Cahier des clauses de cybersécurité pour les offres SAAS

Une image contenant texte, noir et blanc, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

|  |
| --- |
| **Identification du document** |
| Référence | CAHIER DES CLAUSES CYBER |
| Date de dernière mise à jour | 09/05/2025 |
| Version | V1.0 |
| Classification | ***Diffusion public*** |
| Nombre de pages | 27 |
|  |  |

**CYCLE DE VIE DU DOCUMENT**

**AUTEUR(S)**

| Fonction | Nom | Date |
| --- | --- | --- |
| RSSI | Christophe Delpierre | 22/05/2024 |
|  |  |  |
|  |  |  |

**HISTORIQUE DU DOCUMENT**

| Version | Date | Description | Détails |
| --- | --- | --- | --- |
| 1.0 | 22/05/2024 | Création du document |  |
|  |  |  |  |
|  |  |  |  |

Table des matières

[1 Fourniture de services SaaS 5](#_Toc197695961)

[2 Politiques de sécurité de l’information et gestion du risque 6](#_Toc197695962)

[3 Organisation de la sécurité de l’information 6](#_Toc197695963)

[3.1 Fonctions et responsabilités liées à la sécurité de l’information 6](#_Toc197695964)

[3.1.1 Séparation des tâches 6](#_Toc197695965)

[3.1.2 Relations avec les autorités 7](#_Toc197695966)

[3.1.3 Relations avec les groupes de travail spécialisés 7](#_Toc197695967)

[3.1.4 La sécurité de l’information dans la gestion de projet 7](#_Toc197695968)

[4 Sécurité des ressources humaines 8](#_Toc197695969)

[4.1 Conditions d’embauche 8](#_Toc197695970)

[4.2 Sensibilisation, apprentissage et formations à la sécurité de l’information 9](#_Toc197695971)

[5 Gestion des actifs 10](#_Toc197695972)

[5.1 Inventaire et propriété des actifs 10](#_Toc197695973)

[6 Contrôle d’accès et gestion des identités 10](#_Toc197695974)

[6.1 Gestion des droits d’accès 10](#_Toc197695975)

[6.2 Revue des droits d’accès utilisateurs 11](#_Toc197695976)

[6.3 Gestion des authentifications des utilisateurs 11](#_Toc197695977)

[6.4 Restriction des accès à l’information 11](#_Toc197695978)

[7 Cryptologie 13](#_Toc197695979)

[7.1 Chiffrement des données stockées 13](#_Toc197695980)

[7.2 Chiffrement des flux 13](#_Toc197695981)

[8 Sécurité liée à l’exploitation 14](#_Toc197695982)

[8.1 Procédures d’exploitation documentées 14](#_Toc197695983)

[8.2 Gestion des changements 14](#_Toc197695984)

[8.3 Mesures contre les codes malveillants 15](#_Toc197695985)

[8.4 Sauvegarde des informations 15](#_Toc197695986)

[8.5 Journalisation des événements 16](#_Toc197695987)

[8.6 Protection de l’information journalisée 17](#_Toc197695988)

[8.7 Synchronisation des horloges 17](#_Toc197695989)

[8.8 Analyse et corrélation des événements 18](#_Toc197695990)

[8.9 Installation de logiciels sur des systèmes en exploitation 18](#_Toc197695991)

[8.10 Gestion des vulnérabilités techniques 19](#_Toc197695992)

[8.11 Administration 19](#_Toc197695993)

[9 Sécurité des communications 20](#_Toc197695994)

[9.1 Cartographie du système d'information. 20](#_Toc197695995)

[9.2 Cloisonnement des réseaux 20](#_Toc197695996)

[9.3 Surveillance des réseaux 20](#_Toc197695997)

[10 Acquisition, développement et maintenance des systèmes d’information 21](#_Toc197695998)

[10.1 Politique de développement sécurisé 21](#_Toc197695999)

[10.2 Procédures de contrôle des changements de système 21](#_Toc197696000)

[10.3 Revue technique des applications après changement apporté à la plateforme d’exploitation 22](#_Toc197696001)

[10.4 Environnement de développement sécurisé 23](#_Toc197696002)

[10.5 Développement externalisé 23](#_Toc197696003)

[10.6 Test de la sécurité et conformité du système 23](#_Toc197696004)

[10.7 Engagements de confidentialité 24](#_Toc197696005)

[11 Gestion des incidents liés à la sécurité de l’information 25](#_Toc197696006)

