d'une visibilité complète sur les incidents suivis par le COSSIM et le CERT-RENATER et dispose, via le HFDS, d'un lien fonctionnel avec les centres de réponse à incidents.

Le COSSIM et le CERT-RENATER participent à la cellule opérationnelle de crise cyber (COCC), coordonnée par le FSSI en lien avec le dispositif ministériel de veille et d'alerte (CMVA) et le centre ministériel de crise (CMC).

4.5. *Les pôles nationaux d'appuis et de ressources pour la sécurité numérique*

Chaque ministère peut composer des pôles nationaux d'appuis et de ressources pour la sécurité numérique.

La liste complète des pôles nationaux du numérique, décrivant leurs missions et leur organisation, est communiquée annuellement au FSSI.

Selon leurs missions et compétences, les pôles nationaux d'appuis et de ressources pour la sécurité numérique peuvent être sollicités par le FSSI pour participer au dispositif ministériel de gestion de crises nationales d'origine cyber.

5. **Les instances ministérielles de la sécurité du numérique**

L'organisation des instances ministérielles pour la sécurité du numérique est déclinée selon les principes définis dans l'instruction interministérielle n° 1337/PM/SGDSN/ANSSI.

Un comité stratégique ministériel de la sécurité du numérique (COSTRAT SECNUM) est constitué par ministère. Il est présidé par le ministre ou son représentant et se réunit au moins une fois par an. Le HFDS en assure le secrétariat.

Il présente les synthèses de sécurité numérique du périmètre ministériel et détermine les orientations stratégiques pour la sécurité du numérique.

Le COSTRAT SECNUM MENJ associe les AQSSI ministériels, un AQSSI représentant les régions académiques, un AQSSI représentant les académies, le DNE ou son représentant, le FSSI et le RSSI ministériel. Les dirigeants des établissements publics y sont conviés.

Le COSTRAT SECNUM MESR associe les AQSSI ministériels, un représentant de France Universités (FU), un représentant de la conférence des grandes écoles (CGE), un représentant de la conférence des directeurs des écoles françaises d'ingénieurs (CDEFI), le DNE ou son représentant, le FSSI et le RSSI ministériel. Les dirigeants des EPST y sont conviés. Sont également associés au titre de leurs missions pour le secteur, le directeur du GIP RENATER et le directeur du GIP AMUE.

Le COSTRAT SECNUM MSJOP associe les AQSSI ministériels, le dirigeant de l'INSEP, le dirigeant de l'agence nationale du sport, un représentant de CREPS, le DNE ou son représentant, le FSSI et le RSSI ministériel.

Un comité ministériel de pilotage de la sécurité numérique (COPIL SECNUM) est constitué par ministère.

Il est présidé par le HFDS ou son représentant et se réunit au moins deux fois par an. Le FSSI en assure le secrétariat.

Il examine les activités et états des lieux liés à la sécurité numérique, réalise un suivi des homologations, des plans d'amélioration continue, de la gestion des incidents et de la prise en compte de la sécurité numérique. Il traite les points d'arbitrage techniques ou relatifs aux processus de sécurité du numérique.

Le COPIL SECNUM MENJ associe les CSN et les RSSI du ministère, le sous-directeur socle numérique de la DNE ou son représentant, le responsable du COSSIM, un représentant des CSN de région académique, un représentant des RSSI de région académique, un représentant des CSN d'académie, un représentant de RSSI d'académie, des RSSI d'établissement public.

Le COPIL SECNUM MESR associe les CSN et les RSSI du ministère, le sous-directeur socle numérique de la DNE ou son représentant, les responsables du COSSIM et du CERT-RENATER, un RSSI représentant les universités, un RSSI représentant les grandes écoles, un RSSI représentant les EPST. Sont également associés le RSSI de RENATER et le RSSI de l'AMUE.

Le COPIL SECNUM MSJOP associe les CSN et les RSSI du ministère, le sous-directeur socle numérique de la DNE ou son représentant, le responsable du COSSIM, le responsable SI de la direction des Sports, le RSSI de l'INSEP, un RSSI représentant les CREPS.

6. **Processus principaux pour la sécurité numérique**

6.1. *Cartographie des risques*

Chaque ministère élabore et actualise annuellement une cartographie des risques, incluant les risques numériques principaux. Les risques font l'objet d'un examen dans un comité dédié afin de déterminer un plan de réduction et de maitrise des risques.

La démarche est également fortement recommandée en établissement public et fait l'objet d'un suivi au sein d'un comité propre à l'établissement.

