

PROJETS DES SYSTEMES D'INFORMATION (PROJETS SI)

RÈGLES DE SÉCURITÉ

Référence	SSI-REG-PRJ_Projets des Systèmes d'Information_V1.2
Clef GED	72639
Version	V1.2
Classification	Interne
Date	01/07/2020
État	Final
Auteur(s)	Filière Sécurité des SI
Approbateur(s)	Sylvain Lambert
Validation	Direction de la Maîtrise des Risques

Identification du document		
Référence	Titre du document	
SSI-REG-PRJ_Projets des Systèmes d'Information_V1.2	Projets des Systèmes d'Information (Projets SI)	
Version	État du document	Auteurs
1.2	Final	Filière Sécurité des SI

Classification	
Niveau	Diffusion
Interne	Le personnel de Pôle Emploi et à ses tiers formellement autorisés (ayant signé une convention, charte de sécurité, clause de confidentialité,...)

Mises à jour		
Version	Date	Nature de la modification
1.0	13/01/2009	Création du document
1.1	10/02/2017	Mises à jour dans le cadre de la refonte du référentiel initiée en 2016
1.2	01/07/2020	Mises à jour dans le cadre de la directive NIS (conformité OSE)
1.2	22/11/2021	Modification de « Projets informatiques » en « Projets des Systèmes d'Information »

Relectures et validations				
Version	Relu par	Direction	Date	Statut
1.0	RSSI Mylène Zerbib	DSI	13/01/2009	Validé
1.0	Robert Laupy	DGA-QMR	10/06/2009	Validé
1.1	RSSI Sylvain Lambert	DSI	10/02/2017	Validé
1.1	Robert Laupy	DGA-QMR	21/03/2017	Validé
1.2	RSSI Sylvain Lambert	DSI	01/07/2020	Validé

Documents de référence	
Référence	Titre du document
[1] Colibri 196557	Demande de dérogation
[2] Colibri 262087	Développement sécurisé
[3] Colibri 72649	Accès au SI de pôle emploi par des tiers
[4] Colibri 208129	Guide de développement sécurisé
[5] Colibri 72643	Classification et protection de l'information
[6] Colibri 72673	Intégration de la Sécurité dans les Projets – Méthode ISP

SOMMAIRE

1. PRÉAMBULE	5
1.1. Principes fondateurs de la Politique Générale de Sécurité des SI	5
1.2. Enjeux et objectifs du document.....	5
1.3. Champ d'application	6
2. RÔLES ET RESPONSABILITÉS.....	7
3. RÈGLES DE SÉCURITÉ.....	9
3.1. Rôle et engagement des acteurs.....	9
3.2. Choix des technologies et documentation.....	11
3.3. Développement.....	12
3.4. Gestion des projets SI.....	13
3.5. Environnement Technique.....	15
4. ANNEXES.....	17
4.1. Liste des règles.....	17
4.2. Glossaire	18

Règles typographiques

Les termes écrits en vert et soulignés sont définis dans le glossaire de ce document.

Les règles de la thématique « Projets des Systèmes d'Information (Projets SI) » sont préfixées par le sigle « **PRJ-** » et sont numérotées par ordre d'apparition. Elles sont définies dans un encart bleu clair comme figuré ci-dessous :

Définition de la règle

Pour certaines règles, des préconisations, recommandations, commentaires ou des évolutions prévisibles sont détaillés au-dessous de la règle.

Préconisations :

La maîtrise d'œuvre est orientée vers une solution pour couvrir la règle de sécurité.

Recommandations :

L'utilisateur est orienté vers un comportement, un usage, afin de respecter la règle de sécurité.

Commentaires :

Des précisions sont apportées afin d'éclairer la règle énoncée.

1. PRÉAMBULE

1.1. PRINCIPES FONDATEURS DE LA POLITIQUE GÉNÉRALE DE SÉCURITÉ DES SI

Les Systèmes d'Information hébergent de nombreuses données qui revêtent un caractère stratégique et qui constituent un patrimoine essentiel que Pôle Emploi a l'obligation de protéger efficacement.

Pour ce faire, la Direction adopte une Politique Générale de Sécurité des SI qui s'inscrit dans le cadre de la politique de gestion des risques ; cette politique protège les informations et leurs traitements ainsi que les ressources hébergées par les Systèmes d'Information de Pôle Emploi.

