



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Politique de sécurité numérique de l'administration territoriale de l'Etat

PGSN – C01

Version 1.5

Préambule

Afin de répondre aux enjeux de proximité et de lisibilité envers le citoyen, l'Etat poursuit sa transformation pour le rendre plus proche du terrain et pour mieux adapter les décisions aux réalités locales. Les préfetures et les directions départementales interministérielles déclinent les politiques publiques des ministères au sein des territoires.

Créées par décret du 3 décembre 2009, les directions départementales interministérielles, issues de la fusion des anciennes directions départementales, se caractérisent par leur vocation interministérielle. Le décret 2020-1050 du 14 août 2020 les rattache au ministère de l'intérieur les rassemblant sous la responsabilité du préfet de département. Pour les outre-mer, les services de l'Etat ont été créés par décret du 8 juin 2010, par le titre I du décret du 17 décembre 2010 et par le chapitre III du décret du 30 décembre 2015 susvisés, en Guadeloupe, à la Martinique, à La Réunion et dans le département de Mayotte.

Créés par décret du 7 février 2020, les secrétariats généraux communs départementaux exercent leurs missions au profit de la préfeture et des DDI. Ils gèrent les fonctions et moyens mutualisés en matière budgétaire, d'achat public, d'affaires immobilières, de systèmes d'information et de communication, de logistique, de ressources humaines, de relation avec la médecine de prévention et de mise en œuvre des politiques d'action sociale au bénéfice des agents des directions et services précédemment mentionnés.

La sécurité numérique représente une garantie pour le citoyen de la résilience des actions de l'Etat dans les territoires et la menace d'origine cyber n'a jamais été aussi élevée. De nombreux incidents médiatisés témoignent régulièrement de son augmentation structurelle, le cyberspace devenant un lieu de conflits géopolitiques, de compétition économique, de criminalité organisée et d'expression de la contestation radicale.

Dans ce contexte, il apparait inéluctable que l'action du préfet de département en matière de sécurité numérique, doive se développer dans les prochaines années. Il s'agira en premier lieu de s'assurer que des attaques informatiques ne viennent pas perturber le fonctionnement des administrations dont il est responsable. Il s'agira également de mieux intégrer la thématique de la cyber-sécurité dans ses missions de prévention des risques et de gestion des crises.

Ainsi la présente politique prend notamment en compte ces nouvelles responsabilités du ministère et la doctrine constante du haut fonctionnaire de défense, qu'elle vient renforcer.

Table des matières

Article 1.	Intégration dans le corpus de la sécurité numérique du ministère de l'intérieur	4
Article 2.	Cadre obligatoire de la PSN-ATE.....	4
Article 3.	Champ d'application.....	4
Article 4.	Date d'effet et révision.....	4
TITRE I -	Organisation de la sécurité numérique pour l'administration territoriale de l'Etat	5
Chapitre 2 –	La chaîne décisionnelle de sécurité numérique	5
Article 5.	L'autorité qualifiée en sécurité des systèmes d'information.....	5
Chapitre 2 –	La chaîne fonctionnelle de la sécurité numérique.....	6
Article 6.	Le conseiller à la sécurité du numérique.....	6
Article 7.	L'assistant local à la sécurité du numérique	7
Chapitre 3 –	La chaîne opérationnel de sécurité numérique et de cyberdéfense	9
Article 8.	Centre de cyberdéfense du ministère de l'intérieur	9
Article 9.	Le responsable de la sécurité des systèmes d'information	9
Article 10.	L'assistant local à la sécurité des systèmes d'information.....	9
TITRE II :	La gouvernance de la sécurité numérique de l'administration territoriale de l'Etat	11
Article 11.	Les comités de gouvernance	11
Article 12.	Le comité national de la sécurité numérique de l'ATE.....	11
Article 13.	Le comité départemental de la sécurité numérique.....	11
Article 14.	Les comités de suivi départementaux de la sécurité numérique.....	12
TITRE III :	Gestion du risque numérique.....	14
Article 15.	Homologation de sécurité.....	14

Article 1. Intégration dans le corpus de la sécurité numérique du ministère de l'intérieur

La politique de sécurité numérique de l'administration territoriale de l'Etat (PSN-ATE) vient préciser la politique générale du ministère de l'intérieur (PGSN-MI) pour les services déconcentrés mentionnés à l'article 3.

La PSN-ATE est complétée par le document [PGSN-B04] du corpus documentaire de la sécurité numérique du ministère de l'intérieur.