6.2. *Identification des SI prioritaires*

Chaque AQSSI réalise annuellement l'identification des systèmes d'information prioritaires de son périmètre, en regard de l'importance de ses services et infrastructures numériques dans l'exercice des missions principales de son champ de responsabilités.

En administration centrale et en services déconcentrés, le HFDS, assisté du FSSI, organise la campagne d'identification et de synthèse des SI prioritaires. A l'issue de chaque campagne, un référentiel des SI prioritaires avec impacts nationaux est élaboré par le FSSI.

Les SI prioritaires avec impacts sur des missions nationales bénéficient de plans de sécurisation renforcés et font l'objet d'une déclaration à l'agence nationale de la sécurité des systèmes d'information.

En établissements publics, ces actions sont organisées par le dirigeant, assisté par son RSSI. Ces éléments sont internes à l'établissement mais peuvent sur demande être mis à disposition du HFDS, du FSSI et de l'ANSSI.

Un modèle documentaire pour conduire l'identification de SI prioritaires est proposé par le FSSI.

6.3. *Homologation de sécurité des SI*

L'homologation de sécurité est une décision formelle prise par l'autorité qualifiée de la sécurité des systèmes d'information, ou par toute personne désignée par l'AQSSI appelée autorité d'homologation (AH), à qui elle délègue cette fonction. La démarche d'homologation permet d'attester que les risques pesant sur la sécurité ont été identifiés et que les mesures nécessaires pour maîtriser ces risques sont mises en œuvre. Elle atteste également que les éventuels risques résiduels ont été identifiés et acceptés par l'AQSSI.

L'homologation de sécurité s'impose à tous les SI concourant aux missions de l'Etat et des organismes placés sous sa tutelle (4), ainsi qu'aux systèmes d'information soumis à des réglementations spécifiques (5).

L'homologation formelle intervient avant toute mise en production de tout nouveau service numérique.

Pour les périmètres concernés par la présente instruction, la démarche d'homologation de sécurité est adaptée en fonction des enjeux et de la sensibilité du SI à homologuer. Une directive ministérielle précisera les modalités de réalisation des homologations.

6.4. *Gestion des incidents et de crise d'origine cyber*

La gestion des incidents de sécurité numérique permet de qualifier et de traiter tout évènement d'origine malveillante qui porte atteinte à la disponibilité, à l'intégrité ou à la confidentialité des services et données numériques.

Les incidents, ou suspicion d'incidents, de sécurité numérique sont signalés par :

– les usagers de services numériques auprès du support informatique de proximité, qui évalue l'incident puis le notifie au RSSI du périmètre. Le RSSI déclare ensuite l'incident à son centre de réponse à incident de référence ;
– les administrateurs de services numériques qui signalent au RSSI du périmètre ou, à défaut, au centre de réponse à incident de référence ;
– des acteurs de veille et de réponses en sécurité numérique (CERT-Fr, autres CERT, RSSI d'autres secteurs…) ;
– des dispositifs de détection automatisée des menaces (antivirus, pare-feu, systèmes de supervision ou de détection d'évènements…)

Les incidents de sécurité avérés font l'objet d'une évaluation des impacts par le centre de réponse à incident selon une échelle de quatre niveaux :

– 1 – négligeable : pas d'impact opérationnel sur l'activité du périmètre, ni sur la sécurité des personnes et des biens ;
– 2 – limité : impact opérationnel avec dégradation limitée de l'activité (fonctionnement en mode dégradé), pas d'impact sur la sécurité des personnes et des biens ;
– 3 – important : impact opérationnel important pouvant entrainer l'arrêt d'une partie des activités d'un périmètre, avec d'éventuels impacts sur la sécurité des personnes et des biens ;
– 4 – maximal : impact opérationnel maximal entrainant l'arrêt immédiat et prolongé des activités du périmètre concerné ou impact important sur une ou plusieurs missions nationales.

Tous les incidents avec impacts de niveau égal ou supérieur à « 2 – limité » font l'objet d'une signalisation par le RSSI au centre de réponse à incident de sécurité du numérique de référence (6) pour l'entité.

Les incidents de sécurité de niveaux 3 et supérieur font l'objet d'une déclaration par le centre de réponse à incident, ou à défaut le FSSI, à l'ANSSI.

Le centre de réponse à incident apporte une assistance dans l'analyse des symptômes, le diagnostic, le traitement et la réaction aux incidents. Il se coordonne avec d'autres centres de réponse à incidents et acteurs opérationnels de la sécurité numérique.

