LËTZ PREPARE!
STRATÉGIE NATIONALE DE RÉSILIENCE

# GUIDE PRATIQUE

## Mettre en place la sécurité de l'information – Les étapes clés pour bien débuter

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

## Contactez-nous

En cas de question ou de besoin d'accompagnement concernant l'application du présent document, le Haut-Commissariat à la protection nationale (HCPN), dans sa fonction d'Agence nationale de la sécurité des systèmes d'information (ANSSI), se tient à votre disposition.

**POUR TOUTE DEMANDE,**
**VOUS POUVEZ NOUS CONTACTER :**

support@anssi.etat.lu • T. 247-88930

## Où trouver nos informations ?

L'ensemble de nos informations, documents et outils est accessible en ligne :

Notre Extranet ANSSI

Notre GovSpace

# Introduction

## Objectif du guide

Ce guide a pour objectif de décrire comment débuter la sécurité de l'information, en présentant les bonnes pratiques permettant à une entité de prendre rapidement en main la gestion de la sécurité de l'information. Il s'agit d'une démarche inscrite dans une logique d'amélioration continue, reposant sur des étapes itératives qui permettent d'apprendre de ses erreurs, d'ajuster son dispositif et de renforcer progressivement sa maturité.

À noter que le présent guide ne couvre pas les aspects de la sécurité des informations classifiées visées par la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

## À qui s'adresse ce guide ?

Ce guide est destiné aux ministères, administrations et services de l'État, qu'ils soient ou non soumis aux obligations de la directive européenne (UE) 2022/2555 sur la sécurité des réseaux et des systèmes d'information dite « directive NIS 2 ».

Il vise à les accompagner dans la mise en œuvre des bases d'un dispositif de sécurité de l'information adapté à leur taille, à leurs ressources et à leurs enjeux.

Il s'adresse principalement aux acteurs de la sécurité de l'information au sein de ces entités, tels que les membres de la direction ou les délégués à la sécurité de l'information.

## Comment utiliser ce guide ?

Ce guide a été conçu pour être utilisé de manière simple et flexible, afin de s'adapter aux besoins spécifiques de chaque entité. Il se compose de trois phases progressives, à déployer selon les priorités et les ressources de chaque entité, dans le respect des obligations réglementaires.

**PHASE 1**
Initiation et planning

**PHASE 2**
Les fondations de la sécurité

**PHASE 3**
Mise en œuvre

**Nous vous recommandons d'utiliser ce guide avec l'approche suivante :**

### → PHASAGE

Suivez les trois phases du guide dans l'ordre, en commençant par la phase « Initiation et planning ». Chaque étape est conçue pour vous accompagner progressivement dans la mise en place de mesures de sécurité de l'information adaptées aux spécificités de votre entité.

### → MODULARITÉ

Certaines phases ou actions sont déjà mises en œuvre au sein de votre entité, concentrez-vous sur les étapes restantes. Ce guide a été conçu pour offrir une flexibilité suffisante afin de s'adapter à la taille, aux ressources et au niveau de maturité de chaque entité.

### → PROGRESSIVITÉ

Chaque étape prépare la suivante, assurant une progression logique et une construction cohérente du dispositif de sécurité de l'information.

# SOMMAIRE

# PHASE 1

## INITIATION ET PLANNING

# 1. Définition du périmètre

**OBJECTIF**

Identifier et protéger les services métiers vitaux afin de garantir la continuité des missions essentielles de l'entité, en évaluant les impacts potentiels d'une interruption, les interdépendances entre services et les dépendances vis-à-vis des prestataires critiques.

## Services métiers vitaux : ce qu'il faut savoir

Les services métiers vitaux regroupent les activités prioritaires qui permettent à une entité d'accomplir sa mission. Leur interruption pourrait entraîner des conséquences majeures sur les plans opérationnel, réputationnel, légal et/ou financier.

Avant de pouvoir les protéger, il est nécessaire de recenser l'ensemble des services proposés par l'entité, qu'ils soient destinés aux usagers externes (p. ex. citoyens ou entités tierces) ou aux opérations internes.

La protection de ces services repose sur l'application des principes fondamentaux de la sécurité de l'information :

- Confidentialité : seules les personnes autorisées peuvent accéder à l'information,
- Intégrité : l'information reste exacte, complète et non altérée,
- Disponibilité : les services et les informations sont accessibles au moment opportun.

## Analyse de l'impact d'une interruption

Une fois la liste des services établie, il convient d'évaluer pour chacun d'eux l'impact potentiel en cas d'interruption ou de compromission.

Cette analyse permet d'identifier les services métiers vitaux, dont la continuité est indispensable à l'accomplissement de la mission de l'entité. Pour la conduire efficacement, il est recommandé de s'interroger sur les axes suivants :

**IMPACT SUR LA RÉPUTATION**

- Une interruption ou une faille de ce service métier pourrait-elle nuire à l'image ou à la confiance des usagers, partenaires ou du public ?
- Une panne prolongée pourrait-elle entraîner des plaintes, une couverture médiatique négative ou un scandale public ?
- Une mauvaise gestion de ce service pourrait-elle compromettre la crédibilité de l'entité auprès de ses parties prenantes ?

**IMPACT OPÉRATIONNEL**

- Ce service métier est-il indispensable au fonctionnement d'autres services ou processus internes ?
- Une interruption bloquerait-elle les activités de plusieurs collaborateurs ou équipes ?
- Ce service est-il utilisé quotidiennement pour assurer une mission essentielle ou la continuité des opérations de l'entité ?

