Annexe à l'arrêté du Chef du gouvernement n° 3-17-25 du 7 safar 1447 (1er août 2025) fixant le référentiel des exigences de qualification des prestataires de services Cloud

RÉFÉRENTIEL DES EXIGENCES DE QUALIFICATION DES PRESTATAIRES DE SERVICES CLOUD

1. Contexte et objectifs

Les responsables des entités et infrastructures d'importance vitale doivent, lorsqu'ils ont recours à des services Cloud pour l'hébergement, la gestion ou l'exploitation de leurs systèmes ou données sensibles, faire appel à des prestataires qualifiés par l'autorité nationale de cybersécurité (Direction Générale de la Sécurité des Systémes d'Information), selon les dispositions prévues par le décret n° 2-24-921 du 18 rabii II 1446 (22 octobre 2024) relatif au recours aux prestataires de services Cloud par les entités et les infrastructures d'importance vitale disposant de systèmes d'information ou de données sensibles.

Le présent référentiel, qui s'inspire des meilleures pratiques internationales, définit les exigences spécifiques auxquelles doit se conformer un prestataire de services cloud, désigné ci-après par « prestataire de services », pour être qualifié à fournir des services conformément aux dispositions du décret précité.

2. Processus de qualification

Le processus de qualification se déroule en quatre (04) étapes conformément aux exigences des articles 6,7,8,9 et 10 du décret précité n°2-24-921.

Le modèle de demande de qualification ainsi que les modèles d'engagement constituant le dossier de qualification sont publiés sur le site web de l'autorité nationale de cybersécurité.

En ce qui concerne l'examen du dossier, l'autorité nationale de cybersécurité peut demander, en plus des documents requis au titre de l'article 6 du décret n°2-24-921, tous documents ou informations complémentaires utiles à l'instruction du dossier concernant le prestataire de services lui-même ou un ou plusieurs de ses sous-traitants. Elle peut aussi demander toute explication ou justification, notamment au sujet des statuts de la société, de l'identité des associés, des personnes impliquées dans la gestion et l'exploitation des services ou des attestations de référence.

3. Exigences de qualification des Prestataires de services cloud :

Dans le cadre de la qualification, les exigences ci-après détaillées sont opposables aux prestataires de services uniquement sur le périmètre (systèmes et plateformes) qui est sous leur responsabilités. Le modèle de répartition des responsabilités entre prestataire de services et l'entité ou l'infrastructure d'importance vitale disposant de systèmes d'information ou de données sensibles désignées dans le présent référentiel par « commanditaire », est donné à titre indicatif.

IaaS	PaaS	SaaS
Données	Données	Données
Applications	Applications	Applications
Runtimes	Runtimes	Runtimes
Middlewares	Middlewares	Middlewares
Systèmes d'Exploitation	Systèmes d'Exploitation	Systèmes d'Exploitation
Virtualisation	Virtualisation	Virtualisation
Serveurs	Serveurs	Serveurs
Stockage	Stockage	Stockage
Réseaux	Réseaux	Réseaux

: Responsabilité du prestataire de services

: Responsabilité du commanditaire

Sont assimilés à des services IaaS dans le cadre du présent référentiel les prestations de type hébergement externe classique qu'il soit dédié ou partagé. Les services de colocation ne sont pas régis par le présent référentiel.

3.1. Politiques de sécurité de l'information et gestion du risque

Ce chapitre a pour objet de garantir que le prestataire de services dispose de politiques et d'instructions en matière de sécurité qui couvrent les exigences de sécurité tout en soutenant les besoins métier liés à la fourniture du service. Ces politiques doivent être clairement définies, accessibles et suivies pour assurer la conformité et la gestion des risques de sécurité.

3.1.1. Politique de sécurité des systèmes d'information

Le prestataire de services doit élaborer une politique de sécurité des systèmes d'information pour son service qui doit être approuvée formellement par la direction du prestataire de services, et qui doit respecter les dispositions des textes législatifs et réglementaires nationaux, ainsi que les normes et les référentiels en vigueur notamment celles du présent référentiel qui fixe les critères de qualification.

Cette politique doit être communiquée et mise à disposition de manière appropriée à toutes les parties prenantes concernées internes et externes au prestataire de services.

Elle doit être mise à jour régulièrement, et autant de fois que survient un changement majeur susceptible d'affecter le service.

La politique de sécurité des systèmes d'information **doit** être révisée au moins annuellement par le prestataire de services. La révision doit prendre en compte au minimum :

- Les changements organisationnels et techniques dans la fourniture du service cloud.
- Les changements législatifs et réglementaires affectant l'environnement du prestataire de services.

3.1.2. Analyse des risques

Le prestataire de services doit mener et documenter une analyse du risque pour l'ensemble du périmètre du service en utilisant une méthode documentée garantissant la reproductibilité et la compatibilité de la démarche.

Le prestataire de services doit prendre notamment en considération lors de l'analyse des risques :

- Les différents besoins de sécurité en matière de confidentialité, disponibilité et intégrité qui peuvent émaner des commanditaires ;
- Les risques susceptibles d'affecter un ou plusieurs de ces critères de sécurité ;
- Les risques liés à une défaillance des mécanismes de séparation des ressources de l'infrastructure technique (mémoire, calcul, stockage, réseau) partagées entre différents commanditaires ;
- Les risques associés à l'effacement incomplet ou non sécurisé des données stockées sur les espaces de mémoire ou de stockage partagés entre commanditaires, en particulier lors des réallocations de ces espaces ;
- Les risques liés à l'exposition des interfaces d'administration sur un réseau public ;
- Risques organisationnels et techniques découlant de dépendances vis-à-vis de tiers (fournisseurs, sous-traitants, etc.) ;

— Les risques liés aux évènements naturels et sinistres physiques ;

— Les risques liés à la séparation des tâches ;

— Les risques liés aux environnements de développement.

Le prestataire de services doit lister, dans un document spécifique, les risques éventuels liés à l'existence de législations étrangères ayant pour objectif la collecte de données ou métadonnées des commanditaires sans leur consentement préalable. Ce document doit être communiqué aux commanditaires à leur demande.

La direction du prestataire de services doit approuver les risques résiduels identifiés dans l'appréciation des risques.

Le prestataire de services doit mettre à jour le registre des risques suite à une analyse des risques annuelle et à chaque fois qu'un changement significatif susceptible d'impacter le service se produit.

3.2. Organisation de la sécurité de l'information

3.2.1. Rôles et responsabilités

Le prestataire de services doit créer et mettre en place une organisation interne dédiée à la sécurité afin d'assurer la définition, l'implémentation et le suivi du fonctionnement opérationnel de la sécurité du système d'information au sein de son organisation.

Le prestataire de services doit désigner un responsable de la sécurité des systèmes d'information et un responsable de la sécurité physique.

Le prestataire de services doit clairement définir et attribuer les responsabilités en matière de sécurité du système d'information pour le personnel impliqué dans la prestation du service.

Le prestataire de services doit vérifier que les responsabilités en matière de sécurité de l'information restent pertinentes après tout changement majeur susceptible d'affecter le service.

3.2.2. Séparation des tâches

Le prestataire de services doit identifier les risques associés à des cumules de responsabilités ou de taches, les prendre en compte dans l'appréciation des risques et mettre en œuvre des mesures pour réduire ces risques.

3.2.3. Relations avec les autorités

Le prestataire de services doit établir des relations appropriées avec les autorités compétentes en matière de cyber sécurité et de protection de données à caractère personnel, et le cas échéant avec les régulateurs sectoriels concernés, selon la nature des informations confiées par le commanditaire au prestataire de services.

3.2.4. La sécurité de l'information dans la gestion de projet

Le prestataire de services doit établir une documentation comprenant une estimation des risques avant tout projet susceptible d'avoir un impact sur le service, et ce quelle que soit la nature du projet.

