Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité
des systèmes d'information

# Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (*cloud computing*) - référentiel d'exigences

Version 1.3 du 30/07/2014

| HISTORIQUE DES VERSIONS | | | |
|---|---|---|---|
| DATE | VERSION | EVOLUTION DU DOCUMENT | REDACTEUR |
| XX/XX/XXXX | X.X | Version publiée pour commentaires. | ANSSI |
| XX/XX/XXXX | X.X | Première version applicable.<br>Modifications principales :<br>• Modification 1<br>• Modification 2 | ANSSI |

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg

75700 Paris 07 SP

qualification@ssi.gouv.fr

SOMMAIRE

# 1. Introduction

## 1.1. Présentation générale

### 1.1.1. Contexte

Le *Référentiel Général de Sécurité* (RGS) définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Il propose également des bonnes pratiques en matière de sécurité des systèmes d'information que les autorités administratives sont libres d'appliquer.

Dans ses évolutions, le RGS permet la qualification de nouveaux types de prestataires, tels que les prestataires d'audit par exemple.

Au titre de la qualification de nouveaux types de prestataires, le présent référentiel couvre l'offre de services sécurisés de *cloud computing*, et vise la qualification au sens RGS de prestataires proposant une offre de services en nuage.

L'approche consistant à contractualiser spécifiquement la sécurité dans chaque projet d'hébergement externalisé a montré ses limites: les offres sont le plus souvent packagées, de sorte qu'une négociation a posteriori par chaque client est peu envisageable ; de plus, il est également illusoire d'inciter chaque client à procéder à des audits réguliers des services offerts.

Une approche centralisée, définissant un référentiel favorisant l'émergence d'offres qualifiées, a ainsi été retenue : on estime qu'elle permet de traiter la problématique sécurité de manière globale et efficace, les offreurs disposant d'un cadre stable dans lequel s'inscrire pour aller vers la qualification et les usagers pouvant baser leur confiance sur cette qualification.

### 1.1.2. Objet du document

Le présent document liste les exigences et recommandations que les prestataires qualifiés proposant une offre sécurisée de service d'informatique en nuage doivent respecter.

Ce référentiel a vocation à permettre la qualification des prestataires proposant une offre de services d'informatique en nuage, ci-après dénommés «prestataires», selon les modalités décrites au chapitre 3.

Il permet au client de disposer de garanties sur la compétence du prestataire, sur la qualité des services qu'il fournit, et sur la confiance qu'il peut lui accorder avant de lui confier des données.

Il peut être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire, pour la mise en nuage des données de tous les types d'entités.

Les prestataires doivent respecter les règles générales qui leur sont imposées en leur qualité de professionnel, notamment celles concernant leur devoir de conseil vis-à-vis de leurs clients, ainsi que la législation nationale.

### 1.1.3. Structure du document

Le chapitre 2 décrit les activités concernées par le présent référentiel.

Le chapitre 3 présente les modalités de la qualification, qui atteste de la conformité des prestataires d'offre de service en nuage aux exigences qui leur sont applicables.

Le chapitre 4 présente les échelles des besoins de sécurité.

Les chapitres 5 à 18 présentent en quatorze domaines les exigences applicables.

## 1.2. Identification du document

Le présent référentiel est dénommé « Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (*cloud computing*) - référentiel d'exigences». Il peut être identifié par son nom, numéro de version et sa date de mise à jour.

## 1.3. Définitions et acronymes

### 1.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont les :

| | |
|---|---|
| **ANSSI** | Agence nationale de la sécurité des systèmes d'information |
| **RGS** | Référentiel général de sécurité |
| **EBIOS** | Expression des besoins et identification des objectifs de sécurité |
| **CNIL** | Commission nationale de l'informatique et des libertés |
| **ARJEL** | Autorité de régulation des jeux en ligne |
| **ASIP Santé** | Agence des systèmes d'information partagés de santé |
| **SaaS** | *Software as a service* |
| **PaaS** | *Platform as a service* |
| **IaaS** | *Infrastructure as a service* |
| **CSPN** | Certification de sécurité de premier niveau |
| **PASSI** | Prestataire d'audit de la sécurité des systèmes d'information |

### 1.3.2. Définitions

**Audit** - processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure les exigences d'un référentiel sont satisfaites.

**Bien** - tout élément représentant de la valeur pour le prestataire.

***Cloud computing (informatique en nuage)*** – modèle permettant un accès aisé, à la demande et au travers d'un réseau, à un ensemble partagé de ressources informatiques.

**État de l'art** - ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles à un instant donné, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.

**Incident lié à la sécurité de l'information** – un incident lié à la sécurité de l'information est indiqué par un ou plusieurs événement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information.

**Menace** – cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme.

**Mesure** – moyen de gérer un risque, comprenant la politique, les procédures, les lignes directrices, et les pratiques ou structure organisationnelles, et pouvant être de nature administrative, technique, gestionnaire ou juridique.

**Politique** – intentions et dispositions générales formellement exprimées par la direction d'une entité.

**Prestataire** – organisme proposant une offre de services sécurisés en nuage et visant la qualification.

**Prestataire d'audit de la sécurité des systèmes d'information** - organisme réalisant des prestations d'audit de la sécurité des systèmes d'information. Il est dit qualifié si un organisme de qualification a attesté de sa conformité au Référentiel d'exigences des prestataires d'audit de la sécurité des systèmes d'information

**Risque** – combinaison de la probabilité d'un événement de sécurité et de ses conséquences.

**Sécurité d'un système d'information** – ensemble des moyens techniques et non-techniques de protection, permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles.

**Système d'information** – ensemble organisé de ressources (matériel, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.

**Tiers** – personne ou organisme reconnu(e) comme indépendant(e) du prestataire.

**Vulnérabilité** – faiblesse d'un bien ou d'un groupe de biens pouvant être ciblé par une menace.

# 2. Activités visées par le référentiel

Ce chapitre présente les différentes activités de *Cloud* sur lesquelles on fait porter des exigences, le cas échéant spécifiques, décrites aux chapitres 5 à 18.

## 2.1. Fourniture de service SaaS

Cette offre concerne la mise à disposition d'applications d'entreprise : outils de gestion de la relation client, outils collaboratifs, messagerie, *Business Intelligence*, outils de gestion intégré, etc. Le prestataire offre une fonction opérationnelle et gère de façon transparente pour l'utilisateur l'ensemble des aspects techniques requérant des compétences informatiques. Le client garde la possibilité d'effectuer quelques paramétrages de l'application.

## 2.2. Fourniture de service PaaS

Cette offre concerne la mise à disposition de plates-formes de *middleware*, de développement, de test, d'exécution d'applications. Le prestataire gère et contrôle l'infrastructure technique (réseau, serveurs, OS, stockage, etc.). Le client est responsable du déploiement des applications et de leur paramétrage.

## 2.3. Fourniture de service IaaS

Cette offre concerne la mise à disposition de ressources informatiques (puissance CPU, mémoire, stockage etc.). Le modèle IaaS permet au client de disposer de ressources externalisées virtualisées. Celui-ci garde le contrôle sur le système d'exploitation (OS), le stockage, les applications déployées ainsi que sur certains composants réseau (pare-feu, par exemple).

# 3. Qualification des prestataires proposant une offre de services sécurisés d'informatique en nuage

## 3.1. Modalités de la qualification

Le Référentiel contient les exigences et les recommandations à destination des prestataires de services d'informatique en nuage.