1.2. ENJEUX ET OBJECTIFS DU DOCUMENT

Les Projets SI sont exposés à des risques pouvant impacter de manière importante Pôle Emploi. Des incidents ou manquements vis-à-vis des référentiels de Pôle Emploi au niveau des Projets SI peuvent notamment :

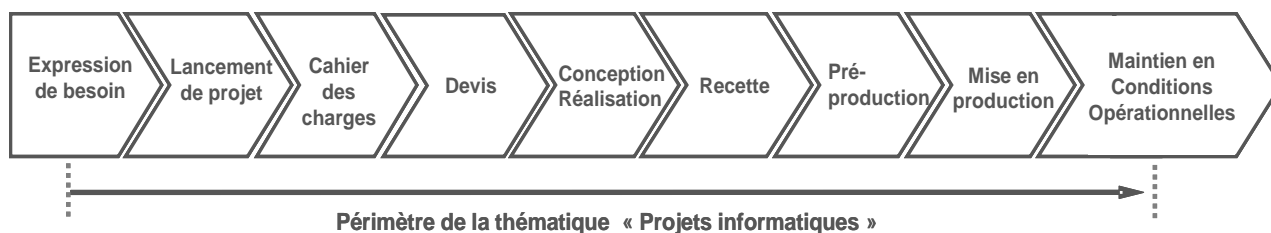
- Conduire à la perte, à la divulgation ou à la modification erronée d'informations pendant le déroulement du Projet,
- Conduire à mettre en production des Systèmes d'Information comportant des failles de sécurité, pouvant mettre en péril les informations manipulées ou apporter des failles aux autres composants des SI de Pôle Emploi,
- Entraîner un non-respect des obligations contractuelles et légales en vigueur.
- Ainsi, la prise en compte de la Sécurité des SI dans le déroulement des Projets SI est essentielle pour :
 - ▶ Protéger les informations sensibles propres au projet (cahier des charges, code source, spécifications détaillées, planning, etc.).
 - ▶ Garantir la sécurité du produit cible du projet (application, infrastructure) dès sa conception.
 - ▶ Maintenir dans le temps la sécurité des SI dans lesquels vient s'insérer le produit cible.

Dans la mesure où Pôle Emploi a fondé les évolutions de ses Systèmes d'Information sur le fonctionnement en **mode Projet**, la protection des Projets SI et de leurs informations est par conséquent primordiale.

Le présent document définit les règles de sécurité relatives aux Projets SI de Pôle Emploi.

1.3. CHAMP D'APPLICATION

Le document thématique couvre l'ensemble des Projets SI, sur le périmètre de la Direction des Systèmes d'Information. Il définit le cadre de **prise en compte de la sécurité SI** dans le déroulement de tout Projet SI¹, de la phase de cadrage jusqu'à la fin de vie du produit cible mis en œuvre :



Le document thématique adresse l'ensemble des acteurs des Projets, à savoir les Chefs de Projet MOA et MOE, leurs équipes et les prestataires intervenant contractuellement dans le cadre de Projets SI.

Les principes de ce document sont détaillés dans la **Méthode d'Intégration de la Sécurité dans les Projets (ISP)**.

En cas de non-applicabilité d'une des règles du présent document, une procédure de dérogation doit être engagée. Cette demande de dérogation [1] sera transmise au Responsable de la Sécurité des Systèmes d'Information (RSSI).

Les règles d'utilisation des données peuvent être dépendantes du niveau de leur classification en termes de confidentialité. La classification utilisée est celle définie dans la thématique « Classification et Protection de l'information » [5].

La règle CLA-10 précise les quatre niveaux de classification de confidentialité des documents :

- **Public** : pour tous les documents électroniques et papier de portée publique diffusable sans restriction,
- **Interne** : pour tous les documents électroniques et papier limités à un usage interne à Pôle emploi et à ses tiers formellement autorisés (ayant signé une convention, charte sécurité, clause de confidentialité, ...),
- **Restreint** : pour tous les documents électroniques et papier réservés à des communautés fermées de personnes,
- **Confidentiel** : pour tous les documents électroniques et papier réservés à des communautés fermées de personnes et réclamant des protections spécifiques dans leur communication et leur manipulation.

¹ La thématique « Support et Exploitation » vient compléter la présente thématique dans la mesure où elle couvre les projets d'étude et d'apport en expertise et en conseil.