En fonction de l'impact et de l'évolution de l'incident, le FSSI peut activer la cellule opérationnelle de crise cyber (COCC) et en informe le HFDS.

La COCC permet de réunir les moyens des centres de réponse à incidents (COSSIM et CERT-RENATER) et d'associer tous les acteurs opérationnels pertinents pour la maitrise de la situation (RSSI, experts techniques…).

La COCC permet d'évaluer l'impact global et les scénarios d'évolutions possibles, d'éclairer les AQSSI et décideurs sur la conduite à tenir, identifie les mesures conservatoires et de remédiation et réalise des communications si besoin d'urgences, à destination des acteurs de gestion de la crise et du numérique.

Si le centre ministériel de crise (CMC) est activé, la COCC constitue l'une des cellules d'appui au CMC.

6.5. *Gestion des vulnérabilités et des alertes de sécurité*

La gestion des vulnérabilités et des alertes de sécurité permet d'éviter qu'une faille ou menace confirmée ne puisse provoquer un incident de sécurité numérique avec impacts sur les données ou le fonctionnement des services numériques.

Les signalements de vulnérabilités et alertes peuvent émaner :

– d'acteurs de veille et de réponse aux incidents en sécurité numérique, comme le CERT-FR (ANSSI) et d'autres CERT nationaux ou sectoriels ;
– de lanceurs d'alertes (dits « hackeurs éthiques ») signalant des vulnérabilités à l'ANSSI dans le cadre de l'article 47 de la loi pour une République numérique n° 2016-1321 du 7 octobre 2016 (7) ;
– de personnels internes signalant au RSSI du périmètre, qui qualifie puis, si confirmé, réalise la déclaration à son centre de réponse à incident de référence (COSSIM ou CERT-RENATER) ;
– d'acteurs internes de la sécurité opérationnelle (RSSI, COSSIM, CERT-RENATER, FSSI…) qui disposent de solutions de détection de vulnérabilités et d'évènements de sécurité du numérique.

Les types d'alertes sont :

– les **injonctions** formelles, qui sont émises par l'ANSSI vers le HFDS. Elles requièrent une réponse obligatoire. Chaque injonction fait l'objet d'une campagne par sondage organisé par le FSSI à destination de chaque RSSI des entités composant le périmètre. A l'issue de la campagne d'injonction, une synthèse des réponses est transmise par le HFDS à l'ANSSI ;
– le signalement **d'alertes critiques**, qui font l'objet d'une notification vers chaque RSSI d'entité concernée et précisent l'élément concerné. Chaque signalement doit être acquitté par le RSSI et sa remédiation doit faire l'objet d'un retour au centre de réponse à incident l'ayant signalé ;
– les **vulnérabilités standards**, qui sont transmises par les listes de diffusion dédiées à cet usage à destination des RSSI. Il n'est pas demandé d'acquittement mais chaque acteur détermine si ce composant est présent dans son périmètre et procède dans les plus brefs délais aux mises à jour ou, à défaut, à la mise en protection des éléments vulnérables.

6.6. *Maintien en condition opérationnelle de sécurité*

Le maintien en condition opérationnelle de sécurité (MCOS) permet de garder les services et les infrastructures numériques à un niveau de sécurité qui garantit leur sécurité de fonctionnement et de protection des données.

Le MCOS comprend le durcissement de la configuration des ressources déployées, le déploiement, éventuellement en urgence, des correctifs publiés par les éditeurs et fournisseurs afin de traiter les vulnérabilités applicatives ou techniques, la mise à jour des dispositifs de sécurité et l'anticipation de l'obsolescence technologique des ressources utilisées.

Les procédures de MCOS sont définies conjointement par les services en charge d'applications et d'infrastructures et par le responsable de la sécurité des systèmes d'information (RSSI) du périmètre.

Ces procédures sont ensuite appliquées par les équipes en charge du suivi opérationnel des services ou infrastructures numériques (DNE, DSI, services en maitrise d'œuvre de SI).

Pour les services exploités dans des infrastructures externes nuagiques (cloud), un plan d'assurance sécurité (PAS) doit être élaboré lors de la phase de contractualisation. Ce PAS doit décrire la politique de maintien opérationnel en condition de sécurité, qui est contrôlée ensuite par les responsables applicatifs et le RSSI du périmètre.

Pour les ministères et le numérique des missions nationales, en cas de défaut du maintien en conditions de sécurité d'un service, l'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) responsable du service numérique, ou à défaut le fonctionnaire de sécurité des systèmes d'information (FSSI) qui s'appuie sur les centres de réponses à incident, pourront demander l'arrêt des ressources concernées jusqu'à la correction des failles et le cas échéant, à l'assainissement du service concerné.

