CADRE GENERAL

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

LE GROUPE LA POSTE

Paris, le 13/02/2020

Lettre d'engagement du Président-directeur général,

La protection de l'information et la confiance dans ceux qui la transmettent sont les deux piliers historiques de La Poste. Depuis plus de 500 ans, elle s'applique à garantir cette sécurité et à mériter cette confiance. Assurément, les modalités de transmission de l'information évoluent avec le temps, mais la mission reste la même.

Aujourd'hui, les nouvelles activités immatérielles font naître un immense besoin de confidentialité, de protection et de sécurité, qui ne peut être satisfait que par des opérateurs bénéficiant de la confiance des citoyens-consommateurs. C'est donc pour rester fidèle à sa vocation d'origine que La Poste a engagé sa transition numérique : elle veut offrir au plus grand nombre l'assurance de la protection de sa vie privée. Cette sécurité, nous y sommes attachés par notre identité et notre sens des responsabilités. Assurer cette sécurité, c'est maintenir La Poste à hauteur de son histoire.

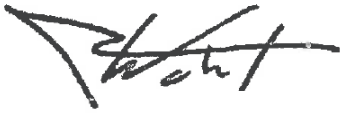
Pour ce faire, La Poste doit commencer par assurer à ses collaborateurs, chargés de cette mission, les moyens de travailler dans ce nouvel univers numérique[1].

La protection du patrimoine informationnel du Groupe, de ses Branches et Filiales commence donc par la Politique de Sécurité des Systèmes d'Information au niveau du Groupe (PSSI-G), qui pose un cadre commun destiné à l'ensemble des postiers, depuis la genèse des projets jusqu'aux tournées des facteurs.

Fruit de l'expérience et des réflexions des Branches, ce cadre commun rappelle à tous :

- Les enjeux de la protection de l'information ;
- Les principes de gestion et de traitement des risques « cyber » ;
- L'organisation et les responsabilités en matière de protection de l'information.

Il reviendra à chaque entité du Groupe de la décliner et de la compléter par les procédures opérationnelles adaptées à ses métiers, son organisation et ses activités. L'implication de tous, depuis les managers jusqu'aux collaborateurs est indispensable pour en rendre la lettre vivante et continuer de préserver la confiance de nos concitoyens.



Philippe Wahl

[1] Le « numérique » fait partie intégrante du champ global des SI et, s'entend ici sous toutes ses formes, terminaux digitaux, objets connectés, etc.

1 Préambule

1.1 Cadre de référence de la PSSI-G

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.

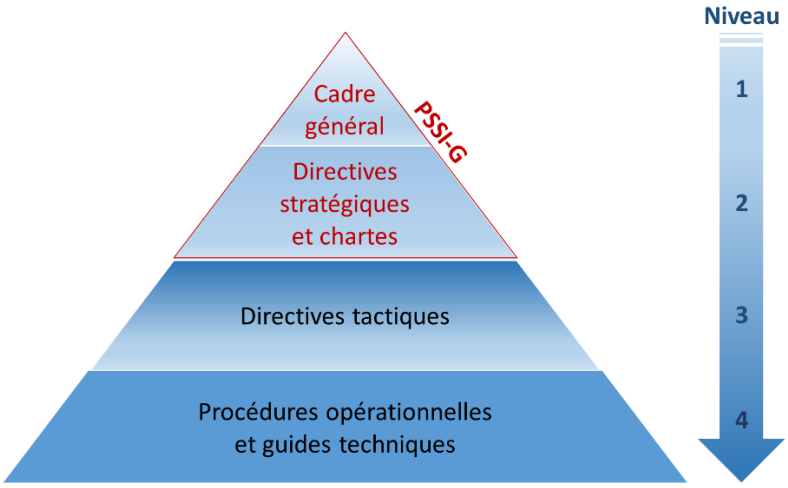


Figure 1 : les 4 niveaux du dispositif de sécurité du Groupe

1.2 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 entités ;
- 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.

1.3 Validité, révision et processus d'exception

La PSSI-G est applicable dès sa publication.

La période de mise en conformité pour les SI existants est de trois ans.

