HODI

Host different.

Plan d'Assurance Sécurité

Date	Version	Auteur
13/02/2022	Version initiale	Julien Tessier
15/09/2023	Ajout opérateurs de cloud redondants géographiquement Ajout mise à jour sans redémarrage par OpenSSL, Glibc et MySQL dans le futur	Julien Tessier
20/10/2023	Ajout datacenter île Maurice	Julien Tessier
07/12/2023	Ajout Observatoire de la Cybersécurité de l'Océan Indien	Julien Tessier

Table des matières

1. Introduction

Objet et périmètre

Le Plan d'Assurance Sécurité permet de décrire les engagements pris par Hodi en termes de sécurité des données et applications hébergées sur sa plateforme d'hébergement.

Le PAS s'applique à tous les services fournis aux clients, notamment l'hébergement web et les serveurs virtuels, managés ou non.

Abréviations

Les abréviations suivantes sont utilisées dans ce document :

- ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
- PAS : Plan d'Assurance Sécurité
- PCA : Plan de Continuité d'Activité
- PRA : Plan de Reprise d'Activité
- PSSI : Politique de Sécurité du Système d'Information
- RGPD : Règlement Général sur la Protection des Données
- SI : Système d'Information
- VPN : Virtual Private Network
- ZTNA : Zero Trust Network Access

Documents de référence

Les documents de référence sont les Conditions Générales de Service et la Politique de confidentialité de Hodi, disponibles sur https://hodi.host/, et le RGPD.

2. Enjeux et objectifs

La sécurité de la plateforme d'hébergement et du SI de Hodi est une composante essentielle de la protection des intérêts propres de Hodi, ainsi que celle de ses clients.

Il est donc impératif qu'une PSSI soit mise en œuvre, et qu'elle prenne en compte les principaux risques encourus et identifiés :

- Risque d'indisponibilité des informations et applications, et des systèmes les traitant.
- Risque de divulgation, ou perte de confidentialité, accidentelle ou volontaire des informations fournies par nos clients et pour lesquelles nous agissons en tant que sous-traitant.
- Risque d'altération, ou perte d'intégrité, qui pourrait amener à une perte d'information pour nos clients.

Les objectifs de mise en œuvre de la PSSI sont :

- D'améliorer et formaliser la gestion de la sécurité de la plateforme d'hébergement.

- Prévoir l'extension des services actuels en proposant des services hébergés dans d'autres cloud
- S'assurer du respect par Hodi de ses obligations légales en ce qui concerne la gestion des données personnelles (cf. RGPD)
- Créer une culture de la sécurité auprès des équipes de Hodi, de ses sous-traitants et de ses clients.

3. Gestion des risques

La direction générale de Hodi souhaite que les risques de sécurité de l'information qui pourraient conduire à une rupture de services inacceptable pour les clients soient gérés de manière continue.

Une analyse des risques a été réalisée selon la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), méthodologie qui est maintenue par l'ANSSI.

Cette analyse de risques a donné lieu d'une part à la mise à jour de la PSSI, et d'autre part à un plan d'actions d'évolution des mesures de sécurité mises en œuvre.

4. Politique de Sécurité du Système d'Information

La PSSI est diffusée à l'ensemble des personnes concernées, et Hodi met en œuvre les formations et informations nécessaires à sa compréhension, sa bonne mise en œuvre et son respect.

La PSSI est un document interne à Hodi et confidentiel. Le PAS reprend les informations de la PSSI, communicables aux clients, et selon un plan permettant de faciliter sa lecture et compréhension.

5. Organisation de la sécurité de l'information

Organisation

Chaque salarié possède une fiche de poste qui décrit ses missions, son positionnement au sein de l'organisation de Hodi, ses principales activités, et les savoir-faire et savoir-être qu'il doit maîtriser pour mener à bien ses missions.

La sécurité est pilotée au niveau stratégique au minimum une fois par an lors d'une revue de direction dédiée à la sécurité.

Veille

Hodi est membre du MEDEF Réunion et l'association Digital Réunion, association régionale réunissant les acteurs du secteur du numérique, et entretient des liens avec l'Observatoire de la Cybersécurité de l'Océan Indien, afin de suivre les évolutions dans le domaine de la sécurité de l'information.

