DIRECTIVE STRATEGIQUE

08. SECURITE LIEE A L'EXPLOITATION

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 les mesures relatives à la sécurité liée à l'exploitation.

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 un 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
Donnée sensible	Informations qui révélant la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique
Evènement de sécurité	Changement d'état d'un système lié à sa protection et indiquant l'émergence d'un risque
Poste de travail	Hors client léger
Pré-production	Etape permettant de valider la conformité d'une solution construite et de sa capacité à la mise en production
Protection antipollution	Ensemble des dispositifs permettant de protéger les systèmes contre les principales menaces cyber (virus, spam, etc.)

3 Règles de sécurité applicables

3.1 Procédures et responsabilités liées à l'exploitation

Objectif : s'assurer de l'exploitation conforme et sécurisée des moyens de traitement de l'information.

3.1.1 Documentation des procédures d'exploitation

Les procédures d'exploitation doivent être documentées et mises à disposition des acteurs concernés.

3.1.1.1 Gestion de la documentation

Les différentes procédures garantissant la bonne exploitation des SI doivent être documentées.

Ce corpus documentaire doit être centralisé, stocké de façon protégé (quel que soit son support, électronique ou papier) conformément à la directive « 04. Gestion des actifs et classification », accessible au seul personnel habilité.

Les procédures figurant dans cette documentation doivent avoir été préalablement testées et sont soumises à un processus de contrôle des changements.

Cette documentation doit être mise à jour à chaque changement ou de façon régulière et formellement validée par le directeur d'exploitation.

3.1.1.2 Contenu sécurité des procédures d'exploitation

Ces procédures doivent couvrir :

- L'installation et la configuration des systèmes ;
- Le traitement et la manipulation de l'information, qu'ils soient automatisés ou manuels ;
- Les sauvegardes ;
- Les exigences de planification, y compris les interdépendances avec d'autres systèmes, et les heures de démarrage de la première tâche et d'achèvement de la dernière tâche ;
- Les instructions pour gérer les erreurs ou autres conditions exceptionnelles susceptibles d'apparaître lors de l'exécution de la tâche, y compris les restrictions sur l'emploi des utilitaires systèmes (cf. directive « 5. Contrôle d'accès ») ;

- Les relations avec l'assistance technique et la hiérarchie, incluant les relations avec l'assistance technique externe, en cas de difficultés techniques ou d'exploitation inattendues ;
- Les instructions particulières sur la manipulation des supports et des données de sortie (cf. directive « 02. Mobilité ») ;
- La procédure de redémarrage et de récupération du système à appliquer en cas de défaillance du système ;
- La gestion du système de traçabilité et de l'information des journaux système ;
- La gestion des secrets de productions ;
- La surveillance des procédures ;
- La remontée des incidents (cf. directive « 13. Gestion des incidents de sécurité informatique »).

3.1.2 Gestion des changements

L'ensemble des changements apportés à l'organisation, aux processus Métiers, aux systèmes et aux moyens de traitement de l'information ayant des impacts sur la sécurité de l'information doit être contrôlé.

3.1.2.1 Processus

Un processus de gestion des changements doit être formalisé et mis en œuvre pour contrôler les modifications apportées à l'organisation, aux processus Métiers, aux systèmes et moyens de traitement de l'information qui influent sur la sécurité de l'information.

Les changements doivent être traités de manière identique sur les environnements de production et hors production.

Le processus de gestion des changements doit notamment garantir :

- Que tout changement de configuration ou de matériel sur un composant SI est :
  - réalisé uniquement par les équipes habilitées et formées à de telles opérations,
  - formellement validé et respectant le principe de ségrégation des tâches,
  - tracé (modifications effectuées, identifiant de l'intervenant, etc.),
  - évalué, au travers notamment de tests de non régression,
  - ne dégrade pas le niveau de sécurité initial offert par le réseau,
  - accompagné d'une procédure de « retour arrière » testée, validée et documentée.

- Qu'après chaque changement significatif, une reconfiguration systématique des règles de sécurité - ou au minimum une revue de ces règles - est réalisé.

Le déploiement des correctifs de sécurité sur les composants SI doivent être réalisé conformément au processus de gestion des changements.

3.1.2.2 Résilience

Lorsqu'un correctif ou un paramétrage, testé et validé est appliqué sur un environnement nominal, celui-ci doit être reporté automatiquement ou manuellement sur les dispositifs de secours afin d'assurer la résilience.

