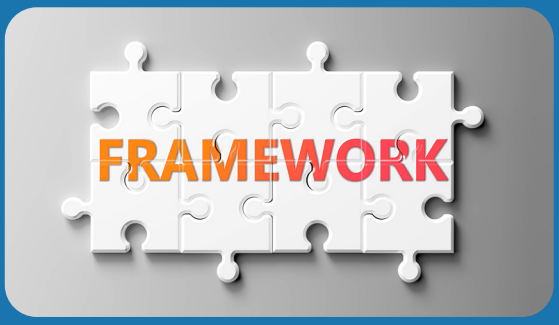
GUIDE

Guide d'utilisation du référentiel de sécurité de l'information



Introduction

Ce document vise à fournir un guide d'utilisation des documents composant le référentiel de sécurité de l'information fournit aux administrations et services de l'État (ci-après, « entités ») par le Haut-Commissariat à la protection nationale (HCPN), dans le cadre de sa fonction d'Agence nationale de la sécurité des systèmes d'information (ANSSI). Ce référentiel s'inscrit dans le cadre de la Politique Générale de Sécurité de l'Information (PGSI) de l'État, qui fixe les orientations générales en matière de sécurité de l'information, et est complété par le guide pratique de l'ANSSI « Mettre en place la sécurité de l'information – Les étapes clés pour bien débuter », qui en propose une déclinaison opérationnelle en actions concrètes.

Le présent référentiel constitue un modèle de référence. Chaque entité est invitée à l'adapter à sa taille, ses ressources, ses enjeux de sécurité, afin d'assurer une mise en œuvre proportionnée et efficace des mesures de sécurité de l'information.

Architecture

La Politique Générale de Sécurité de l'Information (PGSI) de l'entité

La PGSI constitue le document fondateur et central de la sécurité de l'information de l'entité. Elle fixe les orientations stratégiques et les objectifs qui encadrent l'ensemble des démarches en matière de sécurité de l'information. Elle établit ainsi le point de départ et le cadre de référence pour la mise en œuvre de la sécurité de l'information, en cohérence avec les exigences NIS2 et ISO/IEC 27001, sans détailler les mesures opérationnelles.

La politique et les lignes directrices de la gestion de l'organisation de la sécurité de l'information

Ces documents définissent le cadre d'organisation de la sécurité de l'information et proposent des recommandations concrètes pour sa mise en œuvre. Ils visent à structurer la gouvernance, en précisant les rôles, les responsabilités et les mécanismes de coordination, afin d'assurer une gestion cohérente et efficace de la sécurité de l'information. A ce titre, ils constituent un domaine transverse qui structure la gouvernance de l'ensemble des politiques thématiques, en garantissant une mise en œuvre des mesures de sécurité adaptée au fonctionnement de l'entité.

Les politiques thématiques de sécurité

Les politiques thématiques de sécurité couvrent les principaux domaines de la sécurité de l'information et proposent un ensemble de mesures et de bonnes pratiques permettant à chaque entité d'adapter les mesures en fonction de son contexte et de ses risques.

Les mesures sont classées en mesures fondamentales, constituant un socle commun applicable à l'ensemble des entités, et en mesures complémentaires, adaptées aux entités présentant des enjeux de sécurité plus élevés, en fonction de leur taille, de leurs ressources ou de leur exposition aux risques.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale
Agence nationale de la sécurité
des systèmes d'information

Les lignes directrices

Les lignes directrices contiennent un ensemble de recommandations visant à faciliter la mise en œuvre concrète des mesures décrites dans les politiques thématiques de sécurité, conformément aux bonnes pratiques. Elles précisent comment mettre en œuvre ces mesures de sécurité.

Chaque mesure peut être mise en œuvre selon trois niveaux de recommandation :

- Niveau 1 : recommandations de base, applicables à l'ensemble des entités ;
- Niveau 2 : recommandations de renforcement, destinées aux entités présentant des enjeux de sécurité plus importants, au regard de leur taille, de leurs ressources ou de leur exposition aux risques ;
- Niveau 3 : recommandations avancées, destinées aux entités les plus exposées ou présentant des enjeux de sécurité élevés.