Hodi participe régulièrement à des évènements et webinars sur les évolutions dans les domaines réglementaires, techniques, organisationnels et sur les produits.

Les équipes de Hodi suivent l'actualité publiée par l'ANSSI.

Gestion des risques dans les projets

La méthodologie projet élaborée par Hodi impose la prise en compte de la notion de risques dans tout nouveau projet.

Mobilité et télétravail

Les accès à distance, pour les salariés habilités, sont réalisés par l'intermédiaire d'une connexion sécurisée VPN. Chaque salarié dispose d'un accès individuel sur ce VPN.

6. Sécurité des ressources humaines

Embauche

Un projet « **arrivée** » formalisé permet de structurer l'intégration de tout nouveau collaborateur. Les droits d'accès aux informations et aux applications peuvent évoluer selon le statut de l'intégration (durée minimale de présence, période d'essai terminée, ...).

Confidentialité

Tout collaborateur de Hodi a signé une clause de confidentialité dans son contrat de travail et s'est engagé à la respecter et à la faire respecter.

Hodi s'engage à mettre en œuvre tous moyens, techniques et organisationnels, pour assurer la sécurité et la confidentialité des données qui lui sont confiées.

Sensibilisation à la sécurité

Le projet « **arrivée** » de tout nouveau collaborateur prévoit une sensibilisation à la sécurité. Des sessions de sensibilisation sont organisées de façon annuelle, en présentiel ou sous forme de webinar.

Départ

Un projet « **départ** » formalisé permet de structurer les actions à mener au départ de tout collaborateur, et en particulier la fermeture de ses comptes d'accès aux différentes ressources auxquelles il avait droit.

7. Gestion des actifs

Inventaire et identification des actifs

Tous les actifs de la plateforme d'hébergement, ainsi que ceux de tous les collaborateurs Hodi, sont identifiés et inventoriés.

Mise au rebut des actifs

Les supports physiques qui contiennent des données sont détruits physiquement avant leur mise au rebut.

La seule exception est l'envoi à un constructeur d'un disque dur dans le cadre de la gestion d'un matériel sous garantie, c'est le constructeur dans ce cas qui s'engage à la destruction physique du matériel.

8. Gestion des d'accès

Politique de mot de passe

Chaque utilisateur est identifié par un identifiant unique et un mot de passe fort.

La politique de mot de passe pour les utilisateurs des services hébergés est la suivante :

- Personnalisation par l'utilisateur lors de sa première connexion
- Taille minimale : 12 caractères
- Complexité : lettre majuscule, lettre minuscule, chiffre et symbole
- Fréquence de changement : tous les 90 jours
- Pas de réutilisation des 5 derniers mots de passe
- Verrouillage après 6 tentatives infructueuses

Les identifiants et mots de passe sont individuels et confidentiels, ils ne sont donc pas stockés par les équipes techniques Hodi. Si pour quelque raison que ce soit un intervenant technique a besoin de connaître le mot de passe d'un utilisateur, il sera demandé à ce dernier de le changer avant de le communiquer au technicien, et il sera obligé de le réinitialiser lors de sa connexion suivante.

Les comptes d'administration suivent les mêmes règles que celles des utilisateurs. Ces mots de passe sont stockés dans une base sécurisée et chiffrée.

Gestion des sessions inactives

Les postes de travail de Hodi sont configurés pour que les sessions inactives pendant 10 minutes soient automatiquement verrouillées.

Les salariés sont par ailleurs sensibilisés à la nécessité de verrouiller leur session quand ils s'éloignent de leur poste de travail.

Gestion des droits d'accès

Les droits d'accès sont gérés au travers d'un annuaire centralisé, hébergé et maintenu par un éditeur du marché reconnu. L'accès à l'annuaire par les logiciels utilisés par Hodi se fait au moyen d'une connexion LDAP chiffrée avec en utilisant un compte de service dédié, ou au moyen d'un SSO SAML. L'accès anonyme à l'annuaire centralisé n'est pas autorisé.