En dernier recours, le haut fonctionnaire de défense et de sécurité (HFDS) peut prendre cette décision pour toute ressource du ministère et pour des services et infrastructures numériques portant des missions nationales.

6.7. *Inspections, audits et contrôles de sécurité numérique*

Les audits et contrôles ministériels de sécurité du numérique font l'objet d'un plan annuel proposé par le FSSI au HFDS, en lien avec les AQSSI et les RSSI des périmètres concernés. Des audits et contrôles en dehors du programme annuel peuvent néanmoins être diligentés en complément selon les besoins.

Les audits et contrôles ministériels des systèmes d'information le plus sensibles – les SI d'importance vitale (SIIV) ou les SI essentiels (SIE) déclarés à l'ANSSI – sont réalisés par l'ANSSI ou par un prestataire d'audit de la sécurité des systèmes d'information qualifié par l'ANSSI (PASSI LPM pour les SIIV, PASSI RGS pour les SIE).

Les audits et contrôles des autres systèmes d'information ministériels ou à portée nationale sont réalisés par des prestataires d'audits qualifiés par l'ANSSI (PASSI RGS) ou par le pôle interne national de compétence et expertises affecté aux audits de sécurité numérique (DNE), sur validation du RSSI ministériel et du FSSI.

Les services déconcentrés et les établissements publics déterminent leurs programmes d'audits et de contrôles pour leur périmètre et veillent à recourir à des prestataires d'audits qualifiés par l'ANSSI (PASSI RGS).

Les inspections ministérielles de sécurité numérique sont réalisées par l'ANSSI, selon un calendrier et des périmètres définis entre les parties.

6.8. *Rapports annuels de sécurité du numérique*

Chaque AQSSI et dirigeant communique un rapport annuel de la sécurité du numérique, selon un format commun élaboré au niveau interministériel communiqué par l'ANSSI.

Le FSSI réalise une campagne annuelle de remise des rapports de sécurité numérique et réalise une synthèse pour le HFDS. Les éléments de synthèse font l'objet d'une présentation en COSTRAT de sécurité numérique du périmètre.

6.9. *Règles de sécurité*

Le référentiel de règles de sécurité s'appuie sur la politique de sécurité des systèmes d'information de l'Etat (PSSI-E), complété pour les SI relevant de réglementations spécifiques par des mesures complémentaires.

Une directive de « politique opérationnelle de sécurité du numérique » (POSN) complètera la PSSI-E et précisera les règles de sécurité applicables. Ce document aura valeur de recommandations pour les établissements publics.

Tous les agents publics en charge de systèmes d'information doivent respecter ces règles de sécurité, suivre les recommandations définies en application de celles-ci et utiliser les infrastructures et les outils mis à leur disposition dans les conditions d'usages précisées.

---

(1) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000027677984.

(2) Incidents avec impacts métiers : 2 – limité, 3 – important, 4 – maximal, se référer aux définitions du chapitre 5.4.

(3) Computer Emergency Response Team.

(4) Article 1er du décret no 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique.

(5) RGS, II901, IGI1300…

(6) Voir le « 4.4 Les centres de réponse à incident de sécurité du numérique ».

(7) https://www.ssi.gouv.fr/actualite/vous-souhaitez-declarer-une-faille-de-securite/.

7. **Annexe A1**
Rôle et missions détaillées des acteurs de la chaine fonctionnelle de la sécurité numérique

7.1. *Le ministre*

Le ministre est responsable du système d'information et de communication de son ministère. A ce titre, il s'assure que l'ensemble des infrastructures et services logiciels informatiques de son ministère sont sous la responsabilité d'une autorité qualifiée en sécurité des systèmes d'information. Le ministre s'assure de la maîtrise des risques numériques ayant un impact sur l'exécution des missions de son ministère.

Le ministre est garant de la bonne prise en compte de la stratégie numérique de l'Etat et de la politique de sécurité numérique de l'Etat, dans l'élaboration de la politique publique portée par son ministère. Il valide les orientations ministérielles en matière de sécurité numérique ainsi que la politique ministérielle de sécurité numérique. Il s'assure de la prise en compte de la sécurité numérique dans l'élaboration et la mise en œuvre d'une stratégie de résilience numérique, notamment des plans de continuité et de reprise d'activité pour les missions essentielles portées par son ministère ainsi que dans l'élaboration et la mise en œuvre du dispositif de gestion de crise ministériel.

