DIRECTIVE STRATEGIQUE

11. GESTION DE PROJET

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

Statut du document	Validé
Version	V 2.0
Date d'enregistrement	28/10/2020
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 gestion des projets.

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	Toute ressource nécessaire à la réalisation de ses objectifs. On distingue les actifs essentiels et les actifs supports
Chief Data Officer (CDO)	Le CDO ou directeur des données, a la responsabilité de créer un environnement permettant aux différents responsables de l'entreprise d'accéder aux informations dont ils ont besoin facilement et en toute sécurité
Confidentialité	Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés
Data protection officer ou Délégué à la Protection des données	Le Délégué à la Protection des données (DPD) ou DPO remplace le Correspondant Informatique et Libertés (CIL), qui pouvait être désigné de façon facultative dans l'entreprise comme garant de l'application de la loi « informatique et libertés ». Le DPD a pour mission d'assurer une veille et un conseil interne auprès de l'employeur sur les obligations de protection des données personnelles. Il est également le référent de la CNIL
Disponibilité	Propriété d'être accessible et utilisable à la demande par une entité autorisée. Le critère de disponibilité d'un actif est décrit en fonction de conditions prédéfinies d'horaires et de délais
Intégrité	Propriété de protection de l'exactitude et de l'exhaustivité des actifs. Le critère d'intégrité défini la nécessité, pour un actif d'être identique et inaltérable dans le temps et dans l'espace et de certifier son exhaustivité, sa validité et sa cohérence
Maîtrise d'ouvrage	La maîtrise d'ouvrage (MOA) est la personne pour qui est réalisé le projet. Elle est l'entité porteuse d'un besoin, définissant l'objectif d'un projet, son calendrier et le budget consacré à ce projet

3 Règles de sécurité applicables

3.1 Exigences de sécurité projets

Objectif : veiller à ce que la sécurité de l'information fasse partie intégrante des SI tout au long de leur cycle de vie, en respectant notamment les exigences spécifiques pour les SI fournissant des services sur les réseaux publics.

Au sein du Groupe La Poste, les règles de sécurité applicables aux projets correspondent aux exigences définies selon la catégorie du Système d'Information :

- Les SI dits « **réglementés** », qui doivent strictement se conformer à la règlementation en vigueur au regard de la loi, conformément à la PSSI-G et tel que décrit dans la directive « 16. Réglementaire ». Le Règlement Général sur la Protection des Données (RGPD) s'applique à tous les SI, sans pour autant les qualifier en tant que SI réglementés ;
- Les SI dits « **non réglementés** », n'ayant pas à répondre aux exigences d'une réglementation nationale ou internationale, se doivent néanmoins d'être conformes à la PSSI-G et respecter, de ce fait, les exigences de la présente directive.

Tous les SI du Groupe La Poste doivent faire l'objet d'une analyse de risque dont le niveau de détail dépendra du type de SI, déterminé par le questionnaire d'auto-évaluation. Le processus complet est décrit dans la procédure opérationnelle « Homologation de sécurité et sécurisation des Systèmes d'Information ».

Seuls les SI réglementés ou identifiés comme « critiques » feront l'objet d'une homologation complète.

3.1.1 Identification des exigences de sécurité de l'information

Les exigences liées à la sécurité de l'information sont considérées comme la résultante de 4 sources :

- Les contraintes externes ;
- Les risques ;
- Les besoins en sécurité exprimés par les Métiers ;
- Les spécificités en cas d'appel à des prestataires externes.

Elles peuvent alors prendre la forme de besoins fonctionnels, de mesures supplémentaires ou s'appuyer sur des directives et des outils existants au sein du Groupe La Poste.

3.1.1.1 Contraintes externes

La direction « Métier » propriétaire du projet doit identifier et documenter l'ensemble des contraintes externes, liées à l'environnement stratégique, concurrentiel ou législatif :

- La valeur stratégique des informations auxquelles l'équipe projet a accès, ainsi que celles des partenaires ou des concurrents impliqués ;
- Les législations ou réglementations susceptibles d'encadrer l'utilisation des informations (juridiction dans laquelle elles sont générées, traitées, achevées, stockées) et/ ou des technologies de l'information en présence (chiffrement, etc.) ;
- La mise en application des règlements et directives du Groupe La Poste.

Pour ce faire, en fonction du contexte les acteurs pertinents doivent être sollicités : Maîtrise d'Ouvrage (MOA), Ressources Juridiques, Data Protection Officer (DPO), Chief Data Officer (CDO), etc.

