# DIRECTIVE STRATEGIQUE

# 01. ORGANISATION DE LA SECURITE DE L'INFORMATION

## POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DU GROUPE LA POSTE

| | |
|---|---|
| **Statut du document** | Validé |
| **Version** | V 1.0 |
| **Date d'enregistrement** | 20/09/2019 |
| **Responsable du document** | DSGG/DCG |

# Table des matières

# 1 Préambule

## 1.1 Objet du document

Cette directive fait partie du référentiel documentaire de la Politique de Sécurité des Systèmes d'Information du Groupe (PSSI-G). Elle décrit l'organisation de la Sécurité des Systèmes d'Information (SSI) du Groupe La Poste.

Elle doit établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information, en cohérence avec le Cadre Général.

## 1.2 Positionnement dans le cadre de référence

La Sécurité des Systèmes d'Information (SSI) du Groupe La Poste s'inscrit dans un cadre structuré en quatre niveaux :

- **Niveau 1** : *le cadre général*, qui fixe les objectifs, les principes généraux en matière de sécurité des SI et l'organisation permettant d'assurer un déploiement homogène des règles du Groupe La Poste ;
- **Niveau 2** : *les chartes et les directives stratégiques* de la PSSI-G, qui regroupent les règles permettant l'application du cadre général, dont le document présent ;
- **Niveau 3** : *les directives tactiques* décrites au niveau entité s'ajoutent aux directives stratégiques afin d'intégrer des éléments spécifiques à la gouvernance et au contexte d'emploi des SI des entités telles que mentionnées dans le champ d'application ;
- **Niveau 4** : *les procédures opérationnelles et guides techniques*, qui décrivent de manière explicite, les mesures d'application et de mise en œuvre de la PSSI-G.

Ce présent document est de niveau 2. La directive doit être lue et connue de toute personne travaillant pour le Groupe La Poste, y compris les prestataires intervenants sur le périmètre des SI du Groupe La Poste, tel que défini dans le champ d'application.

## 1.3 Champ d'application

La PSSI-G s'adresse à tous les acteurs du Groupe La Poste, de ses branches et de ses filiales intervenant, ou contrôlant les SI, notamment :

- Les Responsables de la Sécurité des Systèmes d'Information (RSSI) des entités ;
- L'Audit Informatique du Groupe (AIG) et les services en charge du contrôle interne ;
- Le Service de Lutte Contre la Cybercriminalité (SLCC) de la Direction des Systèmes d'Information Groupe (DSI/G) et les centres de supervision de la cybersécurité des branches et filiales ;
- Les acteurs intervenant au quotidien sur l'ensemble des SI du Groupe :
  - l'ensemble des collaborateurs,
  - les partenaires, prestataires et fournisseurs (contractuellement ou par le biais de conventions) dès lors qu'ils stockent, traitent ou utilisent des données issues du SI du Groupe La Poste.

Le RSSI complétera une matrice d'applicabilité qui déterminera :

- Le périmètre d'application des règles ;
- La possibilité de mise en œuvre ;
- La justification de non applicabilité.

## 1.4 Validité, révision et processus d'exception

La directive est applicable dès sa validation.

Elle doit être mise en œuvre dès publication sur tous les nouveaux projets applicatifs et d'infrastructures. La période de mise en conformité pour les SI déjà existants est de trois ans.

Cette directive pourra évoluer pour prendre en compte des retours d'expériences, imprécisions ou modifications des textes de référence.

Les demandes de révision sont à envoyer à la Direction de la Cybersécurité Groupe (DCG) : direction.cyber@laposte.fr.

La définition des exceptions aux règles est décrite dans le Cadre Général. La gestion des exceptions est documentée conformément au processus mis en place.

