Plan d'Assurance Sécurité

Infomaniak Network

Sommaire

1. Historique 5
2. A propos de ce document 6
3. Introduction 7
3.1. Object du document 7
3.2. Domaine d'application 7
3.3. Evolution 7
3.4. Définitions 7
4. Bonnes pratiques 8
5. Gestion des risques 8
6. Politique de sécurité de l'Information 8
7. Organisation de la sécurité de l'information 9
7.1. Rôles et responsabilités 9
7.2. Gouvernance 9
7.3. Relation avec les organismes et les autorités 9
7.4. Veille et sécurité 10
8. Sécurité des ressources humaines 10
8.1. Recrutement 10
8.2. Gestion de la confidentialité 10
8.3. Sensibilisation à la sécurité 11
8.4. Charte informatique 11
8.5. Compétences et formations 11
8.6. Fin de contrat 12
9. Gestion des actifs 12
9.1. Inventaire 12
9.2. Licences logicielles 12
9.3. Identification et classification des actifs 12
9.4. Mises à jour, antivirus et chiffrement des supports 12
9.5. Nomadisme 13
9.6. Gestion des supports et matériels amovibles 13
9.7. Mise au rebut 13
10. Contrôle d'accès et gestion des identités 13
10.1. Politique de mot de passe 13
10.2. Gestion des droits 14
10.3. Revue des droits 14
10.4. Suppression des accès 14
11. Cryptographie 15
11.1. Utilisation de la cryptographie 15

11.2. Utilisation de protocoles chiffrés 15
11.3. Mobilité 15
12. Sécurités physiques et environnementales 15
12.1. Localisation 15
12.2. Centres de données 15
12.2.1. Sécurité physique des sites et contrôle d'accès 15
12.2.2. Sécurité des matériels 16
12.2.3. Système de détection, d'alarme et d'extinction automatique 16
12.3. Bureaux 16
12.3.1. Sécurité physique des sites et contrôle d'accès 16
12.4. Bureau vide et écran vide 16
13. Sécurité liée à l'exploitation 17
13.1. Veille cybersécurité 17
13.2. Données 17
13.2.1. Classification des données 17
13.2.2. Chiffrement des données 17
13.2.3. Intégrité des données 17
13.3. Gestion des changements 17
13.4. Protection contres les logiciels malveillants 18
13.5. Politique de sauvegarde 18
13.6. Journalisation 18
13.7. Synchronisation des horloges 18
13.8. Supervision 19
13.8.1. Principes 19
13.8.2. Astreintes 19
14. Sécurité des communications 19
14.1. Architecture technique 19
14.2. Internet 19
14.3. Réseaux wifi 19
14.4. Equipements de sécurité 20
14.4.1. Pare-feu 20
14.4.2. IDS 20
14.4.3. Anti DDoS 20
15. Acquisition, développement et maintenance des systèmes d'information 20
15.1. Cycle de vie de développement sécurisé 20
15.2. Séparation des environnements de développement, de test et opérationnels 21
16. Relation avec les fournisseurs 21
17. Gestion des vulnérabilités et des incidents 21
17.1. Gestion des vulnérabilités 21
17.2. Scanner de vulnérabilités 22

17.3. Programme de bug bounty 22
17.4. Gestion des incidents de sécurité 22
17.5. Gestion de crise 22
18. Gestion de la continuité d'activité 23
18.1. Continuité du pilotage 23
18.2. PCA et Résilience 23
18.3. Bilan d'impacts sur l'activité 23
18.4. RPO et RTO 23
18.5. Plan de tests 24
19. Conformité 24
19.1. Normes et réglementations 24
19.1.1. ISO 27001 24
19.1.2. LPD et RGPD 24
19.2. Audit 24
19.2.1. Audit interne 24
19.2.2. Audit externe 25
19.2.3. Audit technique 25
19.2.4. Audit client 25

1. Historique

Date	Auteur	Fonction	Nature de la modification
13.05.2025	Johann Laqua	RSSI	Changement du logo de l'entreprise, mise à jour des chapitres sur la sécurité physique, ajout du chapitre pour les définitions
19.04.2024	Johann Laqua	RSSI	Finalisation du document pour une première publication
14.02.2024	Johann Laqua	RSSI	Première version du document

2. A propos de ce document

Le but de ce document est de présenter le Plan d'Assurance Sécurité d'Infomaniak Network SA.