Lorsqu'un établissement, une direction ou un service est sous la tutelle de plusieurs ministères, les ministres concernés décident du ministère de référence sur les sujets relatifs à la sécurité numérique.

7.2. *Le haut fonctionnaire de défense et de sécurité (HFDS), secrétaire général des ministères*

Le haut fonctionnaire de défense et de sécurité conseille les ministres du périmètre pour les questions relatives à la sécurité numérique et leur propose la politique ministérielle de sécurité numérique qu'il anime. Il est également l'interlocuteur privilégié du directeur général de l'ANSSI. Pour ce faire, Il s'appuie sur un haut fonctionnaire adjoint de défense et de sécurité, chef du service de défense et de sécurité.

Le haut fonctionnaire de défense et de sécurité est membre du comité stratégique interministériel de la sécurité numérique et participe à l'instance stratégique ministérielle de la sécurité numérique. Il préside l'instance ministérielle de pilotage de la sécurité numérique.

7.3. *Le fonctionnaire de sécurité des systèmes d'information (FSSI)*

Le fonctionnaire de sécurité des systèmes d'information (FSSI), désigné par le ministre, est placé sous l'autorité hiérarchique du haut fonctionnaire adjoint de défense et de sécurité, au sein du service de défense et de sécurité (SDS).

Il accompagne les autorités qualifiées de la sécurité des systèmes d'information (AQSSI), pilote la mise en œuvre de la sécurité numérique et contribue, en lien avec la direction du numérique en charge des plans de continuité et de reprise informatique, aux stratégies de résilience numérique dans les plans de continuité et de reprise d'activité.

Lorsqu'un système d'information et de communication est critique pour la réalisation des missions de plusieurs directions de son ministère, le FSSI, en lien avec les directions et autorités qualifiées en sécurité des systèmes d'information concernées, propose au HFDS la direction qui en a la responsabilité.

Il contrôle l'application des exigences de sécurité (par exemple par des états des lieux, audits, contrôles, bilans). Il contribue à la gestion de crise en conseillant les autorités ministérielles et en participant aux dispositifs de gestion de crise ministériel.

Le FSSI est un des interlocuteurs privilégiés de l'agence nationale de la sécurité des systèmes d'information au sein du ministère sur les sujets de mise en œuvre de la sécurité numérique ou liés au suivi de la feuille de route ministérielle de sécurité numérique.

En tant qu'animateur et coordinateur de la chaîne fonctionnelle de sécurité des systèmes d'information, il dispose d'un accès à l'ensemble des déclarations d'incidents du périmètre. Il s'assure que les incidents de sécurité les plus significatifs sont notifiés à l'agence nationale de la sécurité des systèmes d'information dans les plus brefs délais. Pour ce faire, il s'appuie sur les centres ministériels et sectoriels de réponse aux incidents de sécurité des systèmes d'information.

Il organise la relation avec les établissements publics pour les sujets relatifs à la sécurité numérique.

Le FSSI dispose de FSSI adjoints en charge de secteurs opérationnels, qui participent à la continuité de la fonction de FSSI et disposent des attributs des missions de FSSI.

Le FSSI participe au comité interministériel de pilotage de la sécurité numérique. Il assure le secrétariat, en appui du HFDS, de l'instance stratégique ministérielle de la sécurité numérique et de l'instance ministérielle de pilotage de la sécurité numérique. Il anime et coordonne, en lien avec le HFDS, la chaîne fonctionnelle de sécurité des systèmes d'information pour le ministère dont il dépend. Il organise la relation entre son ministère et les établissements publics dont son ministère a la tutelle pour les sujets relatifs à la sécurité numérique.

7.4. *Les autorités qualifiées de la sécurité des systèmes d'information (AQSSI)*

L'autorité qualifiée de la sécurité des systèmes d'information est responsable de la sécurité des systèmes d'information et de communication qui contribuent à l'exécution des missions et du périmètre dont elle a la charge. L'autorité qualifiée de la sécurité des systèmes d'information ne peut déléguer cette responsabilité. A ce titre, elle est responsable, en particulier, de :

– l'élaboration et le maintien à jour d'une cartographie des risques numériques principaux et des SI associés pour son périmètre ;
– le maintien en condition opérationnelle et de sécurité de ces systèmes ;
– la planification des audits de sécurité de ces systèmes.