3.1.3 Gestion de la capacité

L'utilisation des ressources doit être surveillée et adaptée aux stricts besoins requis. Une gestion de la capacité est mise en œuvre et les besoins futurs anticipés.

3.1.3.1 Gestion des évolutions des socles techniques

Les besoins d'évolution doivent être anticipés afin de pouvoir dimensionner au mieux les socles techniques et garantir le bon niveau de performance et de fonctionnement des SI du Groupe La Poste.

Les entités du Groupe La Poste doivent être en mesure de détecter les problèmes liés au dimensionnement afin de pouvoir identifier les risques (délais, coûts et ressources clés) susceptibles de porter atteinte à la sécurité liée à l'exploitation.

3.1.4 Séparation des environnements de développement, de test et d'exploitation

Les environnements de développement, de test et d'exploitation doivent être cloisonnés afin de réduire les risques d'accès et les changements non autorisés ainsi que les contaminations dans l'environnement en exploitation.

3.1.4.1 Isolation et étanchéité des environnements et des données de production

Les différents environnements doivent être cloisonnés et étanches.

L'environnement de test doit être à isopérimètre de l'environnement d'exploitation, c'est-à-dire techniquement et technologiquement

similaires à la production pour assurer la pertinence des mises en production.

L'utilisation de données de production non anonymisées est proscrite lors des tests en pré-production ou lors des phases de développement.

Les passages en production sont formellement documentés.

Tous les tests sont effectués hors de la production.

Toutes les exceptions à ce chapitre sont formellement validées par le responsable Métier et réduites au cas exceptionnel.

Les personnels travaillant sur les environnements de développement et de test ont des droits restreints, dont l'environnement d'exploitation est exclu.

3.2 Protection contre les logiciels malveillants

Objectif : garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.

3.2.1 Mesures de protection

Conformément aux principes définis dans la directive « 01. Organisation de la sécurité de l'information » :

- Chaque entité du Groupe La Poste est en charge ou délègue à ses exploitants la lutte contre les codes malveillants sur son périmètre, et met en œuvre l'organisation et les moyens nécessaires à l'application de la présente directive sur son périmètre ;
- Le RSSI de chaque entité s'assure de l'application du présent chapitre sur son périmètre.

La protection contre les logiciels malveillants est fondée sur les préconisations décrites dans les paragraphes suivants de ce document.

3.2.1.1 Formalisation des mesures de protections

Une procédure formalise l'interdiction d''utilisation de logiciels non autorisés et indique les mesures de protection qu'il convient de prendre pour se protéger des risques liés aux fichiers et logiciels obtenus aussi bien depuis ou via les réseaux externes que sur tout autre support.

Des procédures listent les responsabilités, assurent la protection des systèmes contre les logiciels malveillants, la formation à l'utilisation de

ces systèmes, le signalement et la récupération après une attaque par des logiciels malveillants.

Des plans appropriés de continuité de l'activité sont rédigés afin de prévoir comment récupérer après une attaque, les sauvegardes de tous les logiciels et données nécessaires, et prévoient les dispositions pratiques de récupération.

Des processus sont prévus pour obtenir une information exacte en rapport avec les logiciels malveillants. S'assurer que les bulletins d'alerte sont diffusés à tous les acteurs impliqués du Groupe La Poste et qu'ils sont informés de la marche à suivre.

3.2.1.2 Application des mesures de protection

Mettre en œuvre les contrôles empêchant ou détectant :

- L'utilisation de logiciels non autorisés ;
- L'accès aux sites web connus et listés pour leur malveillance ou le contenu contraire à la politique du Groupe La Poste en tant que tels.

Les mesures suivantes sont également prévues :

- Organisation de la gestion des vulnérabilités techniques afin de réduire les failles pouvant être exploitées par des logiciels malveillants ;
- Réalisation de revues régulières des logiciels autorisés et mener une investigation formelle sur la présence de tout logiciel non approuvé ;
- Automatisation du processus de détection des codes malveillants pour définir, formaliser et mettre en œuvre une surveillance permanente, afin de déclencher au plus tôt les mesures adéquates ;
- Planification des mesures d'isolation des environnements les plus sensibles en cas d'attaque.

3.2.1.3 Mise en œuvre du dispositif de protection antipollution

L'installation et à la mise à jour régulière de logiciels de détection et de remédiation pour analyser les matériels et les supports à titre de mesure de précaution ou comme tâche de routine sont organisées.