La PSSI-G est révisée sur proposition du Comité Cybersécurité du Groupe (CCG) et approuvée en Comité des SI du Groupe (CSIG), conformément au processus de changement de la PSSI-G, afin de prendre en compte :

- L'évolution des menaces et les retours d'expérience des traitements d'incidents ;
- Les résultats d'analyses de risques ainsi que les actions découlant de contrôles ou d'audits ;
- L'évolution des contextes organisationnel, juridique, règlementaire et technologique.

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 ce document. La gestion des exceptions est documentée conformément au processus mis en place.

2 Organisation et principes généraux de la Sécurité des Systèmes d'Information

2.1 Organisation

Un SI est un ensemble organisé de ressources matérielles, logicielles et humaines destiné à élaborer, traiter, stocker, acheminer et présenter l'information.

La Sécurité des Systèmes d'Information (SSI) recouvre l'ensemble des moyens techniques, organisationnels et humains qui doivent être mis en place dans le but de garantir, au juste niveau requis, la sécurité des informations du Groupe La Poste et des systèmes qui en assurent l'élaboration, le traitement, la transmission, le stockage et la destruction.

La SSI vise donc à assurer la confidentialité, la disponibilité, l'intégrité et la traçabilité des systèmes d'information du Groupe La Poste. Elle protège ainsi contre les menaces intentionnelles et non intentionnelles pouvant affecter les SI.

La PSSI-G évolue pour intégrer l'évolution des technologies, des usages et le développement de nouvelles activités stratégiques.

2.2 Principes généraux de Sécurité des Systèmes d'Information

La mise en œuvre de la PSSI-G est organisée autour des principes suivants :

- La PSSI-G est compatible avec la loi et les réglementations applicables au Groupe La Poste SA et à ses entités ;
- La PSSI-G repose sur l'organisation de la chaîne fonctionnelle SSI déployée au sein des entités ;
- Chaque entité doit assurer la formation, la sensibilisation et la validation des compétences en SSI de son personnel ;
- Toute personne qui interagit avec les SI du Groupe doit avoir les compétences minimales requises en SSI ;
- La formalisation systématique de l'analyse des risques des SI permet de définir les mesures de sécurité à appliquer ;
- Les mesures de sécurité sont priorisées et proportionnées en fonction du niveau de risques des SI ;

- La sécurité des SI traite de la confidentialité, de l'intégrité, de la disponibilité et de la traçabilité des informations traitées par les SI du Groupe ;
- Les domaines d'actions de la SSI couvrent la protection de l'information, l'identification et la réponse aux incidents et la résilience des SI ;
- Le Groupe évalue sa capacité de réaction et de résilience face aux incidents de cybersécurité ;
- Les activités liées aux SI intègrent, dès leur conception, la prise en compte des exigences de cybersécurité ;
- La maturité SSI est évaluée dans le cadre d'un processus d'amélioration continue ;
- L'ensemble des procédures de cybersécurité est documenté et testé.

L'information du Groupe est protégée selon les principes de la défense en profondeur. Le concept de défense en profondeur permet de construire une défense globale en coordonnant plusieurs lignes de défense qui doivent être cohérentes entre elles et adaptées aux enjeux.

A cet effet, les lignes de défense mises en place couvrent tous les aspects de l'information et des SI. Aussi peuvent-elles être d'ordre humain (notamment la sensibilisation des collaborateurs et prestataires employés à la sécurité du SI), organisationnel ou technique.

3 Rôles et responsabilités de la SSI

La PSSI-G établit les rôles et responsabilités des acteurs en charge de la SSI au sein du Groupe La Poste et en décrit les attributions par niveaux :