**IMPACT LÉGAL**

- Ce service métier est-il soumis à des obligations légales, réglementaires ou contractuelles spécifiques ?
- Une défaillance pourrait-elle entraîner une non-conformité ou exposer l'entité à des sanctions, amendes ou litiges juridiques ?
- Des textes légaux ou contrats imposent-ils que ce service soit maintenu en continu ou exploité dans des conditions de sécurité spécifiques ?

**IMPACT FINANCIER**

- Une interruption de ce service métier pourrait-elle entraîner des pertes financières, des pénalités contractuelles ou des coûts supplémentaires imprévus ?
- La remise en état ou la gestion des conséquences d'une panne nécessiterait-elle des dépenses importantes ou non budgétées ?
- Une indisponibilité prolongée pourrait-elle déséquilibrer le budget de l'entité ou compromettre la réalisation d'une mission essentielle ?

Il est essentiel d'identifier les relations et interdépendances entre les services afin de comprendre les effets en cascade qu'une défaillance pourrait entraîner. Certains services ou entités de support, a priori non vitaux, peuvent en réalité soutenir des fonctions internes essentielles comme par exemple, une base de données partagée dont l'indisponibilité affecterait plusieurs départements.

## Identification des prestataires et des dépendances

Commencer par inventorier l'ensemble des prestataires contribuant au fonctionnement des services de l'entité, qu'il s'agisse de prestataires informatiques, d'infrastructures, de support métier ou de services utilitaires.

Pour chacun d'eux, évaluer le niveau de dépendance et de criticité, en analysant l'impact qu'aurait une interruption ou une défaillance de leurs prestations sur les opérations de l'entité.

Cette évaluation devrait permettre d'identifier les prestataires dont les services sont essentiels à la continuité des activités, notamment ceux dont l'indisponibilité pourrait entraîner l'arrêt ou la dégradation des services métiers vitaux.

**POUR EN SAVOIR PLUS**

Utiliser le formulaire de dépendances fourni par l'Institut Luxembourgeois de Régulation (ILR) pour répertorier les dépendances

# 2. Auto-évaluation

**OBJECTIF**

Évaluer la situation actuelle en matière de sécurité de l'information, puis déterminer les actions à entreprendre pour atteindre le niveau de maturité visé.

## Évaluation de la maturité actuelle

Commencez par réaliser un état des lieux à l'aide du tableau d'auto-évaluation de l'ILR, qui vous guidera à travers les principaux objectifs de sécurité définis par l'ENISA.

Pour chaque objectif, évaluez les mesures existantes et déterminez votre niveau de maturité (ou de sophistication) selon l'échelle suivante : 0 (N/A ou sans mesure), 1 (basique), 2 (standard industriel) à 3 (état de l'art). Chaque niveau supérieur ne peut être atteint que si les prérequis du niveau précédent sont remplis.

L'évaluation devrait s'appuyer sur des preuves concrètes et vérifiables, telles que des politiques internes, des plans de gestion des incidents ou tout autre document démontrant l'existence des mesures en place. Si la mesure n'existe pas encore, indiquez ce qui la remplace temporairement.

La note ne devrait pas être surestimée : le questionnaire est conçu de manière progressive afin de refléter fidèlement le niveau de maturité et de soutenir une démarche d'amélioration continue.

## Définir le niveau de maturité visé

Une fois cet état des lieux établi, il convient ensuite de déterminer le niveau de maturité visé pour chaque objectif de sécurité, en tenant compte notamment des éléments suivants :

- Les exigences réglementaires applicables à l'entité, notamment la directive NIS2 et toute autre réglementation pertinente ;
- Le niveau de risque opérationnel, évalué au regard des enjeux de sécurité de l'entité, notamment la criticité de ses systèmes et la sensibilité de ses données ;
- Les ressources disponibles, qu'il s'agisse des compétences internes, des outils ou du budget alloué à la sécurité.

Pour une entité qui débute la mise en place de son dispositif de sécurité de l'information, il est recommandé de viser à court terme le niveau 1 (basique).

En revanche, lorsqu'une entité présente des enjeux significatifs en matière de sécurité de l'information et de continuité d'activité, elle devrait viser au minimum le niveau 2 (standard industriel).

## Identification et analyse des écarts

Une fois l'auto-évaluation réalisée, identifiez, pour chaque objectif de sécurité, les actions à entreprendre pour atteindre le niveau de maturité visé. Ces actions constitueront la base du plan d'action à mettre en œuvre.

**POUR EN SAVOIR PLUS**

Des recommandations en relation avec l'auto-évaluation seront publiées sur l'Extranet de l'ANSSI.

Réalisez l'état des lieux à l'aide du tableau d'auto-évaluation de l'ILR.

# 3. Macro-cartographie des risques

**OBJECTIFS**

Obtenir une vision consolidée et hiérarchisée des principaux risques susceptibles d'affecter la sécurité et la continuité des services métiers vitaux, de faciliter la prise de décision au niveau de la direction et d'orienter les priorités du plan d'action.

**NOTE IMPORTANTE**

Il est recommandé aux entités d'appuyer prioritairement leurs travaux en matière de sécurité de l'information sur les résultats de l'auto-évaluation. L'élaboration d'une macro-cartographie des risques est également encouragée car elle permet notamment de prioriser efficacement les actions à mettre en place lors du plan d'action, mais cette étape demeure facultative.

La macro-cartographie des risques en matière de sécurité de l'information constitue un outil stratégique permettant d'obtenir d'une vue d'ensemble claire et hiérarchisée des menaces majeures susceptibles d'affecter la continuité et la sécurité des services métiers vitaux d'une entité.