La qualification est réalisée conformément au processus de qualification et permet d'attester de la conformité du prestataire aux exigences du Référentiel.

Les exigences doivent être respectées par les prestataires de services d'informatique en nuage dans le but d'obtenir la qualification. Les recommandations sont données à titre de bonnes pratiques et ne font pas l'objet d'une quelconque vérification en vue de la qualification.

Pour vérifier que le prestataire respecte les exigences des chapitres 5 à 18, l'organisme de qualification audite les lieux liés à la prestation visée par la qualification.

## 3.2. Portée de la qualification

Le prestataire de services sécurisés d'informatique en nuage peut demander la qualification pour tout ou partie des activités décrites au chapitre 2 pour un certain niveau de sécurité (voir chapitre 4).

Le prestataire de services d'informatique en nuage qualifié garde la faculté de réaliser des prestations de services en dehors du périmètre pour lequel il est qualifié, mais ne peut, dans ce cas, se prévaloir de la qualification sur ces prestations.

Une prestation qualifiée peut être associée à d'autres prestations complémentaires (développement, intégration de produits de sécurité, etc.) sans perdre le bénéfice de la qualification.

# 4. Niveaux de sécurité

On distingue dans ce référentiel deux niveaux de qualification des prestations de *cloud* :

- le premier niveau, dit élémentaire, est conçu pour offrir un niveau de protection équivalent à celui requis par la PSSIE ;
- le second, dit standard, offre une protection encore plus robuste, qui permet notamment d'envisager le traitement de données sensibles de niveau Diffusion Restreinte.

Le annexe 1 offre une grille de lecture entre ces niveaux et quelques scénarios d'usage des prestations, en fonction de la sensibilité des données à protéger.

Le niveau élémentaire correspond ainsi à un niveau de sécurité pouvant permettre le stockage et le traitement de données sensibles se caractérisant par les besoins suivants :

- Intégrité vérifiable : la perte d'intégrité des informations est susceptible d'avoir des incidences mineures, n'induisant pas de fortes perturbations. Une perte d'intégrité est tolérée mais doit être détectable.
- Diffusion interne : information ou support interne pouvant circuler librement au sein de l'entité mais ne devant pas être diffusé à l'extérieur.
- Traçabilité pour information : l'utilisation de la fonction, les accès et les traitements effectués sur les données doivent être tracés. La trace concerne tout le système, mais aucun niveau de détail n'est exigé. Elle peut n'être accessible que localement.
- Disponibilité de l'information : évaluée de niveau élémentaire selon une échelle partagée et contractualisée entre le prestataire et le client.

Le niveau standard correspond à un niveau de sécurité pouvant permettre le stockage et le traitement de données sensibles se caractérisant par les besoins suivants :

- Intégrité totale : la perte d'intégrité des informations est susceptible d'avoir des incidences importantes et globales au niveau de l'organisation. Une perte d'intégrité doit être immédiatement détectée et corrigée.
- Diffusion restreinte : information ou support dont la diffusion est limitée à un cercle très restreint de personnes ayant le besoin d'en connaître et dont la divulgation pourrait mettre en péril la pérennité de l'entité.
- Traçabilité légale : l'utilisateur de la fonction, les accès et traitements effectués sur les données doivent être tracés de manière individuelle, directement ou non, et il doit y avoir une garantie de non répudiation de la trace par l'utilisateur. La trace doit contenir une signature numérique.
- Disponibilité de l'information : évaluée de niveau standard selon une échelle partagée et contractualisée entre le prestataire et le client.

La mention « *Niveau standard* » signifie par la suite que l'exigence s'applique spécifiquement pour ce niveau. En l'absence de précision, l'exigence s'applique pour les niveaux élémentaire et standard.

# 5. Risques et politiques de sécurité

## 5.1. Périmètre

a) Le prestataire doit définir le périmètre qu'il souhaite qualifier et établir la liste des exigences applicables en accord avec le périmètre retenu.

b) Le prestataire doit déterminer le niveau de sécurité visé pour sa qualification.

## 5.2. Analyse de risques

a) Le prestataire doit effectuer une analyse de risques couvrant le périmètre de la qualification et se basant sur les besoins de sécurité correspondant au niveau visé de qualification.

b) Le prestataire est susceptible d'avoir à gérer des informations ayant des sensibilités différentes dans son offre et doit faire apparaitre cette gestion dans l'analyse de risques.

c) Les risques résiduels doivent être validés par la direction du prestataire et peuvent être transmis sur simple demande aux RSSI des clients avec accord de non-divulgation.

d) L'analyse de risques doit être mise à jour annuellement.

e) L'analyse de risques doit être réalisée en utilisant une méthode documentée et garantissant la reproductibilité et comparabilité (par exemple la méthode EBIOS[1]).

## 5.3. Politiques de sécurité

a) Le prestataire doit définir, dans une politique générale de sécurité, ses engagements en matière de sécurité des systèmes d'information. Ce document doit en particulier exprimer des engagements quant au respect de la législation française (en matière de traitement des données à caractère personnel, traitement de données sensibles, etc.) selon la nature des informations confiées.

b) Le prestataire doit préciser, dans des politiques de sécurité détaillées, les différentes mesures mises en œuvre. Ces documents couvrent au moins les domaines suivants :

   a. Organisation de la sécurité ;
   b. Sécurité des ressources humaines ;
   c. Gestion des biens ;
   d. Contrôle d'accès et gestion des identités ;
   e. Cryptologie ;
   f. Sécurité physique et environnementale ;
   g. Sécurité des opérations ;
   h. Acquisition, développement et maintenance ;
   i. Relation avec les sous-traitants ;
   j. Gestion des incidents ;

[1] http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

k. Gestion de la continuité des activités ;

l. Conformité.

c) Les politiques de sécurité sont revues annuellement.

d) Les politiques de sécurité doivent être validées par la direction du prestataire.

e) Le stockage et le traitement des données doivent être opérés en France.

f) Le prestataire doit documenter et communiquer au client la localisation du stockage et du traitement des données.

g) Les produits participants à la prestation et visibles du client doivent être régionalisés en français.

h) Le prestataire doit fournir un support de premier niveau francophone localisé en France.

i) Les clauses de ce référentiel sont applicables dans la mesure où les produits qualifiés existent.

## 5.4. Périmètre

c) Le prestataire doit définir le périmètre qu'il souhaite qualifier et établir la liste des exigences applicables en accord avec le périmètre retenu.

d) Le prestataire déterminera le niveau de sécurité de sa qualification.

## 5.5. Contrôle du niveau de sécurité

j) Le prestataire doit contrôler le respect des politiques de sécurité et identifier toute non-conformité.

k) Le prestataire doit formellement accepter les risques résiduels et les non-conformités aux politiques de sécurité établies.

l) *Niveau standard :* cette acceptation doit se traduire par une décision d'homologation de sécurité prononcée par la direction du prestataire, et communiquée à ses clients.

# 6. Organisation de la sécurité de l'information

## 6.1. Attribution des responsabilités en matière de sécurité de l'information

a) Le prestataire s'engage à opérer la prestation à l'état de l'art.

b) Les responsabilités de chacune des parties (prestataires et clients) doivent être clairement contractualisées et documentées.

c) Le prestataire doit formaliser les tâches qui lui incombent et celles qui incombent au client.

d) *Niveau standard :* le prestataire doit identifier les risques associés à des responsabilités ou des cumuls de taches incompatibles.

e) *Niveau standard :* le prestataire doit mettre en place des outils d'administration et de support dédiés au client.

f) Le contrat doit faire apparaître les éléments à la responsabilité du prestataire et ceux qui en sont explicitement exclus.