La directive « 15. Conformité et contrôle » référence de manière non exhaustive les règlements et législations liés à la SSI applicables aux projets du Groupe.

3.1.1.2 Expressions de besoins de sécurité

La direction « Métier » doit formellement exprimer les besoins de sécurité de l'information concernée par le projet, ainsi que les processus associés, en termes de Disponibilité (D), d'Intégrité (I), Confidentialité (C) et Traçabilité (T). Ces besoins résultent de la criticité évaluée des actifs, telle que prévue dans la directive « 04. Gestion des actifs et classification ».

3.1.1.3 Exigences en cas de contractualisation externe

Des exigences complémentaires de sécurité doivent être assurées dans les relations contractuelles aussi bien pour les achats de matériel et de logiciel, que pour la sous-traitance de développement informatique (cf. directive « 12. Relation avec les fournisseurs »).

Concernant l'acquisition de matériels ou de progiciels :

- Un processus formel de sélection, de test et d'acquisition doit être décrit et appliqué. Celui-ci se base sur les exigences de sécurité identifiées et traitées lors des précédentes étapes ;
- Les recommandations fournies avec le produit, liées à la configuration de la sécurité doivent être évaluées et mises en œuvre en correspondance avec les environnements ;
- Les critères d'acceptation doivent inclure la satisfaction aux exigences de sécurité, par le produit d'origine ou via des mesures complémentaires. En particulier on doit s'assurer de leur :
  - pérennité : les applications achetées sont produites par des sociétés pérennes dans le domaine qui doivent s'engager à les maintenir dans leur offre,
  - condition de sécurité : les certifications relatives à la sécurité du produit sont prises en compte (certification/qualification ANSSI, critères communs, etc.),
  - maintien des conditions de sécurité : les produits sont régulièrement analysés en termes de sécurité et font l'objet de correction dans des délais compatibles avec les exigences de sécurité.

Les réponses à ces exigences sont présentées dans un Plan d'Assurance Sécurité, rédigé par le fournisseur.

3.1.1.4 Suivi des exigences dans les projets

Tel que décrit dans les procédures de « Méthodologie de projet des SI », les exigences doivent être prises en compte par l'organisation du projet tout au long de son cycle de vie, en présentant dans un corpus documentaire l'ensemble des mesures prévues pour y satisfaire.

Le retrait ou la fin de vie d'un système d'information est un projet en soi, qui doit se conformer à la même démarche.

3.1.1.5 Analyse des risques

Les risques liés aux SI doivent être identifiés au plus tôt et documentés. Plusieurs méthodes d'analyses de risques peuvent être appliquées, conformément à la norme ISO/CEI 27005. A titre d'exemple :

- MEHARI® ;
- EBIOS® 2010.

Toute nouvelle fonctionnalité d'un SI doit déclencher une mise à jour de l'analyse de risques, afin de vérifier qu'elle ne génère pas un risque supplémentaire.

3.1.2 Sécurisation des services d'application sur les réseaux publics

Les services concernés sont notamment ceux qui permettent :

- L'authentification à un espace utilisateur ;
- Le renseignement de formulaires avec données confidentielles (personnelles, financières, etc.) ;
- L'établissement d'une transaction commerciale, etc.

3.1.2.1 Convention de services

Les conditions de service sur lesquelles s'appuient les échanges applicatifs sont documentées dans une convention de service et prévoient :

- Une description détaillée des processus d'autorisation liés aux personnes qui peuvent approuver le contenu, émettre ou signer des documents transactionnels clés ;
- Les moyens d'assurer une information pleine et entière des utilisateurs ou des partenaires engagés dans les échanges applicatifs, quant aux autorisations qui leur sont accordées pour la fourniture ou l'utilisation du service ;
- Les moyens mis en place pour satisfaire les exigences en matière de confidentialité ;
- Les moyens mis en place pour satisfaire les exigences d'intégrité ;
- Les moyens mis en place pour satisfaire les exigences de preuve de la répartition et de la réception des documents-clés et de non-répudiation des éléments substantiels de la transaction (parcours d'achat, catalogues produits, bons de commandes, appels d'offre, cookies, etc.) ;
- La responsabilité juridique induite par toute transaction frauduleuse.

Ces documents peuvent prendre la forme de contrats ou de conventions avec les tiers (ex. prestataires SaaS, IaaS, etc.).