# 2 Glossaire

| Terme | Description |
|---|---|
| Activité critique | Désigne les activités indispensables au bon fonctionnement du Groupe. Ces activités ne peuvent être remplacées ou substituées |
| Administrateur | Désigne tout agent quelle que soit sa fonction, qui a pour rôle et missions d'assurer le bon fonctionnement et la sécurité des ressources des Systèmes d'Information (SI) de La Poste placées sous sa responsabilité (tels que les serveurs, les équipements réseaux, les équipements de sécurité, les applications, les bases de données, les postes de travail utilisateurs, etc.), au titre de son activité |
| Confidentialité | Propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés. Le critère de confidentialité d'un actif fixe son niveau de protection et la typologie des ressources autorisées à y accéder |
| Délégation | Fait de confier une tâche à une autre personne. La délégation ne désengage pas le délégant de sa responsabilité |
| Incident | Evénement de sécurité identifié correspondant à une menace et affectant le fonctionnement nominal de tout ou partie d'un système d'information. Un incident porte atteinte à la disponibilité, l'intégrité, la confidentialité ou la traçabilité d'un système d'information |
| Système d'Information | Applications, services, actifs informationnels ou autre composante permettant la prise en charge de l'information |
| Tiers | Désigne un organisme ou une personne reconnu(e) comme indépendant(e) du Groupe La Poste et de ses entités |

# 3 Règles de sécurité applicables

Pour atteindre les objectifs de sécurité des SI du Groupe La Poste, celui-ci s'appuie sur les principes suivants :

**Principe 1 : la sécurité de l'information est conforme aux lois, règlements, et meilleures pratiques.** La sécurité de l'information est formalisée, mise en œuvre, exploitée, contrôlée, mise à jour et améliorée en continu conformément aux lois, règlements et meilleures pratiques des normes ISO/CEI 2700x.

**Principe 2 : la gestion des risques en matière de sécurité du SI est régulière, alignée aux objectifs stratégiques du Groupe La Poste, et proportionnée.** L'identification, appréciation et traitement des risques sont effectués régulièrement. Les mesures de réduction des risques sont mises en œuvre en s'assurant que leurs coûts sont proportionnels aux bénéfices obtenus. La gestion des risques est revue régulièrement dans une optique d'amélioration continue de la sécurité.

**Principe 3 : la mise œuvre de la sécurité du SI est progressive et pragmatique.** La mise en œuvre des mesures de sécurité (qui découlent de la gestion régulière et proportionnée des risques) est réalisée de manière pragmatique, en traitant en priorité les risques les plus importants.

## 3.1 Organisation interne

Objectif : établir un cadre de gestion pour engager, puis vérifier la mise en œuvre de la sécurité de l'information au sein des entités.

### 3.1.1 Fonctions et responsabilités liées à la sécurité de l'information

La responsabilité de la sécurité de l'information s'étend à l'ensemble des personnes physiques ou morales accédant aux SI du Groupe La Poste et notamment tout collaborateur interne ou externe.

#### 3.1.1.1 Fonctions et chaînes de responsabilités

Les responsabilités en matière de sécurité de l'information pour le Groupe La Poste sont décrites dans le Cadre Général de la PSSI-G.

La responsabilité de la sécurité de l'information est répartie entre les acteurs des chaînes de gouvernance, de cybersécurité, des systèmes d'information et du contrôle des risques.

