DIRECTIVE STRATEGIQUE

13. GESTION DES INCIDENTS DE SECURITE INFORMATIQUE

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

Statut du document	Validé
Version	V 1.1
Date d'enregistrement	28/11/2019
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 les mesures relatives à la gestion des incidents de sécurité informatique.

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
Alerte	Les alertes sont des documents pouvant prendre plusieurs formes (notification, rapport, ticket, etc.) destinés à prévenir d'un danger immédiat
Collaborateur	Personne physique travaillant au sein du Groupe La Poste ou d'une de ses filiales
Entité	Terme générique désignant La Poste maison-mère, ses branches, ses holdings et ses filiales
Evénement	Occurrence ou changement d'un ensemble particulier de circonstances
Faille	Vulnérabilité dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces
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
INDIS	Application Intranet d'instruction des incidents de sûreté
Point de contact	Responsable ou adresse/numéro de téléphone fonctionnel pour la prise en compte d'évènements

3 Règles de sécurité applicables

3.1 Gestion des incidents liés à la sécurité de l'information et améliorations

Objectif : garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des évènements et des failles liés à la sécurité.

3.1.1 Responsabilités et procédures

Les responsabilités et les procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information sont établies.

3.1.1.1 Formalisation de l'organisation

Une procédure formelle de gestion des incidents de sécurité doit être définie, communiquée et tenue à jour. Elle doit définir les responsabilités de chacun au sein des processus afférents :

- La planification et la préparation des réponses aux incidents ;
- La surveillance, la détection, l'analyse et le signalement des évènements et des incidents ;
- La journalisation des activités de gestion des incidents ;
- L'appréciation et la prise de décision relatives aux événements et à failles liées à la sécurité de l'information ;
- La mise en place d'une échelle de classification des incidents et des événements ;
- La réponse à incident prévoit la communication interne et externe ;

Les procédures doivent garantir la fiabilité des personnels impliqués dans ces processus de gestion des incidents : compétences, nomination d'un point de contact, mise à jour des listes de diffusion et de contacts.

Le processus de signalement inclut :

- La mise en place de formulaires spécifiques destinés à faciliter le suivi ;
- Les actions à mettre en œuvre lorsqu'un évènement lié à la sécurité survient (par exemple, noter le type de défaillance, le dysfonctionnement constaté, etc.) ;
- La prévenance immédiate du responsable servant de point de contact ;

- L'exécution des seules actions autorisées ;
- Les retours d'informations de la résolution des incidents.

La DSGG mettra à disposition de tous les collaborateurs un outil de signalement de tout événement ou faille lié à la SSI, nommé INDIS.

3.1.1.2 Procédure d'escalade

Une procédure d'escalade est prévue, depuis la cellule de veille de l'entité jusqu'à celle de son centre opérationnel cyber s'il existe ou à la DCG, en fonction de critères de sévérité ou criticité à définir conjointement. Cette escalade doit être à même de pouvoir garantir la prise en compte et le suivi opérationnel des alertes.

La procédure prévoit l'information de la DCG lors de tout déclenchement, dans les meilleurs délais.

3.1.2 Signalement des événements liés à la sécurité de l'information

Les événements liés à la sécurité de l'information sont signalés dans les meilleurs délais par les voies hiérarchiques appropriées.

3.1.2.1 Information des collaborateurs

Les utilisateurs doivent être informés de leur obligation de signaler sans délai tout événement présentant un risque en matière de SSI (par exemple, dysfonctionnement logiciel ou matériel, violation d'accès, etc.).

Ils doivent notamment connaître :

- La procédure de signalement pour application ;
- Le point de contact auquel se référer.

3.1.3 Signalement des failles liées à la sécurité de l'information

Tout salarié ou contractant tiers utilisant les systèmes et services d'information du Groupe La Poste doit signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

3.1.3.1 Devoir de signalisation des failles de sécurité

Tous les salariés et contractants utilisant les SI doivent signaler, selon une procédure définie, toute faille de sécurité observée ou soupçonnée.

Les tests techniques pour rechercher et démontrer les failles de sécurité des SI du Groupe La Poste doivent faire l'objet d'un cadrage et d'une autorisation par le RSSI de l'entité.

3.1.4 Appréciation des événements liés à la sécurité de l'information et prise de décision

Une qualification des événements liés à la sécurité de l'information est réalisée afin de décider s'ils sont classés comme incidents de sécurité.