Elle est principalement destinée aux acteurs impliqués dans la gouvernance de la sécurité de l'information au sein d'une entité :

- La direction : pour disposer d'une vue d'ensemble des enjeux de sécurité et appuyer les décisions d'investissement ou de priorisation ;
- Les responsables de services métiers : pour comprendre les risques pesant sur leurs activités vitales et contribuer à leur évaluation ;
- Le Délégué à la Sécurité de l'Information (DSI) ainsi que le Délégué à la Protection des Données (DPD) : pour orienter les actions de protection ;
- Le service informatique : pour aligner ses priorités sur les enjeux métiers et contribuer à la définition et au traitement des risques majeurs de l'entité.

Contrairement à une analyse de risques détaillée, centrée par exemple sur un service, un projet ou actif technique, la macro-cartographie se concentre sur les risques de haut niveau et les processus métiers vitaux.

La démarche repose sur l'identification et l'évaluation de scénarios types, qui devraient être complétés et/ou adaptés au contexte et aux missions de l'entité. Ces scénarios traduisent des situations plausibles et significatives, permettant de mesurer l'impact et la vraisemblance des risques. Ils peuvent inclure :

- une attaque par ransomware entraînant l'indisponibilité de systèmes critiques ;
- le vol d'identifiants ou la compromission de comptes,
- la compromission d'un fournisseur impactant la chaîne de services ;
- une attaque par déni de service (DDoS) perturbant la disponibilité des services en ligne.

**POUR EN SAVOIR PLUS**

Un template de macro-cartographie des risques sera publié sur l'Extranet de l'ANSSI.

# 4. Le plan d'action pluriannuel

**OBJECTIF**

Planifier et piloter la mise en œuvre des actions de sécurité afin de réduire les risques prioritaires, renforcer la conformité NIS2 et assurer une amélioration continue du dispositif de sécurité de l'information.

**NOTE IMPORTANTE**

Il est recommandé de prioriser en premier lieu les actions relevant du périmètre direct de l'entité. Si la dépendance aux fournisseurs est élevée, les mesures liées à la chaîne d'approvisionnement devraient être placées au même rang de priorité.

## Détermination des actions de sécurité

Les actions de sécurité à mettre en œuvre devraient être définies principalement sur la base des résultats de l'auto-évaluation et, le cas échéant, complétées par les enseignements issus de la macro-cartographie des risques.

## Planifier et prioriser les actions de sécurité

Les actions de sécurité devraient être priorisées en fonction de :

- Leur impact sur la sécurité des services métiers vitaux, de leur capacité à atténuer les risques identifiés et de leur contribution à la conformité avec les exigences de la directive NIS2 ;
- Des recommandations formulées par l'ILR, ainsi que de celles issues des audits internes ou externes, lorsqu'ils existent ;
- Leur potentiel de gains rapides ("quick wins"), c'est-à-dire des actions peu coûteuses mais à fort impact, permettant de générer rapidement des résultats tangibles et de favoriser une dynamique positive ;
- Leur aptitude à répondre simultanément aux écarts constatés lors de l'auto-évaluation et aux risques mis en évidence dans la macro-cartographie (lorsqu'elle existe).

## Le plan d'action pluriannuel

Afin d'assurer une vision stratégique cohérente et un pilotage progressif et structuré des initiatives en matière de sécurité de l'information, l'entité devrait regrouper et formaliser l'ensemble des actions prévues au sein d'un plan d'action pluriannuel, d'une durée indicative de trois ans.

Le plan d'action peut décrire, pour chaque action de sécurité retenue, les éléments suivants :

- L'action concrète à mettre en œuvre ;
- La priorité de mise en œuvre ;
- Le ou les objectifs de sécurité adressés ;
- Pour les entités ayant réalisé une macro-cartographie, le ou les risques adressés.
- Le responsable désigné pour leur exécution ;
- Le délai prévu pour sa mise en œuvre ;
- Ainsi que les ressources humaines, techniques et budgétaires nécessaires à leur réalisation.

Il devrait faire l'objet d'une validation par la direction, garantissant ainsi son alignement avec les orientations stratégiques de l'entité et la mise à disposition des ressources nécessaires à sa mise en œuvre.

## Pilotage et suivi

Le pilotage du plan d'action devrait être coordonné par le DSI, en lien avec la direction et les responsables opérationnels concernés. Il repose sur un suivi régulier de l'avancement des mesures, permettant d'évaluer les progrès réalisés, d'identifier les obstacles et de proposer les ajustements nécessaires.

Des revues périodiques, au minimum annuelles, devraient être organisées afin d'actualiser les priorités, de réviser les échéances et d'informer la direction de l'état d'avancement global. Ce dispositif contribue à assurer la cohérence, la continuité et l'efficacité de la démarche de sécurité.

**CONSEILS PRATIQUES**

- Impliquez les responsables métiers, le DPD ainsi que les autres fonctions clés (p. ex. service juridique ou conformité) pour identifier les besoins de sécurité réels et éviter les mesures déconnectées du terrain.
- Identifiez 5 actions clés à engager la première année, plutôt que d'éparpiller les efforts.
- Classez les mesures dans trois niveaux de priorité : immédiate (0-6 mois), à moyen terme (6-18 mois) et à long terme (>18 mois).
- Créez des tableaux de bord dynamiques permettant de visualiser en temps réel l'avancement du plan d'action.
- Préparez des rapports concis présentant l'état d'avancement, les réalisations et les défis en cours aux parties prenantes, notamment au Comité de Sécurité de l'Information (cf. « Phase 2 : Les fondations de la sécurité »).

# PHASE 2

## LES FONDATIONS DE LA SÉCURITÉ

# 1. Organisation de la sécurité

**OBJECTIF**

Mettre en place une gouvernance structurée et cohérente de la sécurité de l'information, garantissant la coordination des actions, la maîtrise des risques et la gestion encadrée des dérogations afin d'assurer un équilibre durable entre sécurité et exigences opérationnelles.