3.1.2.2 Critères d'application des exigences de sécurité

Les exigences de sécurité du projet sont mises en œuvre en prévoyant :

- Une politique d'identification et d'authentification (cf. directive « 05. Contrôle d'accès ») qui permette de garantir l'identité des accédants ;
- Une politique de cryptographie (cf. directive « 06. Cryptographie ») qui garantisse la confidentialité et l'intégrité des documents clés, ainsi que de toutes les transactions (commandes, détails de paiement, coordonnées de livraison et de confirmation de réception, etc.) ;
- Les besoins Métier concernant la sécurisation des transactions ;
- La prise en compte des exigences de résistance aux attaques (garantie de la disponibilité des interconnexions réseau requises, (protection de l'information sensible).

3.1.3 Protection des transactions liées aux services d'application

L'information impliquée dans les transactions liées aux services d'application est protégée afin d'empêcher une transmission incomplète, des erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa réémission.

3.1.3.1 Mesures de sécurité relatives aux transactions

Les mesures de sécurité sont adaptées au niveau des risques et des besoins de sécurité associés à chaque type de transaction. Le cas échéant, elles satisfont aux exigences légales et réglementaires encadrant l'activité concernée.

Protéger les transactions revient à prévoir les mesures nécessaires pour garantir :

- La traçabilité des échanges et le maintien en conditions de sécurité des accès :
  - les informations secrètes d'authentification utilisateur de toutes les parties sont valables et ont fait l'objet d'une vérification,
  - la transaction demeure confidentielle,
  - La confidentialité des informations personnelles de toutes les parties impliquées est maintenue,
  - lorsqu'une autorité de confiance est utilisée, la sécurité est intégrée et imbriquée tout au long du processus de gestion de bout en bout des certificats ou des signatures.
- L'intégrité de la transaction :
  - utilisation de signatures électroniques par chacune des parties impliquées dans la transaction,

- stockage des détails hors de tout environnement accessible au public,
- support de stockage non exposé ni directement accessible depuis Internet.

❑ La confidentialité de la communication :

- chiffrement du canal entre toutes les parties impliquées,
- sécurisation des protocoles utilisés entre les parties.

3.2 Sécurité des développements et d'assistance technique

Objectif : s'assurer que les questions de sécurité de l'information sont prises en compte et documentées dans le cadre du cycle de développement des SI.

3.2.1 Politique de développement sécurisé

Tous les développements doivent intégrer des procédures qui garantissent la juste application des règles de sécurités qui s'appliquent tant pour un service, une architecture, un logiciel ou un système.

3.2.1.1 Sécurité des environnements de développement

Les ressources informatiques matérielles et logicielles utilisées pour les activités de développement ou de maintenance doivent être séparées de celles utilisées dans un environnement de production. Cette séparation doit être au moins logique, mais de préférence physique.

De même un cloisonnement, au minimum logique, doit permettre d'isoler les environnements de développement des environnements de tests.

Une gestion adaptée des accréditations doit être mise en place afin de garantir la cohérence des périmètres d'action de chaque typologie d'utilisateurs sur les différents environnements définis. Sauf cas particuliers formellement soumis à encadrement, les équipes de développement ne doivent pas accéder à l'environnement de production (données et programmes en exploitation).

3.2.1.2 Sécurité dans la phase de réalisation

Les spécifications techniques doivent couvrir les exigences de sécurité dès la phase de conception.

Les règles relatives à la sécurité du développement doivent être documentées, maintenues et utilisées.

L'intégrité du développement est garantie par la mise en place de :

- Référentiels sécurisés ;
- Système de contrôle des versions ;
- Guides de sécurisation (durcissement) des ressources informatiques ;
- Normes de développement applicatif ;
- Normes d'intégration aux zones cloisonnées des réseaux ;
- Normes de traçabilité informatique ;
- Standards de sécurité sectoriels.

Si le développement est réalisé par un tiers, le même respect des normes de développement sécurisé en vigueur est exigé.

Des points de contrôle doivent s'assurer du respect de ces règles à chaque jalon du projet.

3.2.1.3 Maintien des compétences des intervenants

L'entité responsable du projet doit s'assurer que les ressources justifient d'un niveau de connaissance en sécurité conforme aux enjeux et aux risques relatifs au projet :

- Les développeurs sont formés aux techniques de programmation sécurisée pour les nouveaux développements ;
- L'entité est en mesure de renforcer les capacités des développeurs à éviter, découvrir et corriger les vulnérabilités ;
- L'entité capitalise pour partager, mutualiser et enrichir les standards de codage sécurisé.

3.2.2 Contrôle des changements apportés au système

Les changements apportés au système dans le cycle de développement sont vérifiés conformément aux procédures de contrôle des changements en vigueur au sein de l'entité.