Les analyses réalisées incluent :

- Une analyse récurrente des disques locaux des machines ;

- Une analyse de tout fichier reçu sur les réseaux ou via toute forme de support de stockage, pour s'assurer de l'absence de logiciels malveillants avant utilisation ;
- Une analyse des pièces jointes aux courriers électroniques et des fichiers téléchargés pour s'assurer de l'absence de logiciels malveillants avant utilisation ;
- Une analyse des pages web pour s'assurer de l'absence de contenus malveillants.

Le logiciel doit fonctionner en permanence, depuis le démarrage des équipements informatiques jusqu'à leur arrêt et doit être protégé et contrôlé régulièrement afin de prévenir de toute modification.

En cas d'arrêt volontaire ou accidentel de la solution antipollution, elle doit pouvoir être relancée automatiquement.

Tout poste de travail est équipé d'un pare-feu personnel actif, configuré en fonction de son contexte réseau d'utilisation. La configuration du pare-feu personnel est gérée de manière centralisée afin de permettre sa mise à jour et notamment celle des politiques de filtrage (flux autorisés ou proscrits).

La connexion directe ou indirecte aux réseaux internes d'équipements non fournis par le Groupe La Poste n'est pas autorisée.

3.3 Protection des données utilisateurs

Objectif : se protéger de la perte de données.

3.3.1 Sauvegarde des informations

Des sauvegardes de l'information, des logiciels et des images des différents systèmes utilisés doivent être réalisées et testés régulièrement conformément à la procédure en vigueur au sein de l'entité.

3.3.1.1 Procédure de sauvegarde

Il est nécessaire d'avoir une procédure de sauvegarde, à jour sur les périmètres applicatifs et systèmes. Les exigences métiers doivent être prises en compte sur la fréquence et la durée de conservation des sauvegardes.

Cette procédure prévoit l'enregistrement exact et complet des sauvegardes à des intervalles réguliers et permet de reconstituer à tout

moment l'environnement de production. Elles sont stockées dans un lieu distant (hors site principal), protégé des menaces physiques et environnementales.

Les supports et les procédures sont testées régulièrement afin d'en vérifier le bon fonctionnement et l'intégrité.

Les tests de restauration doivent permettre de contrôler l'utilisation des sauvegardes en situation d'urgence.

Une surveillance quotidienne s'assure de l'intégralité de l'exécution des sauvegardes et remédie les défaillances rencontrées.

Le directeur de la production est garant de la mise en place de ces contrôles.

3.4 Journalisation et surveillance

Objectif : enregistrer les évènements et générer des preuves.

3.4.1 Journalisation des événements

Les obligations d'inventaires correspondent :

- Au minimum aux obligations légales, réglementaires et contractuelles externes s'imposant au Groupe La Poste (cf. directive « 12. Relation avec les fournisseurs ») ;
- A des choix internes du Groupe La Poste tout en respectant les règles déontologiques applicables conformément à la charte de déontologie du Groupe La Poste ;
- Aux dispositions prévues dans la directive « 04. Gestion des actifs et classification ».

3.4.1.1 Mesures de journalisation

Lorsque cela est pertinent, des informations doivent être collectées afin de compléter les journaux d'évènements en garantissant le principe de « moindre trace ».

L'accès aux journaux doit être restreint aux équipes informatiques habilitées.

Les systèmes doivent être configurés pour conserver une trace des événements de sécurité. Les événements doivent être stockés de manière centralisée et protégés contre toute altération.

Les journaux d'événement contiennent par exemple les informations suivantes :

- Les identifiants utilisateurs ;
- Les activités du système ;
- La date, l'heure et les détails relatifs aux événements significatifs, par exemple les ouvertures et fermetures de session ;
- L'identité ou l'emplacement du terminal si possible et l'identifiant du système ;
- Les enregistrements des tentatives d'accès au système, réussies et avortées ;
- Les enregistrements des tentatives d'accès aux données et autres ressources, réussies ou avortées ;
- Les modifications apportées à la configuration du système ;
- L'utilisation des privilèges ;
- L'emploi des utilitaires et des applications ;
- Les fichiers qui ont fait l'objet d'un accès et la nature de l'accès ;
- Les adresses et les protocoles du réseau ;
- Les alarmes déclenchées par le système de contrôle d'accès ;
- L'activation et la désactivation des systèmes de protection, tels que les systèmes antivirus et les systèmes de détection des intrusions ;
- Les enregistrements des transactions réalisées par les utilisateurs dans les applications.