3. Introduction

3.1. Object du document

Le présent document établit notre Plan d'Assurance Sécurité (PAS), qui peut être annexé à nos contrats avec nos clients. Ce plan définit les engagements pris par Infomaniak Network pour répondre aux exigences contractuelles en matière de Sécurité des Systèmes d'Information (SSI). Ces dernières ont pour but :

- De garantir la protection des ressources des systèmes d'information utilisés dans la prestation de services convenus contractuellement ;
- De protéger nos clients contre tout préjudice pouvant résulter de l'indisponibilité de ces ressources, ainsi que de toute violation de leur intégrité ou confidentialité.

Notre Plan d'Assurance Sécurité (PAS) détaille les différentes dispositions liées à la sécurité, y compris les mesures physiques, organisationnelles, procédurales et techniques que nous avons mises en place.

3.2. Domaine d'application

Ce document concerne les services gérés par les équipes d'Infomaniak Network, de même que leurs activités.

3.3. Evolution

Toute modification apportée au Plan d'Assurance Sécurité (PAS) donne lieu à une nouvelle version de ce document. Les changements effectués sont consignés et datés dans l'historique des versions inclus dans le document.

Le Plan d'Assurance Sécurité (PAS) est examiné au minimum une fois par an par les responsables de la conformité et de la sécurité des systèmes d'information, puis approuvé par la direction.

3.4. Définitions

RSSI : Responsable de la sécurité des systèmes d'information
ISO : Organisation internationale de normalisation
EBIOS : Expression des besoins et identification des objectifs de sécurité
Red team : équipe de sécurité axée sur des exercices et des tests de sécurité offensive comprenant des personnes de différents départements.
ASDPO : Association suisse des délégués à la protection des données
NCSC : National cyber security centre
CERT : Computer emergency response team
RH : Ressources humaines
HTTPS : Hypertext transfer protocol secure

SSL : Secure sockets layer
IMAPS : Internet message access protocol secure
SMTPS : Simple mail transfer protocol secure
POP3S : Post office protocol 3 secure
IDS : Intrusion detection system
DDoS : Distributed denial of service
CVE : Common vulnerabilities and exposures
PCA : Plan de continuité d'activité
RPO : Recovery point objective
RTO : Recovery time objective
LPD : Loi fédérale sur la protection des données
RGPD : Règlement général de protection des données

4. Bonnes pratiques

La sécurité d'Infomaniak Network est pilotée par un comité de sécurité, ainsi qu'une équipe de conformité suivant les standards de la norme ISO 27001 pour l'ensemble de l'entreprise. Infomaniak Network est certifié ISO 27001:2022 sur les périmètres et activités suivants :

Développement et fourniture d'infrastructures en nuage, de services web, d'applications, d'assistance à la clientèle, de maintenance opérationnelle des centres de données.

5. Gestion des risques

Infomaniak Network a formalisé une évaluation écrite des risques qui couvre l'intégralité du champ d'application du plan d'assurance sécurité, en appliquant une méthodologie documentée garantissant la reproductibilité et la comparabilité de la démarche.

Ce processus d'évaluation des risques comporte une analyse, une gestion ainsi que des plans de mitigation des risques, aboutissant à des mesures et des projets concrets.

En outre, Infomaniak Network s'appuie sur des méthodes largement reconnues telles qu'EBIOS RM pour gérer les risques dans le cadre de son système de management de la sécurité de l'information (SMSI).