Article 2. Cadre obligatoire de la PSN-ATE

La PSN-ATE constitue le cadre obligatoire dans lequel les services déconcentrés mentionnés à l'article 3 inscrivent leurs actions liées à la sécurité numérique.

En cas d'impossibilité opérationnelle de mise en œuvre d'une des dispositions prévues, le haut fonctionnaire de défense (HFD) rend les arbitrages des demandes de dérogation. La responsabilité de ces demandes est définie à l'article 5.

Article 3. Champ d'application

La PSN-ATE s'applique aux :

1. Services de préfectures ;
2. Directions départementales interministérielles ;
3. Secrétariats généraux communs (SGC) ;
4. Secrétariats généraux communs départementaux (SGCD) ;
5. Services déconcentrés de l'Etat relevant du ministère de l'intérieur et placés sous l'autorité du préfet dans les départements, régions et collectivités d'outre-mer à l'exception des services déconcentrés relevant de directions de la police nationale ou de la gendarmerie nationale.

Des dispositions spécifiques sont prévues pour les ministères responsables des politiques publiques mises en œuvre par les services déconcentrés précités.

Article 4. Date d'effet et révision

La mise en œuvre de la PSN-ATE est engagée dès sa publication.

Le comité national de la sécurité numérique (COSEC ATE), défini à l'article 11, en assure annuellement le suivi.

Toute demande d'évolution ou d'adaptation de la PSN-ATE est soumise au COSEC ATE pour instruction.

La PSN-ATE est révisé en tant que de besoin et au plus tard tous les trois ans.

La PSN-ATE est révisée lors des évolutions réglementaires modifiant le champ d'application défini à l'article 3 ou impliquant un ajustement des dispositions prévues.

TITRE I - Organisation de la sécurité numérique pour l'administration territoriale de l'Etat

Chapitre 2 – La chaîne décisionnelle de sécurité numérique

Article 5. L'autorité qualifiée en sécurité des systèmes d'information

Le préfet de département est l'autorité qualifiée en sécurité des systèmes d'information (AQSSI) des services déconcentrés mentionnés à l'article 3 à l'échelle du département.

Il est le garant de la résilience numérique des services déconcentrés mentionnés à l'article 3 à l'échelle du département.

Il est responsable de l'exécution des mesures organisationnelles et techniques du corpus documentaire de sécurité numérique du ministère de l'intérieur.

Il est responsable de l'intégration du volet cyber dans les plans de continuité d'activité des services déconcentrés mentionnés à l'article 3 à l'échelle du département.

Il est responsable du rapport annuel de la sécurité numérique défini à l'article 25 de la PGSN-MI sur le périmètre relevant de son autorité.

Il est responsable de la constitution des demandes de dérogation à la PSN-ATE des services déconcentrés mentionnés à l'article 3 à l'échelle du département.

Il propose au HFD la liste des systèmes d'information essentiel (SIE) des services déconcentrés mentionnés à l'article 3 à l'échelle du département.

Il transmet les décisions d'homologation au sens de l'article 32 de la PGSN-MI :

1. Pour les systèmes d'information locaux, aux acteurs suivants :
 - a. Le préfet délégué à la défense et à la sécurité de la zone pour les systèmes d'information locaux des services déconcentrés mentionnés à l'article 3 ;
 - b. Le FSSI du ministère de l'intérieur.
2. Pour les systèmes d'information désignés comme essentiels au sens de l'article 33 de la PGSN-MI, aux acteurs suivants :
 - a. Le Haut-fonctionnaire de défense ;
 - b. Le Haut-fonctionnaire de défense adjoint ;
 - c. Le Préfet délégué à la défense et à la sécurité de la zone ;
 - d. Le FSSI du ministère de l'intérieur.

Il est assisté par un conseiller à la sécurité du numérique.

Chapitre 2 – La chaîne fonctionnelle de la sécurité numérique

Article 6. Le conseiller à la sécurité du numérique

Le périmètre du conseiller à la sécurité du numérique (CSN) s'établit sur les services déconcentrés mentionnés à l'article 3 à l'échelle du département.

Après accord du préfet de zone de défense et de sécurité ou du préfet délégué à la défense et à la sécurité de la zone et des préfets des départements concernés, le périmètre du CSN peut s'étendre à plusieurs départements sur une même zone de défense. L'arrêté de nomination conjointe fixe les modalités de l'extension de son périmètre.

La désignation du CSN s'effectue conformément à l'article 12 de la PGSN-MI.

Il est habilité au secret de la défense nationale conformément au document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur.