3.2.2.1 Documentation et traçabilité des changements

Des procédures formelles sont mises en place et obligatoirement appliquées lors de l'introduction de nouveaux systèmes ou de changements importants aux systèmes existants.

Elles couvrent les thèmes suivants :

- Une appréciation du risque, une analyse d'impacts du changement et des spécifications de sécurité ;

- Les documents de référence de spécifications, de phase de tests, de contrôle qualité et de mise en production et ces documents prévoient que :
  - la phase de test soit réalisée dans un environnement isolé des environnements de production et de développement,
  - cet environnement intègre des correctifs ou des mises à jour des systèmes d'exploitation des applications et des produits.
- Que les développeurs n'ont accès qu'aux parties du système nécessaires pour leur permettre d'effectuer leur travail ;
- Tout changement fait l'objet d'un accord formel.

Les mises à jour automatiques doivent faire l'objet d'une analyse d'impact quant à l'intégrité et la disponibilité du système (pas de mises à jour automatisées sur des systèmes critiques, qui seraient susceptibles de les faire échouer). Ces dispositions intègrent les correctifs logiciels, les « services pack » et autres mises à jour.

Les procédures doivent être documentées, validées et obligatoirement utilisées en application de la directive « 08. Sécurité liée à l'Exploitation ».

3.2.2.2 Contrôle des changements

Une procédure formelle de contrôle des changements est mise en œuvre et imposée, dès les étapes de conception et tout au long des opérations de maintenance qui s'ensuivent :

- Tenir à jour un :
  - un enregistrement des niveaux d'autorisation accordés,
  - un contrôle de version pour toutes les mises à jour logicielles,
  - un outil de traçabilité de toutes les demandes de changement.
- Identifier et vérifier :
  - tout logiciel, information, élément de base de données et matériel nécessitant un changement,
  - le code de sécurité critique pour réduire au minimum la probabilité des risques liés aux failles de sécurité connues.
- S'assurer que :
  - un accord formel est obtenu pour les propositions détaillées avant le lancement des travaux,
  - les propositions de changements émanent d'utilisateurs autorisés,
  - les utilisateurs autorisés acceptent les changements avant leur mise en œuvre,

- les commandes et les procédures d'intégrité ne seront pas compromises par les changements,
- la documentation système (document d'architecture technique, spécifications fonctionnelles et techniques, etc.) soit mise à jour après chaque changement, et que l'ancienne documentation soit archivée ou éliminée conformément aux règles d'élimination des archives et dans le respect des règles de confidentialité,
- les procédures exploitation soient mises à jour en fonction des changements,
- la mise en œuvre des changements soit programmée de manière à ne pas perturber les activités de l'organisation.

3.2.3 Revue technique des applications après changement apporté à la plateforme d'exploitation

Les applications critiques Métiers sont revues et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité dès lors que des changements sont apportés à l'ensemble la pile logicielle (systèmes d'exploitation, bases de données, middlewares, frameworks techniques et applications hébergées sur la plateforme).

3.2.3.1 Revue technique des changements

Une procédure décrit les étapes de cette revue pour vérifier que les changements qui ont été mis en production respectent les prérequis suivants :

- La vérification du fonctionnement et de l'intégrité des applications hébergées sur la plateforme ;
- La notification des changements en temps opportun, afin que les parties prenantes réalisent les tests et revues appropriés avant leur mise en œuvre ;
- La mise à jour des Plans de Continuité de l'Activité conformément à la directive « 14. Plan de Continuité d'Activité ».

3.2.4 Restrictions relatives aux changements apportés aux progiciels

La modification des progiciels est limitée au strict minimum et contrôlée.

3.2.4.1 Modifications des progiciels

Les guides méthodologiques de réalisation doivent indiquer que les changements apportés à des progiciels (fournis par des éditeurs) font l'objet de restrictions :

- La politique de gestion des mises à jour doit être appliquée (cf. directive « 08. Sécurité liée à l'Exploitation ») afin que les progiciels bénéficient des versions et des correctifs les plus récents ;
- Les changements doivent être documentés et testés avec soin (par un organisme indépendant si nécessaire) afin de pouvoir les réappliquer aux versions ultérieures, le cas échéant ;
- Les modifications requises spécifiquement par l'entité responsable du projet doivent faire l'objet d'une procédure de dérogation. Cette dérogation est établie à partir :
  - du risque de compromettre les commandes intégrées et le processus de vérification de l'intégrité ; A ce titre, et conformément aux normes de réalisation de tels changements sont réalisés à partir d'une copie clairement identifiée du logiciel, la version originale de celui-ci étant sauvegardée en gestion de configuration,
  - de la possibilité d'obtenir les changements souhaités auprès de l'éditeur, sous la forme de mises à jour conformes à la prestation en vigueur,
  - du consentement de l'éditeur, si c'est nécessaire,
  - des conséquences en cas de refus, dont l'éventualité du transfert de responsabilité de la maintenance du logiciel suite à des changements,
  - de la compatibilité avec les autres logiciels en service.