En cas d'impact potentiel sur la sécurité du service, le prestataire de services doit informer par écrit le commanditaire et l'autorité nationale de cybersécurité des impacts potentiels, des mesures d'atténuation mises en place et des risques résiduels y associés.

3.3. Sécurité des ressources humaines

3.3.1. Personnel de confiance

A l'embauche, le prestataire de services doit mettre en œuvre une procédure de vérifications des informations des candidats conformément à la réglementation en vigueur, à l'éthique, aux exigences métier et à la classification des actifs informationnels accessibles.

Le prestataire de services doit renforcer ces vérifications pour s'assurer que les antécédents du personnel disposant de privilèges d'administration étendus sur les composants logiciels et matériels de l'infrastructure ne posent aucun risque quant aux responsabilités qui leur sont confiées.

3.3.2. Termes et Conditions d'embauche

Une charte doit être élaborée par le prestataire de services en conformité avec la politique de sécurité des systèmes d'information. Elle doit être validée par la hiérarchie, communiqué et signée ou acceptée par l'ensemble des personnes impliquées dans la fourniture du service.

Cette charte doit contenir, entre autres :

- Un rappel des exigences législatives et réglementaires applicables dans le contexte de l'activité ;
- Les règles générales d'utilisation des ressources informatiques notamment les méthodes, outils et techniques validés par le prestataire de services ;
- Les clauses de confidentialité et non divulgation des informations manipulées.

Le prestataire de services doit inclure, dans les contrats de travail du personnel ayant des privilèges d'administration élevés sur l'infrastructure du service, un engagement de responsabilité, en lien avec la protection du secret professionnel et de la propriété intellectuelle. Les privilèges d'administrations élevés concernent des actions telles que l'élévation de privilèges, la réalisation d'actions sans traces techniques, et la possibilité de désactiver ou altérer ces traces.

3.3.3. Formation et sensibilisation du personnel

Le prestataire de services doit veiller à ce que les employés soient sensibilisés à leurs responsabilités en matière de sécurité des systèmes d'information et aux moyens dont ils disposent pour s'acquitter de ces responsabilités.

Le prestataire de services doit organiser régulièrement, selon un programme préétabli et validé par le responsable de la sécurité des systèmes d'information (RSSI), des sessions de formation et de sensibilisation au profit de son personnel en matière de sécurité des systèmes d'information adapté au service et aux missions des personnels.

3.3.4. Processus disciplinaire

Le prestataire de services doit mettre en place un processus disciplinaire formel applicable à l'ensemble des personnes impliquées dans la fourniture du service qui enfreignent les règles de la politique de sécurité des systèmes d'information.

3.3.5. Rupture, terme ou modification du contrat de travail

Afin de préserver la confidentialité et l'intégrité de l'information de ses commanditaires, le prestataire de services doit définir et assigner dans les contrats de travail les responsabilités liés à la

confidentialité et à la non-divulgation suite à la résiliation, à la rupture ou à la modification de tout contrat avec une personne impliquée dans la prestation du service.

3.4. Gestion des actifs

3.4.1. Inventaire et propriété des actifs

Le prestataire de services doit tenir à jour un inventaire de l'ensemble des équipements utilisés pour fournir le service. Cet inventaire doit préciser pour chaque équipement :

- Les identifiants (noms, adresses IP, adresse MAC, etc.) ;
- La fonction ;
- Le modèle ;
- La localisation ;
- Le propriétaire ;
- Les besoins de sécurité[1].

Le prestataire de services doit tenir à jour un inventaire de l'ensemble des logiciels utilisés pour le service, et qui précise, pour chaque logiciel, sa version et les équipements sur lesquels il est installé.

Le prestataire de services doit s'assurer de la validité des licences des logiciels durant la prestation de service.

3.4.2. Classification des actifs

Les actifs doivent être classifiés et, si possible, étiquetés en fonction des besoins de protection de l'information qu'ils traitent, stockent ou transmettent. Cette classification doit être effectuée selon un schéma uniforme déterminé par les responsables des actifs et qui prend en compte les besoins de sécurité identifiés pour chaque actif.

3.4.3. Marquage et manipulation de l'information

Le prestataire de services doit mettre en place une procédure pour le marquage et la manipulation des informations nécessaires à la fourniture du service.

3.4.4.Gestion des supports amovibles

Le prestataire de services doit documenter et mettre en œuvre une procédure pour la gestion des supports amovibles, conformément aux besoins de sécurité relatifs à la fourniture du service.

Lorsque des supports amovibles sont utilisés sur l'infrastructure technique ou pour des tâches d'administration, ces supports doivent être dédiés à un usage spécifique.

3.4.5. Restitution des actifs

Le prestataire de services doit documenter et mettre en place une procédure de restitution des actifs permettant de s'assurer que chaque personne impliquée dans la prestation de service restitue tous les actifs en sa possession à la fin de son contrat.

[1] Le besoin de sécurité correspond à une propriété de sécurité à garantir pour un actif informationnel en matière de confidentialité, d'intégrité et de disponibilité.

3.4.6. Retrait du Matériel

Le retrait des matériels utilisés pour la fourniture du service cloud nécessite une approbation formelle du responsable de la sécurité des systèmes d'information et doit inclure la suppression complète et permanente des données ou la destruction appropriée des supports de stockage.

3.5. Contrôle d'accès et gestion des identités

3.5.1. Politique de contrôle d'accès

Le prestataire de services est tenu de mettre en place et de documenter une politique de contrôle d'accès aux systèmes, réseaux et services sur la base des exigences métier et de sécurité de l'information en respectant le principe du moindre privilège.

La politique de contrôle d'accès doit être mise à jour annuellement et à chaque changement majeur susceptible d'avoir un impact sur le service.

3.5.2. Enregistrement et désinscription des utilisateurs

Le prestataire de services doit mettre en œuvre et documenter une procédure formelle d'enregistrement et de désinscription des utilisateurs de systèmes d'information, destinée à permettre l'attribution de droits d'accès.

Le prestataire de services est tenu de créer des comptes nominatifs lors de l'enregistrement des utilisateurs placés sous sa responsabilité.

Le prestataire de services doit mettre en place des mesures et moyens nécessaires pour garantir que la désinscription d'un utilisateur entraîne la suppression de tous ses accès aux ressources du système d'information du service, ainsi que l'effacement de ses données, conformément à la procédure d'enregistrement et de désinscription des utilisateurs précitée.

3.5.3. Gestion des droits d'accès

Le prestataire de services est tenu de mettre en place et de documenter une procédure pour gérer l'attribution, la modification et le retrait des droits d'accès aux ressources du système d'information du service.

Le prestataire de services doit mettre à la disposition de ses commanditaires les outils et les moyens permettant de distinguer les rôles des utilisateurs du service, en fonction de leurs responsabilités fonctionnelles.

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

Le prestataire de services doit pouvoir fournir, pour chaque utilisateur créé par ses soins, qu'il soit sous sa responsabilité ou celle du commanditaire, la liste détaillée de tous les droits d'accès qu'il possède sur les différents actifs du système d'information du service.

Le prestataire de services doit établir une liste de droits d'accès incompatibles entre eux. Lors de l'attribution de droits d'accès à un utilisateur, il doit veiller à ce que cet utilisateur ne détienne pas de droits incompatibles au titre de la liste précédemment établie.

Le prestataire de services doit intégrer dans la procédure de gestion des droits d'accès les actions de révocation ou de suspension des droits pour tout utilisateur.

3.5.4. Revue des droits d'accès utilisateurs

Le prestataire de services doit effectuer une révision annuelle des droits d'accès des utilisateurs sur son périmètre de responsabilité.

Le prestataire de services doit fournir au commanditaire un outil permettant de faciliter l'examen des droits d'accès des utilisateurs sous sa responsabilité.