## Responsabilité de la direction

La directive NIS2 renforce le rôle central de la direction dans la gouvernance de la sécurité de l'information. Les membres des organes de direction ont la responsabilité de valider les mesures pour gérer les risques liés à la cybersécurité, veiller à leur mise en œuvre, et peuvent être tenus responsables en cas de manquement.

Ils doivent également se former régulièrement afin de comprendre les menaces, évaluer les risques et suivre efficacement la posture de sécurité de leur organisation. Ils doivent offrir une formation similaire à leur personnel.

## Le délégué à la sécurité de l'Information

La direction devrait nommer un Délégué à la Sécurité de l'Information (DSI), également appelé Responsable de la Sécurité des Systèmes d'Information (RSSI) dans le secteur privé. Il agit comme un chef d'orchestre, s'assurant que l'ensemble des mesures techniques, organisationnelles, et humaines sont implémentées pour maintenir la confidentialité, l'intégrité, et la disponibilité des actifs numériques.

Afin de lui permettre d'exercer pleinement ses responsabilités, il devrait idéalement être rattaché directement à la direction. À défaut, il devrait disposer d'un accès régulier et direct aux instances dirigeantes.

## Le comité de sécurité de l'information

Pour les entités de taille significative, la création d'un Comité de Sécurité de l'Information (CSI) constitue une étape essentielle pour instaurer une gouvernance cohérente, efficace et durable. Ce comité favorise la prise de décision éclairée en matière de sécurité en réunissant notamment la direction, le DSI, le responsable informatique, les représentants métiers et le DPD autour d'une vision commune des priorités et des risques.

## Gestion des dérogations

La mise en place d'un processus de gestion des dérogations permet d'encadrer, de manière formalisée, les exceptions temporaires aux règles de sécurité lorsque leur application immédiate s'avère impossible ou inadaptée (par exemple, l'utilisation temporaire d'un outil non validé).

Chaque dérogation devrait être dûment justifiée, documentée, limitée dans le temps et approuvée selon le niveau de risque associé, puis faire l'objet d'un suivi permettant le retour à la conformité dans des délais acceptables.

**POUR EN SAVOIR PLUS**

Un modèle de description de fonction de DSI est disponible sur l'Extranet du HCPN/ANSSI.

Une politique et des lignes directrices en relation avec l'organisation de la sécurité seront publiées sur l'Extranet de l'ANSSI.

Des formations à destination des agents occupant une fonction de management (p. ex. cadres dirigeants) et/ou travaillant dans le domaine informatique (p. ex. DSI) seront ajoutées au catalogue de l'Institut national d'administration publique (INAP) en 2026.

# 2. Référentiel de sécurité

**OBJECTIF**

Structurer et formaliser le référentiel de sécurité de l'information, en s'appuyant sur des cadres de référence reconnus et une hiérarchie documentaire cohérente avec la PGSI de l'État, afin d'assurer la cohérence et l'application effective des mesures de sécurité.

## Cadres de références et bonnes pratiques

Dans un premier temps, le DSI devrait s'appuyer sur des référentiels adaptés pour orienter la rédaction des documents, sans chercher à appliquer de manière exhaustive des normes complexes. Les bonnes pratiques issues des normes internationales (ISO/IEC 27001, 27002, 22301, etc.) constituent une base solide pour structurer la démarche de sécurité. Elles peuvent être complétées par les guides et recommandations de l'ENISA.

## PGSI, politiques, procédures et guides

La construction du référentiel de sécurité peut s'organiser selon une logique pyramidale :

- Au sommet, l'entité devrait définir sa Politique Générale de Sécurité de l'Information (PGSI), définissant notamment ses objectifs de sécurité et son organisation. Établie en conformité avec la PGSI de l'État, elle devrait être adaptée à son contexte, ses missions et ses enjeux de sécurité spécifiques ;
- Les politiques thématiques précisent les mesures applicables à chaque domaine de la sécurité (gestion des risques, gestion des accès, continuité, etc.) ;
- Enfin, les procédures et guides opérationnels traduisent ces mesures en actions concrètes, décrivant comment appliquer et maintenir les mesures de sécurité au quotidien.

Afin de faciliter cette formalisation, le HCPN/ANSSI mettra à disposition des entités des documents permettant de construire le référentiel de sécurité de chaque entité :

- un modèle de PGSI pour les entités,
- des modèles de politiques générales thématiques et des lignes directrices fournissant des recommandations d'implémentation,
- ainsi que des guides pratiques détaillant la mise en œuvre concrète de ces recommandations.

## Validation

La validation du référentiel de sécurité devrait suivre la hiérarchie des documents :

- La PGSI devrait être approuvée par la direction, attestant son engagement et son caractère obligatoire ;
- Les politiques thématiques devraient être validées par le Comité de Sécurité de l'Information (CSI), si celui-ci existe, ou à défaut par la direction ;
- Les procédures et guides opérationnels devraient être validés par le responsable concerné ou le DSI.

**CONSEILS PRATIQUES**

- Privilégiez des documents concis et ciblés, adaptés à leur audience (direction, métiers, IT, etc.), pour favoriser leur appropriation.
- Associez les parties prenantes clés (direction, IT, métiers, DPO) dès la rédaction pour garantir l'adhésion et l'applicabilité.
- Utilisez des fiches pratiques et checklists pour accompagner les procédures et faciliter leur application quotidienne.
- Des documents permettant de compléter ce référentiel de sécurité, pour les aspects spécifiques de la protection des données à caractère personnel, sont régulièrement publiés sur le SharePoint du CGPD.