2. RÔLES ET RESPONSABILITÉS

Le présent chapitre a pour but de définir les fonctions intervenant dans les processus de définition, d'application et de contrôle des règles de sécurité des Projets SI.

Ces fonctions regroupent des missions et des responsabilités qui correspondent à un ou plusieurs acteurs, directions, dans l'organisation de Pôle Emploi.

- **Le Métier, commanditaire du Projet** (Propriétaire d'informations)
 - ▶ Approuve la classification du produit cible du Projet et des informations propres à ce Projet proposée par la MOA.
 - ▶ Valide les habilitations et instruit les déclarations CNIL en relation avec le CIL (si nécessaire).
 - ▶ Exprime les besoins de sécurité sur les biens essentiels associés au produit cible du projet.
 - ▶ Participe et valide à la retranscription des besoins de sécurité en événements redoutés à couvrir.
- **Le Chef de Projet Maîtrise d'ouvrage (MOA)**
 - ▶ Identifie, classe et protège les informations propres du Projet.
 - ▶ Conduit la classification du produit cible du projet, et pilote la définition et la mise en œuvre des mesures de protection appropriées.
 - ▶ Exprime les exigences de sécurité du produit cible du Projet.
 - ▶ Réalise les déclarations CNIL en relation avec le CIL (si nécessaire).
- **Le Chef de Projet Maîtrise d'œuvre (MOE)**
 - ▶ Prend en charge la sécurité du Projet tout au long de sa durée de vie.
 - ▶ Garantit la qualité et la sécurité du Projet conformément aux besoins de sécurité et aux exigences exprimées par la Maîtrise d'Ouvrage. En particulier, décline les exigences de sécurité de la Maîtrise d'Ouvrage en mesures techniques permettant d'assurer un niveau de protection conforme à la classification du produit cible, et de maîtriser les risques identifiés.
- **Les membres du Projet SI**
 - ▶ Respectent les règles de sécurité relatives au Projet et aux SI auxquels ils sont habilités.
- **Le Responsable Sécurité des Informations dans le processus de Fabrication et d'amélioration des produits (RSI-Fab)**
 - ▶ Suit les projets en lien avec le Département Sécurité,
 - ▶ S'approprie et diffuse au sein des directions les guides méthodologiques d'analyse des risques et d'intégration de la sécurité dans les projets SI,
 - ▶ Aide les métiers à l'expression des besoins de sécurité afférents à leurs projets SI,
 - ▶ Accompagne les MOA fonctionnelles lors de la qualification des niveaux de services de sécurité permettant de satisfaire ces besoins,
 - ▶ S'assure de l'instruction des livrables sécurités et vérifie la complétude des tests effectués dans le cadre des recettes au regard des risques et besoins exprimés,
 - ▶ Si le projet doit se conformer au Règlement Général sur la Protection des Données (RGPD), vérifie que le processus à engager l'est bien,
 - ▶ Si le projet doit se conformer au Référentiel Général de Sécurité, vérifie que le processus à engager l'est bien.

- Le Département **Sécurité des SI**
 - ▶ Dispose des prérogatives nécessaires pour contrôler l'application des dispositifs de sécurité en cohérence avec la classification du Projet.
 - ▶ Cadre et coordonne les actions de sensibilisation relatives à l'application des règles du présent document, pour toutes les étapes d'un Projet et pour toutes les populations concernées.
 - ▶ Assiste les différents acteurs du projet et le RSI-Fab pour intégrer la sécurité dans les projets SI.
- Le Département **Architecture**
 - ▶ Identifie les solutions permettant de couvrir les besoins de sécurité exprimés.
 - ▶ Consolide le référentiel de solutions standard, des solutions ayant adressées les nouveaux besoins de sécurité.