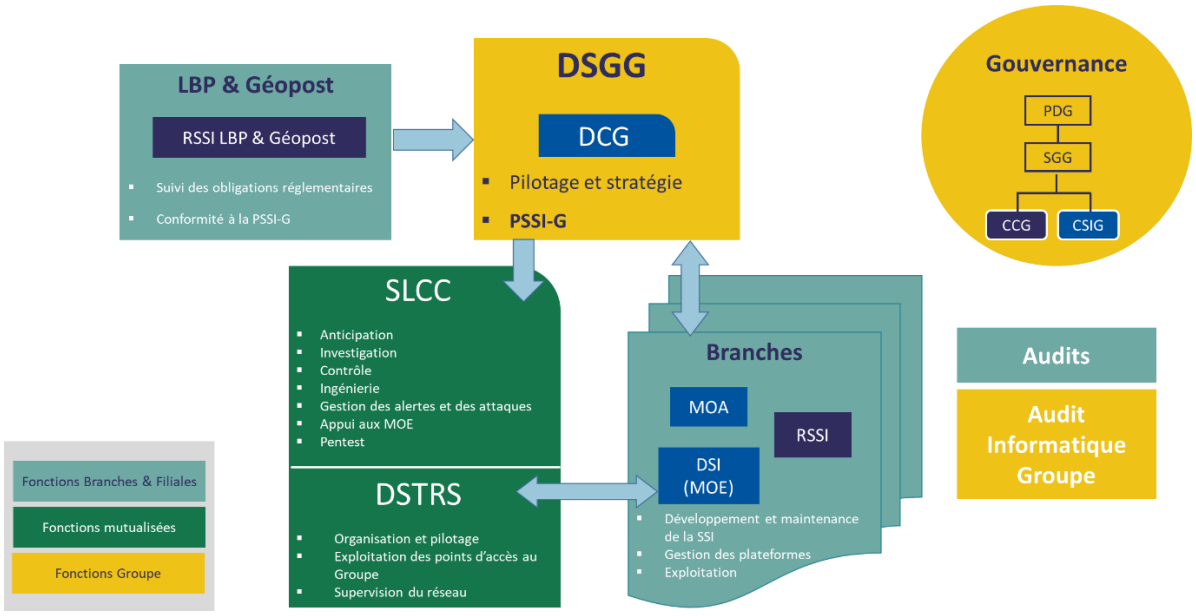


Figure 2 : le dispositif de cybersécurité du Groupe

3.1 Gouvernance

3.1.1 Secrétaire Général du Groupe (SGG)

La gouvernance de la cybersécurité est placée sous l'autorité du Secrétaire Général du Groupe (SGG). Il préside les instances de gouvernance des SI et de sécurité des SI (Comité Cyber Groupe et Comité des Système d'Information du Groupe) qui valident la stratégie de sécurité et s'assurent de l'intégration de la sécurité des projets.

3.2 Pilotage stratégique

3.2.1 Directeur de la Sécurité Globale du Groupe (DSGG)

Le DSGG assure la responsabilité du pilotage de l'ensemble du dispositif de cybersécurité du Groupe, de ses branches et de ses filiales. Le DSGG a pour responsabilité de proposer la stratégie de sécurité des SI, de faire diffuser la diffusion et de s'assurer du contrôle de l'application de la PSSI-G.

Dans ce cadre, le DSGG tient la fonction d'Officier de Sécurité (OS) du Groupe et exerce la tutelle fonctionnelle de la Direction des Services Télécom Réseau et Sécurité.

Le DSGG met en place l'organisation nécessaire pour :

- Animer et contrôler le déploiement de la PSSI-G dans les entités du Groupe ;
- Assurer la cohérence et l'homogénéité des plans d'action cybersécurité des entités ;
- Réaliser un reporting régulier aux instances appropriées : CSIG, CCG et au Comité des Risques du Groupe. Ce reporting porte sur la maîtrise des risques liés à la SSI et la conformité à la PSSI-G de l'ensemble des entités ;
- Mener des contrôles et investigations en cas de crise.

3.2.2 Directeur de la Cybersécurité du Groupe (DCG)

Le DCG coordonne l'ensemble du dispositif de cybersécurité du Groupe et de ses entités.

Il est responsable de la conception des mesures de cybersécurité, de l'animation et de la formation des différents acteurs. Il est assisté des RSSI des entités en charge des éventuelles adaptations aux règles spécifiques de leurs activités.

Le DCG assure la tutelle fonctionnelle du SLCC.

Le DCG assure les missions d'expertise légale au profit du Groupe et la coordination avec les services de sécurité de l'État. Dans l'éventualité de la judiciarisation d'une affaire, il dirige les actions des spécialistes du SLCC ou fait appel à des experts indépendants. Il suit aussi les opérations de contre-mesure de surveillance technique des bureaux et fait contrôler les locaux du siège du Groupe.