# 3. Accompagnement des projets

**OBJECTIF**

Assurer l'intégration systématique de la sécurité de l'information dès la conception, en identifiant les besoins de protection, en impliquant le DSI dès le lancement des projets et en définissant les étapes clés nécessaires pour garantir la maîtrise des risques tout au long du cycle de vie des systèmes et services.

## Intégrer la sécurité dès la conception

L'intégration de la sécurité de l'information dès la conception (principe de « *security by design* ») vise à anticiper les risques avant qu'ils ne se concrétisent et à garantir que les mesures de protection soient intégrées au cœur même des projets.

Cette approche consiste à prendre en compte les exigences de sécurité, telles que la confidentialité, l'intégrité et la disponibilité, dès les premières phases de conception et de planification, plutôt que d'intervenir a posteriori.

Au cours de la phase de conception d'un projet, la nécessité d'allouer un budget dédié à la sécurité (p. ex. pour des outils, tests ou formations) devrait être déterminée.

## Informer le DSI dès le lancement de projets

Le DSI devrait être informé dès le démarrage de tout projet susceptible d'avoir un impact sur la sécurité du système d'information.

Cette implication précoce lui permet d'identifier les enjeux de sécurité, de proposer les mesures adaptées et d'assurer leur cohérence avec les objectifs métiers.

Pour cela, il est nécessaire que le DSI maintienne des échanges réguliers avec les parties prenantes clés de l'entité (direction, gestionnaire de projets, responsable informatique, responsables métiers, DPD, etc.) afin d'intégrer la sécurité de manière transversale dans toutes les initiatives.

## Identification des besoins en termes de sécurité

Il est important de détecter dès la phase de conception les projets présentant un risque et, le cas échéant, de mobiliser le DSI afin de coordonner l'implémentation des mesures de protection appropriées.

À cet effet, un questionnaire type, fourni par le DSI au chef de projet, peut servir d'outil de pré-évaluation des risques de sécurité pour tout nouveau projet ou modification impactant le système d'information. À travers une série de questions ciblées, la sensibilité des données traitées, les modalités d'accès et d'hébergement ainsi que les contraintes réglementaires associées seraient identifiées.

## Détermination des étapes clés du projet

Sur la base de ce questionnaire, le DSI identifie les étapes de sécurité prioritaires à intégrer tout au long du projet. Ces étapes peuvent inclure la réalisation d'une analyse de risques, la réalisation d'une analyse d'impact à la protection des données (AIPD), la réalisation d'une revue de code, la documentation de l'architecture sécurité, la documentation des instructions nécessaires à la gestion des accès ou la réalisation de tests de pénétrations.

**POUR EN SAVOIR PLUS**

Une politique et des lignes directrices en relation avec la gestion des incidents de sécurité seront publiées sur l'Extranet de l'ANSSI.

# 4. Gestion des incidents liés à la sécurité de l'information

**OBJECTIF**

Assurer une gestion efficace et maîtrisée des incidents de sécurité, afin de limiter les impacts, renforcer la résilience et prévenir la récurrence des événements de sécurité.

## Préparation

La première étape consiste à désigner une instance responsable de la gestion des événements et incidents de sécurité, chargée notamment de coordonner en interne la réponse à un incident de sécurité. Il est essentiel de sensibiliser les utilisateurs à l'importance du signalement rapide de tout événement suspect ou anomalie.

En l'absence de ressources internes suffisantes, l'entité devrait identifier à l'avance les prestataires externes spécialisés capables d'intervenir rapidement, parmi lesquels le HCPN/GOVCERT qui met notamment à disposition des entités étatiques un service de réponse aux attaques informatiques et aux incidents de sécurité majeurs.

Enfin, l'entité devrait veiller à conserver et exploiter des journaux d'activités (systèmes, applications, équipements réseau, etc.) suffisamment complets et horodatés, afin de permettre l'identification de l'origine, du déroulement et des impacts réels d'un incident de sécurité.

## Processus de gestion des incidents

Lorsqu'un incident de sécurité est détecté, un processus de gestion des incidents devrait être mis en œuvre afin d'en assurer le traitement complet et maîtrisé. Ce processus comprend notamment :

- L'analyse et la qualification de l'incident, visant à confirmer sa nature, son périmètre, sa gravité et ses impacts potentiels (p. ex. sur les services, les citoyens ou les informations de l'entité) ;
- La gestion et la résolution, incluant les mesures de confinement, d'éradication et de rétablissement des services affectés ;
- La phase post-incident, consistant à mener une analyse approfondie (post-mortem) pour notamment tirer les enseignements nécessaires afin d'accroître la résilience de l'entité.

## Notification des incidents importants

Conformément à la directive NIS2, toute entité est tenue de notifier les incidents importants à l'autorité compétente, y compris lorsque ceux-ci surviennent chez un fournisseur, selon les modalités suivantes :

- Alerte précoce : une première notification doit être transmise à l'autorité compétente dans un délai de 24 heures après la prise de connaissance d'un incident important ;
- Notification formelle : dans un délai maximum de 72 heures, une notification plus détaillée doit être soumise. Elle présente notamment une évaluation préliminaire de l'incident, accompagnée, si possible, des indicateurs de compromission identifiés ;
- Rapport final : au plus tard un mois après la notification formelle, un rapport final doit être transmis, reprenant les conclusions de l'analyse post-incident, les causes racines, les impacts constatés et les mesures correctives mises en œuvre.

**POUR EN SAVOIR PLUS**

Une politique et des lignes directrices en relation avec la gestion des incidents de sécurité seront publiées sur l'Extranet de l'ANSSI.

Les notifications devront être effectuées via le portail SERIMA de l'ILR, facilitant la conformité et la communication avec les autorités compétentes.