6. Politique de sécurité de l'Information

Infomaniak Network a une Politique de sécurité qui se trouve à cette adresse :
https://www.infomaniak.com/documents/politique_SI_EE_fr.pdf

Ce document expose clairement nos engagements et objectifs en matière de sécurité de l'information.

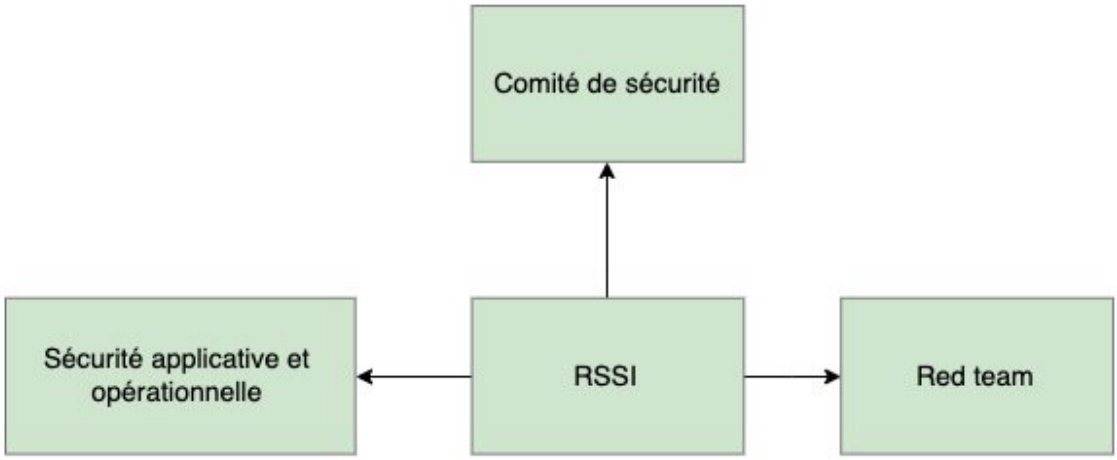
7. Organisation de la sécurité de l'information

Pour structurer notre approche en matière de sécurité des systèmes d'information (SSI), nous avons mis en place plusieurs outils complémentaires : un organigramme spécifique à la SSI, une politique de sécurité des systèmes d'information (PSSI) interne, ainsi qu'un système de management de la sécurité de l'information (SMSI). Ces éléments sont essentiels pour garantir l'application rigoureuse et cohérente de nos procédures de sécurité.

7.1. Rôles et responsabilités

Les responsabilités en matière de sécurité ont été définies et attribuées.

Infomaniak Network a désigné un Responsable de la Sécurité des Systèmes d'Information (RSSI). Celui-ci supervise l'ensemble des mesures techniques et organisationnelles mises en œuvre dans le cadre de notre stratégie globale de sécurité de l'information.



7.2. Gouvernance

Une équipe dédiée à la gouvernance est instaurée aux niveaux stratégique et opérationnel.

Cette équipe se réunit régulièrement afin de superviser les questions relatives à la sécurité des systèmes d'information. Les procès-verbaux de ces réunions sont conservés de manière sécurisée.

7.3. Relation avec les organismes et les autorités

Infomaniak Network est membre d'association professionnelles (ASDPO) et entretien des relations avec les autorités (NCSC et Cyber Security Hub) pour les évolutions dans le domaine de la sécurité de l'information.

7.4. Veille et sécurité

Une veille de la sécurité, technique et légale, est en place et menée au sein de l'activité. Elle permet de prévenir les risques spécifiquement liés aux activités d'Infomaniak Network.

Infomaniak Network s'appuie sur un partenariat avec une société spécialisée en cybersécurité pour avoir une surveillance sur le darkweb pour les actifs sensibles qui sont sous sa responsabilité.

8. Sécurité des ressources humaines

8.1. Recrutement

Notre département RH applique une procédure de recrutement pour chaque candidat à l'embauche, avec des mesures de sécurité proportionnelles par rapport au niveau de classification de chaque employé et aux risques identifiés.