3.3 Pilotage opérationnel

3.3.1 Responsable de la Sécurité des Systèmes d'Information (RSSI)

Chaque entité du Groupe nomme un RSSI qui pilote la chaîne fonctionnelle SSI de son entité.

Le RSSI est responsable de la mise en œuvre de la SSI au sein de ses entités. Il est également responsable de la diffusion et de l'application de la PSSI-G, notamment au travers de la rédaction de procédures opérationnelles.

- Le RSSI complétera une matrice d'applicabilité pour chaque directive stratégique de la PSSI-G. Cette dernière précisera :
- Le périmètre d'application des règles ;
- La possibilité de mise en œuvre ;
- La justification de non applicabilité.

Chaque RSSI :

- Conseille sa Direction des Systèmes d'Information, les responsables métiers et les maîtrises d'ouvrage de ses entités pour les sujets relatifs à la SSI ;
- Est membre de droit des cellules de crise en cas d'incident affectant la SSI de ses entités. Il met en place un dispositif assurant une permanence opérationnelle pour permettre une réaction immédiate en cas d'incident de cybersécurité ;
- Référence les solutions de sécurité utilisées au sein de ses entités et participe, en collaboration avec la DCG, au référencement des solutions de sécurité pour le Groupe.

3.3.2 Maîtrise d'œuvre (MOE)

3.3.2.1 Directeur des Systèmes d'Information (DSI)

Le DSI, en tant que MOE, est garant de la mise en œuvre, de l'exploitation des moyens informatiques et de l'application opérationnelle des instructions en cas d'incidents de sécurité.

Le DSI veille à ce que les SI qu'il déploie soient conformes aux exigences SSI exprimées par sa chaîne fonctionnelle SSI en lien avec la PSSI-G.

Ses responsabilités sont :

- De mettre en place l'organisation, les processus et les outils nécessaires à la mise en œuvre et à l'amélioration continue de la sécurité du SI et du système de management de la sécurité du SI ;
- De proposer aux directions générales un arbitrage du plan de traitement des risques de la sécurité du SI ;
- De soutenir et de conseiller les entités métier dans toutes les activités de gestion des risques de sécurité dans leur domaine, ou dans l'application des mesures de sécurité ;

- D'acquérir, de développer, de mettre en œuvre, d'exploiter, de faire évoluer, de surveiller les SI conformément aux directives et procédures de sécurité.

3.3.2.2 Acteurs de la sécurité opérationnelle

Les centres opérationnels de sécurité du Groupe (SLCC et centre de supervision de la sécurité - Security Operations Center - LBP), les directions de la sécurité opérationnelle des entités sont en charge de la mise en œuvre de la sécurité des systèmes d'information. A cet effet, elles déclinent les directives stratégiques de la PSSI-G en directives tactiques et produisent les procédures opérationnelles conformes à la PSSI-G.

3.3.3 Maîtrise d'ouvrage (MOA)

Les directions générales ou les directions Métiers sont MOA. Elles sont responsables du niveau de sécurité associé aux SI et aux informations que ceux-ci créent, hébergent ou transmettent.

Les MOA restent, quelle que soit l'organisation opérationnelle retenue, décisionnaires en matière de gestion des données. Elles sont garantes de la réalisation des analyses des risques, de la définition de la criticité des données et des traitements, de la validation du risque résiduel accepté et de la définition du niveau de sécurisation attendu.

Assisté par les RSSI, les MOA doivent :

- Identifier les besoins de sécurité et les exigences légales dans leur domaine ;
- Identifier les actifs, les menaces et les vulnérabilités propres à leur domaine ;
- Analyser, évaluer et suivre les risques afin de déterminer les niveaux de sécurité requis et la protection la plus appropriée ;
- Assurer l'application de la PSSI-G dans leur périmètre, et auprès de leurs bénéficiaires, usagers, partenaires et fournisseurs ;
- Assurer l'utilisation des SI conformément aux directives et procédures de sécurité.