Dans le cadre de la méthodologie de gestion de projets AGILE, de nouvelles équipes aux rôles suivants peuvent être définies, notamment avec la méthode SCRUM :

- Une équipe projet de **Product Owner**
 - ▶ Rédige un cahier des charges de fonctionnalités
 - ▶ Priorise les fonctionnalités
 - ▶ Réalise la backlog de produit « au fil de l'eau »
 - ▶ Contrôle la réalisation des [User Stories](#) (besoins et idées des parties prenantes)
- Les **équipes de développement** en Scrum
 - ▶ Estiment la complexité de réalisation des User stories
 - ▶ Définissent un plan de fabrication de niveau tâche de réalisation
 - ▶ Développent le produit
- Une **équipe de test**
 - ▶ Contrôle le produit livré à chaque itération
 - ▶ Remonte des anomalies et participe à l'identification de nouvelles User stories
 - ▶ Apporte son expertise du(es) métier(s)

3. RÈGLES DE SÉCURITÉ

3.1. ROLE ET ENGAGEMENT DES ACTEURS

PRJ-01 Responsabilité des acteurs des projets SI

Il est de la responsabilité de chaque participant à un projet SI de concourir à la mise en œuvre d'un système sécurisé, répondant aux objectifs du projet et cohérent avec le cadre de référence SSI.

Tous les acteurs intervenant dans les projets SI doivent être **sensibilisés** aux problématiques de Sécurité des SI.

Recommandations :

Les Chefs de Projet MOA et MOE ou toutes personnes en responsabilité des livrables du produit informeront leurs équipes notamment sur la **confidentialité** des informations du Projet. Ils veilleront à ce que leurs équipes respectent les bonnes pratiques liées à la **confidentialité** telles que la protection des documents, le principe du « bureau net » (aucun papier **sensible** ne doit rester sur le bureau), la discrétion dans leurs communications...

PRJ-02 Conformité légale et réglementaire

Sur chacun de ses projets, la Maîtrise d'Ouvrage et la Maitrise d'Œuvre, en relation avec la Direction Juridique, s'assure que le produit cible est **conforme à toute législation, obligation contractuelle ou réglementation** applicables à l'utilisation des technologies de l'information.

Commentaires :

Par exemple : Loi Informatique et Libertés, Loi pour la confiance dans l'économie numérique, Loi sur la Sécurité Financière, exigences comptables, etc.

PRJ-03 Prise en compte de la sécurité dans les contrats avec les Tiers

Les Chefs de Projet MOA et MOE veillent à ce que les **clauses sécurité** soient intégrées aux contrats de prestation qu'ils souscriraient avec des Tiers dans le cadre de projets SI.

Recommandations :

Les clauses sécurité spécifient les mesures SSI que le prestataire doit respecter dans le cadre de ses activités.

Avant toute mise en production d'une composante des SI dont le développement a été effectué par un **tiers**, il est nécessaire que le prestataire vérifie l'adéquation entre le résultat et les spécifications, au niveau de la sécurité. Une analyse de la composante par le personnel interne est recommandée.

Les acteurs des Projets peuvent se référer aux documents suivants :

- La thématique « Développement Sécurisé » [2].
- La thématique « Accès au SI de pôle emploi par des tiers » [3].

PRJ-04 Convention de service

Une **convention de service** doit être établie entre les entités utilisatrices et les exploitants afin de spécifier les engagements relatifs à la sécurité des SI.

Commentaires :

Le but des conventions de service est notamment de préciser :

- Les performances attendues,
- Les exigences de **disponibilité**, **intégrité**, **confidentialité**, **preuve** (délais de reprise sur incidents, modes dégradés éventuels, fréquence et exigences pour les sauvegardes et restaurations, modalités de journalisation et de contrôle ...).

Les acteurs des Projets peuvent se référer à la convention de service.

3.2. CHOIX DES TECHNOLOGIES ET DOCUMENTATION

PRJ-05 Élaboration d'un référentiel d'Architecture

Un **référentiel d'Architecture** doit être constitué par la Maîtrise d'Ouvrage Architecture : il doit comprendre à la fois des architectures techniques et des solutions matérielles et logicielles qui composent ces architectures.

Recommandations :

Ce référentiel est systématiquement soumis aux projets. Tout recours par un projet à une solution non référencée doit être justifié et transmis pour avis à la Maîtrise d'Ouvrage Architecture.

PRJ-06 Critères de sélection des éléments du référentiel d'Architecture

Les éléments constituant le référentiel d'Architecture doivent être choisis en **prenant en compte les aspects relatifs à la sécurité SI**, et notamment la couverture des risques relatifs à la perte des critères de sécurité qui sont : **Disponibilité, Intégrité et Confidentialité**.