3.5.5. Gestion des authentifications des utilisateurs

Le prestataire de services doit documenter et mettre en œuvre une procédure de gestion des comptes utilisateurs et des droits d'accès pour les utilisateurs internes et externes, ainsi que pour les composants systèmes impliqués dans les processus d'autorisation automatisés. Cette procédure doit porter sur :

- L'assignation de noms d'utilisateur uniques, la gestion des droits d'accès basée sur le principe du moindre privilège et du besoin de savoir, ainsi que la séparation des tâches (par exemple, la gestion des comptes d'utilisateur séparée de l'approbation de l'accès) ;
- La gestion des moyens d'authentification, y compris l'émission et la réinitialisation des mots de passe, la mise à jour des listes de révocation de certificats (CRL) et l'importation des certificats racines en cas d'utilisation de certificats d'authentification, etc ;
- L'implémentation d'outils d'authentification multi-facteurs afin de répondre aux différents scénarios d'utilisation prévus au présent référentiel ;
- La mise en place des systèmes qui génèrent des mots de passe ou évaluent leur robustesse lorsque l'authentification par mot de passe est en place.

Tout mécanisme d'authentification doit inclure un verrouillage du compte après un nombre déterminé de tentatives échouées.

Dans le cadre d'un service SaaS, le prestataire de services doit offrir à ses commanditaires des solutions d'authentification multi-facteurs pour l'accès des utilisateurs finaux si besoin.

Lorsque des comptes techniques, non nominatifs, sont nécessaires, le prestataire de services doit mettre en place des mesures permettant aux utilisateurs de s'authentifier d'abord avec leur compte nominatif avant d'accéder à ces comptes techniques pour en assurer la traçabilité d'usage.

3.5.6. Accès aux interfaces d'administration

Les comptes d'administration sous la responsabilité du prestataire de services doivent être gérés à l'aide d'outils et d'annuaires séparés de ceux utilisés pour la gestion des comptes utilisateurs sous la responsabilité du commanditaire.

Les interfaces d'administration fournies aux commanditaires doivent être séparées de celles utilisées par le prestataire de services et ne doivent pas permettre de se connecter aux comptes d'administrateurs sous la responsabilité du prestataire de services.

Les interfaces d'administration utilisées par le prestataire de services ne doivent pas être accessibles depuis un réseau public, et ne doivent pas permettre la connexion des utilisateurs sous la responsabilité du commanditaire.

Dans le cadre d'un service SaaS, les interfaces d'administration fournies aux commanditaires doivent être distinctes de celles permettant l'accès des utilisateurs finaux.

Une authentification multi-facteurs doit être exigée avant toute interaction entre un utilisateur et une interface d'administration et les flux d'administration doivent être authentifiés et chiffrés conformément aux exigences du présent référentiel.

Lorsque le prestataire de services utilise un service IaaS comme socle technique pour fournir d'autres services de type PaaS ou SaaS, les ressources utilisées par le prestataire de services ne doivent jamais être accessibles via l'interface publique réservée aux commanditaires du service IaaS.

Lorsque le prestataire de services utilise un service PaaS comme socle technique pour fournir d'autres services de type SaaS, les ressources attribuées à l'usage du prestataire de services ne doivent en aucun cas être accessibles via l'interface publique destinée aux autres commanditaires du service PaaS.

3.5.7. Restriction des accès à l'information

Le prestataire de services doit mettre en place des mesures de séparation appropriées entre ses différents commanditaires.

Le prestataire de services doit instaurer des mesures de séparation adéquates entre le système d'information du service et ses autres systèmes d'information (bureautique, gestion informatique, gestion technique des bâtiments, contrôle d'accès physique, etc.).

Le prestataire de services doit concevoir, développer, configurer et déployer le système d'information du service en garantissant au minimum une séparation entre l'infrastructure technique et les équipements utilisés pour administrer les services et les ressources qu'elle héberge.

Dans le cadre du support technique, si le diagnostic et la résolution d'un problème rencontré par un commanditaire nécessitent un accès à ses données, le prestataire de services doit :

- N'autoriser l'accès aux données du commanditaire qu'après consentement explicite du commanditaire ;
- Vérifier que la personne à qui l'accès doit être autorisé a satisfait aux vérifications de l'exigence 3.3.1 du présent référentiel ;
- Considérer les actions menées, une fois l'accès autorisé, comme des actions d'administration et les journaliser comme telles ;
- Supprimer l'autorisation d'accès aux données du commanditaire au terme de ces actions.

Dans le cas d'une intervention réalisée à distance par une personne localisée hors du territoire marocain (Cas de prestaires de services qualifiés niveau 1), mettre en œuvre une passerelle sécurisée (poste de rebond) par laquelle la personne devra se connecter et permettant une supervision (autorisation ou interdiction des actions, demandes d'explications, etc..) en temps réel, par une personne ayant elle-même satisfait aux vérifications de l'exigence 3.3.1 du présent référentiel.

3.6. Cryptographie

3.6.1. Politique d'utilisation de la cryptographie et de la gestion des clés

Le prestataire de services doit documenter, communiquer et appliquer une politique de cryptographie qui couvre les procédures de cryptage et la gestion des clés. La politique d'utilisation de la cryptographie doit :

- Exiger l'utilisation de mécanismes cryptographiques et de protocoles de réseau sécurisés conformes aux meilleures pratiques de l'état de l'art ;

— Être alignée avec le schéma de classification de l'information en place ;

— Spécifier des exigences pour la génération, le stockage, l'archivage, la récupération, la distribution, le retrait et la suppression des clés ;

— Tenir compte des exigences juridiques en vigueur concernant la cryptographie, notamment la loi n°43-20 relative aux services de confiance pour les transactions électroniques et du décret n°2-22-687 du 21 rabii II 1444 (16 novembre 2022) pris pour son application.

3.6.2. Chiffrement des données en transmission

Le prestataire de services doit établir des procédures et des mesures techniques pour garantir que les données transmises sur les réseaux publics soient cryptées de manière sécurisée. L'accent est mis sur l'authentification et le cryptage des données en transit.

Le prestataire de services doit utiliser les versions les plus récentes et réputées sécurisées des protocoles de chiffrement des communications.

3.6.3. Chiffrement des données stockées

Le prestataire de services doit établir et déployer un mécanisme de chiffrement qui empêche la récupération des données des commanditaires lors de la réattribution d'une ressource ou de la récupération du support physique.

Dans le cas de service de Niveau 2, les clés privées utilisées pour ce cryptage doivent être uniquement connues du commanditaire :

- Dans le cas d'un service IaaS, cet objectif pourra être atteint :
  - Par un chiffrement du disque ou du système de fichier, lorsque le protocole d'accès en mode fichiers garantit que seuls des blocs vides peuvent être alloués (par exemple stockage de type NAS « Network Attached Storage ou serveur de stockage en réseau » dans lequel un bloc physique n'est effectivement affecté qu'au moment de l'écriture),
  - Par un chiffrement par volume dans le cas d'un accès en mode bloc (par exemple stockage de type SAN « Storage Area Network » ou stockage local), avec au moins une clé par commanditaire ;
- Dans le cas d'un service PaaS ou SaaS, cet objectif pourrait être atteint en mettant en œuvre un chiffrement applicatif au sein du périmètre du prestataire de services, où chaque commanditaire dispose au moins d'une clé de chiffrement dédiée.

Le prestataire de services doit utiliser une méthode de chiffrement des données respectant les règles et les bonnes pratiques de sécurité, à savoir :

— Utiliser des algorithmes de chiffrement reconnus pour leur fiabilité au niveau international ;

— S'assurer que les longueurs de clé sont suffisantes pour garantir la sécurité des données contre les attaques connues. Suivre les recommandations en matière de longueur de clé pour chaque algorithme utilisé ;

— Adapter le choix des mécanismes cryptographiques en fonction des besoins spécifiques de sécurité de chaque application ou contexte, en tenant compte de la sensibilité des données traitées.

Le prestataire de services doit appliquer un chiffrement aux données stockées sur les supports amovibles et les supports de sauvegarde qui doivent quitter le périmètre de sécurité physique du

système d'information du service en fonction des exigences de sécurité liées à la classification des données (voir exigence 3.4.2 du présent référentiel).