[11.1 Responsabilités et procédures 25](#_Toc197696007)

[11.2 Signalements liés à la sécurité de l’information 25](#_Toc197696008)

[11.3 Appréciation des événements liés à la sécurité de l’information et prise de décision 25](#_Toc197696009)

[11.4 Réponse aux incidents liés à la sécurité de l’information 25](#_Toc197696010)

[11.5 Tirer des enseignements des incidents liés à la sécurité de l’information 25](#_Toc197696011)

[11.6 Recueil de preuves 25](#_Toc197696012)

[12 Continuité d’activité 26](#_Toc197696013)

[12.1 Organisation de la continuité d’activité 26](#_Toc197696014)

[13 Conformité 27](#_Toc197696015)

[13.1 Identification de la législation et des exigences contractuelles applicables 27](#_Toc197696016)

[13.2 Revue indépendante de la sécurité de l’information 27](#_Toc197696017)

# Fourniture de services SaaS

Ce service concerne la mise à disposition par le prestataire d’applications hébergées sur une plateforme d’informatique en nuage. Le commanditaire n’a pas la maîtrise de la plateforme en nuage sous-jacente. Le prestataire gère de façon transparente pour le commanditaire l’ensemble des aspects techniques requérant des compétences informatiques. Le commanditaire garde la possibilité d’effectuer quelques paramétrages métier dans l’application.

Exemples : « CRM », outils collaboratifs, messagerie, Business Intelligence, « ERP », etc.

Ces exigences de sécurité s’appuient sur le référentiel SecNumCloud de l’ANSSI :

<https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf>

Un cadre de réponse est proposé au soumissionnaire selon le cas pour un chapitre entier ou pour un sous chapitre :

|  |
| --- |
| *Exemple de cadre de réponse,* |

# Politiques de sécurité de l’information et gestion du risque

Principes

Le prestataire doit opérer la prestation à l’état de l’art pour le type d’activité retenu : utiliser des logiciels stables bénéficiant d’un suivi des correctifs de sécurité et paramétrés de façon à obtenir un niveau de sécurité optimal.

Le prestataire doit appliquer le guide d’hygiène informatique de l’ANSSI [HYGIENE], niveau renforcé, au système d’information du service.

1. Politique de sécurité de l’information

Le prestataire doit documenter et mettre en œuvre une politique de sécurité de l’information relative au service.

2. Appréciation des risques

Le prestataire doit documenter une appréciation des risques couvrant l’ensemble du périmètre du service.

 Décrivez ci-dessous comment vous répondez à ces exigences

|  |
| --- |
| *Cadre de réponse* |

# Organisation de la sécurité de l’information

## Fonctions et responsabilités liées à la sécurité de l’information

Le prestataire doit documenter et mettre en œuvre une organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l’information au sein de son organisation.

### Séparation des tâches

Le prestataire doit identifier les risques associés à des cumuls de responsabilités ou de tâches, les prendre en compte dans l’appréciation des risques et mettre en œuvre des mesures de réduction de ces risques.

### Relations avec les autorités

Il est recommandé que le prestataire mette en place des relations appropriées avec les autorités compétentes en matière de sécurité de l’information et de données à caractère personnel et, le cas échéant, avec les autorités sectorielles selon la nature des informations confiées par le commanditaire au prestataire.

### Relations avec les groupes de travail spécialisés

Il est recommandé que le prestataire entretienne des contacts appropriés avec des groupes de spécialistes ou des sources reconnues, notamment pour prendre en compte de nouvelles menaces et les mesures de sécurité appropriées pour les contrer.

### La sécurité de l’information dans la gestion de projet

Le prestataire doit documenter une estimation des risques préalablement à tout projet pouvant avoir un impact sur le service, et ce quelle que soit la nature du projet.

Dans la mesure où un projet affecte ou est susceptible d’affecter le niveau de sécurité du service, le prestataire doit avertir le commanditaire et l’informer par écrit des impacts potentiels, des mesures mises en place pour réduire ces impacts ainsi que des risques résiduels le concernant.