La journalisation des évènements permet de mettre en œuvre une surveillance et des remontées d'alertes relatives à la sécurité du système.

La journalisation doit prendre en compte les mesures appropriées pour assurer la protection de la confidentialité des informations à caractère personnel, conformément à la directive « 15. Conformité et contrôle ».

3.4.1.2 Traçabilité des accès et des opérations

Les traces électroniques portant sur des accès au SI et / ou des opérations réalisées au sein de ce SI sont collectées afin de permettre d'identifier l'utilisateur accédant et / ou réalisant les opérations en question, dans le respect de la réglementation en vigueur et du Règlement Général sur la Protection des Données.

3.4.1.3 Traçabilité des données sensibles

L'évaluation du niveau de traçabilité requis des accès aux données sensibles du SI doit être évaluée au travers de l'analyse de risques.

3.4.2 Protection et conservation des traces numériques

Les journaux et plus globalement l'ensemble des moyens de journalisation et l'information journalisée doivent être protégés en intégrité et confidentialité.

3.4.2.1 Niveau de sécurité des traces électroniques

Le niveau de sécurité doit permettre de protéger les traces électroniques contre l'altération, la modification ou la suppression des journaux.

Le stockage et les mesures conservatoires doivent protéger les journaux systèmes des dysfonctionnements.

La sécurité d'une trace informatique enregistrée au sein du SI du Groupe La Poste est du ressort du propriétaire (le « Métier ») de cette trace (cf. directive « 04. Gestion des actifs et classification »).

3.4.2.2 Traces contenant des données à caractère personnel

Les systèmes de gestion des traces électroniques pouvant contenir des données à caractère personnel se conforment à la législation en vigueur (cf. directive « 15. Conformité et contrôle »).

3.4.3 Journaliser les opérations des comptes à privilèges

Les activités des administrateurs et opérateurs système sont journalisés. Ces journaux doivent être protégés et contrôlés régulièrement.

3.4.3.1 Gestion des journaux

Les journaux administrateurs et opérateurs systèmes font l'objet d'un enregistrement afin de pouvoir tracer les actions des utilisateurs dotés de privilèges.

Ces journaux doivent être protégés afin de garantir l'imputabilité des actions et, revue pour assurer l'intégrité des journaux.

Les administrateurs et opérateurs systèmes ne peuvent effacer ou modifier les journaux concernant leurs activités.

3.4.3.2Contrôle des activités

Pour vérifier la conformité des activités d'administration système et réseau, il est possible d'utiliser un système de détection d'intrusion ou

un bastion d'administration hors du contrôle des administrateurs systèmes et réseaux.

3.4.4 Mise en œuvre d'une référence de temps

Les horloges de l'ensemble des SI de l'entité sont synchronisées avec une source de référence temporelle unique.

3.4.4.1 Procédure de synchronisation

L'horloge de l'ensemble des systèmes de traitement de l'information doit être synchronisée avec un référentiel temporel.

Le référentiel temporel par défaut au sein du SI du Groupe La Poste est le Temps Universel Coordonné (ou UTC).

La synchronisation des horloges doit faire l'objet d'un suivi régulier :

- Une procédure permettant de garantir l'obtention et la synchronisation avec l'heure de référence ;
- Une procédure de contrôle des dérives éventuelles doit être mise en œuvre ;
- Toute divergence subite représente un incident de sécurité et doit être traité comme tel, de même que toute modification formelle de l'horloge d'un dispositif enregistrant des traces électroniques.

3.4.4.2 Gestion de la preuve

Le paramétrage des horloges garantit la précision des journaux d'audit, utile lors d'investigations ou de remise de preuves lors de procédures légales.

Ce contrôle est à la charge du directeur de l'exploitation.

3.5 Inventaire et maîtrise des socles logiciels en exploitation

Objectif : garantir l'intégrité des systèmes en exploitation.

3.5.1 Installation de logiciels

L'installation de logiciels sur les systèmes en exploitation fait l'objet de procédures documentées et mises à jour.

3.5.1.1 Tests préalables avant installation

Les applications et le logiciel du système d'exploitation ne sont autorisés qu'après une série de tests ayant donné des résultats satisfaisants.

Les tests sont réalisés sur un système isolé, dédié et à isopérimètre de l'environnement d'exploitation.