Les membres permanents de l'équipe Hodi disposent de comptes d'accès en permanence. L'administration courante des environnements hébergés est réalisée par l'Espace Client Hodi par l'intermédiaire de mécanismes automatisés en interaction avec les plateformes d'hébergement. L'accès par les autres personnels techniques n'est autorisé que pour la durée d'affectation ou d'intervention prévue.

L'administration d'un serveur dédié à un client, qui est totalement étanche vis-à-vis des autres serveurs hébergés, peut être sous la responsabilité de Hodi, du client, ou celle d'un tiers du choix du client. Dans le cas où l'administration n'est pas sous la responsabilité de Hodi, la sécurité de ce serveur est sous l'entière responsabilité du client.

Revue des droits d'accès

Les droits d'accès d'administration à l'ensemble du SI Hodi sont revus au minimum une fois par an.

Traçabilité des accès

Tous les accès au SI et ses outils périphériques sont historisés, qu'il s'agisse des connexions des salariés Hodi, des sous-traitants Hodi, ou des clients. Les tentatives d'accès infructueuses au SI et aux outils périphériques sont aussi historisées.

Les données historisées comportent notamment la date et heure, le nom d'utilisateur utilisé et son adresse IP.

Certaines données historisées (serveurs web et FTP notamment) sont accessibles directement par le client sur son Espace Client. Les autres ne sont accessibles qu'aux équipes techniques de Hodi, et pourront être communiquées au client sur demande légitime.

Ces données sont conservées pendant un an, conformément aux règlements en vigueur.

9. Cryptographie

Transfert de données

Tout transfert de données vers la plateforme d'hébergement est réalisé par l'intermédiaire de liens sécurisés et chiffrés. Si des données confidentielles doivent transiter soit sur un média amovible, soit dans un mail, ces données doivent être chiffrées en respectant les règles en vigueur.

Chiffrement

Les équipes techniques Hodi utilisent des logiciels de chiffrement s'appuyant sur l'AES 256, y compris pour les VPN.

Certificats

Les certificats utilisés par les équipes techniques Hodi proviennent d'autorités de certifications publiques et reconnues, et n'ont donc pas à accepter des certificats présentés comme invalides par le navigateur.

Supports amovibles et disques durs

Les supports amovibles et disques durs des postes, portables ou non, des équipes Hodi sont chiffrés.

10. Sécurité physique et environnementale

Localisation

Les datacenters où Hodi opère des serveurs sont choisis pour leur sécurité, leur haut niveau de disponibilité, leur localisation géographique et pour leur impact environnemental.

Sécurité des datacenters

Les datacenters sont au moins de Tier 3 avec les principales caractéristiques suivantes :

- Zone non inondable
- Sécurité électrique :
    - double alimentation électrique
    - onduleurs
    - groupes électrogènes N+1
    - serveurs en double alimentation
- Sécurité physique :

    - présence sur site
    - télésurveillance 365j x 24h
    - accès par badge
    - traçabilité des accès
    - vidéosurveillance
- Sécurité incendie :
    - détection précoce d'incendie, la présence d'aérosols d'incendie et de fumée est détectée dans l'air ambiant et l'air extérieur
    - compartiments coupe-feu avec des parois ignifuges
    - système d'extinction avec réduction de l'oxygène et sprinklers
- Pour les datacenters en Europe continentale, alimentation par énergie 100% renouvelable

Les datacenters hébergeant des données de clients sont situés uniquement sur le territoire de l'Union Européenne, sauf demande expresse du client, comme par exemple la volonté de localiser son hébergement mutualisé à l'île Maurice.