De plus, cette qualification doit permettre de détecter si des données à caractère personnel sont concernées par l'incident.

3.1.4.1 Qualification des incidents de sécurité selon leur criticité

Tout événement détecté doit faire l'objet d'une analyse et d'une qualification par une personne compétente en utilisant l'échelle de classification des incidents. Les Métiers sont amenés à contribuer à la phase de qualification à partir de leur contexte.

La catégorisation et la mesure des volumes (matrice de criticité) permettent d'identifier les conséquences et l'étendue d'un incident. Lorsque l'incident concerne des données à caractère personnel la directive du DPO relative aux violations de données à caractère personnel du 4 mars 2019, est appliquée. Cette directive définit la procédure à suivre pour évaluer la gravité de la violation de données à caractère personnel et la notifier à la CNIL.

3.1.5 Réponse aux incidents liés à la sécurité de l'information

La réponse aux incidents de sécurité est faite conformément aux procédures en vigueur.

3.1.5.1 Responsabilité

La réponse aux incidents s'effectue conformément à la procédure de gestion et de suivi des incidents de sécurité par le point de contact et tout autre acteur concerné (Métiers, Directeur des SI, Tiers, etc.).

3.1.5.2 Mise en œuvre

Tout incident de sécurité détecté doit conduire à la définition et à la mise en œuvre de mesures de réaction, visant à limiter au maximum les impacts de l'incident.

La réponse à l'incident prévoit :

- Le recueil de preuves dès que possible après l'incident ;
- Une analyse ;
- Une remontée d'informations ;
- L'assurance que toutes les tâches concernant la réponse sont correctement journalisées en vue d'une analyse ultérieure ;
- La communication de l'existence d'un incident aux autres personnes internes et externes à l'entité ou aux organisations ayant besoin d'en connaître ;
- Le traitement des failles constatées causant ou contribuant à l'incident ;
- La clôture formelle de l'incident et son enregistrement.

Une analyse postérieure à l'incident est effectuée pour identifier la source de l'incident.

3.1.5.3 Escalade et passage en gestion de crise

Les processus de gestion de crise spécifiques doivent être documentés et activés en cas d'incident majeur, suivant les principes édictés dans les procédures opérationnelles.

3.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information

Une capitalisation des analyses et des résolutions des incidents de sécurité est réalisée afin d'en réduire la probabilité ou, les conséquences d'incidents ultérieurs.

3.1.6.1 Capitalisation sur les incidents

Suite à l'analyse et à la résolution d'incidents, une concaténation des informations recueillies (quantification, qualification et coûts) est réalisée dans une base de connaissance afin d'identifier les incidents récurrents ou ayant des conséquences graves.

Tout incident de sécurité identifié comme significatif doit faire l'objet d'un retour d'expérience.

La mise en œuvre de plans d'actions issus de ces bilans « post-incident » doit faire l'objet d'un suivi et d'actions de contrôle.

La capitalisation sur les incidents contribue à enrichir les actions de sensibilisation et de formation des utilisateurs, administrateurs, opérateurs et managers.

Elle permet également d'identifier les axes d'amélioration des mesures (au niveau des processus, au niveau des infrastructures SI, au niveau de l'organisation, etc.).

3.1.7 Recueil de preuves

Des procédures d'identification, de recueil, d'acquisition et de protection de l'information sont définies puis appliquées afin de collecter et conserver des preuves valables.

3.1.7.1 Procédure de gestion des preuves

Une procédure de gestion des preuves est formalisée, tenue à jour et appliquée afin de pouvoir anticiper toute action judiciaire, assurantielle ou disciplinaire.

Elle prévoit les processus suivants :

- L'identification consistant à la recherche, la reconnaissance et la documentation de preuves potentielles ;
- Le recueil consistant à rassembler des éléments physiques pouvant contenir des preuves potentielles ;
- La création d'une copie des données ;
- La garantie de l'intégrité d'origine des preuves potentielles.

Dans le cadre de la gestion d'un dossier d'assurance, il convient de prévoir la collecte de documents et preuves tangibles permettant de lister :

- les mesures engagées ;
- les dommages engendrés;
- et coûts générés.

3.1.7.2 Opposabilité des preuves

Des dispositions spécifiques doivent être mises en œuvre afin de garantir l'opposabilité des traces numériques collectées en cas d'actions potentielles en justice.

Il est recommandé de contacter la DCG en cas d'incident pouvant entraîner la judiciarisation.