Les vérifications suivantes sont faite :

- Contrôle de l'identité du candidat
- Vérification des compétences du poste
- Vérification des références du candidat
- Vérification du casier judiciaire
- Vérification poussée des antécédents pour les candidats aux hauts niveaux de sécurité

8.2. Gestion de la confidentialité

Les contrats de travail stipulent clairement les responsabilités du personnel en matière de sécurité de l'information.

Une clause de confidentialité, extraite des conditions générales du contrat de travail, engage le personnel à respecter strictement la confidentialité des données sensibles et privées auxquelles il a accès dans le cadre de ses fonctions chez Infomaniak. Toute violation de cette clause entraîne des conséquences pour le contrevenant.

En outre, un processus disciplinaire formel a été établi et communiqué à tous les membres du personnel ainsi qu'aux autres parties prenantes concernées. Ce processus prévoit des sanctions appropriées à l'égard de toute personne ayant enfreint la politique de sécurité de l'information.

8.3. Sensibilisation à la sécurité

Nous organisons des sessions d'intégration en matière de sécurité afin de vérifier la conformité des postes de travail, tout en sensibilisant les collègues aux risques relatifs à la sécurité des systèmes d'information (SSI), à nos procédures de sécurité physique et logique.

Pendant ces sessions, nous présentons également des documents importants comme notre Politique de Sécurité de l'Information (PSI) ainsi que nos Directives Générales concernant la sécurité.

Chaque année, nous élaborons un programme de sensibilisation en utilisant divers outils d'évaluation portant sur divers thèmes relatifs à la sécurité et à la cybersecurité. Cela inclut des campagnes de phishing et de social engineering, entre autres.

Plusieurs communications aux collaborateurs sont réalisées par e-mail dans le but de les sensibiliser aux risques de sécurité de l'information, à la protection des données, aux cyber-risques ainsi qu'aux mises à jour de notre système de management de la sécurité de l'information.

8.4. Charte informatique

Infomaniak Network dispose de Directives Générales en matière de Sécurité, équivalentes à une charte informatique, qui sont régulièrement mises à jour et communiquées à tous les membres de notre entreprise.

Dès leur embauche et chaque année, ils s'engagent solennellement à les respecter, faute de quoi des sanctions disciplinaires pourraient être prises à leur encontre.

8.5. Compétences et formations

Chaque année, lors des entretiens individuels, le département des ressources humaines mène une enquête auprès des salariés afin d'évaluer leurs besoins en matière de formation. Un programme de formation annuel est ensuite établi pour identifier les formations nécessaires pour combler :

- Les lacunes en termes de compétences d'un employé, d'une équipe ou d'un service ;
- Les besoins de développement continu des compétences.

Les formations proposées peuvent être dispensées en interne ou par des prestataires extérieurs.

Plusieurs formations techniques sont proposées tout au long de l'année par des délégués ou des experts en cybersécurité, ainsi que des rapports et statistiques trimestriels sur les vulnérabilités qui pourraient impacter nos systèmes, afin de renforcer les compétences de notre personnel.

8.6. Fin de contrat

Une procédure de sortie ou de résiliation de contrat a été mise en place et communiquée à tous les responsables concernés dans l'entreprise. Cette procédure vise à assurer que le collaborateur n'a plus accès ni physique ni logiciel au système d'information de l'entreprise.

9. Gestion des actifs

9.1. Inventaire

Infomaniak Network établit des inventaires d'actifs essentiels et de biens de soutien. Ces derniers sont recensés dans notre système de gestion de la sécurité de l'information (SMSI) ainsi que dans nos évaluations des risques.

Nous révisons ces actifs chaque année grâce au SMSI et procédons à leur mise à jour via des processus automatisés en fonction des exigences des différentes équipes internes.