Sécurité du cloud

Hodi installe ses serveurs virtuels sur des clouds existants et impose les contraintes suivantes aux opérateurs de ces cloud :

- Disponibilité architecture supérieure à 99.95% dans l'Union Européenne et 99.5% dans le reste du monde
- Supervision en temps réel, 24h/24 et 7j/7
- Firewalls réseau haute disponibilité
- Anti-DDoS
- Architecture virtuelle permettant au cloud de continuer à fonctionner de manière optimale même en cas d'arrêt de deux serveurs physiques
- Contrat de support avec l'éditeur de la solution de virtualisation
- Stockage distribué
- Déplacement automatique des serveurs virtuels en cas de défaillance d'un serveur physique

Pour les opérateurs de cloud redondants géographiquement, les contraintes suivantes sont ajoutées :

- Réplication en temps réel sur deux datacenters
- Interconnexion des deux datacenters par deux liens fibres optiques sur des parcours différents pour prévenir le risque de coupure physique du lien
- Déplacement automatique des serveurs virtuels en cas de défaillance du datacenter

11. Sécurité liée à l'exploitation

Procédures d'exploitation

Hodi documente ses procédures d'exploitation, procédures qui sont mises à jour régulièrement au moyen d'un logiciel de gestion documentaire.

Données

Hodi classifie les données sur trois niveaux :

- Public
- Limité
- Confidentiel

Dans ce cadre, les données clients sont classées « Confidentielles ».

Certaines offres de Hodi nécessitent un transfert de données depuis le client, ou une infrastructure opérée par un tiers pour son compte, vers la plateforme d'hébergement Hodi sous la responsabilité de Hodi. Dans ce cadre, Hodi privilégie les transferts directs entre la source et la plateforme d'hébergement. Dans le cas où le transfert direct n'est pas possible, Hodi s'engage à supprimer toutes données stockées sur des équipements intermédiaires, par exemple serveurs de rebond ou postes de travail, après validation du client du bon transfert des données vers la plateforme d'hébergement.

Segmentation réseau

Hodi opère une segmentation réseau pour séparer les flux d'administration des flux courants d'une part, et pour séparer les serveurs dédiés des clients d'autre part. Un mécanisme de sécurité permet de s'assurer que seuls les salariés autorisés ont accès aux flux d'administration, et que les serveurs des clients n'ont accès qu'à leur segment attitré.

Logiciels malveillants

Tous les serveurs et postes de travail connectés au SI de Hodi sont équipés d'une suite logicielle contre les logiciels malveillants. La disponibilité de mises à jour est vérifiée quotidiennement, elles sont automatiquement téléchargées et déployées sur les équipements.

Sauvegardes

Sauf pour les serveurs hébergés au sein du datacenter de l'île Maurice, les données des clients sont sauvegardées par l'**opérateur de cloud** vers un autre datacenter, sur disque SSD, tous les jours avec une rétention d'une semaine. Hodi n'a pas accès à ces sauvegardes pour éviter qu'une attaque contre l'infrastructure de Hodi puisse détruire ou altérer les sauvegardes en question. La restauration de ces sauvegardes se fait par l'opérateur de cloud à la demande de Hodi. Ces sauvegardes sont réalisées à moins de 200km du datacenter du client pour

permettre une restauration aussi rapide que possible. Cette sauvegarde restaure le serveur dans sa globalité, et est notamment utilisée dans le PRA.

Pour les hébergements mutualisés, et pour les serveurs dédiés ayant souscrit à l'option **JetBackup**, les données des clients sont sauvegardées par Hodi vers un datacenter en Allemagne, différent du datacenter du client, tous les jours avec une rétention de 30 jours pour les hébergements mutualisés, et une rétention définie avec le client pour les serveurs dédiés. Cette sauvegarde exclut les fichiers temporaires et de cache tels que déterminés par Hodi. Cette sauvegarde permet au client de restaurer des éléments individuels par une interface en ligne.

Pour les serveurs dédiés ayant souscrit à l'option **Acronis**, les données des clients sont sauvegardées par Hodi vers un datacenter en Afrique du Sud, avec une fréquence et une rétention définies avec le client. Le transfert des données de cette sauvegarde en dehors de l'Union Européenne est chiffré (sauf demande contraire du client). Les clés de chiffrement ne sont pas transférées hors de l'Union Européenne. Cette sauvegarde permet au client de restaurer des éléments individuels par une interface en ligne.

Ces opérations de sauvegarde sont automatisées et supervisées, ce qui permet de détecter instantanément toute anomalie dans le dispositif.

Tests de restauration

Des tests de restauration sont effectués régulièrement selon un planning préétabli. Les clients peuvent effectuer eux-mêmes des tests de restauration JetBackup ou Acronis.