3.3.4 Direction de l'Audit et des Risques du Groupe

Le management des risques liés à la sécurité des systèmes d'information s'inscrit pleinement dans le dispositif de gestion des risques et de contrôle interne du Groupe, conformément aux dispositions de la Charte du Management des Risques Groupe. Ce management s'organise selon les trois lignes de maîtrise prévues :

- La première ligne de maîtrise des activités est constituée par le management opérationnel (fonctions de MOE et MOA opérationnelles), responsable de l'évaluation et de la diminution des risques au niveau de chaque processus dont il a la charge, et de la communication des informations appropriées à la deuxième ligne de maîtrise.
- La deuxième ligne de maîtrise est constituée des services fonctionnels des branches et du groupe responsables de la sécurité des systèmes d'information (directions sécurité SI, directions système d'information) et des fonctions dédiées à l'animation du dispositif global de maîtrise des risques (fonctions de gestion des risques et de contrôle interne, assurances et conformité). Elle assiste les opérationnels dans l'identification et l'évaluation des principaux risques, structure et maintient le dispositif de maîtrise des risques SI de la branche et du Groupe et rend compte de son fonctionnement.
- La troisième ligne de maîtrise est constituée de l'audit interne/inspection bancaire, responsable de l'évaluation par une approche objective et méthodique des dispositifs de gestion des risques et de contrôle interne mis en œuvre par les deux premières lignes de maîtrise.

3.3.5 Collaborateurs

Toute personne accédant aux SI du Groupe et de ses entités doit se conformer aux règles édictées dans la PSSI-G.

Les obligations des utilisateurs et des administrateurs sont décrites dans la charte utilisateur des SI et la charte administrateur des SI qui sont annexées au règlement intérieur du Groupe La Poste et de ses entités.

Le collaborateur est un maillon essentiel de la cybersécurité. À ce titre il est formé à la cybersécurité.

4 Mise en application de la PSSI-G

4.1 Instances de gouvernance

Deux instances de gouvernance de la SSI existent au sein du Groupe.

4.1.1 Comité des Systèmes d'Information du Groupe (CSIG)

Le CSIG approuve la PSSI-G ainsi que son processus d'évolution. Il valide l'attribution des moyens destinés à la SSI en fonction des risques identifiés et des recommandations du CCG.

4.1.2 Comité Cyber Groupe (CCG)

Le CCG pilote la mise à jour de la PSSI-G et propose les mesures destinées à améliorer le dispositif de cybersécurité du Groupe.

Le CCG est présidé par le DSGG et animé par le DCG.

Les objectifs du CCG sont les suivants :

- Optimiser le fonctionnement des dispositifs de suivi de la menace, de gestion des incidents et de crise ;
- Associer les acteurs stratégiques du Groupe à la définition de la stratégie de cyberdéfense du Groupe ;
- Proposer une stratégie de développement de valeur sur des solutions cyber ;
- Rationaliser les investissements cyber en ayant une approche globale de la sécurité ;
- Favoriser la transformation numérique du Groupe La Poste ;
- Valider les choix de sécurité et les projets cyber du Groupe ;
- Contrôler le suivi des plans d'actions.

4.2 Application et contrôle de la PSSI-G

4.2.1 Diffusion

La PSSI-G est connue de l'ensemble des personnes ayant un accès à l'un des SI du Groupe.

La diffusion et le contrôle de la connaissance de la PSSI-G au sein des entités du Groupe sont du ressort des RSSI des entités.

Les procédures opérationnelles et les guides techniques, concernant des périmètres plus restreints, sont transmis aux seules personnes ayant à en connaître.

La PSSI-G est publiée sous la forme d'une note chartée et sera accessible au format électronique sur le site intranet de la DCG.

4.2.2 Mise en application

La PSSI-G doit être mise en œuvre dès publication pour tous les nouveaux projets applicatifs et d'infrastructures.

La période de mise en conformité pour les SI existants est de trois ans.

La portée de la PSSI-G s'entend sans préjudice des prérogatives et règles de gouvernance interne du Groupe et de ses entités.

4.2.3 Cas de non-application

Les demandes de non-applicabilité à une ou plusieurs règles de sécurité de la PSSI-G sont motivées par le caractère inadapté au périmètre visé. Par exemple, l'entité n'exploite pas de ressources SI dans le Cloud donc les règles de sécurité liées à ce sujet ne s'appliquent pas.