9.2. Licences logicielles

Infomaniak Network est déterminée à garantir l'utilisation de licences valides pour les logiciels tiers au sein de ses équipes internes et prend les mesures nécessaires pour protéger les droits de propriété intellectuelle.

9.3. Identification et classification des actifs

Les actifs sont segmentés, identifiés clairement grâce à une nomenclature et une convention de dénomination établies par les équipes internes. Des contrôles continus et annuels sont mis en place pour garantir la légitimité des accès, la restriction des accès non autorisés et la fiabilité de l'inventaire.

Les données sont classifiées en fonction des besoins de sécurité de l'information de l'organisation, en prenant en compte les exigences de confidentialité, d'intégrité et de disponibilité, ainsi que les préoccupations majeures des parties prenantes.

9.4. Mises à jour, antivirus et chiffrement des supports

Le responsable de la sécurité des systèmes d'information (RSSI) supervise la protection centrale des actifs de l'entreprise, y compris les postes de travail des employés, contre les virus et les logiciels malveillants. Une stratégie de défense contre ces menaces est renforcée par une formation adéquate des utilisateurs.

La sécurité des supports de stockage interne et amovible est assurée par un processus de chiffrement configuré et surveillé.

Des indicateurs clés de performance (KPI) sont suivis régulièrement pour vérifier la conformité et la protection des actifs.

9.5. Nomadisme

Pour garantir la sécurité des informations lors du télétravail, diverses précautions ont été prises. Des directives spécifiques au télétravail ont été élaborées et communiquées au personnel. Il est obligatoire d'utiliser un réseau privé virtuel (VPN) sécurisé pour se connecter aux ressources de l'organisation depuis l'extérieur.

En outre, l'utilisation d'appareils personnels ("Bring Your Own Device", ou BYOD) n'est pas autorisée dans ce contexte.

9.6. Gestion des supports et matériels amovibles

Des directives relatives à l'utilisation des supports amovibles ont été mises en place, diffusées et sont bien connues du personnel. Ces instructions incluent des règles strictes concernant leur utilisation afin de minimiser les risques potentiels et des recommandations pour assurer leur protection.

Par exemple, il peut être demandé de chiffrer les supports amovibles contenant des données confidentielles ou critiques, ou encore de restreindre leur utilisation à certaines circonstances particulières.

9.7. Mise au rebut

Une politique de recyclage du matériel et de désaffectation des actifs a été établie et mise en œuvre pour gérer les actifs sensibles de l'entreprise.

Cette procédure a pour but de fournir des instructions claires sur la façon de traiter tous types de matériel qui stocke des données confidentielles. Cela comprend des règles visant à garantir la destruction sécurisée des données avant le transfert ou l'élimination du matériel, afin d'éviter toute récupération ultérieure de celles-ci.

10. Contrôle d'accès et gestion des identités

10.1. Politique de mot de passe

Les collaborateurs doivent appliquer notre politique de gestion des mots de passe afin de garantir la sécurité de nos comptes et de nos données pendant toute la durée de leur cycle de vie.

Nous nous engageons également à informer nos utilisateurs des exigences spécifiques liées à notre politique de mot de passe, en tenant compte de leurs compétences, de leur rôle et de la sensibilité des ressources qu'ils peuvent accéder.

Voici quelques exemples de bonnes pratiques recommandées dans le cadre de notre politique de mots de passe :

- Obligation d'utiliser un gestionnaire de mots de passe autorisé, pour générer et stocker des mots de passe forts ;
- Créer des mots de passe robustes composés d'au moins douze caractères alphanumériques et spéciaux ;
- Éviter d'utiliser des termes couramment utilisés ou facilement devinables ;
- Ne jamais partager son mot de passe avec quelqu'un d'autre ni le réutiliser pour plusieurs comptes ;
- Configurer une authentification multi-facteurs chaque fois que possible ;

Nous encourageons fortement tous nos utilisateurs à respecter scrupuleusement ces conseils pour contribuer à maintenir un haut niveau de sécurité au sein de notre organisation.