Les conditions de désignation d'un agent sont les suivantes :

1. Agent de catégorie A ;
2. Agent hiérarchiquement rattaché :
 - a. A la direction ou service des sécurités de la préfecture de département ;
 - b. A la direction des services du cabinet de la préfecture de département ;
 - c. A la direction du cabinet de la préfecture de département ;

Il est recommandé d'inscrire la fonction de CSN dans le schéma des emplois de la préfecture.

Il peut être mutualisé dans le respect des conditions suivantes :

1. La quotité de temps de travail est explicitement mentionnée dans l'arrêté de nomination et ne peut pas être inférieure au dimensionnement minimale du poste prévue dans le document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur ;
2. Les missions du CSN et la quotité de temps de travail sont inscrites dans la fiche de poste de l'agent. La liste des missions du CSN est précisée dans le document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur ;
3. Lors de l'entretien annuel d'évaluation, la thématique d'au moins un des objectifs est la sécurité numérique.

Il assiste dans les 12 mois suivant sa nomination à la formation initiale des CSN.

Il est assisté dans l'exercice de ses fonctions de la chaîne fonctionnelle de la sécurité numérique départementale composé :

1. Du responsable de la sécurité des systèmes d'information ;
2. D'assistants locaux à la sécurité du numérique.

Il rédige la note d'organisation précisant la chaîne fonctionnelle de sécurité numérique départementale, la comitologie associée en cohérence avec les articles 12 et 13.

Il est suppléé en cas d'absence et le suppléant est mentionné dans la note d'organisation.

Il transmet la note d'organisation au SHFD.

Il assiste aux comités de direction des services déconcentrés de son périmètre au moins une fois par an.

Il est consulté par l'autorité compétente préalablement à toute proposition de nomination au sein de la chaîne fonctionnelle de la sécurité relevant de son périmètre.

Il s'assure que le volet numérique est pris en compte et formalisé dans les plans de continuité d'activité sur son périmètre.

Il effectue la sensibilisation des autorités (préfets, sous-préfets, directeurs de services déconcentrés et directeurs de préfecture) sur son périmètre.

Il définit le plan de sensibilisation des agents sur son périmètre.

Il pilote, en coordination avec les services de gestion de crise de la préfecture, des exercices réguliers de crise liés à des événements cyber impliquant les autorités et les personnels sur son périmètre au moins tous les 3 ans.

Il coordonne le traitement des incidents de sécurité sur son périmètre, en s'appuyant sur la chaîne opérationnelle de sécurité numérique et de cyberdéfense.

Il conçoit les procédures de gestion d'incident sur son périmètre intégrant :

1. Une communication adaptée ;
2. Les priorités de cloisonnement et de reprise ;
3. L'aspect judiciaire.

Il prépare, en liaison avec le délégué zonal de sécurité numérique (DZSN), défini à l'article 16 de la PGSN-MI, les dossiers d'homologation pour les projets de systèmes d'information sur son périmètre.

Il pilote les contrôles, audits, inspections sur les systèmes d'information de son périmètre.

Il évalue trimestriellement la conformité à la PSN-ATE sur son périmètre sur les axes du plan d'action de renforcement de sécurité numérique arrêté lors du comité national de la sécurité numérique de l'administration territoriale de l'Etat (COSEC ATE) défini à l'article 11.

Il s'assure que les travaux de mise en œuvre d'un circuit arrivée/départ sur son périmètre se déclinent jusqu'à la mise en œuvre ou le retrait de droits sur les systèmes d'informations.

Article 7. L'assistant local à la sécurité du numérique

Le périmètre de l'assistant local à la sécurité du numérique (ALSN) s'établit sur un des services déconcentrés mentionnés à l'article 3 à l'échelle du département.

Le périmètre de l'ALSN peut s'étendre à plusieurs services déconcentrés d'un même département après accord :

1. Des directeurs de services déconcentrés concernés ;
2. Des directeurs de services de préfecture concernés ;
3. Du CSN.

En complément de l'article 14 de la PGSN-MI, l'ALSN est désigné par la direction du service déconcentré ou direction de la préfecture après consultation du CSN.

Il rend compte au CSN.

Il est habilité au secret de la défense nationale sous réserve des dispositions prévues au document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur.

La mutualisation de cette fonction est possible dans les conditions suivantes :

1. La quotité de temps de travail est explicitement mentionnée dans l'arrêté de nomination et ne peut pas être inférieure à la dimension minimale du poste prévue dans le document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur ;
2. Les missions de l'ALSN et la quotité de temps de travail sont inscrites dans la fiche de poste de l'agent. La liste des missions de l'ALSN sont précisés dans le document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur.