3.6.4. Hachage des mots de passe

Le prestataire de services doit uniquement conserver les empreintes des mots de passe des utilisateurs et des comptes techniques.

Le prestataire de services doit mettre en œuvre une fonction de hachage respectant les règles et les bonnes pratiques de sécurité, à savoir :

- Choisir des fonctions de hachage reconnues comme sûres et à jour, en évitant les algorithmes obsolètes ;
- Ajoutez un sel unique (une valeur aléatoire) à chaque mot de passe avant de le hacher pour empêcher les attaques par tables arc-en-ciel et renforcer la sécurité contre les attaques par dictionnaire ;
- S'assurer que la longueur du résultat du hachage est suffisante pour éviter les collisions (deux entrées produisant le même haché).

3.6.5. Non répudiation

Lorsque le prestataire de services met en œuvre un mécanisme de signature électronique pour assurer la non répudiation, il est recommandé que celui-ci fasse appel à des tiers prestataires de confiance déclarés auprès de l'autorité nationale en charge des services de confiance pour les transactions électroniques ou agréés par elle selon le niveau de signature adopté.

3.6.6. Gestion des clés

Le prestataire de services doit mettre en place des procédures et des mesures techniques pour la gestion complète du cycle de vie des clés, incluant la génération, la distribution, le stockage, l'utilisation, la révocation et la destruction. Ces procédures doivent tenir compte des éléments suivants :

- Stocker les clés de manière sécurisée en utilisant des dispositifs de protection appropriée ou des environnements sécurisés ;
- Utiliser des générateurs de clés cryptographiquement sécurisés et conformes aux standards internationaux relatifs à la cryptographie pour garantir l'imprévisibilité et la robustesse des clés ;
- S'assurer que les clés sont transmises de manière sécurisée, en utilisant des mécanismes de chiffrement appropriés pour éviter les interceptions ;
- Limiter l'accès aux clés aux seules personnes ou systèmes autorisés. Mettre en place des contrôles d'accès rigoureux et des politiques d'utilisation adéquates ;
- Mettre en place des procédures pour révoquer rapidement les clés compromises ou obsolètes. S'assurer que les clés révoquées ne peuvent plus être utilisées ;
- Définir des politiques d'expiration des clés pour garantir que les clés utilisées sont toujours valides et pertinentes ;
- Détruire les clés de manière sécurisée lorsqu'elles ne sont plus nécessaires, en s'assurant qu'elles ne peuvent pas être récupérées ou reconstituées.

3.7. Sécurité physique et environnementale

Garantir la prévention d'un accès physique non autorisé aux installations, ainsi que la protection contre le vol, les dommages, la perte ou l'interruption des opérations liées à ces services.

3.7.1. Périmètres de sécurité physique

Le prestataire de services doit mettre en place et documenter des mesures de sécurité qui comprennent le marquage des zones et les moyens de contrôle d'accès.

Le prestataire de services doit identifier des zones publiques, des zones privées et des zones sensibles.

Cette délimitation peut se faire selon la typologie suivante :

- **Zones publiques :** autorisées à toute personne. Aucune ressource dédiée au service ou permettant l'accès à ses composants ne doit être hébergée au niveau de ces zones.
- **Zones privées** : peuvent héberger :
    a) les plateformes et les outils de développement du service ;
    b) les postes d'administration, d'exploitation et de supervision ;
    c) les locaux à partir desquels le prestataire de services opère.
- **Zones sensibles :** Les zones sensibles sont exclusivement dédiées à l'hébergement du système d'information de production du service.

3.7.2. Contrôle d'accès physique

Le prestataire de services doit sécuriser les zones restreintes (Zones privées, zones sensibles) contre les accès non autorisés en mettant en place un dispositif de contrôle d'accès individualisé. Ce dispositif doit assurer la traçabilité des accès du personnel et des tiers autorisés et accompagnés aux zones restreintes, et conserver les enregistrements pour une durée d'au moins trois mois.

Le prestataire de services doit établir et documenter des protocoles spécifiques pour l'accès physique en situation d'urgence.

Le prestataire de services doit afficher à l'entrée des zones restreintes un avertissement indiquant les limites et les conditions d'accès à ces zones.

Le prestataire de services doit définir et documenter les plages horaires et les conditions d'accès aux différentes zones en fonction des profils des personnes autorisées à y accéder.

Le prestataire de services doit mettre en place et documenter des procédures pour accompagner systématiquement les visiteurs dans les zones restreintes et doit également assurer la traçabilité de l'identité des visiteurs conformément à la législation et la réglementation en vigueur.

En cas d'intervention (diagnostic, maintenance, ou administration) par un visiteur tiers dans une zone restreinte, le prestataire de services doit superviser ces actions par un personnel ayant satisfait aux vérifications de l'exigence spécifique 3.3.1 du présent référentiel.

Le prestataire de services doit mettre en place des systèmes de surveillance et de détection pour prévenir les accès non autorisés aux zones restreintes.

Le prestataire de services doit instaurer un système de journalisation des accès physiques aux zones sensibles et procéder à une revue de ces journaux au moins une fois par mois.

Le prestataire de services doit mettre en place des mesures pour assurer qu'il n'y ait aucun accès direct entre une zone publique et une zone sensible.

3.7.3. Travail dans les zones privées et sensibles

Le prestataire de services doit inclure les aspects de sécurité physique dans sa politique de sécurité et lors de l'évaluation des risques conformément au niveau de sécurité requis par la catégorie de la zone.

Le prestataire de services doit établir et mettre en place des procédures relatives au travail en zones privées et sensibles, et s'assurer que ces procédures sont communiquées aux intervenants concernés.

3.7.4. Zones de livraison et de chargement

Les zones de livraison et de chargement, ainsi que tout autre point par lequel des personnes non autorisées peuvent accéder aux locaux sans être accompagnées, sont catégorisées comme des zones publiques.

Le prestataire de services doit séparer les points d'accès de ces zones vers les zones privées et sensibles afin de prévenir les accès non autorisés, ou à défaut mettre en place des mesures compensatoires pour maintenir le même niveau de sécurité.

3.7.5. Sécurité du câblage

Le prestataire de services doit documenter et déployer des mesures visant à sécuriser le câblage électrique et de télécommunication contre les dommages physiques ainsi que les tentatives d'interception.

Le prestataire de services doit établir et tenir à jour un plan de câblage.

Il est recommandé que le prestataire de services mette en place des mesures pour identifier les câbles (comme l'utilisation de codes couleurs, d'étiquetages, etc.) afin de faciliter leur exploitation et réduire les risques d'erreurs de manipulation.

3.7.6. Maintenance des matériels

Le prestataire de services doit mettre en place des mesures pour assurer que l'installation, la maintenance et l'entretien des équipements du système d'information hébergés dans des zones privées et sensibles respectent les exigences de confidentialité et de disponibilité définies dans la convention de service.

Le prestataire de services doit conclure des contrats de maintenance afin de bénéficier des mises à jour de sécurité des logiciels installés sur les équipements du système d'information du service.

Le prestataire de services doit garantir que les supports ne peuvent être renvoyés à un tiers que si les données du commanditaire qui y sont stockées sont chiffrées conformément aux exigences 3.6.1 et 3.6.3 du présent référentiel, ou si elles ont été préalablement effacées à l'aide d'un mécanisme de suppression sécurisée.

Le prestataire de services doit mettre en place des mesures pour assurer que les conditions d'installation, de maintenance et d'entretien des équipements techniques auxiliaires (comme l'alimentation électrique, la climatisation, la protection contre l'incendie, etc.) respectent les exigences de disponibilité définies dans la convention de service.

3.7.7. Sortie des actifs

Le prestataire de services doit établir une procédure pour le transfert hors site des données du commanditaire, des équipements et des logiciels, requérant une autorisation écrite de la direction du prestataire et du commanditaire. Il doit également garantir que les mesures de protection de la confidentialité et de l'intégrité des actifs pendant leur transport soient équivalentes à celles en place sur site.