Brochure CGPD - Prévention et gestion des incidents de sécurité et des violations de données à caractère personnel.

# PHASE 3

## MISE EN ŒUVRE

# 1. Gestion de la continuité des activités

**→ OBJECTIF**

Assurer la continuité des activités vitales de l'entité en élaborant, testant et actualisant des plans de continuité, définissant les solutions nécessaires à la préservation des ressources critiques et garantissant une réaction rapide et coordonnée en cas de crise.

## Établissement des plans de continuité

Les plans de continuité de l'entité devraient couvrir l'ensemble des services métiers vitaux (voir Phase 1 : Initiation et planification – Définition du périmètre) et être fondés sur des scénarios réalistes, visant à préparer la réponse de l'organisation face à des défaillances ou indisponibilités de ses ressources critiques.

Ils devraient comporter des procédures détaillées et des fiches réflexes opérationnelles afin de faciliter la prise de décision et d'assurer une réaction rapide et coordonnée en situation de crise.

Il est recommandé de réaliser en amont une analyse d'impact sur les activités (« Business Impact Analysis »). Cette analyse permet notamment d'identifier les fonctions devant être maintenues en cas de perturbation, de déterminer les délais acceptables de reprise, ainsi que les ressources minimales nécessaires à leur continuité.

Ces plans devraient être adaptés à chaque fois qu'un changement important intervient, afin de garantir que les plans restent toujours à jour et opérationnels.

## Détermination des solutions de continuité

Des solutions adaptées devraient être implémentées pour garantir la continuité des ressources critiques, telles que les ressources humaines, les systèmes informatiques, les infrastructures (bâtiments) et les prestataires critiques.

Par exemple, la mise en place du télétravail, la rotation des équipes ou la redondance des systèmes peuvent contribuer à maintenir un niveau minimal d'activité.

## Tests, exercices et mise à jour

Une fois les plans rédigés, il est recommandé de planifier des tests et des exercices des plans de continuité, afin d'en évaluer la pertinence, l'efficacité et l'opérationnalité.

Ces exercices permettent de vérifier la préparation des équipes, d'identifier les axes d'amélioration des plans de continuité, et de sensibiliser le personnel à ses responsabilités tout en lui apprenant les réflexes à adopter en situation de crise.

**POUR EN SAVOIR PLUS**

Une politique et des lignes directrices en relation avec la gestion de la continuité des activités seront publiées sur l'Extranet de l'ANSSI.

« ISO 22301:2019 Sécurité et résilience – Systèmes de management de la continuité d'activité - Exigences ».

# 2. Gestion des actifs

**OBJECTIF**

Assurer une gestion cohérente et sécurisée des informations et des actifs informatiques, tout au long de leur cycle de vie.

## Une manipulation sûre et adaptée des informations

Une entité devrait veiller à ce que ses utilisateurs manipulent les informations selon les règles qu'elle a établies. En pratique, chaque utilisateur devrait être en mesure d'identifier le niveau de sensibilité applicable et d'appliquer les mesures de protection appropriées. Cette démarche renforce la sécurité globale de l'information et contribue à réduire les risques d'erreur, de fuite ou de mauvaise manipulation.

Du point de vue du département informatique, la catégorisation de la sensibilité des données permet de mieux appréhender leur valeur et de mettre en place des mesures de sécurité proportionnées.

Cette approche permet de concentrer les efforts sur les données les plus sensibles, d'éviter la surprotection des informations peu sensibles et d'optimiser l'utilisation du temps et des ressources.

## Catégorisation de la sensibilité de l'information

La catégorisation de la sensibilité de l'information consiste à évaluer et catégoriser les données, sur base de critères tels que leur nature, leur sensibilité à la divulgation, le volume de données concerné ou le cadre légal. Les informations peuvent être, par exemple, publiques (diffusables sans risque), non publiques (la divulgation non autorisée est non souhaitée mais sans impact majeur), sensibles (divulgation pouvant causer des préjudices financiers, juridiques ou réputationnels) ou très sensibles (informations dont la divulgation mettrait en péril la stratégie ou la viabilité de l'entité).

## Manipulation de l'information

L'entité devrait ensuite définir les règles minimales de protection à appliquer à toutes les informations de l'entité, qu'elles soient physiques ou électroniques, tout au long de leur cycle de vie : création, traitement, transmission, stockage et archivage/destruction.

Les mesures de protection varient selon le niveau de sensibilité : par exemple, les informations publiques ne nécessitent pas de restriction particulière ; les informations non publiques sont réservées aux collaborateurs internes ; les informations sensibles nécessitent un chiffrement pour les échanges externes et les très sensibles font l'objet d'un accès très limité, de transmissions uniquement chiffrées et tracées.

## Inventaire des actifs informatiques

L'inventaire des actifs informatiques vise à recenser l'ensemble des équipements, logiciels et ressources numériques utilisés par l'entité : serveurs, postes de travail, équipements réseau, applications, bases de données, etc. Il peut servir de base pour appliquer de manière standardisée des mesures de sécurité adaptées, telles que le chiffrement, la gestion des correctifs ou le contrôle des accès.

**POUR EN SAVOIR PLUS**

Une politique et des lignes directrices en relation avec la gestion des actifs seront publiées sur l'Extranet de l'ANSSI.

Brochure CGPD - Protection des données et archivage dans l'intérêt public.

# 3. Gestion des prestataires critiques

**OBJECTIF**

Assurer une gestion structurée, sécurisée et continue des fournisseurs et prestataires critiques, en établissant une gouvernance claire, en évaluant leur niveau de sécurité et de résilience, et en maintenant une surveillance régulière garantissant le respect durable des exigences contractuelles et de sécurité.