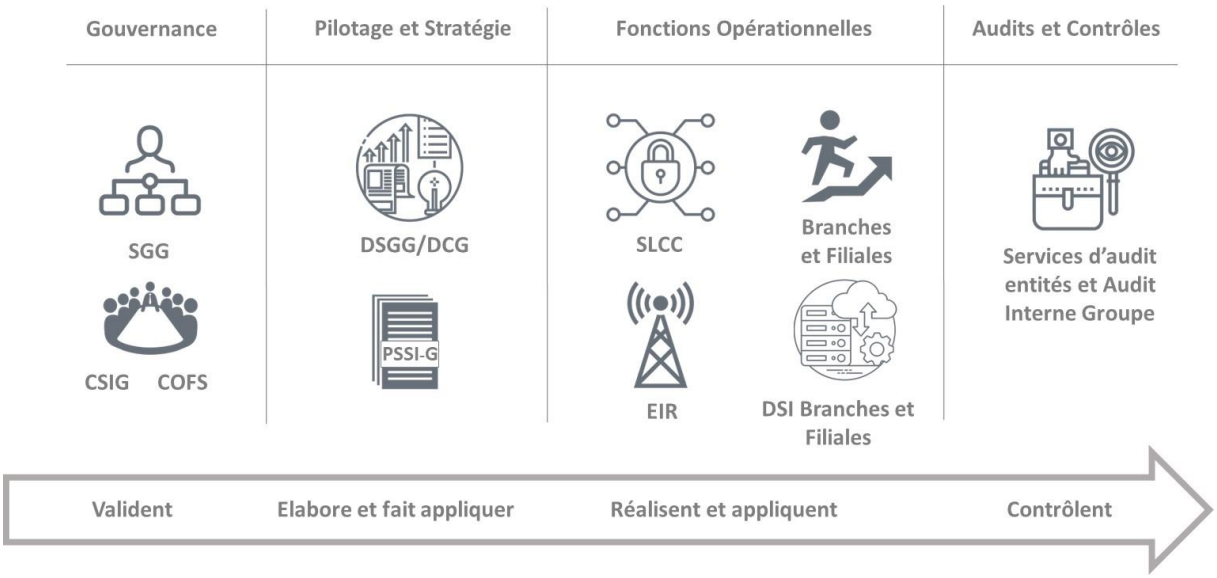


Figure : répartition des rôles et responsabilités de la sécurité de l'information

Les responsabilités relatives à la protection des actifs individuels sont décrites dans la directive « 04. Gestion des actifs et classification ».

Les responsabilités de mise en œuvre des processus de sécurité spécifiques sont ensuite décrites dans les directives concernées.

Les responsabilités liées aux activités de gestion des risques en matière de sécurité de l'information sont détaillées dans la directive « 11. Gestion de projet ». Celle-ci précise que l'acceptation des risques résiduels suite à l'analyse de risques reste de la responsabilité des Métiers. Une procédure complémentaire d'homologation peut détailler les différentes étapes permettant d'atteindre cet objectif lorsque cela est nécessaire.

Chaque actif et processus de sécurité est identifié, documenté et assigné nommément à un collaborateur qui en a la responsabilité.

Sur l'intégralité des sujets liés à la SSI, les différents niveaux d'autorisation sont définis et documentés.

Tout collaborateur exerçant des responsabilités en matière de SSI doit être formé et sensibilisé régulièrement afin de maintenir son niveau de compétences, conformément à la directive « 03. Ressources Humaines ».

Les activités de coordination et de supervision relatives aux questions de sécurité liées aux relations avec les fournisseurs sont identifiées et documentées dans la directive « 12. Relations avec les fournisseurs ».

Le responsable de la sécurité de l'information du Groupe est le Directeur de la Cybersécurité Groupe. A ce titre, il assume la responsabilité de l'élaboration et du contrôle de la mise en œuvre de la PSSI-G.

L'implémentation des ressources et des mesures sont contrôlées par les Responsables de Sécurité des SI (RSSI) des entités.

#### 3.1.1.2 Règles de fonctionnement

Dans le cadre de l'application de la PSSI-G, le RSSI de l'entité doit déterminer les rôles et responsabilités (Réalisation, Approbation, Consultation, Information) relatifs à chaque règle :

- Le RSSI reste le seul et unique approbateur ;
- La documentation est réalisée par chaque responsable des domaines concernés ;
- La DCG est systématiquement informée.

Pour chaque directive, le RSSI complète une matrice d'applicabilité qui détermine :

- Le périmètre d'application des règles ;
- La possibilité de mise en œuvre ;
- La justification de non applicabilité.

#### 3.1.1.3 Délégation

Les personnes en charge des responsabilités en matière de sécurité peuvent déléguer des tâches de sécurité opérationnelles. Les autorités délégatrices demeurent responsables et s'assurent de la bonne exécution de toute tâche déléguée, la subdélégation est interdite.

### 3.1.2 Séparation des tâches

Le détail de la mise en œuvre de ces règles est décrit dans la directive « 05. Contrôle d'accès ».