3.7.8. Recyclage sécurisé du matériel

Le prestataire de services doit établir et mettre en œuvre des procédures pour effacer de manière sécurisée, en utilisant une réécriture de motifs aléatoires, tous les supports de données qui sont mis à disposition d'un commanditaire. Dans les cas où l'espace de stockage est chiffré, il est possible d'effectuer un effacement sécurisé en supprimant la clé de chiffrement correspondante.

3.7.9. Sécurité de l'environnement

Protection contre l'incendie et les fuites d'eau : La protection contre l'incendie et les fuites d'eau doit être assurée par des mesures structurelles, techniques et organisationnelles notamment par des compartiments coupe-feu avec une résistance d'au moins 60 minutes ; des moyens de détection précoce des incendies ou des fuites d'eau, des systèmes d'extinction automatique ou réduction de l'oxygène, et des alarmes incendie et fuites d'eau.

Protection contre les interruptions dues aux pannes de courant : Des mesures doivent être mises en place pour prévenir les interruptions des services liés à l'alimentation électrique ou à la climatisation notamment par l'utilisation de systèmes d'alimentation sans coupure, dit UPS,(Uniterruptible Power Supply) et de générateurs de secours, vérifiés régulièrement.

Surveillance des paramètres opérationnels et environnementaux : Les paramètres de fonctionnement des installations techniques (alimentation, refroidissement, etc.) et les conditions environnementales (température, humidité) doivent être surveillés. Lorsque les paramètres dépassent la plage autorisée, des alertes automatiques doivent être envoyées aux responsables pour prendre des mesures correctives immédiates.

3.8. Sécurité liée à l'exploitation

3.8.1. Procédures d'exploitation documentées

Le prestataire de services est tenu de documenter les procédures d'exploitation, les tenir à jour et de les mettre à disposition de tous les utilisateurs concernés.

3.8.2. Gestion des changements

Le prestataire de services doit mettre en place et documenter une procédure de gestion des changements effectués sur les systèmes et les moyens de traitement de l'information.

Le prestataire de services doit établir et appliquer une procédure permettant, en cas d'opérations susceptibles d'affecter la sécurité ou la disponibilité du service, de transmettre rapidement aux commanditaires les informations suivantes :

- La date et l'heure programmées du début et de la fin des opérations ;
- La nature des opérations ;

— Les impacts sur la sécurité ou la disponibilité du service ;

— Le contact au sein du prestataire de services.

Dans le cadre d'un service PaaS, le prestataire de services doit notifier le commanditaire dès que possible de toute modification prévue sur des éléments logiciels dont il est responsable, lorsque la compatibilité totale ne peut être garantie. Le prestataire de services doit avertir le commanditaire dès que possible de toute modification prévue des éléments du service susceptible de réduire ses fonctionnalités.

3.8.3. Séparation des environnements

Les environnements de développement, de test et de production doivent être séparés pour réduire notamment les risques d'accès ou de changements non autorisés dans les trois environnements.

3.8.4. Protection contre les logiciels malveillants

Le prestataire de services doit documenter et mettre en œuvre les mesures de détection, de prévention et de restauration pour se protéger contre les logiciels malveillants. Cette exigence doit couvrir nécessairement le système d'information du service, y compris les postes de travail gérés par le prestataire et les flux entrants vers ce système.

Le prestataire de services doit établir un programme de sensibilisation pour ses employés concernant les risques des logiciels malveillants et les meilleures pratiques pour minimiser l'impact d'une infection.

3.8.5. Sauvegarde

Le prestataire de services doit élaborer une politique de sauvegarde et de restauration des données qu'il gère dans le cadre du service. Cette politique doit inclure une sauvegarde périodique de toutes les données (informations, logiciels, configurations, etc.) sous sa responsabilité dans le cadre du service.

Le prestataire de services doit mettre en place et documenter des mesures de protection des sauvegardes en conformité avec la politique de contrôle d'accès (voir chapitre 3.5). Cette politique doit également prévoir une revue mensuelle des accès aux sauvegardes.

Le prestataire de services doit tester régulièrement les supports de sauvegarde en s'assurant que les données sauvegardées peuvent être restaurées en temps voulu conformément à une procédure de restauration documentée.

Le prestataire de services doit protéger physiquement les supports de sauvegarde en les plaçant dans un endroit protégé (Armoire ignifuge) ou en les externalisant sur un site suffisamment distant du site principal.

Le ou les sites de sauvegarde sont assujettis aux mêmes exigences de sécurité que le site principal et les communications entre site principal et site de sauvegarde doivent être protégées par chiffrement, conformément aux exigences du chapitre 3.6 du présent référentiel.

3.8.6. Journalisation des évènements

Le prestataire de services doit mettre en place et documenter une politique de journalisation applicable aux composants SI sous sa responsabilité qui servent à fournir les services Cloud et qui inclut 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 de services 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 logiciels malveillants (voir exigence 3.8.4 du présent référentiel) ;
- Les exceptions ;
- Les défaillances ;
- Tout autre événement lié à la sécurité de l'information.

Ces journaux doivent être centralisés et protégés contre les risques de falsification ou d'accès non autorisé. Ils doivent être conservés pour une durée minimale de douze mois.

Le prestataire de services doit, sur demande d'un commanditaire, fournir l'intégralité des événements le concernant dans un format exploitable standardisé (ex : json, Csv ou Xml).

3.8.7. Protection de l'information journalisée

Le prestataire de services doit assurer la protection des équipements de journalisation et des événements enregistrés contre toute menace pouvant affecter leur disponibilité, leur intégrité ou leur confidentialité.

Le prestataire de services doit transférer les événements journalisés vers des serveurs centraux dédiés, en assurant leur protection en termes de confidentialité et d'intégrité, et les conserver sur une machine physique distincte de celle qui les a générés.

Le prestataire de services doit établir une sauvegarde des événements collectés conformément à une politique appropriée.

Le prestataire de services doit exécuter les processus de journalisation et de collecte des événements en utilisant des comptes disposant des privilèges adéquats et nécessaires, tout en limitant l'accès aux événements enregistrés conformément à la politique de contrôle d'accès (voir exigence 3.5.1 du présent référentiel).

3.8.8. Synchronisation des horloges

Pour assurer la précision des journaux d'événements qui peuvent être utilisés lors des investigations, le prestataire de services doit assurer la synchronisation des horloges de l'ensemble des systèmes de traitement de l'information sur une référence de temps commune (service NTP, Network Time Protocol).

3.8.9. Analyse et corrélation des événements

Le prestataire de services doit concevoir et déployer une infrastructure permettant d'analyser et de corréler les événements enregistrés par le système de journalisation, afin de détecter ceux pouvant impacter la sécurité du système d'information du service. Cette analyse doit pouvoir se faire en temps réel ou ultérieurement, pour des événements sur une période allant jusqu'à six mois.

Le prestataire de services doit traiter les alarmes générées par l'infrastructure d'analyse et de corrélation des événements sur une base quotidienne.

3.8.10. Installation de logiciels sur des systèmes en exploitation

Le prestataire de services doit définir et mettre en place un processus de contrôle des logiciels que les utilisateurs peuvent installer sur les équipements du système d'information du service.

Le prestataire de services doit élaborer une procédure pour la gestion de la configuration des environnements logiciels fournis au commanditaire, en particulier pour assurer leur maintien en condition de sécurité.

3.8.11. Gestion des vulnérabilités techniques

Le prestataire de services doit élaborer un processus de veille pour gérer les vulnérabilités techniques des logiciels et des systèmes présents dans le système d'information du service.

Le prestataire de services doit évaluer son exposition à ces vulnérabilités en les intégrant dans l'analyse des risques et mettre en œuvre les mesures de traitement des risques appropriées.