Décrivez ci-dessous comment vous répondez aux exigences du Chapitre Organisation de la sécurité de l’information

|  |
| --- |
| *Cadre de réponse* |

# Sécurité des ressources humaines

## Conditions d’embauche

Le prestataire doit disposer d’une charte d’éthique intégrée au règlement intérieur, prévoyant notamment que :

* les prestations sont réalisées avec loyauté, discrétion et impartialité et dans des conditions de confidentialité des informations traitées ;
* les personnels ne recourent qu’aux méthodes, outils et techniques validés par le prestataire ;
* les personnels s’engagent à ne pas divulguer d’informations à un tiers, même anonymisées et décontextualisées, obtenues ou générées dans le cadre de la prestation sauf autorisation formelle et écrite du commanditaire ;
* les personnels s’engagent à signaler au prestataire tout contenu manifestement illicite découvert pendant la prestation ;
* les personnels s’engagent à respecter la législation et la réglementation nationale en vigueur et les bonnes pratiques liées à leurs activités.

Le prestataire doit faire signer la charte d’éthique à l’ensemble des personnes impliquées dans la fourniture du service.

Décrivez ci-dessous comment vous répondez à ces exigences

|  |
| --- |
| *Cadre de réponse* |

## Sensibilisation, apprentissage et formations à la sécurité de l’information

Le prestataire doit sensibiliser à la sécurité de l’information et aux risques liés à la protection des données l’ensemble des personnes impliquées dans la fourniture du service. Il doit leur communiquer les mises à jour des politiques et procédures pertinentes dans le cadre de leurs missions.

  Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

# Gestion des actifs

## Inventaire et propriété des actifs

Le prestataire doit tenir à jour l’inventaire de l’ensemble des équipements mettant en œuvre le service. Cet inventaire doit préciser pour chaque équipement :

* les informations d’identification de l’équipement (noms, adresses IP, adresses MAC, etc.) ;
* la fonction de l’équipement ;
* le modèle de l’équipement ;
* la localisation de l’équipement ;
* le propriétaire de l’équipement ;

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

# Contrôle d’accès et gestion des identités

Le prestataire doit documenter et mettre en œuvre une politique de contrôle d’accès sur la base du résultat de son appréciation des risques et du partage des responsabilités.

## Gestion des droits d’accès

Le prestataire doit documenter et mettre en œuvre une procédure permettant d’assurer l’attribution, la modification et le retrait de droits d’accès aux ressources du système d’information du service.

Le prestataire doit mettre à la disposition de ses commanditaires les outils et les moyens qui permettent une différenciation des rôles des utilisateurs du service, par exemple suivant leur rôle fonctionnel.

Le prestataire doit tenir à jour l’inventaire des utilisateurs sous sa responsabilité disposant de droits d’administration sur les ressources du système d’information du service.

Le prestataire doit être en mesure de fournir, pour une ressource donnée mettant en œuvre le service, la liste de tous les utilisateurs y ayant accès, qu’ils soient sous la responsabilité du prestataire ou du commanditaire ainsi que les droits d’accès qui leurs ont été attribués.

Le prestataire doit être en mesure de fournir, pour un utilisateur donné, qu’ils soient sous la responsabilité du prestataire ou du commanditaire, la liste de tous ses droits d’accès sur les différents éléments du système d’information du service.

Le prestataire doit définir une liste de droits d’accès incompatibles entre eux. Il 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.

Le prestataire doit inclure dans la procédure de gestion des droits d’accès les actions de révocation ou de suspension des droits de tout utilisateur.

## Revue des droits d’accès utilisateurs

Le prestataire doit réviser annuellement les droits d’accès des utilisateurs sur son périmètre de responsabilité.

## Gestion des authentifications des utilisateurs

Le prestataire doit formaliser et mettre en œuvre des procédures de gestion de l’authentification des utilisateurs. En accord avec les exigences du chapitre 10, celles-ci doivent notamment porter sur :

la gestion des moyens d’authentification (émission et réinitialisation de mot de passe, mise à jour des CRL et import des certificats racines en cas d’utilisation de certificats, etc.).

la mise en place des moyens permettant une authentification à multiples facteurs afin de répondre aux différents cas d’usage du référentiel.

les systèmes qui génèrent des mots de passe ou vérifient leur robustesse, lorsqu’une authentification par mot de passe est utilisée. Ils doivent suivre les recommandations de [G\_AUTH].

Tout mécanisme d’authentification doit prévoir le blocage d’un compte après un nombre limité de tentatives infructueuses.

Dans le cadre d’un service SaaS, le prestataire doit proposer à ses commanditaires des moyens d’authentification à multiples facteurs pour l’accès des utilisateurs finaux.