#### 3.1.2.1 Moindre privilège

Toute personne ne peut accéder qu'aux seules informations ou ressources strictement nécessaires à l'accomplissement de son travail, en conformité avec la PSSI-G, les directives tactiques, procédures opérationnelles et les guides techniques du Groupe La Poste et des entités. Le même principe s'applique à la gestion des accès à privilèges.

#### 3.1.2.2 Ségrégation des tâches

Afin de réduire les opportunités de vol, de consultation, de modification ou d'usages non autorisés ou involontaires d'informations, les rôles et

responsabilités inhérents à leurs fonctions sont assignés à des personnes distinctes.

Des profils utilisateurs sont décrits dans des matrices de séparation des tâches en vue d'attribuer ces droits pour les accès réseaux et applicatifs.

Lorsqu'il est impossible de procéder à la séparation des tâches, d'autres mesures comme la surveillance des activités, des systèmes de traçabilité et la supervision de la direction, doivent être mises en place.

### 3.1.3 Relations avec les autorités

Le Groupe La Poste met en place des relations appropriées avec les autorités compétentes en matière de SSI.

#### 3.1.3.1 Dispositif du Groupe La Poste

Le Groupe La Poste entretient des relations avec les autorités avec lesquelles il est tenu de correspondre dans le cadre de ses activités. Ces relations sont encadrées par des procédures et des processus documentés par les acteurs du Groupe concernés. Les principes du dispositif du Groupe et de la présente directive s'entendent sans préjudice des prérogatives et règles de gouvernance interne du Groupe et de ses entités vis-à-vis de leurs autorités de tutelle et leurs régulateurs.

Les moyens requis dans le cadre de déclaration auprès des autorités sont également décrits dans les cas suivants :

- Déclaration des incidents de sécurité informatique ;
- Suspicion de violation de la loi.

Le dispositif que le Groupe La Poste a mis en place s'intègre dans celui que l'Etat a élaboré pour garantir la continuité des services et de l'activité du pays. Dans ce cadre, le Groupe La Poste est assujetti à des obligations réglementaires auxquelles il se conforme.

La coordination de l'ensemble des mesures d'organisation et de coordination est réalisée par la Direction de la Sécurité Globale du Groupe. Le Directeur de la Sécurité Globale du Groupe tient la fonction règlementaire de Délégué pour la Défense et la Sécurité (DDS) du Groupe. Il est assisté du Directeur de la Cybersécurité Groupe et de son adjoint.

Le DDS et ses adjoints s'appuient, pour la mise en œuvre du dispositif de protection des activités critiques du Groupe, sur les correspondants des

branches et filiales. Leur action est complétée par des DDS locaux, désignés au niveau des différents sites sensibles et chargés des relations avec les préfectures pour la mise en œuvre du dispositif de protection.

Le Directeur de la Cybersécurité Groupe est le correspondant désigné de l'ANSSI pour la mise en œuvre des dispositions cyber, prévues par les articles L.1332-6-1 et suivants du Code de la Défense.

### 3.1.4 Relations avec des groupes de travail spécialisés

Le Groupe La Poste met en place des relations appropriées avec les groupes d'intérêt, les forums spécialisés dans la SSI et les associations professionnelles.

#### 3.1.4.1 Appartenance à des clubs de SSI

Le Groupe La Poste a choisi d'intégrer des groupes de travail spécialisés afin de :

- Connaître les meilleures pratiques et se tenir informé de l'évolution des connaissances relatives à la sécurité ;
- Recevoir toutes les alertes sur les vulnérabilités, les attaques, les correctifs et les conseils de mise en œuvre ou de déploiement de mesures compensatoires ;
- Recevoir des alertes et informations le plus tôt possible ;
- Avoir accès à des conseils de spécialistes sur la sécurité de l'information ;
- Partager et échanger des informations sur les nouvelles technologies, produits, menaces ou vulnérabilités.