3.8.12. Administration

Le prestataire de services doit élaborer une procédure exigeant que les administrateurs utilisent des postes dédiés exclusivement aux tâches d'administration et ayant subi des mesures de durcissement de configuration adaptées.

L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès.

Lorsque le prestataire de services autorise une situation de mobilité pour les administrateurs sous sa responsabilité, il doit l'encadrer par une politique documentée. La solution mise en œuvre doit assurer que le niveau de sécurité de cette situation de mobilité est au moins équivalent au niveau de sécurité hors situation de mobilité.

3.8.13. Surveillance des flux sortants de l'infrastructure

Le prestataire de services doit fournir une capacité d'inspection et de suppression des sortants de l'infrastructure technique relatifs au périmètre du service (informations de facturation, les éventuels journaux nécessaires au traitement d'incidents, etc.) :

- Les sortants doivent pouvoir être expurgés des données pouvant porter atteinte à la confidentialité des données des commanditaires ;
- Cette capacité d'inspection et de suppression doit générer des journaux d'activité et doit pouvoir faire l'objet d'un audit ;
- Les sortants sont traités sur des dispositifs spécifiques opérés et maintenus par le prestataire de services, et hébergés dans une zone cloisonnée du reste de l'infrastructure.

3.8.14. Lignes directrices et recommandations pour les commanditaires du service

Le prestataire de services fournit aux commanditaires des lignes directrices et des recommandations pour l'utilisation sécurisée du service cloud. Ces informations visent à aider le commanditaire dans la configuration, l'installation et l'utilisation sécurisée du service, dans la mesure où cela est applicable au service et aux responsabilités du commanditaire. Les informations fournies couvrent plusieurs aspects, tels que :

- Instructions pour une configuration sécurisée ;
- Sources d'information sur les vulnérabilités connues et les mécanismes de mise à jour ;
- Mécanismes de gestion des erreurs et des journaux ;
- Mécanismes d'authentification ;
- Concepts de rôles et de droits, y compris les combinaisons qui augmentent les risques ;
- Services et fonctions pour l'administration du service cloud par des utilisateurs privilégiés.

3.9. Sécurité des communications

3.9.1. Cartographie du système d'information

Le prestataire de services doit établir et tenir à jour une cartographie du système d'information du service en précisant les composants matériels et logiciels, les architectures des réseaux ainsi que la matrice des flux réseau autorisés.

Les documents de cartographie doivent être maintenus au fil des évolutions apportées aux systèmes d'information et faire l'objet d'une protection adaptée.

3.9.2. Cloisonnement du réseau

Le prestataire de services est tenu de cloisonner le système d'information du service selon la nature des flux (production, administration etc.), le domaine technique (traitement, stockage, etc.) et les niveaux de sensibilité des actifs informationnels connectés.

Le prestataire de services doit isoler, soit physiquement soit par chiffrement, tous les flux de données internes au système d'information du service afin de les protéger des autres systèmes d'information.

Si le réseau d'administration de l'infrastructure technique n'est pas physiquement séparé, les flux d'administration doivent être acheminés à travers un tunnel chiffré.

Le prestataire de services doit déployer et configurer un pare-feu applicatif afin de protéger les interfaces d'administration, accessibles via un réseau public et destinées à ses commanditaires.

3.9.3. Surveillance des réseaux

Le prestataire de services doit mettre en place les moyens appropriés pour la détection et la supervision des événements de sécurité au niveau des principaux nœuds d'interconnexion réseau dans le système d'information du service et pour permettre un traitement et une corrélation entre ces événements de sécurité.

3.10. Acquisition, développement et maintenance des systèmes d'information

3.10.1. Politique de développement sécurisé

Le prestataire de services doit élaborer et mettre en place, conformément aux guides et référentiels élaborés par l'autorité nationale de cybersécurité, une politique de développement sécurisé des logiciels et des systèmes, qui définit notamment :

- Les exigences de sécurité de l'environnement de développement ;
- Les exigences de sécurité dans la phase de conception ;
- Les points de contrôle de la sécurité aux différentes étapes clés du projet ;
- Les référentiels de développement sécurisé à utiliser ;
- Les règles de protection du code source et le contrôle des versions.

Le prestataire de services doit élaborer et mettre en place une formation sur le développement sécurisé spécifiquement adaptée aux employés concernés.

3.10.2. Procédures de contrôle des changements de système

Le prestataire de services doit documenter et mettre en place une procédure pour contrôler les changements apportés au système d'information du service.

Le prestataire de services doit documenter et mettre en place une procédure pour valider les changements apportés au système d'information du service dans un environnement de préproduction avant leur déploiement en production afin de s'assurer qu'elles n'entraînent aucun effet indésirable sur l'activité ou la sécurité du service.

Le prestataire de services doit maintenir un historique des versions des logiciels et systèmes (internes, externes ou commerciaux) déployés, afin de pouvoir, si nécessaire, recréer un environnement complet dans un environnement de test à une date précise. La durée de conservation de cet historique doit correspondre à celle des sauvegardes (voir exigence 3.8.5 du présent référentiel).

3.10.3. Environnement de développement sécurisé

Le prestataire de services doit établir un environnement sécurisé de développement qui assure la gestion complète du cycle de développement du système d'information du service.

Le prestataire de services doit prendre en compte les environnements de développement dans l'appréciation des risques et garantir leur protection conformément aux exigences du présent référentiel.

3.10.4. Développement externalisé

Le prestataire de services doit documenter et mettre en place une procédure pour superviser et contrôler l'activité de développement externalisé des logiciels et des systèmes. Cette procédure doit garantir que le développement externalisé soit conforme à la politique de développement sécurisé du prestataire de services et atteint un niveau de sécurité équivalent à celui d'un développement interne (voir exigence 3.10.1 du présent référentiel).

3.10.5. Test de la sécurité et conformité du système

Le prestataire de services doit soumettre les systèmes d'information, qu'ils soient nouveaux ou mis à jour, à des tests de conformité et de fonctionnalité en matière de sécurité durant 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.

3.10.6. Protection des données de test

Le prestataire de services doit documenter et mettre en place une procédure pour garantir l'intégrité des données de test utilisées en préproduction.

Si le prestataire de services envisage d'utiliser des données de production du commanditaire pour réaliser des tests, il doit obtenir l'accord préalable du commanditaire et anonymiser ces données. Le prestataire de services doit également veiller à préserver la confidentialité des données durant leur anonymisation.

3.11. Relations avec les tiers

3.11.1. Identification des tiers

Le prestataire de services doit tenir à jour une liste exhaustive des parties prenantes impliquées dans la mise en œuvre du service, telles que les hébergeurs, développeurs, intégrateurs, archiveurs, sous-traitants intervenant sur site ou à distance, fournisseurs d'équipements, etc... Cette liste doit détailler le rôle de chaque tiers dans le service ainsi que dans le traitement des données.

Le prestataire de services doit remettre au commanditaire une liste exhaustive des tiers ayant accès aux données et l'informer de tout changement de sous-traitants, afin que le commanditaire puisse exprimer son accord et ce, sans préjudice de l'application du paragraphe 5 de l'article 5 du décret précité n°2-24-921.

3.11.2. La sécurité dans les accords conclus avec les tiers

Le prestataire de services doit s'assurer que les tiers impliqués dans la mise en œuvre du service respectent un niveau de sécurité au moins équivalent à celui de sa propre politique de sécurité. Il doit définir ces exigences spécifiques pour chaque tiers en fonction de sa contribution au service, et les inclure dans les cahiers des charges ou les clauses de sécurité des accords de partenariat. Ces exigences doivent également être intégrées dans les contrats signés avec les tiers.

Le prestataire de services doit inclure, dans les contrats avec chacun des tiers impliqués dans la mise en œuvre du service, des clauses d'audit permettant à l'autorité nationale de cybersécurité ou toute entité mandatée par elle de vérifier que ces tiers respectent les exigences définies dans le présent référentiel.