Lorsque des comptes techniques, non nominatifs, sont nécessaires, le prestataire doit mettre en place des mesures obligeant les utilisateurs à s’authentifier avec leur compte nominatif avant de pouvoir accéder à ces comptes techniques.

## Restriction des accès à l’information

Le prestataire doit mettre en œuvre des mesures de cloisonnement appropriées entre ses commanditaires.

Décrivez ci-dessous comment vous répondez aux exigences du chapitre Contrôle d’accès et gestion des identités

|  |
| --- |
| *Cadre de réponse* |

# Cryptologie

## Chiffrement des données stockées

Le prestataire doit définir et mettre en œuvre un mécanisme de chiffrement empêchant la récupération des données des commanditaires en cas de réallocation d’une ressource ou de récupération du support physique.

## Chiffrement des flux

Lorsque le prestataire met en œuvre un mécanisme de chiffrement des flux réseau, celui-ci doit respecter les règles de [CRYPTO\_B1].

Lorsque le prestataire met en œuvre un mécanisme de chiffrement des flux réseau, il est recommandé que celui-ci respecte les recommandations de [CRYPTO\_B1].

Si le protocole TLS est mis en œuvre, le prestataire doit appliquer les recommandations de [NT\_TLS].

Si le protocole IPsec est mis en œuvre, le prestataire doit appliquer les recommandations de [NT\_IPSEC].

Si le protocole SSH est mis en œuvre, le prestataire doit appliquer les recommandations de [NT\_SSH].

  Décrivez ci-dessous comment vous répondez aux exigences du chapitre Cryptologie

|  |
| --- |
| *Cadre de réponse* |

# Sécurité liée à l’exploitation

## Procédures d’exploitation documentées

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

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Gestion des changements

Le prestataire doit documenter et mettre en œuvre une procédure de gestion des changements apportés aux systèmes et moyens de traitement de l’information.

Séparation des environnements de développement, de test et d’exploitation

Le prestataire doit documenter et mettre en œuvre les mesures permettant de séparer physiquement les environnements liés à la production du service des autres environnements, dont les environnements de développement.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Mesures contre les codes malveillants

Le prestataire doit documenter et mettre en œuvre les mesures de détection, de prévention et de restauration pour se protéger des codes malveillants. Le périmètre d’application de cette exigence sur le système d’information du service doit nécessairement contenir les postes utilisateurs sous la responsabilité du prestataire et les flux entrants sur ce même système d’information.

Le prestataire doit documenter et mettre en œuvre une sensibilisation de ses employés aux risques liés aux codes malveillants et aux bonnes pratiques pour réduire l’impact d’une infection.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Sauvegarde des informations

Le prestataire doit documenter et mettre en œuvre une politique de sauvegarde et de restauration des données sous sa responsabilité dans le cadre du service. Cette politique doit prévoir une sauvegarde quotidienne de l’ensemble des données (informations, logiciels, configurations, etc.) sous la responsabilité du prestataire dans le cadre du service.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Journalisation des événements

Le prestataire doit documenter et mettre en œuvre une politique de journalisation incluant au minimum les éléments suivants : - la liste des sources de collecte ;

* la liste des événements à journaliser par source ;
* l’objet de la journalisation par événement ;
* la fréquence de la collecte et base de temps utilisée ;
* la durée de rétention locale et centralisée ;
* les mesures de protection des journaux (dont chiffrement et duplication) ; - la localisation des journaux.
* Le prestataire doit générer et collecter les événements suivants :
* les activités des utilisateurs liées à la sécurité de l’information ;
* la modification des droits d’accès dans le périmètre de sa responsabilité ;
* les événements issus des mécanismes de lutte contre les codes malveillants
* les exceptions ;
* les défaillances ;
* tout autre événement lié à la sécurité de l’information.

Le prestataire doit conserver les événements issus de la journalisation pendant une durée minimale de six mois sous réserve du respect des exigences légales et réglementaires.

Le prestataire doit fournir, sur demande d’un commanditaire, l’ensemble des événements le concernant.

Il est recommandé que le système de journalisation mis en place par le prestataire respecte les recommandations de [NT\_JOURNAL].

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Protection de l’information journalisée

Le prestataire doit protéger les équipements de journalisation et les événements journalisés contre les atteintes à leur disponibilité, intégrité ou confidentialité, conformément au chapitre 3.2 de

[NT\_JOURNAL].

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Synchronisation des horloges

Le prestataire doit documenter et mettre en œuvre une synchronisation des horloges de l’ensemble des équipements sur une ou 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.