## 6.2. Séparation des rôles

a) *Niveau standard :* dans le cadre d'une offre SaaS, le prestataire doit mettre à la disposition de ses clients les outils et les moyens qui permettent la séparation des rôles des utilisateurs du service.

## 6.3. Relations avec les autorités

a) Il est conseillé au prestataire de mettre en place des relations appropriées avec les autorités compétentes (exemple : ANSSI, CNIL, etc.) ainsi qu'avec les autorités métier le cas échéant (ASIP Santé, ARJEL, etc.).

b) *Niveau standard :* le prestataire doit mettre en place des relations appropriées avec les autorités compétentes (exemple : ANSSI, CNIL, etc.) ainsi qu'avec les autorités métier le cas échéant (ASIP Santé, ARJEL, etc.).

## 6.4. Relations avec les groupes de spécialistes

a) Il est conseillé au prestataire d'entretenir des contacts appropriés avec des groupes de spécialistes ou des forums spécialisés, notamment pour la prise en compte de nouvelles menaces et des mesures de sécurité appropriées pour les contrer.

b) *Niveau standard :* le prestataire doit entretenir des contacts appropriés avec des groupes de spécialistes ou des forums spécialisés, notamment pour la prise en compte de nouvelles menaces et des mesures pour les contrer.

## 6.5. Sécurité de l'information dans la gestion de projet

a) Le prestataire doit effectuer une évaluation du risque lors du déroulement de tout projet pouvant avoir un impact sur son offre, et ce quelle qu'en soit sa nature.

b) *Niveau standard :* toute mise en place d'une offre client doit faire l'objet d'une analyse de risques.

c) *Niveau standard :* dans la mesure où un projet affecte le niveau de sécurité offert au client, ce dernier doit en être averti et informé des impacts potentiels, des mesures mises en place ainsi que des risques résiduels le concernant.

## 6.6. Situation de mobilité

a) Suivant la législation en vigueur, l'accès aux informations du prestataire ou du client en situation de mobilité doit être encadré par des politiques et procédures spécifiques établies par le prestataire et en corrélation avec celles du client, afin de prendre en compte les risques associés.

b) L'accès aux informations du prestataire ou du client en situation de mobilité doit être à un niveau de sécurité équivalent au niveau de sécurité de l'accès à ces mêmes informations hors situation de mobilité.

# 7. Sécurité liée aux ressources humaines

## 7.1. Sélection

a) Le prestataire doit mettre en place une procédure de vérification des informations concernant son personnel pour toute prise de poste, conformément aux lois, aux règlements et à l'éthique.

b) Ces vérifications doivent être proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés. A titre d'exemple, le prestataire peut demander au candidat une copie du bulletin n°3 de son casier judiciaire.

c) *Niveau standard :* des habilitations spécifiques sont requises pour les personnes occupant un poste pouvant les amener à connaître certaines données hébergées, selon la nature sectorielle et la sensibilité des données. Les habilitations spécifiques devront pouvoir être communiquées à la demande du client.

## 7.2. Conditions d'embauche

a) Un engagement de confidentialité (envers les clients tiers, les prestataires, etc.) doit être signé lors de tout contrat d'embauche.

b) Le prestataire doit rendre accessible à ses clients les modèles d'engagement de confidentialité pris par ses employés lors de la signature du contrat d'embauche, le règlement intérieur ainsi que les fiches de postes.

## 7.3. Responsabilités du prestataire

a) Le prestataire doit exiger des salariés, contractants et utilisateurs tiers qu'ils appliquent les règles de sécurité conformément aux politiques et procédures en vigueur.

## 7.4. Sensibilisation, qualification et formations en matière de sécurité de l'information

a) L'ensemble des salariés du prestataire, les contractants et utilisateurs tiers doivent suivre une sensibilisation ou une formation adaptée à la sécurité et recevoir régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions.

## 7.5. Processus disciplinaire

a) Le prestataire doit élaborer et mettre en œuvre un processus disciplinaire formel pour ses salariés, les contractants et les utilisateurs tiers ayant enfreint les règles de sécurité ou la chartre d'éthique.

b) Le prestataire doit rendre accessible à ses clients les modèles de sanctions encourues par le personnel en cas de manquement aux règles de confidentialité.

## 7.6. Fin ou modification de contrat

a) Les rôles et les responsabilités relatives aux modifications ou aux fins de contrats d'un salarié doivent être clairement définis et attribués.

b) Les procédures doivent permettre de révoquer les droits du personnel quittant, même de façon temporaire (sous-traitants) un rôle opérationnel sur le système.

# 8. Gestion des biens

## 8.1. Inventaire des biens

a) Le prestataire doit tenir à jour l'inventaire des équipements, labellisés selon leur fonction ou le niveau de sensibilité des données présentes sur l'équipement, avec leur localisation.

b) L'inventaire doit relier chaque moyen de traitement de l'information à une personne responsable et une liste d'intervenants.

c) *Niveau standard :* le prestataire doit localiser les données de ses clients de façon à garantir les niveaux de sécurité requis. Il tiendra ces éléments à la disposition des clients.

d) Le prestataire doit avoir une liste des licences utilisées dans le cadre de la prestation et il doit s'assurer de leur validité jusqu'à la fin de celle-ci.

## 8.2. Utilisation correcte des biens

a) Le prestataire doit identifier, documenter et mettre en œuvre des règles permettant l'utilisation correcte de l'information et des biens associés aux moyens de traitement de l'information.

## 8.3. Restitution des biens

a) L'ensemble des salariés, contractants et utilisateurs tiers doivent restituer la totalité des biens qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord. Cette restitution fera l'objet d'une procédure établie par le prestataire.

## 8.4. Niveaux de classification de la donnée

a) Le prestataire doit définir si les données liées au service fourni (informations d'administration, support, etc.) sont soumises à une classification particulière selon un référentiel extérieur (ARJEL, ASIP Santé, ANSSI, etc.).

## 8.5. Marquage et manipulation de l'information

a) Il est conseillé au prestataire d'élaborer et de mettre en œuvre un ensemble approprié de procédures pour le marquage et la manipulation de l'information, conformément au niveau de sensibilité défini en 8.4.

b) *Niveau standard :* le prestataire doit élaborer et mettre en œuvre un ensemble approprié de procédures pour le marquage et la manipulation des informations liées aux services, conformément au niveau de sensibilité défini en 8.4.

## 8.6. Gestion des supports amovibles

a) Le prestataire doit élaborer et mettre en œuvre un ensemble approprié de procédures pour la gestion des supports amovibles, conformément au niveau de sensibilité défini en 8.4. *A minima*, ces procédures doivent prévoir le chiffrement des données sensibles sur les supports.

## 8.7. Mise au rebut

a) Au terme du contrat liant le prestataire au client ou en cas de rupture anticipée pour quelle qu'en soit la cause, ou à la demande du client, le prestataire doit effacer l'intégralité des données de celui-ci par réécriture complète de tout support, et ce, dans un délai qui aura fait l'objet d'une clause contractuelle.

b) Si la localisation exacte des données n'est pas possible, les données devront être chiffrées et l'effacement des clés de chiffrement fera office de destruction.

c) *Niveau standard:* le prestataire doit, en complément du chiffrement des données, effacer les copies des données détenues dans ses systèmes informatiques à l'aide d'une solution qualifiée au niveau élémentaire par l'ANSSI et sans délais. Un PV de mise au rebut sécurisée doit être réalisé.

