DIRECTIVE STRATEGIQUE

09. RESEAU

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 au réseau.

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 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.

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
Authentification	L'authentification est l'opération par laquelle un équipement ou un traitement informatique (système, application) vérifie que l'accédant qui souhaite se connecter est bien celui qu'il prétend être. S'authentifier c'est apporter la preuve de son identité. Cette opération peut s'appuyer sur : ▸ Une information que l'accédant connaît : un secret, un mot de passe, etc. ; ▸ Une information que l'accédant possède : une carte à puce, un « token », etc. ; ▸ Une information qui lui est propre : une empreinte digitale, le son de sa voix, etc. Dans le processus de connexion à un SI et à ses ressources, l'authentification est le premier point de contrôle logique. L'authentification est à ce titre un mécanisme incontournable permettant de maîtriser les accès aux ressources du Système d'Information. De sa qualité et de sa robustesse dépendent la sûreté de l'information et sa protection contre des accès illicites
BYOD	L'acronyme « BYOD » est l'abréviation de l'expression anglaise « Bring Your Own Device », qui désigne l'usage d'équipements informatiques personnels dans un contexte professionnel.
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
Poste de travail	Désigne les moyens informatiques utilisés pour la réalisation des tâches professionnelles, communément un ordinateur (hors clients légers)
Service réseau	Les services de réseau comprennent la fourniture de connexion, les services de réseau privé, les réseaux à valeur ajoutée et les solutions de management de la sécurité des réseaux comme les pare-feux et les systèmes de détection d'intrusion
Zone d'administration	Sous-ensemble du SI d'administration dont l'objectif est d'isoler ou cloisonner des ressources d'administration par des mesures de protection adaptées au contexte (ex : filtrage, cloisonnement logique de réseau, authentification, mise en œuvre de VPN IPsec) et en fonction du juste besoin opérationnel. De façon à définir ces zones le plus efficacement possible, il est nécessaire au préalable de définir les zones de confiances du SI administré

Zone de confiance	Ensemble de ressources informatiques regroupées en fonction de l'homogénéité de facteurs divers et variés (liés ou non à la sécurité)

3 Règles de sécurité applicables

Les activités du Groupe La Poste sont rassemblées dans des zones de confiance. Les activités de chaque ensemble présentent des typologies d'échanges et des profils de sécurité similaires (risques contraintes réglementaires, sensibilité des données).

3.1 Management de la sécurité des réseaux

Objectif : garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.

3.1.1 Contrôle des réseaux

L'information contenue dans les SI est protégée grâce à une procédure de gestion et un contrôle des réseaux rigoureux.

3.1.1.1 Rôles et responsabilités en matière de sécurité des réseaux

Les Directeurs des SI, sur leur périmètre de responsabilité, sont responsables de l'application des règles de la présente directive et de leur mise en œuvre.

Seuls les équipements réseau et les réseaux validés par les responsables réseau sont autorisés au sein des sites du Groupe La Poste (interdiction de box internet). Seuls les matériels utilisateurs fournis par l'entreprise sont autorisés à se connecter aux réseaux du Groupe La Poste (BYOD interdit).

3.1.1.2 Cartographie du réseau informatique

Une cartographie du réseau informatique est établie et tenue à jour suivant des procédures définies.

Cette cartographie comprend au minimum les éléments suivants :

- Les caractéristiques du réseau informatique ;
- Les sites reliés et les lignes de communication mises en œuvre ;
- Les flux existant et les applications ou services associés ;
- Les plans d'adressage, de routage et de câblage des réseaux.

Les éléments de la cartographie des réseaux doivent être classifiés conformément à la directive « 04. Gestion des actifs et classification » et protégés en conséquence.

3.1.1.3 Contrôle de la sécurité des réseaux

Les procédures mises en place doivent assurer le contrôle permanent de premier niveau de la sécurité des réseaux.

Ces procédures doivent couvrir au minimum :

- La configuration générale des équipements réseau et sécurité ;
- L'authentification des systèmes sur le réseau ;
- Les modalités pour préserver la confidentialité et l'intégrité des données transmises sur les réseaux ;
- Les règles de filtrage et de sécurité mises en œuvre ainsi que leur évolution ;
- Les modalités de la journalisation ;
- La limitation des connexions des systèmes réseaux ;
- Le Maintien en Condition de Sécurité des composants (matériel et logiciel) de l'infrastructure des réseaux.