Le prestataire de services doit établir et attribuer les rôles et responsabilités liés à la modification ou à la résiliation du contrat avec chaque tiers participant à la mise en œuvre du service.

3.11.3. Surveillance et revue des services des fournisseurs

Le prestataire de services doit établir et mettre en œuvre une procédure pour vérifier régulièrement que les tiers participant à la mise en œuvre du service respectent les exigences du présent référentiel.

3.11.4. Gestion des changements apportés dans les services des tiers

Le prestataire de services doit élaborer une procédure pour suivre les modifications effectuées par les tiers impliqués dans la mise en œuvre du service, afin d'évaluer leur impact potentiel sur la sécurité du système d'information du service.

Lorsque le changement opéré par un tiers impliqué dans la mise en œuvre du service impacte le niveau de sécurité, le prestataire de services doit informer sans délai tous les commanditaires et l'autorité nationale de cybersécurité et prendre les mesures requises pour restaurer le niveau de sécurité antérieur.

3.11.5. Engagements de confidentialité

Le prestataire de services doit élaborer une procédure pour revoir, au moins une fois par an, les exigences en matière d'engagement de confidentialité ou de non-divulgation vis-à-vis des tiers impliqués dans la mise en œuvre du service.

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

3.12.1. Responsabilités et procédures

Le prestataire de services doit documenter et mettre en place une procédure pour répondre rapidement et efficacement aux incidents de sécurité. Cette procédure doit préciser les moyens et délais de communication des incidents de sécurité aux commanditaires concernés, ainsi que le niveau de confidentialité requis pour cette communication.

Le prestataire de services doit informer ses employés ainsi que tous les tiers impliqués dans la mise en œuvre du service de cette procédure.

3.12.2. Signalements liés à la sécurité de l'information

Le prestataire de services doit établir et appliquer une procédure qui demande à ses employés ainsi qu'aux tiers impliqués dans la mise en œuvre du service de signaler tout incident de sécurité avéré ou suspecté, ainsi que toute vulnérabilité de sécurité identifiée.

Le prestataire de services doit élaborer et mettre en place une procédure qui permet à tous les commanditaires de signaler tout incident de sécurité avéré ou suspecté, ainsi que toute faille de sécurité identifiée

Le prestataire de services doit informer immédiatement les commanditaires des incidents de sécurité survenus, ainsi que des mesures recommandées pour en limiter les impacts. Il doit également permettre au commanditaire de sélectionner les niveaux de gravité des incidents pour lesquels il souhaite être notifié.

Le prestataire de services doit notifier les incidents de sécurité [2] aux autorités compétentes conformément aux exigences légales et réglementaires en vigueur.

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

Le prestataire de services est chargé d'évaluer les événements liés à la sécurité de l'information afin de déterminer s'ils doivent être considérés comme des incidents de sécurité. Cette évaluation doit se baser sur une ou plusieurs échelles (estimation, évaluation, etc.) qui ont été préalablement définies en accord avec le commanditaire.

Le prestataire de services doit mettre en place une classification spécifique permettant de distinguer clairement les incidents de sécurité qui concernent les données des commanditaires, en tenant compte des résultats de l'évaluation des risques.

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

Le prestataire de services est tenu de gérer les incidents de sécurité jusqu'à leur résolution complète et doit informer les commanditaires conformément aux procédures établies.

Le prestataire de services doit conserver une archive des documents détaillant les incidents de sécurité.

Pour le niveau 2, le prestataire de services doit solliciter uniquement les services d'un prestataire de réponse aux incidents de sécurité qualifié pour traiter les incidents de sécurité qui demandent une expertise supplémentaire.

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

Le prestataire de services doit documenter et instaurer un processus d'amélioration continue visant à réduire la fréquence et l'impact des types d'incidents de sécurité déjà traités.

Les incidents de sécurité doivent être classés, priorisés et analysés de manière approfondie pour en identifier la cause principale. Cela doit être fait par des experts internes du prestataire de services, avec l'aide éventuelle de prestataires externes de sécurité.

3.12.6. Recueil de preuves

Le prestataire de services doit établir et appliquer une procédure pour enregistrer les informations relatives aux incidents de sécurité, afin qu'elles puissent servir d'éléments de preuve.

3.13. Gestion de la continuité d'activité

3.13.1. Organisation de la continuité d'activité

Le prestataire de services doit préparer un plan de continuité et de reprise d'activités intégrant l'ensemble des solutions pour pallier les arrêts des processus et applications critiques pour le service. Il doit porter notamment sur des solutions de secours informatique (sauvegarde, site de secours, bascule, résilience des réseaux, redondance matérielle et logicielle, etc.)

[2] Incident de sécurité : tout événement affectant la sécurité des systèmes d'information, incluant les incidents de cybersécurité au sens de la loi n° 05-20, ainsi que les violations de données à caractère personnel régies par la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Le prestataire de services doit revoir annuellement le plan de continuité d'activité du service et chaque fois qu'un changement significatif susceptible d'affecter le service intervient.

3.13.2. Mise en œuvre de la continuité d'activité

Le prestataire de services doit mettre en place des procédures pour maintenir la continuité et la disponibilité, conformément aux engagements contractuels envers le commanditaire.

3.13.3. Vérifier, revoir et évaluer la continuité d'activité

Le prestataire de services doit élaborer une procédure pour évaluer le plan de continuité d'activités, afin de vérifier sa pertinence et son efficacité en cas de crise.

3.13.4. Disponibilité des moyens de traitement de l'information

Le prestataire de services doit mettre en place les mesures nécessaires pour assurer la disponibilité du service conformément aux exigences spécifiées dans la convention de service (voir l'exigence 3.15.1 du présent référentiel).

3.13.5. Sauvegarde de la configuration de l'infrastructure technique

Le prestataire de services doit établir une procédure pour réaliser des sauvegardes hors ligne de la configuration de l'infrastructure technique.

3.13.6. Mise à disposition d'un dispositif de sauvegarde des données du commanditaire

Le prestataire de services doit documenter et proposer au commanditaire un service de sauvegarde des données.

3.14. Conformité

3.14.1. Identification de la législation et des exigences contractuelles applicables

Le prestataire de services doit identifier les exigences légales, réglementaires et contractuelles en vigueur applicables au service.

Le prestataire de services doit élaborer et appliquer des procédures pour se conformer aux exigences légales, réglementaires et contractuelles en vigueur applicables au service, ainsi qu'aux besoins spécifiques en matière de sécurité.

Le prestataire de services doit rendre accessible à un commanditaire, sur demande, l'ensemble de ces procédures.

Le prestataire de services doit établir et appliquer un processus de surveillance proactive des exigences légales, réglementaires et contractuelles en vigueur applicables au service.

3.14.2. Revue indépendante de la sécurité de l'information

Revue continue

Le prestataire de services doit élaborer et mettre en œuvre un programme d'audit sur trois ans définissant le périmètre et la fréquence des audits en conformité avec la gestion du changement, les politiques internes, et les résultats de l'appréciation des risques. Ce programme doit prévoir au moins

un audit par an réalisé par un prestataire qualifié d'audit de la sécurité des systèmes d'information. L'ensemble du programme d'audit doit notamment couvrir :

- L'audit de la configuration de l'infrastructure technique du service, réalisé par échantillonnage et englobant tous les types d'équipements et de serveurs présents dans le système d'information du service ;
- Le test d'intrusion des interfaces d'administration exposées sur un réseau public ;
- Le test d'intrusion de l'interface utilisateur pour les services SaaS ;
- Si le service comprend des développements internes, l'audit du code source axé sur les fonctionnalités de sécurité implémentées, avec une approche continue privilégiée ;
- Il est recommandé que le prestataire de services implémente des mécanismes automatisés d'audit de configuration adaptés à l'infrastructure technique du service.