L'AQSSI alloue les ressources nécessaires pour mener à bien les projets de transformation numérique de son périmètre de responsabilité et s'assure à ce titre que les risques numériques sont gérés. Ces éléments sont tenus à la disposition du fonctionnaire de sécurité des systèmes d'information.

L'AQSSI s'assure de la bonne prise en compte de ses orientations en matière de sécurité numérique dans les missions qu'elle porte et dans la stratégie ministérielle du numérique pour laquelle elle rend un avis.

Sur son périmètre de responsabilité, l'AQSSI contrôle l'application des exigences de sécurité numérique auxquelles elle est soumise. Elle intègre dans la programmation de ses contrôles internes le volet relatif à la sécurité numérique.

Elle remet annuellement au HFDS un rapport dans lequel elle intègre l'évaluation du niveau de sécurité numérique et une synthèse des incidents de sécurité ayant impacté ses missions. Ce rapport, issu d'un format proposé par l'ANSSI puis adapté en contexte ministériel et sectoriel, est synthétisé et présenté en instance stratégique ministérielle de la sécurité numérique. Ce rapport annuel permet de consolider et communiquer annuellement au ministère de tutelle les résultats de l'évaluation du niveau de sécurité numérique de l'établissement.

L'AQSSI s'assure de l'élaboration, de la mise en œuvre et du maintien, notamment au travers d'exercices, des plans de continuité et de reprise des activités relevant de son domaine de responsabilité face à des incidents de sécurité.

L'AQSSI s'assure de la définition et de la mise en œuvre d'un processus de gestion des incidents de sécurité ainsi que d'une organisation de gestion de crise face aux incidents de sécurité, en lien avec la chaine ministérielle et sectorielle de traitement des incidents de sécurité des SI.

Le rôle d'autorité qualifiée de la sécurité des systèmes d'information est assumé par chaque responsable devant le ministre d'une ou plusieurs missions ministérielles.

Conformément au décret n° 2019-1088, chaque système d'information et de communication fait l'objet, préalablement à sa mise en œuvre, d'une homologation de sécurité. Sauf pour les exceptions prévues aux articles 6.1.2, 6.2.1 et 6.2.2 de l'instruction générale interministérielle 1300 sur la protection du secret de la défense nationale, l'autorité qualifiée de la sécurité des systèmes d'information est l'autorité d'homologation, par défaut, de chaque système d'information et de communication dont elle est responsable.

Lorsque l'AQSSI peut déléguer l'instruction des démarches d'homologation à une ou plusieurs autorités d'homologation, elle s'assure du respect des recommandations ministérielles et de l'agence nationale de la sécurité des systèmes d'information. En particulier elle veille à ce qu'une seule et unique autorité d'homologation existe pour chaque système d'information et de communication.

Pour l'assister dans l'exercice de ses responsabilités, l'AQSSI nomme un conseiller à la sécurité numérique.

Selon l'organisation précisée dans la présente instruction, l'AQSSI participe à l'instance stratégique ministérielle de la sécurité numérique.

Elle contribue à la chaîne fonctionnelle de sécurité des systèmes d'information.

7.5. *Le conseiller à la sécurité numérique (CSN)*

Le conseiller à la sécurité numérique est désigné par chaque AQSSI. Il conseille et accompagne l'autorité qualifiée dans l'exercice de ses responsabilités.

Sans être un expert de la sécurité du numérique, le CSN dispose d'une connaissance globale des enjeux des métiers du périmètre et d'une culture générale du numérique, lui permettant d'en traduire les enjeux pour le compte de l'AQSSI.

Il est placé sous la responsabilité d'une autorité qualifiée de la sécurité des systèmes d'information et est associé à la gouvernance du périmètre concerné.

Pour ces raisons, le CSN est nécessairement un acteur du pilotage et de la gouvernance du périmètre. A ce titre, il fait partie du comité de direction ou du comité exécutif du périmètre.

Il s'appuie sur les compétences à disposition en matière de sécurité numérique, notamment le RSSI. Il échange également avec le référent à la protection des données. Il peut être chargé d'accompagner les autorités d'homologation dans leurs démarches d'homologation.

Description type des missions d'un conseiller à la sécurité numérique (8) **:**

Nommé par l'autorité qualifiée de la sécurité des systèmes d'information (AQSSI) et placé sous son autorité, le conseiller à la sécurité numérique (CSN) l'assiste dans ses responsabilités relatives à la sécurité des systèmes d'information soutenant les missions de son entité.