Le prestataire doit mettre en place l’horodatage de chaque événement journalisé.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Analyse et corrélation des événements

Le prestataire doit documenter et mettre en œuvre une infrastructure permettant l’analyse et la corrélation des événements enregistrés par le système de journalisation afin de détecter les événements susceptibles d’affecter la sécurité du système d’information du service, en temps réel ou a posteriori pour des événements remontant jusqu’à six mois.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Installation de logiciels sur des systèmes en exploitation

Le prestataire doit documenter et mettre en œuvre une procédure permettant de contrôler l’installation de logiciels sur les équipements du système d’information du service.

Le prestataire doit documenter et mettre en œuvre une procédure de gestion de la configuration des environnements logiciels mis à la disposition du commanditaire, notamment pour leur maintien en condition de sécurité.

Le prestataire doit fournir une capacité d'inspection et de suppression, si nécessaire, des entrants

(contrôle de l’authenticité et de l'innocuité des mises à jour, contrôle de l’innocuité des outils fournis, etc.) relatifs au périmètre de l’infrastructure technique :

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

3 Les entrants sont ici constitués des éléments nécessaires et spécifiques à l’installation de logiciel considérée : éléments logiciels à installer, outils d’installation fournis, etc.

## Gestion des vulnérabilités techniques

Le prestataire doit documenter et mettre en œuvre un processus de veille permettant de gérer les vulnérabilités techniques des logiciels et des systèmes utilisés dans le système d’information du service.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Administration

Le prestataire doit documenter et mettre en œuvre une procédure obligeant les administrateurs sous sa responsabilité à utiliser des terminaux dédiés pour la réalisation exclusive des tâches d’administration, en accord avec le chapitre 4.1 intitulé « poste et réseau d’administration » de [NT\_ADMIN]. Il doit les maîtriser et les maintenir à jour.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

# Sécurité des communications

## Cartographie du système d'information.

Le prestataire doit établir et tenir à jour une cartographie du système d’information du service, en lien avec l’inventaire des actifs, comprenant au minimum les éléments suivants :

## Cloisonnement des réseaux

Le prestataire doit documenter et mettre en œuvre, pour le système d’information du service, les mesures de cloisonnement (logique, physique ou par chiffrement) pour séparer les flux réseau selon :

la sensibilité des informations transmises ;

la nature des flux (production, administration, supervision, etc.) ;

le domaine d’appartenance des flux (des commanditaires – avec distinction par commanditaire ou ensemble de commanditaires, du prestataire, des tiers, etc.) ; - le domaine technique (traitement, stockage, etc.).

## Surveillance des réseaux

Le prestataire doit disposer une ou plusieurs sondes de détection d’incidents de sécurité sur le système d’information du service. Ces sondes doivent notamment permettre la supervision de chacune des interconnexions du système d’information du service avec des systèmes d’information tiers et des réseaux publics. Ces sondes doivent être des sources de collecte pour l’infrastructure d’analyse et de corrélation des événements

  Décrivez ci-dessous comment vous répondez aux exigences du chapitre Sécurité des communications

|  |
| --- |
| *Cadre de réponse* |

# Acquisition, développement et maintenance des systèmes d’information

## Politique de développement sécurisé

Le prestataire doit documenter et mettre en œuvre des règles de développement sécurisé des logiciels et des systèmes, et les appliquer aux développements internes.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Procédures de contrôle des changements de système

Le prestataire doit documenter et mettre en œuvre une procédure de contrôle des changements apportés au système d’information du service.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Revue technique des applications après changement apporté à la plateforme d’exploitation

Le prestataire doit documenter et mettre en œuvre une procédure permettant de tester, préalablement à leur mise en production, l’ensemble des applications afin de vérifier l’absence de tout effet indésirable sur l’activité ou sur la sécurité du service.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

## Environnement de développement sécurisé

Le prestataire doit mettre en œuvre un environnement sécurisé de développement permettant de gérer l’intégralité du cycle de développement du système d’information du service.

## Développement externalisé

a) Le prestataire doit documenter et mettre en œuvre une procédure permettant de superviser et de contrôler l’activité de développement externalisé des logiciels et des systèmes. Cette procédure doit s’assurer que l’activité de développement externalisé soit conforme à la politique de développement sécurisé du prestataire et permette d’atteindre un niveau de sécurité du développement externe équivalent à celui d’un développement interne (voir exigence 14.1 a).