# 9. Contrôle d'accès et gestion des identités

Ce chapitre concerne tous les utilisateurs, qu'ils soient utilisateurs du prestataire, du client, ou des tiers.

## 9.1. Politiques et contrôle d'accès

a) Le prestataire doit établir, documenter et mettre en œuvre une politique de contrôle d'accès sur la base du résultat de son analyse de risque.

b) Le prestataire doit réexaminer la politique de gestion des identités et des contrôles d'accès au moins annuellement.

## 9.2. Enregistrement et suppression des utilisateurs

a) Le prestataire doit établir un outil centralisé permettant de gérer les droits d'accès des utilisateurs sur les ressources nécessaires à la prestation fournie.

b) Le prestataire doit définir une procédure formelle d'enregistrement et de suppression des utilisateurs dans l'outil de gestion des droits d'accès.

c) La suppression d'un utilisateur doit entraîner la suppression de tous ses accès aux ressources du système d'information.

d) Dans une offre de type SaaS, le prestataire appliquera ces éléments sur les utilisateurs de ses clients dans le cadre de leurs responsabilités partagées.

## 9.3. Gestion des droits d'accès

a) Le prestataire doit définir et appliquer une procédure formelle pour contrôler l'attribution, la modification et la suppression de droits d'accès aux ressources nécessaires à la prestation fournie.

b) Dans une offre de type SaaS, le prestataire appliquera cette procédure aux utilisateurs de ses clients dans le cadre de leurs responsabilités partagées suivant le niveau de qualification visé.

c) Le prestataire doit être en mesure de fournir, pour une ressource donnée dans le cadre de la prestation, la liste de tous les utilisateurs y ayant accès et le niveau d'autorisation auquel ils ont un accès.

d) Le prestataire doit être en mesure de fournir, pour un utilisateur donné dans le cadre de sa prestation, la liste de tous les droits d'accès qu'il a sur les différents éléments du système d'information.

e) Le prestataire doit définir une liste de droits d'accès incompatibles entre eux. Le prestataire doit s'assurer, lors de l'attribution de droits d'accès à un utilisateur, qu'il ne possède pas de droits d'accès incompatibles entre eux au titre de la liste précédemment établie.

f) Le prestataire doit revalider annuellement les droits d'accès des utilisateurs selon le principe de besoin d'en connaître.

g) *Niveau standard:* la revue des droits d'accès devra se faire trimestriellement.

h) Les personnes pouvant utiliser des comptes techniques ayant des privilèges élevés devront subir une revalidation trimestrielle de ce besoin.

## 9.4. Gestion des authentifications des utilisateurs

a) La gestion de l'authentification des utilisateurs (administrateurs, etc.) doit être réalisée dans le cadre d'un processus formel. A cet effet, le prestataire de service en nuage doit établir :

   a. des procédures d'émission, de modification et de réémission des facteurs d'authentification (certificats, mots de passe, etc.).

   b. des moyens d'authentification et d'autorisation permettant une authentification à multiples facteurs.

   c. Les systèmes qui génèrent les mots de passe ou vérifient leur robustesse doivent respecter les recommandations de l'ANSSI.

   d. Dans les cas où la gestion des authentifications n'est pas du ressort du prestataire, ce dernier doit la contractualiser.

b) *Niveau standard :* l'authentification des administrateurs doit se faire suivant le principe d'une authentification à double facteur.

c) Les utilisateurs doivent suivre les exigences de la politique de sécurité concernant l'authentification.

## 9.5. Procédure de connexion sécurisée

a) L'accès aux systèmes et aux applications doit reposer sur un mécanisme d'authentification respectant les exigences de la politique de contrôle d'accès.

b) *Niveau standard :* l'authentification à deux facteurs doit être utilisée.

## 9.6. Emploi des utilitaires systèmes

Certains outils d'administration et de supervision ont la capacité de contrôler des applications ou d'écraser des données.

a) Le prestataire doit limiter et contrôler étroitement l'emploi des outils d'administration et de supervision. La liste des utilisateurs ayant besoin de ce type d'outils doit être connue et justifiée. Ces utilisateurs doivent alors être considérés comme relevant de la catégorie des administrateurs, les règles concernant les administrateurs s'appliquant.

b) Le prestataire doit donner les moyens au client d'établir, limiter et contrôler étroitement la liste des utilisateurs ayant accès aux outils d'administration et de supervision. Ces utilisateurs doivent alors être considérés comme relevant de la catégorie des administrateurs, les règles concernant les administrateurs s'appliquant.

*c) Niveau standard :* le prestataire doit empêcher qu'un client ou un de ses utilisateurs puissent perturber le service fourni aux autres clients, particulièrement dans le cas d'un service mutualisé.

## 9.7. Contrôle d'accès pour le respect d'intégrité ou respect de propriété intellectuelle

a) L'accès aux paramétrages des applications et des programmes, aux binaires ou aux codes sources, doit être restreint au personnel autorisé en fonction de la politique de contrôle d'accès, afin de se prévenir de modifications indues.

b) L’accès à toute forme de propriété intellectuelle appartenant au prestataire ou à un client, ainsi que l’utilisation de logiciels propriétaires doit être restreint au personnel autorisé en fonction de la politique de contrôle d’accès et de licences.

# 10. Cryptologie

## 10.1. Chiffrement des données stockées

a) Les données stockées doivent être chiffrées ; le chiffrement doit reposer sur un mécanisme en accord avec les règles et les recommandations de l'*Annexe B1 du Référentiel Général de Sécurité.*

b) La solution de chiffrement doit être qualifiée au moins au niveau élémentaire.

c) *Niveau standard :* la solution de chiffrement doit être qualifiée au moins au niveau standard.

## 10.2. Hachage des mots de passe

a) Seule l'empreinte des mots de passe doit être stockée.

b) La fonction de hachage doit reposer sur un mécanisme en accord avec les règles et les recommandations de l'*Annexe B1 du Référentiel Général de Sécurité.*

c) Les mots de passe doivent être salés avant d'être hachés.

## 10.3. Chiffrement des flux

a) Toutes les communications réseau entre le fournisseur et le client doivent faire l'objet d'un chiffrement.

b) Le chiffrement des flux doit reposer sur un mécanisme en accord avec les règles et les recommandations de l'*Annexe B1 du Référentiel Général de Sécurité.*

c) *Niveau standard :* la solution de chiffrement doit être au moins qualifiée au niveau standard.

## 10.4. Authentification

a) Les mots de passe doivent être en accord avec *les règles et les recommandations de l'ANSSI*.

b) *Niveau standard:* l'authentification du personnel du prestataire doit reposer sur une authentification forte utilisant une solution qualifiée au moins au niveau standard.

## 10.5. Non répudiation

a) La signature électronique des traces doit reposer sur un mécanisme en accord avec les règles et les recommandations de l'*Annexe B1 du Référentiel Général de Sécurité.*

## 10.6. Gestion des clés

a) Les caractéristiques des clés doivent être en accord avec les règles et les recommandations de l'*Annexe B2 du Référentiel Général de Sécurité.*

### 10.6.1. Techniques symétriques

*a)* Les clés secrètes peuvent être stockées dans un conteneur de clés au format logiciel.