3.1.1.4 Mise en place des réseaux filaires

Tout réseau local filaire sur le réseau interne du Groupe La Poste est connu, autorisé et garantit un niveau de sécurité suffisant conformément au résultat de l'analyse de risque, par exemple en mettant en œuvre :

- Le chiffrement des flux via des protocoles sûrs ;
- Les dispositifs de filtrage, limitant les ressources accessibles et les protocoles autorisés.

Compte tenu des enjeux de sécurité, seuls les postes de travail fournis par le Groupe La Poste peuvent s'y connecter.

3.1.1.5 Mise en place des réseaux locaux sans-fil

Tout réseau local sans-fil sur le réseau interne du Groupe La Poste est connu, autorisé et garantit un niveau de sécurité suffisant, notamment en mettant en œuvre :

- L'authentification forte des équipements informatiques connectés ;
- Le chiffrement des flux via des protocoles sûrs ;

- Des dispositifs de filtrage entre l'infrastructure sans-fil et le reste du réseau interne, limitant les ressources accessibles et les protocoles autorisés, sauf dans le cas d'une extension du réseau local.

Les réseaux locaux sans fil professionnels sont différenciés des réseaux locaux sans fil invités.

Seuls les postes de travail fournis par le Groupe La Poste peuvent se connecter sur les réseaux sans fil professionnels.

3.1.1.6 Externalisation de prestation

Dans le cadre d'une prestation d'externalisation de fourniture de connexion, de service de réseau privé et de réseaux à valeur ajoutée (Cloud), la présente directive s'applique au fournisseur.

Les services offrant des solutions de management de la sécurité des réseaux ne peuvent faire l'objet d'externalisation.

3.1.2 Sécurité des services de réseau

Pour l'ensemble des services de réseau, les mécanismes de sécurité, les niveaux de services et les exigences de gestion sont identifiés et intégrés dans des accords de services de réseau (fournis en interne ou externalisés).

3.1.2.1 Choix des équipements réseaux

Le choix des équipements servant à mettre en œuvre les réseaux du Groupe La Poste ne doit en aucun cas constituer une entrave à l'application de la présente directive. Les cahiers des charges doivent donc être rédigés en intégrant les exigences de la présente directive.

3.1.2.2 Niveau de sécurité des réseaux informatiques

Chaque réseau informatique doit mettre en œuvre les composants permettant d'assurer sa sécurité en fonction de ses niveaux de sensibilité maximale Disponibilité, Intégrité, Confidentialité et Traçabilité (D, I, C, T).

Il convient d'identifier les besoins de sécurité nécessaires à chaque réseau afin d'en adapter les exigences et de les intégrer dans les livrables associés.

3.1.2.3 Continuité de service des réseaux

Des niveaux de résilience des services réseaux doivent être clairement définis selon leurs niveaux de sensibilité maximale D, I, C, T.

3.1.2.4 Affectation des adresses IP privées et publiques

L'adressage IP (Internet Protocol) sur les réseaux doit s'appuyer sur les normes existantes (telle que la Request For Comments 1918).

3.1.2.5 Routage et filtrage réseau

Les règles de routage et de filtrage réseau sont validées par les responsables de domaine réseau.

3.1.3 Cloisonnement des réseaux

Tous les groupes de services d'information, d'utilisateurs et de SI doivent être cloisonnés sur les réseaux.

3.1.3.1 Zones de confiance

Les réseaux du Groupe La Poste sont divisés en ensembles de même niveau de sensibilité (D, I, C, T) appelés « zones de confiance ».

3.1.3.2 Zones d'échanges

L'interface entre des zones de confiance interne et le monde extérieur est assurée par une zone d'échange.