**NOTE IMPORTANTE**

Ces recommandations ne s'appliquent pas aux prestataires étatiques (p. ex. CTIE, CGIE ou CCSS), qui feront l'objet de recommandations ultérieures.

## Gouvernance de la relation fournisseur

L'entité devrait mettre en place une gouvernance claire et structurée pour la gestion des fournisseurs et des prestataires critiques, assurant une coordination efficace entre les parties prenantes internes (par exemple les métiers, la fonction sécurité, le juridique, le DPD ou le DSI). Cette organisation devrait permettre un pilotage rigoureux et un suivi cohérent des prestataires.

Les rôles et responsabilités de chaque acteur devraient être officiellement désignés, formalisés et documentés. À titre d'exemple, une personne de contact dédiée devrait être désignée pour chaque prestataire identifié.

## Évaluation des prestataires

Une fois les prestataires critiques identifiés et évalués, lors de « la phase 1 : Initiation et planning », il est recommandé d'obtenir une assurance concernant leur niveau acceptable de sécurité et de résilience.

Pour obtenir cette assurance, les actions suivantes sont à considérer :

- Formaliser les exigences et obligations contractuelles, en intégrant des clauses spécifiques de sécurité et de continuité de service, ainsi qu'une stratégie de sortie pour les prestataires critiques dont dépend fortement l'activité de l'entité.
- Vérifier les certifications du prestataire afin de s'assurer qu'elles sont reconnues, valides et alignées sur les exigences de sécurité de l'entité.
- Réaliser un audit afin de contrôler la conformité du prestataire aux exigences de sécurité définies et d'évaluer l'efficacité des mesures mises en œuvre.
- S'assurer que le prestataire dispose de plans de continuité (PCA) et de reprise d'activité (PRA) régulièrement testés et actualisés.

Les contrats fournisseurs devraient inclure des obligations claires de notification en cas d'incident de sécurité affectant les services fournis, en précisant les modalités de signalement (délais, types d'incidents, canaux de communication, interlocuteurs). Ces dispositions visent à garantir le respect des délais prévus par la directive NIS2 (voir section « 11. Gestion des incidents liés à la sécurité de l'information »).

## Surveillance continue des prestataires critiques

Une saine gestion des prestataires repose sur une surveillance continue et des évaluations périodiques afin de s'assurer du respect durable des engagements contractuels et des exigences de sécurité. Ce suivi peut s'appuyer sur des réunions de coordination régulières, des revues de performance des contrôles documentaires, ou encore des audits.

**POUR EN SAVOIR PLUS**

Une politique et des lignes directrices en relation avec la gestion des relations avec les fournisseurs seront publiées sur l'Extranet de l'ANSSI.

# 4. Sensibilisation et formation

**OBJECTIF**

Renforcer la culture et les compétences en sécurité de l'information au sein de l'entité, en combinant des actions de sensibilisation adaptées avec un programme de formation structuré destiné aux acteurs clés de la sécurité de l'information.

## Sensibilisation

La sensibilisation consiste à accroître la vigilance et la responsabilité des collaborateurs internes et externes face aux risques numériques et à les encourager à adopter les bonnes pratiques de sécurité au quotidien. Elle devrait être réalisée, lors de leur intégration au sein de l'entité, puis de façon continue.

Ils devraient être sensibilisés aux principales cybermenaces (afin d'en comprendre la nature, les impacts potentiels et d'adopter les bons réflexes pour les détecter et y réagir efficacement) ainsi qu'aux règles à respecter lors de l'utilisation des systèmes d'information, telles que définies par la Charte de bonne conduite en matière de sécurité de l'information numérique pour les agents l'État.

La sensibilisation devrait être adaptée aux risques spécifiques auxquels l'entité est exposée ainsi qu'à ses propres règles et procédures de sécurité.

Enfin, la mise en œuvre de simulations de phishing encadrées, telles que réalisées par le HCPN/GOVCERT, contribue à renforcer la vigilance des utilisateurs face aux emails suspects. Ces exercices ont un objectif pédagogique : permettre aux collaborateurs d'apprendre de leurs erreurs sans sanction, afin de consolider la vigilance collective et la culture de sécurité au sein de l'entité.

## Formation

La formation a pour objectif de renforcer les compétences et connaissances nécessaires à la mise en œuvre et à la maîtrise de la sécurité de l'information.

Dans un premier temps, les entités devraient prioriser la formation du DSI ainsi que des cadres dirigeants, afin de renforcer leur rôle et leur implication dans la gouvernance de la sécurité.

Dans un second temps, un plan de formation structuré devrait être établi pour le personnel dont les missions nécessitent un renforcement des compétences en cybersécurité. Les équipes techniques devraient notamment bénéficier de formations spécialisées sur des thématiques telles que les opérations de sécurité informatique (SecOps) ou le développement sécurisé (DevSecOps).

**POUR EN SAVOIR PLUS**

Des supports de sensibilisation sont disponibles sur l'Extranet du HCPN/ANSSI.

L'offre de formation de l'INAP sur les thématiques de la sécurité de l'information et la protection des données à caractère personnel est régulièrement mise à jour et enrichie, et ce pour tous les publics. De nouvelles formations dédiées spécifiquement aux agents occupant une fonction de management (p. ex. cadres dirigeants) et/ou travaillant dans le domaine informatique (p. ex. DSI) seront proposées dans le catalogue 2026.

# 5. Analyse des risques orientée services

**OBJECTIF**

Mettre en place une démarche structurée et progressive d'analyse des risques, adaptée à l'entité, afin d'identifier, évaluer et traiter les risques pesant sur les services métiers vitaux.