*b) Niveau standard:* les clés secrètes doivent être stockées sur un support physique qualifié au niveau standard.

### 10.6.2. Techniques asymétriques

*a) Niveau standard :* la politique de gestion des clés doit être conforme aux règles du niveau ** du RGS.

# 11. Sécurité physique et environnementale

## 11.1. Protection contre les menaces extérieures et environnementales

a) Les centres de données doivent être localisés de manière à minimiser les risques inhérents aux sinistres physiques (incendie, dégât des eaux, etc.) et naturels (climatique, inondation, etc.).

b) Des mesures doivent être mises en place afin de limiter les risques de départ et de propagation de feu et les risques de dégât des eaux.

c) Des mesures doivent être prises pour prévenir et limiter les conséquences d'une coupure d'alimentation électrique du site, de la zone ou des salles, et permettre une reprise conforme au niveau de disponibilité attendu.

d) Des moyens de climatisation doivent être mis en place pour maintenir des conditions de température et d'humidité adaptées aux équipements. Des mesures doivent être prises pour prévenir les pannes de climatisation et en limiter les conséquences.

e) Les équipements de détection et de protection doivent être régulièrement contrôlés, testés et maintenus.

## 11.2. Périmètre de sécurité physique

a) Des périmètres de sécurité doivent être définis, documentés et mis en œuvre. Il convient de distinguer :

   i. les zones publiques, accessibles à tous dans les limites de la propriété du prestataire, qui n'hébergent aucune ressource dévolue à l'offre ou permettant d'accéder à des composantes de celle-ci.
   ii. les zones privées, dont les accès sont contrôlés au moyen d'un badge ; ces zones privées peuvent héberger :
      1. des plateformes de développement des offres.
      2. les locaux à partir desquels les intervenants (administrateurs, exploitants, supports) opèrent.
      3. les moyens de développement d'une part, d'administration d'exploitation et de supervision d'autre part, ne doivent pas être localisés dans une même zone privée.
   iii. les zones sensibles, dont les accès sont contrôlés au moyen d'un badge et d'un code ; ces zones sensibles sont réservées à l'hébergement des infrastructures de production et aux moyens d'administration, d'exploitation ou de supervision.

b) Un plan incluant le marquage des zones et les différents moyens de limitation et de contrôle des accès doit être réalisé.

c) Le prestataire doit intégrer les éléments de sécurité physique dans la politique de sécurité et l'analyse de risque conformément au niveau de sécurité requis par la catégorie de la zone.

d) Il ne doit pas y avoir d'accès direct entre une zone publique et zone sensible.

e) *Niveau standard:* les plates-formes de développement des offres doivent également être hébergées en zones sensibles, en respectant l'exigence de cloisonnement entre les ressources.

## 11.3. Contrôle physique des accès

### 11.3.1. Zones privées

a) Les zones privées doivent être protégées contre les accès non autorisés. Pour ce faire, un contrôle d'accès doit être mis en place, basé sur la détention d'un secret (par exemple : code d'accès) ou la détention d'un moyen personnel (par exemple : badge).

b) Des mesures d'accès dérogatoires en cas d'urgence doivent être établies et documentées.

c) Un avertissement relatif aux limites d'accès sur zone doit être affiché à l'entrée des zones privées.

d) Les plages horaires d'accès doivent être déterminées conformément aux besoins des intervenants et être précisées dans la politique de sécurité.

e) Les visiteurs doivent être systématiquement accompagnés lors de leurs accès et séjours en zone privée.

f) Un dispositif de détection et de surveillance doit être mis en place et opéré en dehors des heures d'accès autorisées.

g) Les pièces inoccupées doivent être systématiquement verrouillées.

### 11.3.2. Zones sensibles

a) Les zones sensibles doivent être protégées contre les accès non autorisés. Pour ce faire, un contrôle d'accès à deux facteurs personnels doit être mis en place.

b) Des mesures d'accès dérogatoires en cas d'urgence doivent être établies et documentées.

c) Un avertissement relatif aux limites d'accès sur zone doit être affiché à l'entrée des zones sensibles.

d) Les plages horaires d'accès doivent être déterminées conformément aux besoins des intervenants et être précisées dans la politique de sécurité.

e) Les visiteurs doivent être systématiquement accompagnés lors de leurs accès et séjours en zone sensible.

f) Des dispositifs de détection et de surveillance, et de vidéoprotection doivent être mis en place et opérés en dehors des heures d'accès autorisées.

g) Les pièces inoccupées doivent être systématiquement verrouillées.

h) Les accès aux zones sensibles doivent être systématiquement journalisés et les traces exploitables contrôlées au moins mensuellement.

## 11.4. Travail dans les zones sécurisées

a) Des procédures propres au travail en zone privée ou sensible doivent être rédigées et connues tous les intervenants concernés.

## 11.5. Zones d'accès public de livraison et de chargement

a) Si les zones de livraison/chargement ou autres sont des points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux, alors ces zones seront de fait considérées comme des zones publiques.

b) Le prestataire doit isoler particulièrement les points d'accès de ces zones vers les zones sécurisées, de façon à éviter les accès non autorisés, ou à défaut, implémenter des mesures compensatoires permettant d'assurer le même niveau de sécurité fonctionnel.

## 11.6. Sécurité du câblage

a) Le câblage doit être protégé conformément aux résultats de l'analyse de risques.

b) Un plan de câblage doit être défini et mis à jour et pris en compte avant tous travaux.

## 11.7. Maintenance du matériel

a) Le prestataire et les tiers doivent s'assurer que les conditions de maintenance et d'entretien du matériel sont conformes à l'exigence de disponibilité.

b) Les matériels doivent faire l'objet de contrats de maintenance.

## 11.8. Sortie d'un bien

a) Une autorisation formelle de la direction du prestataire doit être obtenue avant de pouvoir effectuer le transfert hors site d'un équipement, de données ou de logiciels. Dans tous les cas, le prestataire devra s'assurer que les moyens mis en œuvre pour garantir le niveau de classification de l'équipement, de la donnée ou du logiciel quand il était dans le site, sont garantis hors site, pendant le transport et à destination.

## 11.9. Recyclage sécurisé du matériel

a) Tout support de données appartenant au prestataire et mis au service d'un client doit, lors de son recyclage, être effacé par réécriture complète avant réutilisation pour un autre client ou pour lui-même.

b) *Niveau standard:* cet effacement doit être effectué en mettant en œuvre des moyens qualifiés par l'ANSSI. Un PV de recyclage ou de mise au rebut sécurisée doit être réalisé.

## 11.10. Matériel en attente d'utilisation

a) Le prestataire doit documenter et appliquer une procédure de protection du matériel non utilisé.

# 12. Sécurité liée à l'exploitation

## 12.1. Procédures d'exploitation documentées

a) Le prestataire doit documenter les procédures d'exploitation, les tenir à jour et les rendre accessibles au personnel concerné.

## 12.2. Gestion des changements

a) Le prestataire doit documenter et mettre en place une procédure de gestion des changements apportés aux systèmes et moyens de traitement de l'information.

b) Pour tout changement opéré ayant un impact sur la sécurité, le prestataire doit communiquer à ses clients les informations suivantes :

   a. date et heure programmées du changement,
   b. nature du changement,
   c. annonce lors du début et de fin de la mise en place du changement.