Au sein du Groupe La Poste, trois types de zones d'échange sont définis :

- La zone d'échange externe intègre les fonctions de sécurité requises ciblant principalement sur les couches « infrastructures » du réseau, pour les flux en provenance de réseaux publics ou de tiers avec notamment les fonctions suivantes :
  - le système de lutte contre les dénis de service,
  - le filtrage des flux par des mécanismes de pare-feu au niveau réseau,
  - la terminaison des liaisons chiffrées établies au niveau des couches « basses » du réseau (exemple : Internet Protocol Security).
- La zone d'échange intermédiaire intègre les fonctions de sécurité destinées à protéger le contenu des flux entrants & sortants d'une zone de confiance, notamment les fonctions suivantes :
  - rupture de protocole ou rupture de session,
  - proxification des flux (proxy, reverse proxy, etc.),

- la terminaison des liaisons chiffrées établies au niveau des couches intermédiaires (exemples : Transport Layer Security, Secure Socket shell),
- l'inspection du contenu des flux pour détecter les tentatives d'intrusion, d'exfiltration de données et d'injection de contenu malveillant (exemple : Intrusion Detection System, Intrusion Prevention System, pare feux applicatif, etc.) et identifier les nouvelles formes d'attaques,

❑ La zone d'échange interne intègre les fonctions de sécurité permettant le cloisonnement à l'intérieur d'une zone de confiance, notamment des fonctions suivantes :

- segmentation des sous-réseaux,
- filtrage des flux entre sous-réseaux.

3.1.3.3 Cloisonnement des zones de confiance

Les mécanismes de cloisonnement entre zones de confiance doivent être en mesure de garantir le niveau de sensibilité de leurs données (D, I, C, T).

Les dispositifs de protection peuvent faire partie intégrante de la zone considérée (ex : pare-feu des datacenter), ou être mutualisés aux points d'interconnexion réseau entre les zones (ex : pare-feu local effectuant le cloisonnement entre plusieurs zones démilitarisées).

3.1.3.4 Affectation des ressources aux zones réseaux

Chaque ressource des SI (applications, serveurs, postes de travail, etc.) doit être affectée à une seule et unique zone réseau.

3.1.3.5 Points d'interconnexion entre les zones

Des points d'interconnexion réseau doivent être mis en place pour isoler les différentes zones réseaux. Ces points d'interconnexion peuvent être de différents types :

❑ Passant : aucun filtrage n'est réalisé, l'intégralité des communications est autorisée ;

❑ Permissif : tous les flux et protocoles sont autorisés par défaut. Une analyse de contenu est réalisée, les contenus non-conformes à la PSSI sont bloqués selon un principe de l'interdiction explicite (ou « liste noire ») ;

- Restrictif : seuls les flux et protocoles explicitement autorisés, strictement nécessaires et définis précisément (adresse source, destination, protocole, etc.) sont autorisés (« liste blanche »).

3.1.3.6 Résilience

La résilience d'un point d'interconnexion doit être définie en fonction du niveau de sensibilité (D, I, C, T) de la zone concernée.

3.1.3.7 Interconnexion des zones de confiance

Les équipements d'interconnexion peuvent être utilisés pour réaliser l'interconnexion de plusieurs zones de confiance, sous réserve que les zones concernées aient un niveau de sensibilité compatible (D, I, C, T).

3.1.3.8 Traitement des flux du niveau réseau

Des mécanismes de dépollution adaptés à chaque flux doivent être mis en place.

3.1.3.9 Robustesse du point d'interconnexion

Chacun des points d'interconnexion filtrants doit être opéré au moyen d'équipements de sécurité ayant des fonctionnalités et éventuellement des technologies différentes de façon à limiter la probabilité d'une compromission généralisée.

3.1.3.10 Documentation des flux autorisés

Un référentiel des flux autorisés est obligatoirement tenu à jour pour tous flux ouverts entre des zones de confiance différentes. Cette matrice des flux doit contenir au minimum :

- Les flux autorisés ;
- Les applications et services correspondants ;
- Les points de contact en cas de problème ou en cas d'interruption (au minimum : contact production et sécurité, backup ou équipes concernées) ;
- Des informations de niveau de sensibilité (D, I, C, T).

Cette matrice doit être régulièrement revue et mise à jour par le Responsable du Domaine Réseau.

3.1.3.11 Zones d'administration et de supervision

Au minimum, un réseau logique est mis en œuvre et spécifiquement dédié à l'administration et à la supervision.

Les serveurs d'administration et de supervision doivent être positionnés dans une zone de confiance spécifique nommée « zone d'administration et de supervision ».

Toutes les opérations d'administration et de supervision à destination des équipements doivent être initiées et conduites depuis cette zone.

3.1.3.12 Multiplicité des zones d'administration et de supervision

Chaque zone de confiance est administrée à partir d'une zone d'administration et de supervision.

Une zone d'administration et de supervision peut gérer plusieurs zones de confiance.