La note d'organisation précise les modalités de l'extension du périmètre.

La liste des missions de l'ALSN sont précisés dans le document [PGSN-B01] du corpus de la PGSN-MI.

Il assiste dans les 12 mois suivant sa nomination à la formation initiale des ALSN.

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

Article 8. Centre de cyberdéfense du ministère de l'intérieur

En complément de l'article 8 de la PGSN-MI, le C2MI est le point de contact ministériel vis-à-vis de ses équivalents au sein des ministères responsables des politiques publiques mises en œuvre par les services déconcentrés définis à l'article 3.

Article 9. Le responsable de la sécurité des systèmes d'information

Le périmètre du responsable de la sécurité des systèmes d'information (RSSI) s'établit sur le service opérationnel des systèmes d'information à l'échelle du département.

En complément de l'article 13 de la PGSN-MI, le RSSI est désigné par la direction du SGC(D) après consultation du CSN.

Il rend compte au CSN.

Il est habilité au secret de la défense nationale sous réserve des dispositions prévues au document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur.

Il est recommandé d'inscrire la fonction de RSSI dans le schéma des emplois du SGC(D).

La mutualisation de cette fonction est possible dans les conditions suivantes :

1. La quotité de temps de travail est explicitement mentionnée dans l'arrêté de nomination et ne peut pas être inférieure au dimensionnement minimale du poste prévue dans le document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur ;
2. Les missions du RSSI et la quotité de temps de travail sont inscrites dans la fiche de poste de l'agent. La liste des missions du RSSI sont précisés dans le document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur ;
3. Lors de l'entretien annuel d'évaluation, la thématique d'au moins un des objectifs est la sécurité numérique.

Il assiste dans les 12 mois suivant sa nomination à la formation initiale des RSSI.

Il est suppléé en cas d'absence et le suppléant est mentionné dans la note d'organisation.

Il est assisté dans l'exercice de ses fonctions de la chaîne fonctionnelle de la sécurité numérique départementale par des assistants locaux à la sécurité des systèmes d'information (ALSSI).

Il pilote et/ou contrôle la mise en œuvre des mesures techniques identifiées dans les déclarations d'applicabilité des applications où le service opérationnel des systèmes d'information à l'échelle du département intervient.

Article 10. L'assistant local de la sécurité des systèmes d'information

Le RSSI est libre dans la définition du périmètre d'intervention de l'ALSSI.

En complément de l'article 13 de la PGSN-MI, l'ALSSI est désigné par la direction du SGC(D) après consultation du RSSI.

Il rend compte au RSSI.

Il est habilité au secret de la défense nationale sous réserve des dispositions prévues au document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur.

La mutualisation de cette fonction est possible dans les conditions suivantes :

1. La quotité de temps de travail est explicitement mentionnée dans la lettre de désignation,
2. Les missions de l'ALSSI et la quotité de temps de travail sont inscrites dans la fiche de poste de l'agent. La liste des missions de l'ALSSI sont précisés à l'article 14 de la PGSN-MI ;
3. Lors de l'entretien annuel d'évaluation, la thématique d'au moins un des objectifs est la sécurité numérique.

Il assiste dans les 12 mois suivant sa nomination à la formation initiale des ALSSI.

La liste des missions de l'ALSSI sont précisés dans le document [PGSN-B01] du corpus documentaire de la sécurité numérique du ministère de l'intérieur.

TITRE II : La gouvernance de la sécurité numérique de l'administration territoriale de l'Etat

Article 11. Les comités de gouvernance

Deux niveaux de gouvernance sont définis pour l'ATE : un niveau national et un niveau départemental. Des comités de suivi peuvent se réunir en tant que de besoin tant au niveau national que départemental.

Article 12. Le comité national de la sécurité numérique de l'ATE

Le HFDA du ministère de l'intérieur préside le comité national de la sécurité numérique de l'administration territoriale de l'Etat (COSEC ATE) qui est composé :

1. Des FSSI des ministères dont les politiques publiques sont mises en œuvre par les services déconcentrés mentionnés à l'article 3 ;
2. Des directeurs ou chef de service du numérique des administrations centrales des ministères dont les politiques publiques sont mises en œuvre par les services déconcentrés mentionnés à l'article 3 ou de leur représentant ;
3. Du directeur de la modernisation et de l'administration territoriale ou de son représentant.

Le secrétariat du comité national est assuré par le SHFD du ministère de l'intérieur.