Supervision

Les serveurs, moyens de communication et services sont supervisés en permanence, et des alertes sont positionnées afin que les équipes soient immédiatement informées de toute anomalie potentielle, ou de toute situation pouvant amener à une dégradation du service.

Les alertes sont déclenchées 24h/24, 7j/7 et traitées, le cas échéant, par une équipe d'astreinte.

Pour les éléments critiques de sa plateforme d'hébergement, Hodi a mis en place deux solutions de supervision différentes pour s'assurer de la remontée d'alertes même en cas d'une défaillance de l'une des solutions

Enfin, Hodi s'engage à mettre en place et à maintenir une page publique d'information sur la disponibilité de ses principaux services sur https://status.hodi.host/.

Gestion des mises à jour

Dans le cas des serveurs dédiés où le client n'a pas choisi de confier à Hodi l'administration de ce dernier, aucune mise à jour n'est réalisée par Hodi.

Dans les autres cas, Hodi a choisi de mettre en place des mises à jour automatique la nuit selon la branche « stable » des éditeurs. La branche « stable » est une branche où les éditeurs

mettent à disposition les mises à jour après qu'elles aient été validées sur un échantillon de machines en conditions réelles d'exploitation.

Les hébergements mutualisés sont munis d'un dispositif permettant une mise à jour du noyau du système d'exploitation sans redémarrage du système, afin de disposer le plus rapidement possible de correctifs sur des vulnérabilités critiques, sans interruption de service. Ce dispositif sera étendu à terme à OpenSSL, Glibc et MySQL, sous réserve de mise à disposition par l'éditeur. Les serveurs dédiés peuvent être munis du même dispositif selon les options souscrites par le client.

12. Sécurité des communications

Accès aux outils périphériques du SI

Les parties sensibles des outils périphériques du SI, comme le logiciel de gestion documentaire ou la partie de l'Espace Client réservée aux équipes de Hodi, sont sécurisées par une solution ZTNA du marché fournie par un éditeur reconnu.

Administration et management

Un lien dédié est utilisé par les équipes techniques de Hodi pour toute intervention sur la plateforme d'hébergement, l'accès à ce lien est filtré aux seules personnes habilitées. En cas de rupture ou d'indisponibilité du lien dédié, l'accès peut être réalisé via un serveur de rebond, auquel seules les personnes habilitées ont accès via des protocoles chiffrés. Ce serveur de rebond est aussi accessible, dans le cadre du PCA de Hodi, via un accès HTTPS sécurisé par ZTNA pour permettre la connexion des équipes techniques de Hodi même dans les cas où elles seraient sur un lien public filtré n'autorisant que les accès HTTP et HTTPS.

Les tiers ayant besoin d'intervenir sur la plateforme d'hébergement pour le compte de Hodi, disposent de leurs propres liens chiffrés pour accéder à la plateforme via des protocoles chiffrés.

Pour empêcher tout accès non autorisé, les interfaces d'administrations de la plateforme d'hébergement sont restreintes aux accès depuis ces liens et le serveur de rebond.

Pare-feu

Tous les accès au SI et à la plateforme d'hébergement transitent par des firewalls réseaux. Pour les hébergements mutualisés et pour les serveurs dédiés ayant choisi l'option adéquate, les accès transitent en outre par des firewalls applicatifs (WAF).

Détection d'intrusion

Tous les flux d'accès au SI et à la plateforme sont analysés afin d'identifier et bloquer les flux anormaux et les programmes malveillants.

13. Acquisition, développement et maintenance du SI

Les activités de développement sont conformes aux méthodologies Agile qui sont utilisées par les équipes Hodi. La sécurité et le respect de la vie privée sont prises en compte dès la phase de conception des développements de Hodi dans une logique « security by design » et « privacy by design ».

Les équipes de Hodi utilisent GIT pour historiser les modifications réalisées sur le SI, et automatiser le déploiement des nouvelles versions.

Les environnements de développement et de préproduction sont isolés des environnements de production, utilisent des jeux de données fictives et ne sont accessibles qu'aux utilisateurs habilités.