Recommandations :

Les éléments retenus doivent, au-delà des aspects fonctionnels, satisfaire directement ou indirectement (en s'interfaçant avec d'autres composants) à tout niveau d'exigence de sécurité (selon les 3 facteurs **Disponibilité, Intégrité, et Confidentialité**) potentiellement réclamé par les Métiers. Les nouveaux éléments (ou nouvelles versions) sont testés d'un point de vue sécurité avant d'être intégrés au référentiel. En cas d'écart, le Département Sécurité doit être sollicité pour avis.

Dans le cadre de la démarche projet, le référentiel d'Architecture est notamment utilisé par les équipes de Maîtrise d'œuvre, afin de répondre aux exigences de sécurité et aux risques exprimés par la Maîtrise d'Ouvrage.

PRJ-07 Documentation issue du projet

Tout projet ou évolution de projet doit faire l'objet d'une **documentation** (spécifications, dossier d'exploitation, dossier de maintenance, manuel utilisateur, etc.)

Cette documentation doit être tenue à jour et conservée dans des conditions conformes aux exigences de la Politique de Sécurité des Systèmes d'Information.

3.3. DEVELOPPEMENT

PRJ-08 Respect des standards de développement sécurisé

Le Chef de Projet MOE est garant du respect des **standards de développement sécurisé** et à ce titre, **doit s'appuyer sur la thématique « Développement sécurisé » [2]**.

Recommandations :

Le guide de développement sécurisé [4] recense l'ensemble des bonnes pratiques en matière de développement, en particulier :

- Un contrôle des accès via les référentiels en vigueur,
- S'il est inévitable, un stockage des mots de passe dans des fichiers séparés des données applicatives et du code de l'application,
- Un traitement sécurisé des informations au sein des applications (contrôle des données en entrée et en sortie des applications, contrôle de l'intégrité des données et détection d'erreurs...),
- Absence des failles les plus connues et exploitées des applications web (Injections, XSS, etc).

En outre, afin de faciliter les procédures de mise en production et de maintenance, il est demandé de ne pas coder « en dur » des informations non pérennes (noms de machines, adresses IP, identifiants, configuration, etc.).

3.4. GESTION DES PROJETS SI

PRJ-09 Prise en compte de la sécurité dans tout le cycle de vie des projets

Les aspects liés à la Sécurité des SI doivent être pris en compte durant tout **le cycle de vie de chaque projet SI**, de l'expression des besoins jusqu'à la fin de vie du produit cible mis en œuvre.

La prise en compte de la Sécurité des SI dans les Projets SI doit être réalisée dans le respect de la **Méthode d'Intégration de la Sécurité dans les Projets (ISP)** [6], conduisant à la rédaction d'une analyse de risque.

PRJ-010 Analyse de risque d'un SIE

Les **SIE** doivent faire l'objet d'une analyse de risque dès leur identification et avant la mise en production.

Cette analyse de risque doit être revue lors de l'homologation du SIE et à chaque renouvellement de cette homologation, qui doit avoir lieu au moins tous les 3 ans.

De plus, l'analyse de risque doit être revue à chaque événement modifiant le contexte décrit dans le dossier d'homologation et à chaque changement impactant le SIE.

PRJ-011 Gestion des modifications et évolutions des composantes SI

Toute **modification significative ou évolution d'une composante des SI** en production doit être considérée comme un projet à part entière et, à ce titre, doit être soumise aux mêmes contrôles et à la même rigueur que le projet initial.

PRJ-012 Classification et protection du projet et de ses informations propres

Les Chefs de Projet MOA et MOE doivent identifier, au plus tôt du Projet, les informations, les traitements et les rôles **sensibles** de leur Projet.

Cette classification doit se faire en regard de la classification du produit cible du Projet et en conformité avec la thématique « Classification et Protection de l'information ».

Les Chefs de Projet MOA et MOE sont garants de la sécurité des **informations propres au Projet**, en adéquation avec leur niveau de classification.

Ils émettent donc à ce titre des exigences en termes de sécurité des informations propres au Projet et du produit-cible du Projet.

PRJ-013 Réalisation d'audits de sécurité sur les projets sensibles

Tout projet peut faire l'objet d'un **contrôle de Sécurité SI**.

Préconisations :

Le contrôle de sécurité SI peut être réalisé à différents stades d'avancement du projet :

- Avant la mise en production, afin notamment de valider le respect des exigences de sécurité et la couverture des risques identifiés.
- Sur l'infrastructure en production, afin de valider le maintien dans le temps du niveau de sécurité du produit cible du projet.

