



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Objectifs et règles de sécurité numérique du ministère de l'Intérieur

PGSN – A13

Conformité, audit, inspection, contrôle

Version 1.0

Préambule

Le présent document est une composante à part entière de la politique générale de sécurité numérique du ministère de l'intérieur (PGSN-MI).

Les principes stratégiques de la PGSN-MI et les dispositions générales de l'instruction sont traduits au sein du présent document en objectifs à atteindre, reprenant la structure de la politique de sécurité des systèmes d'information de l'Etat (PSSI-E).

Des règles techniques ou non techniques permettant de contribuer à la réalisation de chaque objectif sont énoncées au sein du présent document :

- Les mesures préfixées par « PSSI-E », suivies de la nomenclature seule, sont des règles inchangées de la PSSI-E de 2014. Des modifications peuvent néanmoins y être effectuées sur l'appellation de certaines fonctions propres au ministère.
- Les mesures préfixées « MI- » sont des mesures venant préciser la règle originale ou définir des règles propres au ministère de l'intérieur, formulées par le SHFD.

Toute dérogation à un objectif ou une règle du présent document, doit se faire en conformité avec la règle *MI-ORG-PGSN-DEROG* du document [PGSN-A01] du corpus de la sécurité numérique.

Conformité, audit, inspection, contrôle

1. Contrôles

Objectif A13-1 : contrôles réguliers. Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

MI-CONTR-SN : contrôles locaux. La conformité à la PSSIE et à la PGSN ministérielle est vérifiée par des contrôles réguliers. Pour les SIE, les constats et les plans d'action sont suivis en COPIL SN ministériel, voire en COSTRAT SN en cas de difficulté. Pour les autres systèmes d'information, les CSN ont pour mission de présenter les conclusions des audits et les plans d'action à leurs autorités respectives. Ils conduisent par ailleurs les actions locales d'évaluation de la conformité à la PGSN-MI et contribuent à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en œuvre, dans le cadre de leur mission.

MI-CONTR-BILAN-SN : bilan annuel. Le HFD établit un bilan annuel de synthèse mesurant le niveau de maturité global du ministère en matière de sécurité numérique, qu'il transmet à l'ANSSI en début d'année civile sur la base des rapports annuels communiqués par chaque AQSSI, élaborés à partir des éléments reçus par ses acteurs SN, pour son périmètre.

MI-CONTR-BILAN-SIIV : bilan annuels des SIIV. Chaque CSN d'un système d'information d'importance vitale d'un opérateur du ministère de l'Intérieur, doit adresser annuellement au SHFD via ISIS, un état des lieux du niveau de sécurité conformément à l'arrêté du 29 mai 2019¹. Cet état des lieux doit être transmis au plus tard le 31 mars de chaque année civile et comporter à minima les éléments suivants :

- Un bilan sur le niveau de conformité aux exigences de la PGSN et son corpus ;
- Le nombre d'incident rencontré au cours de l'année N-1 ;
- Les différents audits de sécurité réalisés ;
- Un état d'avancement :
 - o De la correction des écarts identifiés lors des audits ;
 - o Des mesures identifiées dans les analyses de risques ;
 - o Des chantiers de sécurisation significatifs ;
 - o Du chantier de supervision de sécurité.
- Les ressources du projet (humaines et % budgétaire) affectées à la SSI ;
- Un bilan sur le niveau de conformité global du système vis à vis des exigences de l'arrêté.

¹ Arrêté du 29 mai 2019 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 civiles de l'Etat » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.

MI-CONTR-OUTILS : outils d'audit des SI. Chaque AQSSI est libre dans les choix des outils permettant d'auditer les systèmes d'information dont il est responsable (programme de Bug Bounty, outil d'analyse de vulnérabilité, ...). Quels que soient les résultats des audits réalisés par de tels outils, ils ne peuvent se substituer aux éléments attendus dans les dossiers d'homologation conformément à la démarche d'intégration dans les projets du ministère mais peuvent venir renforcer la démarche d'amélioration continue en vigueur sur l'objet d'analyse.