



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – A07

Architecture des SI

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- », suivies de la nomenclature seule, sont des règles inchangées de la PSSI 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.

Dans la suite du document, le terme « DSI ministérielles » regroupe la direction du numérique et le service des technologies et des systèmes d'information de la sécurité intérieure.

Architecture des centres informatiques

Objectif A7-1 : architecture sécurisée des centres informatiques. Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

PSSIE-ARCHI-HEBERG : principes d'architecture de la zone d'hébergement. D'une manière générale, l'architecture des infrastructures des centres informatiques est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité. Le principe de défense en profondeur doit être respecté, en particulier par la mise en œuvre successive de « zones démilitarisées » (DMZ), d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.

PSSIE-ARCHI-STOCKCI : architecture de stockage et de sauvegarde. Le réseau de stockage/sauvegarde pour les besoins des centres informatiques repose sur une architecture dédiée à cet effet.

MI-ARCHI-PASS : passerelle Internet. Les interconnexions Internet passent obligatoirement par les passerelles nationales homologuées et exploitées par les DSI ministérielles. Pour chaque usage, une configuration spécifique de la chaîne de service, en charge de l'analyse des flux (rupture protocolaire) et de l'authentification, est mise en œuvre¹.

MI-ARCHI-SEP-ENV : séparation des environnements. Les environnements de développement, de qualification et de préproduction doivent être séparés (physiquement ou logiquement) des environnements de production afin de réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.

Dans le but de ne pas constituer une porte d'entrée privilégiée sur le système d'information ministériel, tout environnement doit être maintenu à jour de ses correctifs de sécurité.

MI-ARCHI-PFAU : sécurisation des architectures des plateformes d'appels d'urgence. Dans le cadre de la mise en œuvre de systèmes d'appels d'urgence, des capacités téléphoniques distinctes doivent être mises en œuvre, avec des numéros à 10 chiffres différents :

- Pour les appels directs provenant des réseaux opérateurs ;
- Pour les appels redirigés par des opérateurs privés tel que le syndicat national des sociétés d'assurances.

¹ Se référer au guide d'architecture d'interconnexion sécurisée publié par l'ANSSI : <https://www.ssi.gouv.fr/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/>