Les procédures, guides et modèles

Les procédures précisent, à partir des politiques thématiques et des lignes directrices associées, les modalités opérationnelles permettant de mettre en œuvre les mesures de sécurité au sein de l'entité.

Les guides apportent des explications détaillées, des méthodes et des exemples pratiques permettant de faciliter la mise en œuvre des mesures et des procédures.

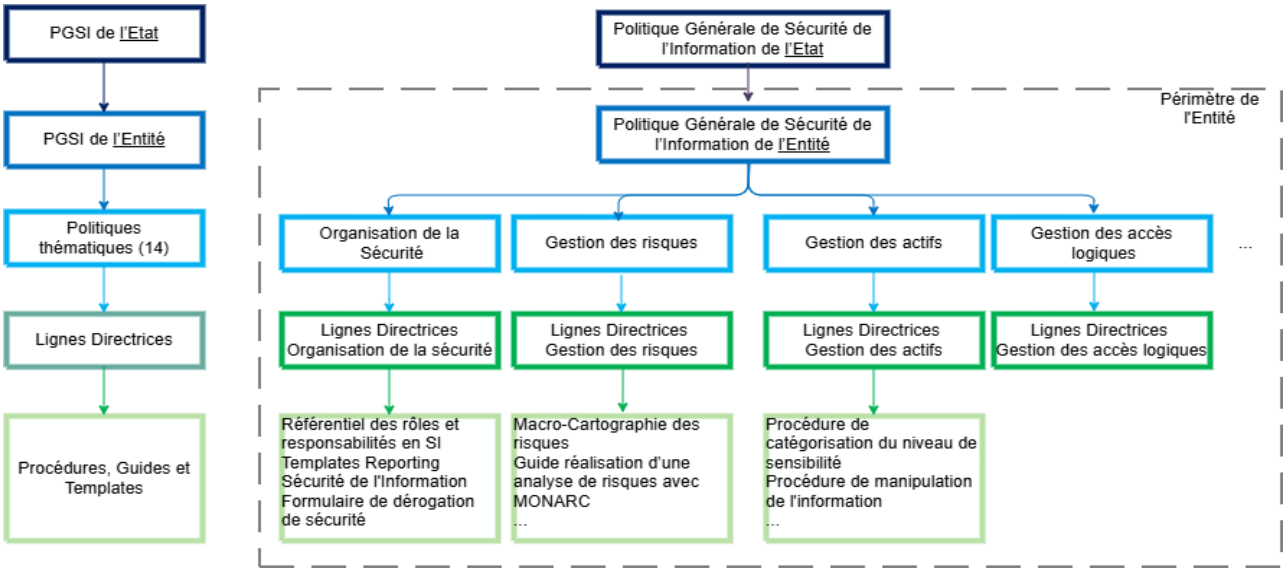
Les modèles (templates) proposent des supports standardisés destinés à harmoniser les pratiques et à faciliter la production des livrables.

Les documents transverses du référentiel

Le référentiel comprend également des documents transverses applicables à l'ensemble de ses composantes :

- Glossaire de la sécurité de l'information afin d'assurer une compréhension commune et une interprétation homogène du référentiel de sécurité.
- Référentiel des rôles et responsabilités en sécurité de l'information, afin de structurer la gouvernance et de clarifier les responsabilités au sein des entités.

Schéma de l'architecture du référentiel de sécurité de l'information



Informations pratiques

L'ensemble des documents mentionnés dans ce guide pratique est disponible sur l'extranet du HCPN dans sa fonction d'ANSSI.

En cas de question ou de besoin d'accompagnement concernant l'application du présent document, le HCPN/ANSSI, se tient à votre disposition.

Pour toute demande, vous pouvez nous contacter :

- Par courriel : support@anssi.etat.lu
- Par téléphone : 247-88930