Les demandes de non-applicabilité nécessitent une justification et, sont réalisées auprès des RSSI des entités. Elles ont une durée déterminée et ne nécessitent pas d'actions de remédiation. Elles sont revues au moins tous les trois ans en fonction des changements ou modifications du périmètre concerné.

La DCG pourra consulter, modifier et contrôler le processus de gestion de ces demandes.

La non-applicabilité n'entraîne pas de non-conformité à ladite règle.

4.2.4 Exceptions aux règles de la PSSI-G

Les exceptions de sécurité à la PSSI-G correspondent à une exemption pour une durée déterminée d'une règle ou d'un ensemble cohérent de règles ne pouvant s'appliquer dans l'immédiat.

Ces demandes d'exception doivent être formalisées auprès des RSSI des entités et intégrer un plan de remédiation. Elles sont accordées pour une durée d'un an maximum et archivées au niveau des branches et filiales.

Les plans de remédiation font l'objet d'un suivi, le temps de la durée de l'exception.

La DCG pourra consulter, modifier et contrôler le processus de gestion de ces demandes.

Les exceptions constituent des écarts aux dites règles jusqu'à clôture du plan de remédiation.

4.2.5 Contrôle de la politique

La PSSI-G et ses directives forment le cadre de contrôle de la SSI au sein du Groupe.

Les points de contrôle sont recensés et mis à disposition dans un SI dédié sur le site intranet de la DCG.

5 Documents d'application

Charte d'utilisation des systèmes d'information
Charte d'administration

Directive « 01. Organisation de la Sécurité de l'information »
Directive « 02. Mobilité »
Directive « 03. Ressources Humaines »
Directive « 04. Gestion des actifs et classification »
Directive « 05. Contrôle d'accès »
Directive « 06. Cryptographie »
Directive « 07. Sécurité physique »
Directive « 08. Sécurité liée à l'Exploitation »
Directive « 09. Réseau »
Directive « 10. Sécurité des communications »
Directive « 11. Gestion de projet »
Directive « 12. Relations avec les fournisseurs »
Directive « 13. Gestion des incidents de sécurité informatique »
Directive « 14. Sécurité de l'information dans le Plan de Continuité d'Activité »
Directive « 15. Conformité et contrôle »

6 Glossaire

Terme	Description
Client	Personne physique ou morale à laquelle La Poste, ses holdings et ses filiales fournissent un bien ou un service contre rétribution dans le cadre d'une activité commerciale
Collaborateur	Personne physique travaillant au sein du Groupe La Poste ou d'une de ses filiales
Cybersécurité	Ensemble des moyens techniques, outils, processus et pratiques permettant de protéger les systèmes d'information, le patrimoine informationnel, l'activité, la pérennité et la réputation des entreprises, de leurs biens et des individus
Entité	Terme générique désignant La Poste maison-mère, ses branches, ses holdings et ses filiales
Fournisseur	Toute personne morale ou établissement fournissant aux entités du Groupe La Poste des biens ou des services nécessaires à leur activité
Loi et réglementation	Ensemble des normes auxquelles les organisations et les individus doivent se conformer sous peine de sanctions.
Menace	Cause potentielle d'un incident indésirable pouvant nuire à un système ou une organisation
Partenaire	Entreprise ou tiers associé au Groupe La Poste dans le cadre d'une collaboration ou d'une mission commune encadrée par une convention
Prestataire	Entreprise ou tiers lié par contrat au Groupe La Poste pour l'accomplissement d'une prestation contre rétribution
Système d'Information	Applications, services, actifs informationnels ou autre composante permettant la prise en charge de l'information

Sigles	Description
AIG	Audit Informatique du Groupe
CCG	Comité Cyber Groupe
CSIG	Comité des Systèmes d'Information du Groupe
DCG	Directeur de la Cybersécurité du Groupe
DSGG	Directeur de la Sécurité Globale du Groupe
DSI/G	Direction des Services d'Information du Groupe
LBP	La Banque Postale
PSSI-G	Politique de Sécurité des Systèmes d'information du Groupe
RSSI	Responsable de la Sécurité des Systèmes d'Information
SGG	Secrétaire Général du Groupe
SLCC	Service de Lutte contre la Cybercriminalité
SSI	Sécurité des Systèmes d'Information