DIRECTIVE STRATEGIQUE

14. SECURITE DE L'INFORMATION DANS LE PLAN DE CONTINUITE D'ACTIVITE

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

Statut du document	Validé
Version	V 1.0
Date d'enregistrement	20/09/2020
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 sécurité de l'information dans le Plan de Continuité d'Activité.

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
Actif essentiel	Ressource informationnel ou processus qui a de la valeur pour l'entité. Les actifs essentiels représentent le patrimoine informationnel, ou les "biens immatériels", que l'entité souhaite protéger, c'est-à-dire ceux pour lesquels le non-respect de la disponibilité, de l'intégrité, de la confidentialité et de la traçabilité, mettrait en cause la responsabilité de l'utilisateur, ou causerait un préjudice à eux-mêmes ou à des tiers
Actif support	Composant technique ou non technique d'un système d'information sur lequel repose un actif essentiel. Les actifs supports regroupent les systèmes informatiques et de téléphonie, les organisations et les locaux qui hébergent les autres actifs supports et fournissent les ressources
Entité	Terme générique désignant La Poste maison-mère, ses branches, ses holdings et ses filiales
Plan de Continuité d'Activité (PCA)	Plan qui identifie les menaces potentielles pour une organisation, ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation. Il fournit un cadre pour construire la résilience de l'organisation, avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeurs
Plan de Continuité Informatique (PCI)	Le Plan de Continuité Informatique (PCI) est une sous partie du Plan de Continuité d'Activité (PCA), destinée à permettre la reprise du Système d'Information (SI) lorsque celui-ci est impacté par une situation de crise, sinistre ou défaillance majeure
Plan de Reprise d'Activité (PRA)	Le Plan de Reprise d'Activité Informatique constitue l'une des composantes d'un Plan de Continuité d'Activité global. Il peut aussi être établit en toute autonomie. Il définit l'ensemble des processus et des moyens humains, matériels et technologiques permettant à l'entreprise de faire face à un sinistre informatique
Sinistre	Événement grave d'origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des pertes et des dommages importants

3 Règles de sécurité applicables

3.1 Continuité de la sécurité de l'information

Objectif : Il convient que la continuité de la sécurité de l'information fasse partie intégrante des systèmes de gestion de la continuité d'activité.

Un Plan de Continuité d'Activité (PCA) a pour objet de décrire l'ensemble des mesures à mettre en œuvre pour garantir à une entité la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant son fonctionnement normal.

Il doit permettre à l'entité de répondre à ses obligations externes (législatives, réglementaires, contractuelles) ou internes (risque de perte de marché, survie de l'entreprise, image) et de tenir ses objectifs.

3.1.1 Organisation de la sécurité de l'information

Les exigences en matière de sécurité de l'information et de continuité du management de la sécurité de l'information sont déterminées par l'entité lors de l'organisation du PCA.

La démarche d'élaboration et de mise en œuvre d'un PCA relève du domaine métier de l'entité et couvre tant la continuité que la reprise après un sinistre.

À ce titre, le PCA inclut dans son périmètre les ressources critiques de l'entité comme les systèmes d'information, les infrastructures, les ressources humaines nécessaires à leur fonctionnement, etc.

3.1.1.1 Intégration de la continuité de la sécurité de l'information

La continuité de la sécurité de l'information doit être intégrée au processus de gestion de la continuité de l'activité de l'entité.

Elle doit être déclinée dans un Plan de Continuité Informatique (PCI) intégré au PCA global de l'entité.

3.1.1.2 Niveau de sensibilité des actifs

Les niveaux de sensibilité des actifs essentiels et supports restent identiques quel que soit le mode d'exploitation nominal ou dégradé.

3.1.1.3 Analyse d'impacts sur l'activité

Les exigences de continuité de la sécurité de l'information applicables aux situations défavorables sont déterminées par une analyse d'impact formelle sur les activités de l'entité.

3.1.1.4 Couverture des exigences

Les exigences de continuité de la sécurité de l'information applicables aux situations défavorables couvrent l'ensemble du périmètre concerné par les SI de l'entité et notamment : les ressources humaines, l'infrastructure, les réseaux et les ressources énergétiques.

3.1.2 Mise en œuvre de la continuité de la sécurité de l'information

Des processus et des procédures permettant de garantir le juste niveau de continuité de la sécurité de l'information lors de sinistres ou de crise sont documentés et mis à jour régulièrement.

3.1.2.1 Organisation

Chaque entité doit mettre en œuvre une structure de gestion adéquate ayant pour mission de préparer et de réagir à un incident impactant la sécurité de l'information.

Cette structure doit disposer de l'autorité, des moyens financiers et des ressources humaines compétentes nécessaires à l'accomplissement de sa mission. Ces personnes doivent être clairement identifiées et nommées.

3.1.2.2 Documentation et procédures

Chaque entité établit et formalise les processus et les procédures de réponse aux incidents et de maintien de la sécurité de son information, notamment en termes de :

- Mesures de sécurité de l'information ;
- Changements à mettre en œuvre pour maintenir ces mesures ;
- Mesures compensatoires en cas d'impossibilité du maintien de ces mesures afin de conserver un niveau acceptable de sécurité de l'information.

Ces procédures sont formellement validées par la direction de chaque entité et maintenues à jour régulièrement.

3.1.3 Vérifier, revoir et évaluer la continuité de l'information

Les documents décrivant les mesures de protection de l'information sont testés à intervalles réguliers pour s'assurer de leur validité et de leur efficacité.

3.1.3.1 Tests des procédures de la continuité de la sécurité de l'information

Chaque entité réalise des exercices réguliers évaluant notamment :

- La cohérence des procédures avec les objectifs de continuité ;
- La stabilité des performances entre la production et les tests ;
- La maîtrise des procédures et des tâches afférentes aux ressources humaines en charge de la mise en œuvre du plan de continuité de la sécurité de l'information ;
- La disponibilité des moyens et des ressources spécifiques conditionnant l'activation du plan de continuité.

Chaque exercice donne lieu à un retour d'expérience formalisé.

3.1.3.2 Mises à jour du plan de la continuité de la sécurité de l'information

Chaque entité effectue une revue régulière de la validité et de l'efficacité des mesures de la continuité de la sécurité de l'information.

Cette revue est systématiquement réalisée lors d'un changement dans l'environnement des SI et après la survenue d'un sinistre.

3.2 Redondances

Objectif : Garantir la disponibilité des moyens de traitement de l'information.

3.2.1 Disponibilité des moyens de traitement de l'information

Des moyens suffisants de redondance sont mis en œuvre afin de répondre aux exigences de disponibilité de l'information.

3.2.1.1 Evaluation des besoins en redondance

Chaque entité identifie et évalue les exigences de son activité avec ses Métiers en matière de disponibilité des SI.

Les composants ou architectures redondants mis en œuvre dans cet objectif, doivent être testés régulièrement. Ces tests intègrent

notamment la validation de leur bon état de marche ainsi que le bon fonctionnement du basculement d'un composant à un autre.

Le test des services redondés génère des risques pour l'intégrité ou la confidentialité de l'information et des SI, qu'il est nécessaire d'étudier dès la conception.