Le Groupe La Poste est membre de groupes spécialisés en cybersécurité suivants :

- Le groupe Inter Computer Emergency Response Teams France (InterCERT-FR) et le Forum of Incident Response and Security Teams (FIRST) qui réunissent un ensemble d'organismes ayant des activités d'IRT (Incident Response Team) au niveau national et international ;
- Le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) et le Club de la Sécurité de l'Information Français (CLUSIF) ;
- Le Cyber Cercle et le Cercle Européen de la sécurité et des Systèmes d'Information.

#### 3.1.4.2 Relais de l'information en interne

Un processus de partage de l'information est développé au sein du Groupe La Poste pour disposer de relais appropriés lors du traitement d'alertes de sécurité de l'information.

Ces informations sont relayées par des supports d'alertes tels que :

- Les bulletins d'annonces des éditeurs et constructeurs ;
- Les bulletins d'alerte d'organismes officiels en sécurité des SI ;
- Les publications internes du SLCC et de la DCG.

### 3.1.5 La sécurité de l'information dans la gestion de projet

Le Groupe La Poste intègre la SSI dans toutes gestions de projets quel qu'en soit la nature et la portée.

#### 3.1.5.1 Intégration de la SSI dans les projets

La sécurité de l'information est intégrée dans la gestion de projet conformément à la directive « 11. Gestion de projet ».

Au minimum les règles suivantes doivent être respectées :

- Intégrer les objectifs en matière de sécurité de l'information aux objectifs du projet ;
- Effectuer une appréciation du risque de sécurité de l'information au commencement du projet pour identifier les mesures nécessaires ;
- Intégrer la sécurité de l'information à toutes les phases de la méthodologie de projet appliquée ;
- Attribuer les responsabilités en matière de SSI à des fonctions spécifiques dans les jalons projet.

## 3.2 Transfert de l'information

Objectif : maintenir la sécurité de l'information transférée au sein du Groupe La Poste et vers des organisations extérieures.

### 3.2.1 Engagements de confidentialité ou de non-divulgation

Les exigences en matière de confidentialité ou de non-divulgation sont identifiées, régulièrement revues et documentées selon les besoins des entités.

#### 3.2.1.1 Formalisation des engagements

Les modalités des engagements de confidentialité ou de non-divulgation doivent être déterminées et formalisées.

Elles spécifient les exigences de protection de l'information sensible en des termes juridiquement exécutoires et sont applicables aux salariés et aux tiers du Groupe La Poste.

Des éléments doivent être ajoutés ou modifiés en tenant compte de la catégorie du tiers et des accès ou du traitement de l'information sensible acceptables pour sa catégorie.

Afin d'identifier les exigences de confidentialité et de non-divulgation, il faut :

- ❑ Définir l'information à protéger (cf. directive « 04. Gestion des actifs et classification ») ;
- ❑ Prévoir la durée d'engagement ;
- ❑ Préciser les actions à entreprendre lorsqu'un engagement arrive à expiration ;
- ❑ Identifier les responsabilités et les tâches des signataires visant à éviter une divulgation non autorisée de l'information ;
- ❑ Identifier la propriété de l'information et la propriété intellectuelle, ainsi que leurs liens avec la protection de l'information sensible ;
- ❑ Utiliser de manière autorisée l'information sensible et les droits du signataire relatifs à l'utilisation de cette information ;
- ❑ Auditer et contrôler les activités impliquant l'utilisation de l'information sensible ;
- ❑ Mettre en place un processus de notification et de signalement d'une divulgation non autorisée ou d'une fuite de l'information sensible ;
- ❑ Définir les modalités de retour ou de destruction de l'information à l'expiration de l'engagement ;
- ❑ Spécifier les actions à entreprendre en cas de violation de l'engagement.

Tout contrat doit comporter une clause d'engagement de confidentialité et de non-divulgation, conformément aux lois et règlements en vigueur dans la juridiction dont elle relève.

#### 3.2.1.2 Revue des engagements

Les exigences en matière d'engagements de confidentialité ou de non-divulgation doivent être revues à intervalles réguliers en cas de changements ayant une incidence sur ces exigences.