3.2.5 Principes d'ingénierie de la sécurité des systèmes

Des principes d'ingénierie de la sécurité des systèmes sont documentés et tenus à jour pour tous les travaux de mise en œuvre de SI.

3.2.5.1 Ingénierie de sécurité pour les Systèmes d'Information

Les guides méthodologiques de développement appliquent des techniques d'ingénierie de sécurité pour les Systèmes d'Information (infrastructures, applications, bases de données, interfaces etc.), qui offrent des recommandations notamment sur les techniques d'authentification de l'utilisateur, les contrôles de session et la validation des données, la suppression de code malveillant, etc.

A cette fin, une procédure de référence est mise en place pour établir, appliquer et contrôler des principes d'ingénierie de la sécurité. Ces principes doivent notamment prévoir :

- De concevoir la sécurité à tous les niveaux de l'architecture (activité, données, applications et technologie) en préservant l'équilibre entre le niveau de sécurité et l'accessibilité à l'information ;
- De s'assurer de l'amélioration des guides méthodologiques, normes et standards en vigueur ;
- D'assurer une veille permanente pour :
  - analyser les avancées réalisées dans les technologies et les solutions appliquées au regard des risques,
  - revoir l'exposition des SI existants par rapport aux évolutions des modèles d'attaques,
  - combattre toute nouvelle menace potentielle.
- D'en assurer la propagation aux SI externalisés (cf. directive « 12. Relation avec les fournisseurs ») :
  - appliquer par le biais de contrats ou d'accords exécutoires,
  - à défaut, confronter le niveau de sécurité fourni par les principes du prestataire avec ses propres principes.
- Ces guides sont régulièrement revus pour assurer un niveau de maturité satisfaisant.

3.2.6 Environnement de développement sécurisé

Un environnement de développement sécurisé pour les tâches de développement et d'intégration du système est mis en place. Celui-ci couvre et sécurise l'intégralité du cycle de développement du système.

3.2.6.1 Couverture du risque dans l'environnement de développement

Un processus doit garantir le niveau de protection et la couverture des risques liés aux tâches individuelles spécifiques au sein de l'environnement de développement.

Ce processus prend notamment en compte :

- La sensibilité des données à traiter, stocker et transférer par le système ;
- Les exigences internes et externes applicables ;
- Les standards de sécurité en vigueur pour les tâches de développement ;

- Le niveau de fiabilité du personnel travaillant dans l'environnement (par exemple en demandant l'extrait de casier judiciaire N° 3) ;
- Le degré d'externalisation associé à la tâche de développement du système ;
- La nécessité d'opérer un cloisonnement entre différents environnements de développement ;
- Le contrôle de l'accès à l'environnement de développement ;
- La surveillance des changements apportés à l'environnement et au code qu'il renferme ;
- Le stockage des sauvegardes à des emplacements sécurisés hors site ;
- Le contrôle des déplacements de données à partir de l'environnement et vers l'environnement.

3.2.7 Développement externalisé

L'activité de développement d'un système externalisé doit être supervisée et contrôlée.

3.2.7.1 Supervision du développement externalisé

En cas de contractualisation de prestations externes, le processus des achats et le déroulement opérationnel doivent documenter le contrôle des éléments suivants :

- Accords de licence, propriété du code et droits de propriété intellectuelle relatifs au contenu externalisé ;
- Exigences contractuelles relatives à la conception sécurisée, au codage et aux pratiques de tests ;
- Enrôlement du développeur prestataire :
  - formation sur le développement sécurisé et sur les vulnérabilités classiques,
  - fourniture du modèle des menaces approuvé,
  - utilisation d'outils permettant de minimiser les erreurs introduites durant le développement,
  - production de documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement, etc.),
  - respect de normes de développement sécurisé, qu'elles soient propres au développeur, publiques ou propres au commanditaire,
  - obligation pour le prestataire de corriger, les vulnérabilités introduites durant le développement et qui lui sont remontées,