## Approche recommandée

L'entité est invitée à réaliser des analyses de risques ciblées sur ses services métiers vitaux, en s'appuyant sur la méthodologie structurée proposée par l'outil MONARC, développé par le Luxembourg House of Cybersecurity (LHC).

Cet outil offre une approche cohérente, reproductible et documentée de l'évaluation des risques, permettant de prioriser les mesures de sécurité à mettre en place, de faciliter la prise de décision et d'assurer un suivi régulier de l'évolution des risques dans le temps.

## Approche pour la première analyse

Le périmètre choisi pour une première analyse doit rester conforme aux obligations légales applicables, notamment celles découlant de la directive NIS2.

Dans la mesure du possible, une entité qui débute dans la mise en œuvre d'analyses de risques orientées services devrait lancer l'analyse de risques sur un périmètre limité, par exemple un seul service métier, afin de se familiariser avec la démarche. Le service sélectionné devrait présenter une complexité maîtrisable, afin de faciliter la compréhension et la conduite de l'exercice. Une fois cette première analyse menée, un retour d'expérience permettra d'identifier les points d'amélioration avant d'étendre progressivement la méthode à d'autres services.

## Modèle d'actifs de support

Pour faciliter la réalisation des analyses de risques, une bibliothèque d'actifs de support prédéfinis a été conçue par le HCPN/ANSSI.

Organisée en trois niveaux progressifs, elle propose des ensembles d'actifs dont le nombre et la granularité augmentent progressivement, afin de s'adapter au niveau de maturité et aux besoins de chaque entité.

Cette approche permet de couvrir les risques les plus significatifs tout en maîtrisant la charge de travail nécessaire à la conduite de l'analyse.

## Accompagnement de l'ANSSI

Le HCPN/ANSSI met à disposition des entités un accompagnement complet pour la réalisation de leur analyse de risques, à travers des séances de coaching gratuites adaptées à chaque phase du processus.

Par ailleurs, le HCPN/ANSSI propose aux entités de l'État l'hébergement d'une instance MONARC dédiée et sécurisée, garantissant la confidentialité, l'intégrité et la disponibilité des données.

**POUR EN SAVOIR PLUS**

L'outil MONARC est disponible sur le site du LHC.

Une politique et des lignes directrices relatives à la gestion des risques, un modèle d'actif de support, ainsi qu'un guide utilisateur pour la réalisation d'analyses de risques avec l'outil MONARC sont publiées sur l'Extranet du HCPN/ANSSI.

# Les 10 actions à mettre en œuvre en priorité

**CES ACTIONS CLÉS DES PHASES 1 ET 2 CONSTITUENT LE SOCLE INDISPENSABLE AVANT DE DÉBUTER LA MISE EN ŒUVRE DE LA PHASE 3.**

## Phase 1 : Initiation et planning

1. Recenser vos services métiers, identifier ceux qui sont « vitaux » et inventorier vos prestataires.
2. Évaluer votre niveau de maturité en sécurité de l'information et définir le niveau de maturité cible adapté à vos enjeux.
3. Élaborer une macro-cartographie des risques (optionnel mais recommandé).
4. Définir un plan d'action pluriannuel, puis le faire valider par la direction.

## Phase 2 : Les fondations de la sécurité

5. Designer un DSI et mettre en place un Comité de Sécurité de l'Information, si nécessaire.
6. Rédiger la Politique Générale de Sécurité de l'Information (PGSI) et la faire approuver par la direction.
7. Rédiger les politiques thématiques ainsi que les procédures associées.
8. Intégrer la sécurité de l'information dans la gestion de projets.
9. Désigner en interne une instance responsable de la gestion des événements et incidents de sécurité de l'information.
10. Préparer la réponse à un incident.

# Glossaire

**ACTIF**
Tout élément ayant de la valeur pour un organisme. Les actifs comprennent, mais sans toutefois s'y limiter, les ressources humaines, matérielles, d'information, intangibles et environnementales. *(Source ISO22300)*.

**AUDIT**
Processus systématique, indépendant et documenté permettant d'obtenir des éléments probants et de les évaluer objectivement afin de déterminer dans quelle mesure les critères d'audit sont remplis. *(Source ISO19011)*.

**PLAN DE CONTINUITÉ DES ACTIVITÉS**
Information documentée qui guide un organisme pour répondre à une perturbation et reprendre, rétablir et restaurer la livraison ou la fourniture de produits et services en cohérence avec ses objectifs de continuité d'activité. *(Source ISO22301)*.

**BUSINESS IMPACT ANALYSIS**
Processus d'analyse de l'impact dans le temps d'une perturbation sur l'organisme. Le résultat est une déclaration et une justification des exigences de continuité d'activité. *(Source ISO22301)*.

**IMPACT**
Résultat d'une perturbation affectant les objectifs. *(Source ISO22301)*.

**INCIDENT**
Un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles. *(Source directive NIS2)*.

**POLITIQUE**
Intentions et orientation d'un organisme telles que formalisées par sa direction. *(Source ISO27002)*.

**PROCÉDURE**
Manière spécifiée de réaliser une activité ou un processus. *(Source ISO20387)*.

**PROCESSUS**
Ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie. *(Source ISO27002)*.

**RISQUE**
Le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise. (*Source directive NIS2)*.

**RÉSILIENCE**
Aptitude à absorber et s'adapter dans un environnement changeant. *(Source ISO 22300)*.

**POUR EN SAVOIR PLUS**

Accédez aux définitions à jour des normes ISO.

**Haut-Commissariat à la Protection Nationale (HCPN)**
Agence nationale de la sécurité des systèmes d'information (ANSSI)
T. 247-88930 • support@anssi.etat.lu