Toute nouvelle version, que ce soit un correctif, une évolution ou une montée de version a fait l'objet de tests et de validations préalables. Une phase de retour arrière est prévue si le moindre dysfonctionnement est constaté suite à une mise à jour.

Lors de l'acquisition de nouveaux systèmes, les besoins de sécurité et de respect de la vie privée sont pris en compte dans le processus de sélection.

14. Relation avec les fournisseurs

Des sous-traitants sont amenés à intervenir sur la plateforme hébergée, il peut s'agir :

- D'un opérateur de cloud
- D'un support technique (par exemple, éditeur d'un logiciel) intervenant à la demande expresse d'un salarié de Hodi ou en cas de détection d'anomalie par la supervision selon la procédure d'escalade de Hodi

Les relations entre ces sous-traitants et Hodi répondent aux exigences liées au RGPD, et prennent en compte les aspects sécurité.

Toutes les interventions des sous-traitants sont tracées et respectent une procédure, notamment en ce qui concerne les affectations des droits d'accès.

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

Dispositifs de détection d'incidents

Hodi a mis en place des dispositifs permettant de détecter des anomalies dans les accès à la plateforme d'hébergement et au SI, de manière automatisée, avec remontée d'alerte auprès des personnes concernées.

Incidents de sécurité

Chaque acteur du SI et de la plateforme d'hébergement, utilisateur ou administrateur, Hodi ou sous-traitant, est sensibilisé à l'importance de signaler tout incident réel ou suspecté. Ceci inclut le vol de moyens informatiques ou de supports de données.

Le signalement des incidents et leur enregistrement sont systématiques. Les clients le font par l'intermédiaire de l'Espace Client Hodi, les utilisateurs internes suivent la procédure mise en place.

Cette procédure décrit les escalades et personnes à alerter selon la gravité de l'incident.

Les données statistiques relatives à la gestion des incidents sont intégrées dans le tableau de bord de la sécurité du SI.

Un incident de type violation de Données Personnelles respecte les obligations liées au RGPD, il peut faire l'objet d'une notification à la CNIL selon les cas.

Gestion de crise

Le plan de gestion de crise intègre les risques liés à l'informatique ainsi que les risques susceptibles d'une incidence sur le SI ou la plateforme d'hébergement.

16. Gestion de la continuité d'activité

PCA et PRA

Hodi dispose d'un PCA et PRA qui couvre notamment le risque cyclonique et qui envisage la disparition totale d'un data-center et/ou d'un opérateur de cloud, notamment grâce à des sauvegardes et des data-centers présents sur différents territoires, ainsi qu'à une attaque de type cryptolocker grâce aux sauvegardes techniquement inaccessibles à Hodi.

Une solution de PRA sur-mesure peut être proposée en option aux clients.

RPO et RTO

Le RPO (Recovery Point Objective, ou Point de Rétablissement des Données) est par défaut de 24 heures. Il peut être réduit selon les options souscrites par le client.

Le RTO (Recovery Time Objective, ou Temps de Rétablissement du Service) n'est pas garanti par défaut, mais en cas de sinistre grave, Hodi s'engage à restaurer dans les meilleurs délais le service avec pleine mobilisation de ses équipes. Le RTO dépend du volume de données à restaurer et de la localisation de la sauvegarde utilisée pour la restauration. Le RTO peut être garanti selon les options souscrites par le client.

17. Gestion de la conformité

Travail en binôme

Lors de la mise en place de nouvelles procédures, les salariés Hodi travaillent toujours en binôme, avec un salarié responsable de la définition de la nouvelle procédure, et un autre responsable de la vérification de la procédure.

Audit interne

Hodi réalise régulièrement des audits internes de ses procédures et son SI. Les sous-traitants de Hodi sont aussi soumis à des audits. En cas de non-conformité entraînant une atteinte à la sécurité, Hodi s'engage à communiquer avec le(s) client(s) concerné(s) dans le périmètre impacté.

Audit client

Les clients peuvent réaliser à leur initiative des audits organisationnels et, pour les clients en serveurs dédiés, peuvent faire réaliser des tests de pénétration sur leurs serveurs. Ces tests et audits sont soumis à la signature de clauses contractuelles spécifiques.