## Test de la sécurité et conformité du système

a) Le prestataire doit soumettre les systèmes d’information, nouveaux ou mis à jour, à des tests de conformité et de fonctionnalité de sécurité pendant le développement. Il doit documenter et mettre en œuvre une procédure de test qui identifie : - les tâches à réaliser ;

les données d’entrée ;

les résultats attendus en sortie.

Décrivez ci-dessous comment vous répondez à ces 3 exigences

|  |
| --- |
| *Cadre de réponse* |

## Engagements de confidentialité

Le prestataire doit documenter et mettre en œuvre une procédure permettant de réviser au moins annuellement les exigences en matière d’engagements de confidentialité ou de non-divulgation vis-à-vis des tiers participant à la mise en œuvre du service.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

# Gestion des incidents liés à la sécurité de l’information

## Responsabilités et procédures

Le prestataire doit documenter et mettre en œuvre une procédure permettant d’apporter des réponses rapides et efficaces aux incidents de sécurité. Ces procédures doivent définir les moyens et délais de communication des incidents de sécurité à l’ensemble des commanditaires concernés ainsi que le niveau de confidentialité exigé pour cette communication.

## Signalements liés à la sécurité de l’information

Le prestataire doit documenter et mettre en œuvre une procédure exigeant de ses employés et des tiers participant à la mise en œuvre du service qu’ils lui rendent compte de tout incident de sécurité, avéré ou suspecté ainsi que de toute faille de sécurité.

## Appréciation des événements liés à la sécurité de l’information et prise de décision

Le prestataire doit apprécier les événements liés à la sécurité de l’information et décider s’il faut les qualifier en incidents de sécurité. Pour l’appréciation, il doit s’appuyer sur une ou plusieurs échelles (estimation, évaluation, etc.) partagées avec le commanditaire.

Note : Les incidents de sécurité incluent les violations de données à caractère personnel.

## Réponse aux incidents liés à la sécurité de l’information

a) Le prestataire doit traiter les incidents de sécurité jusqu’à leur résolution et doit informer les commanditaires conformément aux procédures.

## Tirer des enseignements des incidents liés à la sécurité de l’information

a) Le prestataire doit documenter et mettre en œuvre un processus d’amélioration continue afin de diminuer l’occurrence et l’impact de types d’incidents de sécurité déjà traités.

## Recueil de preuves

Le prestataire doit documenter et mettre en œuvre une procédure permettant d’enregistrer les informations relatives aux incidents de sécurité et pouvant servir d’éléments de preuve.

Décrivez ci-dessous comment vous répondez aux exigences du chapitre Gestion des incidents liés à la sécurité de l’information

|  |
| --- |
| *Cadre de réponse* |

# Continuité d’activité

## Organisation de la continuité d’activité

Le prestataire doit documenter et mettre œuvre un plan de continuité d’activité prenant en compte la sécurité de l’information.

Décrivez ci-dessous comment vous répondez à cette exigence

|  |
| --- |
| *Cadre de réponse* |

# Conformité

## Identification de la législation et des exigences contractuelles applicables

Le prestataire doit identifier les exigences légales, réglementaires et contractuelles en vigueur applicables au service. En France, le prestataire doit considérer au minimum les textes suivants :

## Revue indépendante de la sécurité de l’information

Revue des changements majeurs.

En cas de changement majeur pouvant affecter le service, le prestataire doit faire réaliser une revue indépendante de changement par un prestataire d’audit de la sécurité des systèmes d’information [PASSI] qualifié. Cette revue indépendante de changement doit couvrir en particulier les activités d’audit suivantes :

* audit d’architecture ;
* audit organisationnel et physique ;
* audit de la configuration de l’infrastructure technique du service ;
* un test d’intrusion portant sur les interfaces d'administration du service mises à disposition des commanditaires;

pour un service de type SaaS, un test d'intrusion portant sur l'interface mise à disposition des utilisateurs finaux dans le cadre du catalogue de services, ainsi qu'un audit du code source portant sur les fonctionnalités de sécurité implémentées (authentification, gestion des sessions, gestion du cloisonnement en cas de mode multi-tenant). Si le SaaS rend un service de sécurité de l'information, une certification produit dédiée est nécessaire.

Décrivez ci-dessous comment vous répondez aux exigences du chapitre Conformité

|  |
| --- |
| *Cadre de réponse* |