Revue initiale

Avant l'évaluation pour la qualification du service, le prestataire de services doit réaliser une revue indépendante initiale de la sécurité de l'information par un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié. Cette revue initiale doit inclure notamment :

- Pour les services autres que IaaS (comme PaaS, SaaS, etc.), il est essentiel de réaliser un audit de la configuration des ressources virtuelles ou physiques, ainsi que des systèmes d'exploitation et des logiciels de base (tels que les OS, les middlewares, les bases de données, etc.) inclus dans le périmètre du service.
- Un test d'intrusion visant les interfaces d'administration du service mises à disposition des commanditaires ;
- Pour un service de type SaaS, il est nécessaire de réaliser un test d'intrusion sur l'interface mise à disposition des utilisateurs finaux, ainsi qu'un audit du code source concernant les fonctionnalités de sécurité implémentées telles que l'authentification, la gestion des sessions et la gestion du cloisonnement en cas de mode multi-tenant.

Revue des changements majeurs

En cas de changement majeur susceptible d'affecter le service, le prestataire de services 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 notamment couvrir 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, il est essentiel de réaliser un test d'intrusion sur l'interface mise à disposition des utilisateurs finaux dans le cadre du catalogue de services, ainsi qu'un audit du code source axé sur les fonctionnalités de sécurité implémentées telles que l'authentification, la gestion des sessions et la gestion du cloisonnement en cas de mode multi-tenant. Si le SaaS offre un service de sécurité de l'information, une certification produit dédiée est également requise.

3.14.3. Conformité avec les politiques et les normes de sécurité

Le prestataire de services, par l'intermédiaire du responsable de la sécurité des systèmes d'information, doit régulièrement vérifier que toutes les procédures de sécurité placées sous sa responsabilité sont correctement mises en œuvre afin de garantir leur conformité avec les politiques et normes de sécurité établies.

3.14.4. Examen de la conformité technique

Le prestataire de services doit élaborer documenter et mettre en œuvre une politique pour vérifier la conformité technique du service aux exigences du présent référentiel. Cette politique doit définir les objectifs, les méthodes d'évaluation, la fréquence des vérifications, les résultats attendus ainsi que les mesures correctives à prendre le cas échéant.

3.15. Exigences en ce qui concerne la convention de service, la localisation des données et la protection des données à caractère personnel

3.15.1. Convention de service

Le prestataire de services est tenu de rédiger une convention de service avec chaque commanditaire. Toute modification de cette convention doit être approuvée par le commanditaire.

Le prestataire de services doit préciser dans la convention de service :

- Les obligations, droits et responsabilités de chaque partie, y compris le prestataire de services, les tiers impliqués, et les commanditaires ;
- Les éléments expressément exclus de ses responsabilités, dans le respect des exigences légales et réglementaires en vigueur ;
- La localisation du service. La localisation du support doit être précisée lorsqu'il est réalisé en dehors du territoire marocain.

La convention de service doit être régie par la législation et la réglementation marocaines et spécifier, le cas échéant, tout autre droit qui pourrait être applicable à cette convention.

La convention de service doit préciser que la collecte, la manipulation, le stockage et, de manière générale, le traitement des données liées à l'avant-vente, à la mise en œuvre, à la maintenance et à l'arrêt du service seront effectués conformément aux exigences légales en vigueur.

La convention de service doit préciser que le prestataire de services est tenu de fournir au commanditaire, sur demande, les éléments d'appréciation des risques associés à la soumission des données du commanditaire à la législation d'un pays autre que le Maroc.

Le prestataire de services doit détailler dans la convention de service les mesures techniques et organisationnelles qu'il met en place pour garantir le respect de la législation applicable.

La convention de service doit inclure une clause de révision permettant au commanditaire de résilier la convention sans pénalité en cas de perte de la qualification du service.

Le prestataire de services doit intégrer dans la convention de service une clause de réversibilité permettant au commanditaire de récupérer toutes ses données, qu'elles soient fournies directement par lui ou générées à partir de ses données ou actions dans le cadre du service.

Le prestataire de services doit garantir cette réversibilité en utilisant l'une des méthodes techniques suivantes :

- Fournir les données sous forme de fichiers dans un ou plusieurs formats documentés et exploitables en dehors du service du prestataire de services ;
- Mettre en place des interfaces techniques permettant l'accès aux données selon un schéma documenté et exploitable (API, formats pivots, etc.).

Le prestataire de services doit spécifier dans la convention de service le niveau de disponibilité du service.

Le prestataire de services doit préciser dans la convention de service qu'il n'a pas le droit d'utiliser les données transmises et générées par le commanditaire, ces données étant exclusivement réservées au commanditaire.

La convention de service doit indiquer explicitement que le prestataire de services s'engage à ne communiquer à des tiers, aucune information relative à la prestation fournie au commanditaire, sans avoir obtenu au préalable son autorisation écrite.

Le prestataire de services doit préciser dans la convention de service si les données du commanditaire sont automatiquement sauvegardées. Si ce n'est pas le cas, le prestataire de services doit informer le commanditaire des risques associés et indiquer clairement les étapes que le commanditaire doit suivre pour assurer la sauvegarde de ses données.

Le prestataire de services doit préciser dans la convention de service s'il permet l'accès distant pour l'administration ou le support du système d'information du service.

Le prestataire de services doit indiquer dans la convention de service que :

- Le service est qualifié et fournir l'attestation de qualification ;
- Le commanditaire peut déposer une réclamation concernant le service qualifié auprès de l'autorité nationale de cybersécurité ;
- Le commanditaire autorise l'autorité nationale de cybersécurité à auditer le service et son système d'information pour vérifier la conformité avec les exigences du présent référentiel.

3.15.2. Localisation des données

Le prestataire de services doit documenter et informer le commanditaire de la localisation où les données de ce dernier sont stockées et traitées.

Lorsqu'il s'agit du Niveau 2, le prestataire de services doit stocker, traiter les données sensibles et administrer le service du commanditaire depuis le territoire marocain.

Le prestataire de services doit stocker et traiter les données techniques (telles que les identités des bénéficiaires et des administrateurs de l'infrastructure technique, les données manipulées par le réseau défini par logiciel, les journaux de l'infrastructure technique, l'annuaire, les certificats, la configuration des accès, etc.) au sein du territoire marocain. Cette exigence prend un caractère exclusif lorsqu'il s'agit du niveau 2.

Le prestataire de services peut réaliser des opérations de support aux commanditaires depuis un État hors du territoire marocain. Il doit documenter les types d'opérations pouvant être effectuées depuis cet État et décrire les mécanismes de contrôle d'accès et de supervision assurant le suivi de ces

opérations depuis le Maroc, et ce sans préjudice de l'application du paragraphe 4 de l'article 5 du décret précité n°2-24-921.

3.15.3. Protection des données à caractère personnel

Le prestataire de services est tenu de prouver qu'il respecte les principes de protection des données pour les traitements de données à caractère personnel réalisés pour son propre compte. Il doit fournir des éléments de preuve par rapport aux points suivants :

- Les finalités des traitements sont clairement définies, légitimes et transparentes ;
- La traçabilité des traitements est assurée, tant pour le prestataire de services que pour son commanditaire ;
- Les traitements reposent sur une base légale valide ;
- Les finalités des traitements ne doivent en aucun cas être détournées ;
- Les données traitées doivent être limitées au strict nécessaire, adéquates et pertinentes pour les finalités poursuivies ;
- La qualité des données doit être préservée, en garantissant leur exactitude et leur mise à jour ;
- Les durées de conservation des données doivent être précisément définies et limitées.

Le prestataire de services doit justifier, pour les traitements de données caractère personnel effectués pour son propre compte, qu'il respecte les droits des personnes concernées. Il doit, au minimum, justifier les éléments suivants :

- L'information des usagers doit être fournie de manière loyale et transparente ;
- Le consentement des usagers doit être recueilli de façon explicite, démontrable et rétractable ;
- Les usagers doivent avoir la possibilité d'exercer leurs droits d'accès, de rectification et d'effacement des données ;
- Les usagers doivent également pouvoir exercer leurs droits de limitation du traitement, de portabilité et d'opposition