## 12.3. Séparation des environnements de développement, de test et d'exploitation

a) Le prestataire doit séparer physiquement les environnements de production des autres environnements.

## 12.4. Mesures contre les codes malveillants

a) Le prestataire doit mettre en œuvre des mesures de détection, de prévention et de restauration pour se protéger des codes malveillants.

b) Le prestataire doit mettre en place des procédures appropriées de sensibilisation de ses équipes.

## 12.5. Sauvegarde des informations

a) Le prestataire doit documenter et mettre en place une politique de sauvegarde pouvant inclure les thèmes suivants : objet de la sauvegarde, sa fréquence, les tests, l'éventualité du chiffrement, etc.

b) Le prestataire doit réaliser quotidiennement des copies de sauvegarde des informations, des logiciels et de leurs configurations.

c) Les sauvegardes doit faire l'objet d'une traçabilité revue de façon hebdomadaire.

d) Les sauvegardes doivent être soumises à un essai trimestriel conformément à la politique de sauvegarde convenue, et doivent comporter des essais de restauration.

e) Les sauvegardes doivent être localisées à une distance suffisante des équipements principaux en cohérence avec les résultats de l'analyse de risques et permettant de faire face à des sinistres majeurs.

f) Le prestataire doit chiffrer, à l'aide d'une solution qualifiée au niveau standard par l'ANSSI, les sauvegardes traitées par un tiers.

## 12.6. Journalisation des événements

a) Le prestataire doit créer, collecter et tenir à jour les journaux d'événements enregistrant les activités des utilisateurs, les exceptions, les défaillances et les événements liés à la sécurité de l'information.

b) Le prestataire doit journaliser de la même façon les activités des administrateurs système et des opérateurs système dans des mécanismes de journalisation dédiés.

c) Les journaux doivent être conservés pendant une durée conforme aux exigences légales ou réglementaires dans un bastion ou sur une machine dédiéé.

d) Le prestataire doit pouvoir fournir les journaux concernant un client sur demande de ce client.

## 12.7. Protection de l'information journalisée

a) Le prestataire doit protéger les équipements de journalisation et les informations journalisées contre les atteintes à leur disponibilité, intégrité, confidentialité ou traçabilité.

b) Le prestataire doit estimer l'espace de stockage nécessaire à la conservation locale des journaux lors du dimensionnement des équipements.

c) Les journaux de l'ensemble des équipements du système d'information doivent être transférés de manière sécurisée sur un ou plusieurs serveurs centraux dédiés et stockés de manière sécurisée sur une machine différente de celle qui les a générés.

d) Les processus de journalisation et de collecte doivent être exécutés par des comptes disposant de peu de privilèges et l'accès aux journaux doit être limité à un nombre restreint de comptes ayant le besoin d'en connaître.

## 12.8. Synchronisation des horloges

a) Les horloges des équipements doivent être synchronisées sur plusieurs sources de temps internes cohérentes entre elles. Ces sources pourront elles-mêmes être synchronisées sur plusieurs sources fiables externes, sauf pour les réseaux isolés.

b) L'ensemble des journaux doit être horodaté.

## 12.9. Exploitation des journaux

a) Le prestataire doit interpréter et mettre en corrélation les journaux afin de détecter les événements anormaux, en temps réel ou *a posteriori*.

b) Le prestataire doit contrôler les journaux au moins quotidiennement.

c) *Niveau standard:* le prestataire doit contrôler les journaux au moins toutes les heures.

## 12.10. Gestion des alertes

a) Le prestataire doit opérer ou souscrire une offre qualifiée de services de détection des incidents de sécurité.

## 12.11. Installation de logiciels sur des systèmes en exploitation

a) Le prestataire doit mettre en œuvre et documenter des procédures afin de contrôler l'installation de logiciels systèmes ou applicatifs sur les systèmes en exploitation.

b) Le prestataire doit maintenir la gestion de la configuration des environnements mis à la disposition du client.

## 12.12. Gestion des vulnérabilités techniques

a) Le prestataire doit mettre en place un processus de veille permettant la gestion des vulnérabilités techniques des systèmes.

b) Le prestataire doit évaluer son exposition à ces vulnérabilités, la documenter, et prendre les mesures adéquates afin de couvrir les risques associés.

# 13. Sécurité des opérations

## 13.1. Politiques de sécurité et procédures de traitement et d'échange d'information

a) Le prestataire doit mettre en place des politiques, procédures et mécanismes de sécurité pour protéger toutes les opérations, conformément aux résultats de l'analyse de risque, qui s'effectuent sur son système d'information :
   i. le traitement de l'information qui s'effectue sur les équipements de son système d'information, quel que soit leur type ;
   ii. les échanges d'informations transitant par tous les équipements de télécommunication de son système d'information, quel que soit leur type.

## 13.2. Cartographie de l'installation informatique

a) Cette cartographie doit au minimum comprendre les éléments suivants :
   i. liste des ressources matérielles (avec leur modèle) et logicielles (avec leur version) utilisées ;
   ii. liste des machines déployées associées à leurs attributaires et à leurs paramètres techniques (adresse IP, adresse MAC) ;
   iii. liste des postes et des équipements d'administration ;
   iv. architecture réseau sur laquelle sont identifiés les points névralgiques (connexions externes, serveurs hébergeant des données ou des fonctions sensibles, etc.).

b) Une fois cette cartographie établie, elle doit être maintenue à jour et enrichie avec des éléments liés aux protocoles mis en œuvre (matrices de flux).

## 13.3. Séparation des environnements

c) L'infrastructure du système d'information du prestataire, au niveau système, réseau ou applicatif, doit être conçue, développée, déployée et configurée de manière à respecter le cloisonnement qui est nécessaire d'un point de vue de la sécurité entre un client, le prestataire et des tiers.

d) La politique de sécurité du prestataire décrira précisément pour chaque client ou catégorie de clients les objectifs du cloisonnement mis en œuvre :
   - objectif de cloisonnement avec d'autres clients du prestataire dont le niveau de sécurité requis est différent ;
   - objectif de cloisonnement avec d'autres clients du prestataire dont le niveau de sensibilité des informations est différent ou non compatible à un hébergement sur une ressource commune ;
   - objectif de cloisonnement avec l'environnement du même client pour lequel le niveau de sensibilité des informations est différent ou non compatible à un hébergement sur une ressource commune ;
   - objectif de cloisonnement d'un flux par type de flux ; par exemple :

- flux de données versus flux de données d'un autre type nécessitant un cloisonnement ;
- flux d'administration du client versus flux de données de production du client ;
- flux d'administration du client versus flux d'administration du prestataire ;

Il est recommandé de procéder à des audits réguliers (conformément au chapitre 18) sur l'architecture du système d'information global du prestataire.

e) La gestion des accès utilisateurs doit faire la distinction entre les différentes catégories d'utilisateurs en fonction des actions qu'ils ont à mener sur l'architecture : prestataire, client(s) et tiers.

f) Les applications partagées ainsi que l'infrastructure système et les composants réseau doivent être conçus, développés, configurés et déployés en prenant en compte *a minima* les cloisonnements suivants :

   i. un cloisonnement permettant de séparer le réseau de service et le réseau utilisé pour l'administration et la gestion des services et des ressources.

   ii. un cloisonnement permettant de séparer les environnements de stockage et de traitement des données de sensibilité différente.

g) *Niveau standard :* le cloisonnement permettant d'isoler le stockage et le traitement des données sensibles sera effectué physiquement.