S'appuyant sur sa connaissance métier et en lien avec les experts techniques en sécurité numérique, le CSN :

- conseille l'AQSSI sur les orientations à prendre en matière de maîtrise des risques numériques ;
- dresse une cartographie des missions critiques et des risques stratégiques, puis identifie les SI qui les soutiennent ;
- informe l'AQSSI du niveau de sécurité des systèmes d'information soutenant le métier et propose des priorités en matière de gestion des risques ;
- conseille l'AQSSI et, le cas échéant, les autorités d'homologation en matière d'homologation ;
- conseille l'AQSSI dans sa prise de décision en cas de crise cyber ;
- suit la mise en œuvre des orientations de l'AQSSI en matière de sécurité numérique ;
- s'assure de la bonne prise en compte des besoins de sécurité du métier par les fournisseurs de services numériques ainsi que de la mise en œuvre des démarches de maîtrise des risques numériques ;
- prépare l'AQSSI en vue des instances stratégiques ministérielles de la sécurité numérique et la représente lors des instances ministérielles de pilotage de la sécurité numérique ;
- contribue à l'élaboration du rapport annuel de sécurité que l'AQSSI remet au haut fonctionnaire de défense et de sécurité (HFDS) ;
- promeut des actions de sensibilisation au risque numérique et de diffusion des bonnes pratiques au sein de son périmètre.

Eclairages sur les missions du CSN :

Pour mener ses missions, le CSN doit être un interlocuteur direct de l'AQSSI. Le positionnement adéquat est généralement au sein des plus proches collaborateurs de l'AQSSI, notamment de son cabinet ou du comité de direction qu'il préside.

Le CSN est un expert des activités métier du périmètre. Par sa connaissance des enjeux, il peut identifier les conséquences métier d'éventuels dysfonctionnements ou compromissions des systèmes dont dépend son entité pour l'exécution de ses missions.

Il bénéficie d'une formation de premier niveau à la gestion des risques numériques dispensée par le ministère et par l'ANSSI. Le CSN s'appuie sur les outils et méthodes ministériels définis par le fonctionnaire de sécurité des systèmes d'information (FSSI).

Il est en lien avec le(s) responsable(s) de la sécurité des systèmes d'information (RSSI) du périmètre. Le(s) RSSI propose(nt) des solutions techniques aux besoins qu'il exprime et apporte(nt) des éclairages techniques pour alimenter sa compréhension du risque. Il échange en tant que de besoin avec le(s) délégué(s) à la protection des données (DPD) du périmètre.

La part du temps de travail à consacrer à cette mission est variable selon l'environnement, la taille du périmètre, l'avancée de la transformation numérique ou son rythme.

7.6. *Le directeur du numérique pour l'éducation (DNE)*

Le directeur du numérique pour l'éducation (DNE) définit la stratégie ministérielle du numérique dans laquelle il s'assure de la bonne prise en compte de la sécurité numérique dans les projets et du maintien en condition opérationnelle de sécurité. Il définit le plan de transformation numérique ministériel et le schéma directeur des systèmes d'information et de communication. Il veille d'une part à ce que chaque structure compétente assure la mise en œuvre et l'exploitation sécurisée de systèmes d'information et de communication, et d'autre part à l'élaboration d'une analyse d'impact relative à la protection des données.

Le directeur de la DNE est donc à la fois un AQSSI parmi les autres (participation aux échanges entre AQSSI) mais aussi le représentant d'une organisation participant au pilotage de la sécurité des SI du fait du rôle de la DNE dans la mise en œuvre des systèmes d'information et des dispositifs de sécurité correspondants et du rôle de conseil voire d'alerte dans la prise en compte des enjeux de sécurité dans les projets ou dans la réaction lors de crises, en appui du HFDS et du FSSI. A ce titre, il participe aux COSTRAT sectoriels.

7.7. *Le directeur des systèmes d'information de service déconcentré ou d'établissement public*

Le directeur des systèmes d'information (DSI) définit la stratégie du numérique de son périmètre, en tenant compte des réglementations des SI de l'Etat et des directives ministérielles sur le numérique. Il s'assure de la bonne prise en compte de la sécurité numérique dans les projets et du maintien en condition opérationnelle de sécurité. Il définit le plan de transformation numérique de son périmètre et le schéma directeur des systèmes d'information et de communication. Il veille d'une part à ce que chaque structure compétente assure la mise en œuvre et l'exploitation sécurisée de systèmes d'information et de communication, et d'autre part à l'élaboration d'une analyse d'impact relative à la protection des données.