PRJ-014 Gestion des fins de projets

À l'issue de chaque Projet SI, le code source et les données de configuration doivent être archivés.

Recommandations :

La fin d'un projet est considérée à partir du moment où la solution est déployée en environnement de production et que les équipes opérationnelles en assurent l'exploitabilité.

3.5. ENVIRONNEMENT TECHNIQUE

PRJ-015 Principe de séparation et de sécurisation des environnements

Les environnements de développement, de qualification/recette et de production doivent être **isolés** les uns des autres.

Préconisations :

Cette séparation se décline de manière logique et/ou physique entre les différents environnements (matériels et logiciels distincts, jeux de données distinctes...). Elle se manifeste également par la désignation de responsabilités distinctes pour chaque environnement.

La sécurisation des environnements peut se faire à différents niveaux, notamment en termes :

- De cloisonnement physique et logique ;
- D'habilitations attribuées en cohérence avec ces séparations et en conformité avec la thématique « Contrôle des Accès Logiques ». Les Chefs de Projet s'assurent que les équipes de développement ont accès de manière contrôlée à chaque environnement ;
- D'anonymisation ou d'offuscation des données à caractères personnelles pour les environnements autre que la production ;
- De protection antivirus à jour ;
- De licences pour chacun des environnements, etc.

PRJ-016 Gestion des données en environnement de fabrication

Une prise d'empreinte doit être effectuée de manière régulière pour les environnements de non-production.

Commentaires :

Une prise d'empreinte est un processus qui consiste à récupérer des données de production pour les copier dans un environnement de fabrication.

PRJ-017 Utilisation de données de production pour les tests

L'utilisation des données de production pour tester, qualifier et recetter une application ou une infrastructure ne peut pas être effectuée sans l'accord des Propriétaires d'Informations concernés par ces données.

Les données de production ne peuvent être copiées que si elles sont classifiées de niveau « Public » ou « Interne » en termes de confidentialité.

Dans le cas où elles sont classifiées de niveau « Restreint » ou « Confidentiel », elles doivent être banalisées ou anonymisées, notamment pour tout ce qui concerne les données à « caractère personnel ».

Commentaires :

Par défaut, la Maîtrise d'Ouvrage du Projet est considérée comme étant le Propriétaire d'Informations sur le périmètre des informations et des traitements couverts par le produit cible du projet.

PRJ-018 Conditions de mise en production d'une solution

Une procédure stricte doit garantir que **seules les solutions autorisées par l'Instance décisionnaire sont effectivement mises en production.**

Commentaires :

Le terme « Instance décisionnaire » désigne une instance « GO/NO GO » en charge de se prononcer sur la mise en production effective de la solution. La prise de décision peut être basée sur des critères supplémentaires à d'autres référentiels, exemples :

- La solution répond aux exigences définies dans la méthodologie ISP.
- La solution répond aux critères de qualité et de sécurité du code source suite à un scan automatisé.

Recommandations :

Le Chef de Projet MOE s'assure, avant toute mise en production d'une solution, que :

- Les procédures d'exploitation de la solution sont documentées, testées et validées.
- Les données de sécurité, notamment les couples identifiants/authentifiants, utilisées lors des phases de développement, qualification ou recette sont modifiées, au moyen de procédures documentées.
- Les intervenants ont bénéficié des formations relatives à l'exploitation de la solution et qu'ils disposent des compétences nécessaires et suffisantes à son exploitation. Dans le cas contraire, la mise en production est conditionnée par une formation adéquate ou la définition d'un plan d'action formel par le Chef de Projet MOA.
- Une procédure de « retour-arrière » est définie pour couvrir l'éventualité d'un mauvais fonctionnement affectant tout ou partie des SI.

Pour toutes les informations classifiées « confidentielles », les Chefs de Projet MOA et MOE s'assurent de l'effacement ou de la destruction de tous les supports qui en auraient assuré le stockage et qui ne seraient plus nécessaires lors de la phase de maintien en conditions opérationnelles.