La stratégie de réversibilité est testée avant d'appliquer des modifications.

3.5.1.2 Mise à disposition des logiciels

Seuls les logiciels ayant fait l'objet d'un contrôle et d'un référencement par le Groupe La Poste ou par la Direction des Systèmes d'Information (DSI) peuvent être installés sur les systèmes en exploitation du Groupe La Poste.

Seuls les applicatifs approuvés sont autorisés sur les SI du Groupe La Poste.

Tous choix de nouvelle version prend en compte les exigences Métiers, ainsi que les questions de sécurité liées à la nouvelle version.

3.5.1.3 Installation des logiciels

Afin de garantir l'intégrité des systèmes en exploitation l'installation de logiciels doit être contrôlée au travers de procédures prenant en compte la validation des logiciels et leur installation uniquement réalisée par les administrateurs autorisés.

Un système de contrôle de la configuration est mis en œuvre. Des contrôles sont effectués afin de garantir que seuls ces logiciels autorisés sont installés sur les SI du Groupe La Poste.

3.5.1.4 Maintenance des logiciels

Les correctifs logiciels sont appliqués, après analyse, lorsqu'ils permettent notamment de supprimer ou de réduire les failles de sécurité de l'information.

Pour tous logiciels éditeurs, une maintenance permettant de bénéficier de l'assistance technique de celui-ci est prévue. La DSI doit tenir compte des risques associés à l'utilisation de logiciels hors maintenance ou obsolètes.

3.5.1.5 Sauvegarde des logiciels

Les versions antérieures des logiciels, des paramètres, des procédures, des détails de configuration et des logiciels complémentaires associés sont conservées à titre de mesure de secours.

3.6 Gestion des vulnérabilités techniques

Objectif : empêcher toute exploitation des vulnérabilités techniques.

3.6.1 Processus de gestion

Dès l'identification de vulnérabilités techniques potentielles, une action appropriée dans les meilleurs délais est engagée. Il convient d'appliquer les recommandations suivantes pour établir un processus efficace de gestion des vulnérabilités techniques.

3.6.1.1 Prérequis organisationnel

Un inventaire des actifs exhaustif est tenu jour conformément à la directive « 04. Gestion des actifs et classification ».

Cet inventaire comporte le nom de l'éditeur du logiciel, les numéros de version, l'état de déploiement et le nom de la personne responsable du logiciel au sein de l'organisation et la criticité de l'actif.

3.6.1.2 Organisation de la gestion des vulnérabilités

Des dispositifs formalisés de veille de sécurité des SI doivent être mis en place par chaque entité.

Les listes de ressources d'information permettant de signaler les vulnérabilités techniques afférentes aux logiciels et technologies employée sur les SI du Groupe sont identifiées et tenues à jour.

Ces dispositifs doivent être interfacés avec les dispositifs de gestion des incidents et de gestion de crise du Groupe La Poste. Des procédures techniques sont tenues à jour pour mettre en place les mesures à réaliser en cas d'incident.

Des responsables sont identifiés au sein de l'organisation afin de gérer la stratégie de gestion des correctifs de sécurité (identification, appréciation, application).

Les entités tiennent à jour leur procédure de gestion des correctifs. Celle-ci doit être définie, et adaptée suivant les contraintes et le niveau d'exposition des systèmes. Un délai de réaction aux notifications y est défini en fonction de la criticité du système considéré.

Cette procédure est évaluée à intervalles réguliers afin de s'assurer de son efficacité.

3.6.1.3 Qualification des vulnérabilités

Lorsqu'un correctif logiciel d'une source autorisée est disponible une évaluation des risques associés à l'installation est effectuée. Il est nécessaire de le qualifier avant de les intégrer dans l'environnement d'exploitation afin d'éviter des effets collatéraux indésirables.

Si aucun correctif logiciel n'est disponible, d'autres mesures doivent être prises en fonction de l'évaluation des risques associés à la vulnérabilité :

- La désactivation des services ou des fonctions liés à la vulnérabilité ;
- L'adaptation ou l'ajout de contrôles d'accès, par exemple des pare-feu, aux limites du réseau ;
- Le renforcement du dispositif de surveillance visant à détecter les attaques réelles ;
- Le renforcement de la politique de sensibilisation aux vulnérabilités ;
- L'information des utilisateurs ou d'acteurs clefs afin de signaler tout incident.