7.8. *Le responsable de la sécurité des systèmes d'information*

Le responsable de la sécurité des systèmes d'information (RSSI) est l'acteur clé de la sécurité opérationnelle d'un périmètre d'activité et dispose d'expertises en sécurité du numérique.

Il éclaire l'AQSSI sur les risques opérationnels pesant sur le numérique et produit les états des lieux de sécurité du numérique du périmètre.

Il propose des mesures, actions ou projets afin de réduire ces risques et renforcer la protection des services et données numériques du périmètre concerné.

Il supervise, en lien avec le directeur du numérique ou des systèmes d'information du périmètre, le déploiement des actions de sécurisation et de renforcement de la sécurité du numérique.

Il est l'acteur clé de coordination opérationnelle pour la gestion des incidents de la sécurité numérique du périmètre et participe à la gestion de crises d'origine cyber.

Il contribue à l'intégration de la sécurité numérique dans les projets du périmètre et réalise des audits et des contrôles de la sécurité de son périmètre d'activité.

Il pilote des projets spécifiques de sécurité du numérique.

Les RSSI ministériels et nationaux organisent et animent des réseaux territoriaux de RSSI et de correspondants à la sécurité des systèmes d'information (CSSI). Ils participent et contribuent au déploiement des politiques ministérielles et interministérielles de la sécurité du numérique, en lien avec le FSSI.

Les RSSI d'établissement peuvent, si cela est pertinent pour le contexte, constituer un réseau interne de CSSI, qu'ils animent, dans les directions, composantes ou sites de l'établissement.

Au-delà de la relation privilégiée avec l'AQSSI du périmètre, les RSSI informent et agissent en tant que de besoin en lien avec les délégués à la protection des données (en cas par exemple d'incidents ou de plans d'actions sur la sécurité de données personnelles du périmètre) et les personnels en charge de la sécurité physique et des données réglementées du périmètre (les fonctionnaires de défense et de sécurité et les délégués à la protection des données par exemple).

---

(8) Ces missions peuvent se cumuler avec d'autres activités.

8. **Annexe A2**
Cadre réglementaire

Texte relatifs au numérique, à la sécurité du numérique et des systèmes d'information et de communication :

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 (NOR : *PRMD2135717D*).

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 (NOR : *PRMD2221955A*).

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 (NOR : *PRMG1929496D*).

Le référentiel général de sécurité (RGS) pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges

électroniques entre les usagers et les autorités administratives et entre les autorités administratives (NOR : *PRMX0909445D*).

Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques (NOR : *PRMD1413745A*).

Circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 introduisant la politique de sécurité des systèmes d'information de l'Etat (PSSIE) (NOR : *PRMX1420095C*).

Instruction interministérielle n° 901/SGDSN/ANSSI (II 901) relative à la protection des systèmes d'information sensibles (NOR : *PRMD1503279J*).

Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (NOR : *ECOX0500286R*).

Ordonnance n° 2017-1426 relative à l'identification électronique et aux services de confiance pour les transactions électroniques (NOR : *PRMD1724021R*).

Textes relatifs à la protection des données personnelles :

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (NOR : *JUSC1732261L*).

Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment son article 85 et ses articles 140 et suivants (NOR : *JUSC1911425D*).

Textes concernant des périmètres spécifiques :

Arrêté du 13 juillet 2020 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Recherche publique » (NOR : *PRMD2018060A*) et leurs annexes.

Décret 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique (NOR : *PRMD1809740D*).

Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique (NOR : *PRMD1824939A*).

Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation (NOR : *PRMX1118649D*).

Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation (NOR : *PRMX1227979A*).

Circulaire interministérielle n° 3415/SGDSN/AIST/PST du 7 novembre 2012 de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation (NOR : *PR1vID1238889C*).

Décret n° 2024-430 du 14 mai 2024 portant diverses dispositions relatives à la protection du potentiel scientifique et technique de la Nation (NOR : *PRMD2334561D*).

Texte relatif à la protection du secret de la défense nationale :

Arrêté 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale (NOR : *PRMD2123775A*).

Arrêté du 10 juin 2024 portant approbation de l'instruction ministérielle relative à la protection du secret de la défense nationale au sein des ministères de l'éducation nationale et de la jeunesse, de l'enseignement supérieur et de la recherche et des sports et des jeux olympiques et paralympiques (NOR : *MENG2410980A*).

Texte relatif à l'organisation gouvernementale pour la gestion de crises majeures :

Circulaire n° 6418/SG du 26 septembre 2023 relative à l'organisation gouvernementale pour la gestion des crises majeures (NOR : *PRMX2325876C*).