4. ANNEXES

4.1. LISTE DES REGLES

PRJ-01	Responsabilité des acteurs des projets SI	9
PRJ-02	Conformité légale et réglementaire	9
PRJ-03	Prise en compte de la sécurité dans les contrats avec les Tiers	9
PRJ-04	Convention de service	10
PRJ-05	Élaboration d'un référentiel d'Architecture	11
PRJ-06	Critères de sélection des éléments du référentiel d'Architecture	11
PRJ-07	Documentation issue du projet	11
PRJ-08	Respect des standards de développement sécurisé.....	12
PRJ-09	Prise en compte de la sécurité dans tout le cycle de vie des projets	13
PRJ-010	Analyse de risque d'un SIE	13
PRJ-011	Gestion des modifications et évolutions des composantes SI	13
PRJ-012	Classification et protection du projet et de ses informations propres.....	13
PRJ-013	Réalisation d'audits de sécurité sur les projets sensibles	14
PRJ-014	Gestion des fins de projets	14
PRJ-015	Principe de séparation et de sécurisation des environnements	15
PRJ-016	Gestion des données en environnement de fabrication	15
PRJ-017	Utilisation de données de production pour les tests.....	15
PRJ-018	Conditions de mise en production d'une solution.....	16

4.2. GLOSSAIRE

Confidentialité

La confidentialité est la propriété qui garantit que les informations ne sont accessibles que par des personnes dûment habilitées et que les informations ne peuvent pas être divulguées en dehors des règles établies.

Cette garantie peut être mise en cause par des indiscretions, volontaires ou involontaires, quel que soit le support utilisé (réseau, support physique, etc.).

Disponibilité

La disponibilité est l'aptitude d'un système d'Information à pouvoir être employé par les utilisateurs (individus, entités, processus...) habilités dans des conditions d'accès et d'usage normalement prévues (conditions d'horaires, de délai, de performances...).

Données à « caractère personnel »

Au sens de la loi Informatique & Libertés (n°78-17 du 6 janvier 1978 complétée par la loi du 6 août 2004), une donnée à caractère personnel est une information relative à une personne physique identifiée ou identifiable, directement ou indirectement. Il s'agit de tout :

- Élément d'identification directe (ex : prénom, nom patronymique, numéro de sécurité sociale...)
- Élément propre à la personne et/ou permettant indirectement son identification (ex : photo, numéro de téléphone, adresse IP délivrée par un FAI...)

Le traitement de données à caractère personnel est régi et cadré par la loi Informatique et Libertés, qui soumet le responsable du traitement à des obligations vis-à-vis de la CNIL et des personnes intéressées par le traitement.

Intégrité

L'intégrité est la propriété qui assure qu'une Information n'est modifiée que par les utilisateurs habilités dans des conditions d'accès normalement prévues. L'intégrité doit garantir l'exhaustivité, l'exactitude et la fiabilité de l'Information.

L'intégrité peut être remise en cause par toute altération ou modification non légitime.

Preuve

La preuve correspond aux éléments permettant de prouver l'origine des traitements ou autres événements relatifs à un composant des Systèmes d'Information et d'en reconstituer le déroulement. Il s'agit de pouvoir garantir que l'émission, la modification, la réception d'une information ne soit pas réfutée ou que toutes les actions réalisées sur un composant des Systèmes d'Information puissent être contrôlées et auditées.

La preuve recouvre trois notions complémentaires :

- la traçabilité : obtenir des traces décrivant la manipulation,
- l'imputabilité : pouvoir attribuer une action,
- la non-répudiation : impossibilité de nier une action.

Sensible

La classification des informations repose sur la notion suivante : le propriétaire d'informations classe ses informations et définit leur niveau de sensibilité (non sensible, Sensible, Critique, Stratégique) duquel est déduit le niveau de protection et de service à mettre en œuvre.

SIE

Un SIE (Système d'information essentielle) est un système d'information, qui fournit un service **essentiel** dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

Tiers

Le terme « Tiers » désigne l'ensemble des stagiaires, des prestataires, des fournisseurs, des partenaires et des travailleurs intérimaires employés à titre individuel par Pôle Emploi ; ces personnels sont amenés à travailler, de manière permanente ou occasionnelle, sur les Systèmes d'Information de Pôle Emploi et, de ce fait, à avoir accès à des informations ou à des ressources de Pôle Emploi.

User stories

C'est une phrase simple dans le langage de tous les jours permettant de décrire avec suffisamment de précision le contenu d'une fonctionnalité à développer. La phrase contient généralement trois éléments descriptifs de la fonctionnalité : *Qui ? Quoi ? Pourquoi ?*.

(Fin de document)