## 13.4. Mesures sur les réseaux et les systèmes

a) Les services, protocoles et ports utilisés doivent être documentés et leur utilisation justifiée. Si des services, protocoles ou ports réputés non sûrs doivent être néanmoins utilisés, des mesures compensatrices doivent être mises en place dans une logique de défense en profondeur. La documentation et des schémas d'architecture système et réseau doivent identifier clairement les environnements sensibles et les flux de données pour lesquels la conformité légale, statutaire ou réglementaire est à considérer.

b) Des mesures doivent être mises en œuvre pour appliquer des techniques de défense en profondeur telles que recommandées par l'ANSSI pour la protection des systèmes (durcissement des systèmes d'exploitation, configuration des machines virtuelles) et pour la détection et la réponse aux attaques réseau associées à un comportement anormal du trafic (par exemple, MAC *spoofing* ou ARP *poisoning*) et / ou par déni de service (DDoS).

## 13.5. Sécurité des services

a) Pour tous les services, le prestataire doit identifier les fonctions, les niveaux de service et les exigences de gestion, et les intégrer dans tout accord sur les services, que ces services soient fournis en interne ou en externe.

b) Le prestataire doit rendre accessible à ses clients les spécifications des fonctionnalités réseau, notamment la capacité et la redondance des réseaux.

# 14. Acquisition, développement et maintenance des systèmes d'information

## 14.1. Politique de développement sécurisé

a) Le prestataire doit établir des règles de développement des logiciels et des systèmes, et les appliquer aux développements internes ou les faire appliquer contractuellement dans le cas de développements externes.

b) Le prestataire doit assurer une formation suffisante en développement sécurisé aux personnes concernées.

## 14.2. Environnement sécurisé de développement interne

a) Le prestataire doit établir un environnement sécurisé de développement qui englobe l'intégralité du cycle de développement du système.

b) Le prestataire doit en assurer la protection conformément aux résultats de l'analyse de risques.

## 14.3. Développement externalisé

a) Le prestataire doit superviser et contrôler l'activité de développement externalisé du système, en veillant à ce que celui-ci ait un niveau de sécurité final équivalent à un développement interne.

## 14.4. Procédures de contrôle des changements apportés au système

a) Le prestataire doit contrôler les changements apportés au système dans le cycle de développement en utilisant des procédures formelles de contrôle des changements.

b) Le prestataire doit valider les changements sur un environnement spécifique avant leur mise en production.

c) Le prestataire doit communiquer à ses clients les changements opérés sur l'architecture ayant un impact sur la sécurité.

## 14.5. Revue technique des applications après modification de la plateforme d'exploitation

a) Lorsque des changements sont apportés aux plateformes d'exploitation, le prestataire doit revoir et tester les applications métier critiques afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

## 14.6. Restrictions relatives aux changements apportés aux progiciels.

a) En cas d'utilisation de progiciels, le prestataire ne doit les modifier qu'en cas d'absolue nécessité et dans les limites des accords de licence.

b) En cas de modification dans un progiciel, celui-ci doit être contrôlé, testé et validé si besoin par l'éditeur afin de conserver l'intégrité du support et de la maintenance associés.

## 14.7. Phase de test de la sécurité du système

a) Le prestataire doit soumettre les systèmes, nouveaux ou mis à jour, à des tests et à des vérifications pendant les processus de développement. Ce processus requiert la mise en place d'un programme détaillé des tâches et des données de test d'entrée, avec les résultats attendus en sortie.

## 14.8. Protection des données de test

a) Le prestataire doit établir une procédure de test précisant que le jeu de données de test est créé pour assurer à la fois la vraisemblance des données et leur exploitabilité.

b) Les données de test doivent être rendues anonymes par un outil si celles-ci sont des données de production.

# 15. Relations avec les tiers

## 15.1. Identification des tiers

a) Le prestataire d'offre d'informatique en nuage doit identifier l'ensemble des tiers participant à la mise en œuvre de l'offre à qualifier (hébergeur, développeur, intégrateur, archiveur, sous-traitant opérant sur site ou à distance pour les tâches d'administration etc.).

b) Il doit identifier toutes les prestations externalisées qui participent à la fourniture de l'offre.

## 15.2. La sécurité dans les accords conclus avec les tiers

a) Le prestataire doit reporter vers le tiers concerné des exigences de sécurité au moins équivalentes à celles que le prestataire s'engage à mettre en œuvre dans sa propre politique de sécurité. Il le fera au travers d'exigences dans les cahiers des charges ou de clauses de sécurité dans les accords de partenariat. Ces exigences doivent être contractualisées.

b) *Niveau standard:* le prestataire doit également contractualiser, sous la forme de clauses d'auditabilité, la possibilité d'auditer les mesures mises en œuvre par les tiers pour répondre aux exigences formulées.

## 15.3. Contrôle, revue et audit

a) Le prestataire doit contrôler, revoir et auditer les mesures mises en place par les tiers. Les audits et contrôles peuvent être effectués sur une base déclarative.

b) *Niveau standard:* le prestataire doit auditer ses principaux fournisseurs du point de vue des risques.

## 15.4. Gestion du changement avec les tiers

a) Dans la mesure où un changement de tiers affecte le niveau de sécurité offert au client, ce dernier doit en être informé et ce changement doit apparaître dans le contrat qui les lie.

b) Le prestataire doit en avertir l'organisme de qualification.

## 15.5. Engagements de confidentialité

a) Le prestataire doit identifier et réexaminer au moins annuellement les exigences en matière d'engagements de confidentialité ou de non-divulgation vis-à-vis des tiers, conformément à ses besoins.

# 16. Gestion des incidents liés à la sécurité de l'information

## 16.1. Responsabilités et procédures

a) Le prestataire doit élaborer des politiques et procédures pour apporter des réponses rapides et efficaces aux incidents de sécurité. Ces politiques et procédures doivent également définir les moyens de communication des incidents de sécurité aux clients concernés, et le niveau de sécurité exigé pour cette communication.

b) Les employés et sous-traitants doivent être informés de ces politiques et de ces procédures.

c) *Niveau standard*: le prestataire doit identifier les points de contact et mettre en place une relation avec les autorités compétentes (conformément au chapitre 6.3).

## 16.2. Gestion de crise

a) Le prestataire doit mettre place et documenter une procédure de gestion de crise prenant en compte les aspects suivants :

   a. modalités de déclenchement de crise ;

   b. mise en place de la cellule de crise ;

   c. liste des acteurs et définition de leur rôle ;

   d. déroulement de la crise ;

   e. mise en place d'un canal de communication en interne et avec les clients.

## 16.3. Appréciation des événements liés à la sécurité de l'information et prise de décision

a) Les incidents doivent être qualifiés selon une échelle partagée entre le prestataire et le client afin d'identifier les incidents de sécurité et leur gravité.

b) La classification adoptée doit permettre d'identifier clairement les incidents de sécurité touchant des données sensibles ou des services critiques du point de vue du client, conformément aux résultats de l'analyse de risques.

c) Le client choisit les niveaux de gravité des incidents pour lesquels il souhaite être informé.