en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation,
    - l'accès aux ressources SI internes du Groupe La Poste ou des filiales doit être réalisé via les solutions de raccordement sécurisées du Groupe,
    - désignation d'un correspondant sécurité qui sera contacté en cas d'alerte sécurité.
- Test de conformité de la qualité et de la précision des livrables ;
- Preuves montrant que les seuils de sécurité ont été utilisés pour établir les niveaux minimums acceptables en matière de sécurité apportée aux SI et de la confidentialité des données personnelles ;
- Preuves montrant qu'il a été procédé à suffisamment de tests pour garantir l'absence de contenus volontairement ou involontairement malveillants à la livraison ;
- Preuves montrant qu'il a été procédé à suffisamment de tests pour garantir l'absence de vulnérabilités connues ;
- Accords de séquestre, par exemple si le code source n'est plus disponible ;
- Droit contractuel de procéder à un audit des processus et des contrôles de développement ;
- Documentation efficace sur l'environnement servant à créer les livrables ;
- Conformité aux lois en vigueur et de la vérification de l'efficacité des mesures, dont l'entité en charge du projet reste responsable.

Ces mesures doivent s'appliquer en complément des mesures prévues dans la directive « 12. Relation avec les fournisseurs ».

3.2.8 Phase de test de la sécurité du système

Durant le développement, des tests de fonctionnalité de la sécurité sont réalisés.

3.2.8.1 Test de sécurité

Lors d'une acquisition, d'un développement ou d'une évolution d'un système matériel ou logiciel, les produits nécessitent d'être soumis à des tests.

Pour ce faire, un corpus documentaire de tests doit décrire les moyens requis et les démarches envisagées (stratégie de tests), ainsi que le détail des tâches, des données de test d'entrée, et les résultats attendus en sortie sous un certain nombre de conditions (plan de tests).

En complément, les tests des développements in situ sont réalisés dès le début par l'équipe de développement (tests unitaires).

Ensuite, les bonnes pratiques de gestion de projet (aussi bien pour les développements in situ et externalisés) prévoient une phase d'intégration, à savoir des tests de conformité indépendants (par exemple, par les propriétaires Métiers ou leur MOA) pour garantir que le système fonctionne comme prévu et uniquement comme prévu.

3.2.9 Test de conformité du système

Des tests de conformité et les critères associés sont systématiquement déterminés pour les nouveaux SI, les mises à jour et les nouvelles versions.

3.2.9.1 Test de conformité

Pour assurer la conformité des systèmes à l'issue du projet, les documentations des tests doivent couvrir :

- Les exigences liées à la sécurité de l'information ;
- Le respect des pratiques de développement sécurisé des systèmes ;
- Les systèmes intégrés et les composants reçus ;
- Les mesures de sécurité complémentaires et les actions correctives apportées aux manquements de sécurité.

La phase d'intégration doit se dérouler dans un environnement s'apparentant au maximum à l'environnement de production pour garantir que le système n'introduira pas de vulnérabilités en fonctionnement nominal.

La stratégie de tests peut prévoir que les tests s'appuient sur des outils automatiques (par exemple : analyseurs de code, scanneurs de vulnérabilités, etc.) sous réserve qu'ils aient été préalablement validés.

3.3 Données de test

Objectif : garantir la protection des données utilisées pour les tests.

3.3.1 Protection des données de test

Les données de test sont sélectionnées, protégées et contrôlées.

3.3.1.1 Données de test

Dans le cadre des campagnes de tests, les données contenant des données personnelles, confidentielles ou sensibles, ne doivent pas être utilisées. Elles ne doivent pas non plus correspondre à des données d'exploitation, ni être réelles.

Les données nécessaires aux tests doivent être épurées ou anonymisées de tous les détails et contenus sensibles. D'une façon générale, une procédure concernant les données d'exploitation doit être rédigée et appliquée pour réaliser des tests. Elle doit tenir compte des mesures de protection suivantes :

- Mise en œuvre des procédures de contrôle d'accès à l'identique des systèmes en production ;
- Obtention d'une nouvelle autorisation chaque fois qu'une information d'exploitation est copiée dans un environnement de test ;
- En cas d'utilisation de données personnelles : obligation d'anonymisation ou pseudonymisation des données préalablement au test ou utilisation de jeux fictifs ;
- Suppression des données de l'environnement de test immédiatement après la fin des tests ;
- Journalisation de toute reproduction et utilisation de l'information d'exploitation, afin de créer un système de traçabilité.