S'il n'est pas possible de tester correctement le correctif logiciel, l'application du correctif peut être repoussée à une date ultérieure, afin d'évaluer les risques inhérents à sa mise en œuvre.

3.6.1.4 Application des correctifs de sécurité

Tout déploiement d'un composant logiciel ou d'un correctif doit s'intégrer aux procédures de gestion des changements.

En fonction du caractère d'urgence présenté par la vulnérabilité technique et l'évaluation du risque, le correctif peut être immédiatement appliqué.

Le correctif de sécurité doit être déployé sur l'ensemble du parc matériel et logiciel afin de garantir l'exhaustivité de la protection.

Une main courante de toutes les procédures entreprises est tenue à jour.

3.6.2 Installation de logiciels par l'utilisateur

L'installation non contrôlée de logiciels sur des dispositifs informatiques génère des risques tels que :

- l'introduction de vulnérabilités ;
- des fuites de l'information ;
- la perte d'intégrité ou d'autres incidents liés à la sécurité de l'information,
- la violation des droits de propriété intellectuelle.

L'installation de logiciels par les utilisateurs est interdite, sauf exception prévue et encadrée selon les termes prévus dans le cadre général de la PSSI-G.

3.6.2.1 Mesures de restriction

Une politique stricte est instaurée sur le type de logiciels que les utilisateurs peuvent installer.

Afin de garantir la sécurité des SI une procédure concernant l'installation de logiciels doit être mise en place.

Les logiciels installés sur les postes de travail doivent répondre aux exigences suivantes :

- Ils sont fournis par le Groupe La Poste ;
- Ils sont installés par les équipes compétentes de Groupe La Poste (support informatique) ;
- Les logiciels installés correspondent à un besoin, dans le cadre d'un usage professionnel. Les composants non utilisés ou non nécessaires doivent être désactivés ou supprimés ;
- Les logiciels et matériels installés font l'objet d'un support (éditeur, tiers partenaire, support interne, etc.) ;
- Les logiciels et matériels installés font l'objet d'une acquisition de licences d'utilisation, s'ils y sont soumis ;
- Une qualification technique du composant logiciel doit être réalisée au préalable de l'installation du logiciel additionnel ;
- Les droits d'administrations liés aux logiciels sont strictement limités aux utilisateurs ayant besoin d'avoir un accès privilégié à ces logiciels.

3.7 Evaluation de la sécurité du SI

Objectif : réduire au minimum l'incidence des activités de contrôle et d'audit sur les systèmes en exploitation.

3.7.1 Mesures préventives

Les exigences d'audit et les activités impliquant des contrôles sur les systèmes en exploitation doivent être planifiées avec soin afin de réduire au minimum les perturbations sur ces systèmes.

3.7.1.1 Convention d'audit

Des prestations telles que les audits de sécurité des SI du Groupe La Poste interne ou externe (cf. directive « 12. Relation avec les fournisseurs ») sont prévues et décrites dans des mesures contractuelles spécifiques, incontournables dans le cas de tests d'intrusion ou d'évaluation de vulnérabilités par exemple.

Dès lors, une convention d'audit doit être signée entre les parties. Elle prévoit au minimum les éléments suivants :

- Les exigences d'audit liées à l'accès aux systèmes et aux données ;
- Le périmètre des tests techniques d'audit ;
- La validation formelle des opérations d'investigation, par du personnel interne ;
- La remise en l'état initial des systèmes testés ;
- L'assurance de l'auditeur couvrant de manière adéquate l'ensemble de la prestation d'audit ;
- Les tests d'audit pouvant compromettre la disponibilité du système sont réalisés en dehors des heures de travail ;
- Une fois l'audit terminé, l'auditeur s'engage à effacer toutes les données en sa possession.

3.7.1.2 Cadre de la prestation d'audit

Tout audit de sécurité doit être réalisé sous le pilotage d'un responsable interne au Groupe La Poste.

Un cadre de réalisation de la prestation est posé afin de respecter les bonnes pratiques suivantes :

- Limiter les tests d'audit à un accès en lecture seule des logiciels et des données au maximum ;

- Les accès autres qu'en lecture seule ne sont autorisés que pour les copies séparées des fichiers système ;
- Une sauvegarde complète du périmètre audité est effectuée avant la prestation d'audit ;
- Contrôler et journaliser tous les accès afin de disposer d'une traçabilité faisant référence ;
- L'accès aux outils de contrôle et d'audit doit être restreint et maîtrisé.