Le comité national assiste le HFDA dans l'exercice de ses fonctions à la définition et l'arbitrage des orientations stratégiques relatives à la sécurité numérique et à la cyberdéfense de l'administration territoriale de l'Etat.

A ce titre il fixe les axes du plan action de renforcement de sécurité numérique.

Egalement, il examine :

1. Le suivi de la progression générale du niveau de conformité à la PSN-ATE ;
2. La présentation de la synthèse des menaces pesant sur les systèmes d'information et des incidents significatifs ayant impacté le fonctionnement des services ;
3. Le suivi des homologations de sécurité des systèmes d'informations en particulier ceux soumis au référentiel général de sécurité dans le cadre de l'exécution des politiques publiques des services déconcentrés mentionnés à l'article 3 et au titre des communications électroniques entre autorités administratives ;
4. Les propositions d'évolution de la PSN-ATE ;
5. L'examen des demandes de dérogations avant transmission au HFD.

En cas de changement législatif ou réglementaire ayant un impact sur l'application de la PSN-ATE, un COSEC ATE peut être convoqué afin de valider les adaptations nécessaires.

Article 13. Le comité départemental de la sécurité numérique

L'AQSSI préside le comité départemental de la sécurité numérique (COSEC-D ATE) sur son périmètre.

Il est composé :

1. Des directeurs de préfecture ;
2. Des directeurs des services déconcentrés du champ d'application définis à l'article 3 ;
3. Du CSN et du RSSI ;
4. Du référent protection des données du département.

Le secrétariat du comité départemental est assuré par le CSN ou le RSSI. Le secrétariat est responsable de l'élaboration et de la diffusion du compte-rendu de ces comités, dont un exemplaire doit être systématiquement envoyé au SHFD.

Le COSEC-D ATE peut être inclus dans un comité de pilotage existant présidé par l'AQSSI.

Il se réunit au moins une fois par an.

Il statue sur :

1. La préparation des demandes d'évolutions de la PSN-ATE pour arbitrage en COSEC ATE la conformité du département à la PSN-ATE ;
2. Le suivi des incidents sécurité numérique ;
3. La préparation des demandes de dérogation aux exigences de la PSN-ATE au regard des risques de sécurité numérique ;
4. La liste des contrôles de sécurité numérique envisagés sur certains systèmes d'information parmi ceux jugés essentiels ;
5. Le suivi de la mise en œuvre des plans d'action de réduction des écarts identifiés lors des contrôles.

Article 14. Les comités de suivi départementaux de la sécurité numérique

Le CSN réunit le comité de suivi de la sécurité numérique départemental (CSSN-D) sur son périmètre.

Il est composé :

1. Des directeurs des services déconcentrés mentionnés à l'article 3 si des arbitrages sont attendus à ce niveau ;
2. Du chef du service opérationnel des systèmes d'information à l'échelle du département ;
3. Du RSSI ;
4. Des ALSN et ALSSI.

Il est recommandé de l'inclure dans un ou des comités existants au niveau départemental.

Il se réunit au moins une fois par trimestre.

Il peut se réunir notamment pour :

1. Le suivi des plans de remédiation ;
2. Le suivi des démarches d'intégration de la sécurité dans les projets locaux (DISSIP) ;

3. Le suivi de la mise en œuvre des plans d'action de réduction des écarts identifiés lors des contrôles.

TITRE III : Gestion du risque numérique

Article 15. Homologation de sécurité.

L'AQSSI désigne comme autorité d'homologation d'un système d'information local le directeur dont le service déconcentré assure le rôle de maîtrise d'ouvrage.

L'AQSSI désigne comme autorité d'homologation d'un système d'information local ayant plusieurs services déconcentrés comme maîtrise d'ouvrage, un des directeurs de ces services.

Une démarche d'intégration de la sécurité dans les projets tel que la DISSIP pour le ministère de l'intérieur est impérative en cas de projet de mutualisation de systèmes d'information entre les services déconcentrés mentionnés à l'article 3 et tout autre service déconcentré de l'Etat.

Tous les systèmes d'information font l'objet d'une homologation de sécurité traitant spécifiquement des risques associés à la pratique du télétravail.

Le processus d'homologation d'un système d'information essentiel implique la présence du SHFD dès la réunion de lancement.

Le FSSI de l'autorité administrative en charge des systèmes d'information nécessaires à l'exécution des politiques publiques par les services déconcentrés mentionnés à l'article 3 transmet les décisions d'homologations de ces systèmes au FSSI du ministère de l'intérieur.

FIN DU DOCUMENT