## 16.4. Signalement des événements liés à la sécurité de l'information

a) Le prestataire doit mettre en place un processus de gestion des incidents de sécurité.

b) Les incidents doivent être communiqués aux autorités compétentes conformément aux exigences réglementaires.

c) Les incidents de sécurité qualifiés de critiques doivent être communiqués sans délai aux clients, et des préconisations doivent être faites aux clients pour limiter les impacts des incidents détectés.

d) Le prestataire doit exiger de ses employés et de ses sous-traitants qu'ils rendent compte de tout incident de sécurité, avéré ou suspecté.

e) Le processus doit prendre en compte la possibilité des clients d'informer le prestataire de tout incident de sécurité, avéré ou suspecté, dans le périmètre de la prestation.

## 16.5. Réponse aux incidents liés à la sécurité de l'information

a) Les incidents de sécurité doivent être traités jusqu'à leur résolution et les clients doivent être informés conformément aux procédures.

b) *Niveau standard* : un service spécifique de gestion de crise doit être prévu.

## 16.6. Tirer des enseignements des incidents liés à la sécurité de l'information

a) Un processus d'amélioration continue doit être mis en place et documenté afin de permettre que la connaissance des incidents déjà détectés et traités entraîne une diminution de l'occurrence et de l'impact des incidents similaires à venir.

## 16.7. Recueil de preuves

a) Le prestataire doit documenter des procédures et mettre en œuvre des moyens adaptés pour enregistrer les informations pouvant servir d'éléments de preuve.

b) Le prestataire doit archiver les documents détaillant les incidents traités.

# 17. Continuité d'activité

## 17.1. Organisation de la continuité d'activité

a) Le prestataire doit mettre en place et documenter un plan de continuité d'activité incluant les aspects de sécurité.

## 17.2. Mise en œuvre de la continuité d'activité

a) Le prestataire doit élaborer et mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne.

## 17.3. Vérifier, revoir et évaluer la continuité d'activité

a) Le prestataire doit soumettre à essai et mettre à jour annuellement les plans de continuité de l'activité afin de s'assurer qu'ils sont actualisés et efficaces en situation de crise.

## 17.4. Disponibilité des moyens de traitement de l'information

a) Le prestataire doit mettre en œuvre une redondance des équipements d'infrastructure permettant de se prémunir des interruptions de service (par exemple : panne de courant, panne de réseau, etc.).

b) Les équipements redondants doivent être localisés à une distance suffisante des équipements principaux en cohérence avec l'analyse de risques et permettant de faire face à des sinistres majeurs (par exemple : destruction de salle machine, etc.).

c) Les exigences de disponibilité doivent être contractualisées entre le prestataire et le client.

# 18. Conformité

## 18.1. Identification de la législation et des exigences contractuelles applicables

a) Pour tout contrat établi avec le prestataire, le droit français s'applique et doit être pris en compte dans les politiques de sécurité. Le tribunal compétent est français.

b) Le prestataire doit respecter toutes les exigences légales, réglementaires et contractuelles en vigueur, ainsi que la procédure utilisée par le prestataire pour satisfaire à ces exigences (par exemple : données à caractère personnel, droits de propriété intellectuelle, secteurs métiers, etc.).

c) Le prestataire doit mettre ces documents à disposition de ses clients.

d) Le prestataire doit réaliser une veille active des exigences légales, réglementaires et contractuelles en vigueur.

## 18.2. Revue indépendante de la sécurité de l'information

a) Le prestataire doit rédiger un plan d'audit définissant les cibles et les fréquences de contrôle en accord avec la gestion du changement, les politiques, et les résultats des analyses de risques.

b) Des audits tiers doivent être réalisés annuellement par des prestataires d'audit de la sécurité des systèmes d'information qualifiés.

c) *Niveau standard*: le client peut demander un audit selon les clauses prévues dans le contrat qui le lie au prestataire.

## 18.3. Conformité avec les politiques et les normes de sécurité

a) Les responsables doivent s'assurer régulièrement de l'exécution correcte de l'ensemble des procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les politiques et normes de sécurité.

## 18.4. Examen de la conformité technique

a) Le prestataire doit rédiger une politique concernant la vérification de la conformité technique contenant des points tels que :

   a. Objectifs
   b. Méthodes
   c. Fréquence
   d. Résultats
   e. Mesures correctrices

# 19. Annexe 1 : Grille de lecture

La présente annexe présente une grille de lecture afin d'aider les utilisateurs à choisir les architectures de d'informatique en nuage recommandées en fonction des catégories de données qu'elles hébergent.

Chaque utilisateur est invité à déterminer sa propre échelle de sensibilité en disponibilité, en intégrité, en traçabilité et en confidentialité en fonction de ses besoins et de l'analyse qu'il fait des risques qui pèsent sur ses structures, ses missions et les données qu'il héberge.

En fonction de ces échelles et suite à cette analyse de risques, l'entité choisit l'architecture (niveau élémentaire ou niveau standard) sur laquelle il souhaite héberger ces données.

## 19.1. Type de données qui peuvent être stockées sur une architecture de niveau élémentaire

*Caractérisation :*

Les informations sont celles dont la diffusion, l'altération, la traçabilité ou l'indisponibilité porte préjudice aux intérêts ou à l'efficacité de l'utilisateur sans toutefois remettre en cause son fonctionnement, ses missions ou sa pérennité.

*Exemples* :

Les informations internes qui ne sont pas destinées à être diffusées au public :

- documents de travail ;
- documents comptables ;
- informations relatives au fonctionnement et l'organisation de l'utilisateur, etc.

Les informations dont la diffusion, l'altération, la traçabilité ou l'indisponibilité peuvent engager la responsabilité pénale de l'utilisateur :

- les informations protégées par le secret des correspondances qui s'applique de façon générale[2] ;
- les informations personnelles protégées par la loi « Informatique et Liberté » [3] ;

[2] Article 226-15 du code pénal « le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions ».

[3] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

## 19.2. Type de données qui peuvent être stockées sur une architecture de niveau standard

*Caractérisation :*

Les informations sont celles dont la diffusion, l'altération, la traçabilité ou l'indisponibilité porte gravement préjudice aux intérêts, au fonctionnement, aux missions ou à la pérennité de l'utilisateur.

*Exemples* :

Les informations dont la diffusion, l'altération, la traçabilité ou l'indisponibilité peuvent engager la responsabilité pénale de l'utilisateur :

- les informations dont le détenteur est assujetti au secret professionnel [4] comme les informations dont les détenteurs sont assujettis au secret des délibérations ;
- les informations dont la destruction, la falsification, le détournement ou l'utilisation frauduleuse porterait atteinte aux intérêts nationaux ;
- les informations internationales confiées à la France relevant d'un accord de sécurité ;
- les documents administratifs ne devant pas être communiqués au public et ne devant être communiqués qu'à l'intéressé [5] ;
- les informations portant la mention « Diffusion restreinte » de *l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale* qui sont des informations particulièrement sensibles en confidentialité.

Les informations dont la diffusion, l'altération, la traçabilité ou l'indisponibilité peuvent porter atteinte aux missions ou au fonctionnement de l'utilisateur :

- les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication à des autorités publiques étrangères est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou de l'ordre public [6] ;
- les informations constitutives du patrimoine scientifique et technique [7] ;
- les informations dont dépend la sécurité d'un système qui manipule des informations sensibles et les informations vitales pour le fonctionnement d'un système dont la disponibilité est importante pour l'entité ;
- les informations prévues par l'article 6 de la loi « Accès aux documents administratifs[8]».

---

[4] Article 226-13 du code pénal « la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende ».

[5] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

[6] Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

[7] Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation.

[8] Loi n°78 -753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.