10.2. Gestion des droits

Cette attribution des accès est organisée par département, en accordant uniquement les permissions nécessaires en fonction des tâches assignées à chaque individu.

Toute demande d'autorisation doit être soumise via des canaux internes prédéfinis et approuvée après examen approfondi.

10.3. Revue des droits

Une revue annuelle des droits d'accès est effectuée par le RSSI et les délégués à la sécurité.

Des contrôles de sécurité annuels sont réalisés pour les différents services internes et externes, les ordinateurs de bureau, les accès aux réseaux sans fil et Wi-Fi.

La gestion avancée des accès internes fait l'objet d'une vérification automatique et annuelle via des outils internes.

10.4. Suppression des accès

La suppression des accès des employés d'Infomaniak Network est associée au processus RH de gestion des entrées et sorties. Ce processus de sortie est rigoureusement suivi à l'aide d'outils internes dédiés, sous la direction de responsables désignés pour entreprendre les actions requises.

11. Cryptographie

11.1. Utilisation de la cryptographie

Des règles pour l'utilisation efficace de la cryptographie, notamment la gestion des clés cryptographiques, sont définies et mises en œuvre.

Infomaniak Network a établi et mis en œuvre une Politique de contrôle cryptographique et de chiffrement, qui a été diffusée et est connue de l'ensemble de son personnel.

11.2. Utilisation de protocoles chiffrés

Infomaniak Network et ses collaborateurs veillent à utiliser des protocoles de réseau sécurisés aussi souvent que possible, tant sur les réseaux publics comme Internet qu'au sein de son réseau interne. Par exemple, nous favorisons l'utilisation de HTTPS pour la navigation web, de IMAPS, SMTPS ou POP3S pour la messagerie, et de SSH (Secure Shell) pour les opérations d'administration système.

11.3. Mobilité

Les collaborateurs de l'entreprise Infomaniak Network utilisent uniquement leurs ordinateurs portables pour se connecter à distance sur le réseau interne sécurité de l'entreprise.

12. Sécurités physiques et environnementales

12.1. Localisation

Les centres de données d'Infomaniak Network sont situés exclusivement en Suisse et appartiennent entièrement à l'entreprise.

12.2. Centres de données

12.2.1. Sécurité physique des sites et contrôle d'accès

Les locaux font l'objet d'une surveillance constante grâce à un système de caméras de vidéosurveillance, afin de prévenir tout accès physique non-autorisé.

L'accès aux centres de données et aux serveurs est protégé par plusieurs sas et par un système de contrôle d'accès électronique pourvu d'une identification biométrique. Afin de renforcer encore davantage la sécurité du centre de données, chaque secteur et chaque allée desservant les racks sont équipés d'un système de reconnaissance faciale.

L'accès aux salles serveurs est restreint à un nombre limité de membres du personnel de l'entreprise, spécialement formés et autorisés dans les zones de travail segmentées en fonction des besoins spécifiques des différentes équipes.

12.2.2. Sécurité des matériels

Les centres de données sont tous certifiés ISO 27001, ISO 14001 et bénéficient d'une redondance n+1 au niveau de l'alimentation électrique, backbone fibre optique, du refroidissement, des groupes électrogènes et des onduleurs afin de garantir un fonctionnement sans interruption de vos infrastructures techniques.

12.2.3. Système de détection, d'alarme et d'extinction automatique

Nos sites sont monitorés et entièrement équipés de systèmes de détection d'incendie. Nos systèmes d'extinction, calibrés pour chaque type d'environnement d'un centre de donnée, assurent l'extinction automatique dans les zones où un feu pourrait démarrer. Ces systèmes opèrent dans les pièces contenant des équipements électriques comme les onduleurs, les batteries ou les tableaux électriques. Ce dispositif de surveillance fonctionne en permanence et est régulièrement testé.

12.3. Bureaux

12.3.1. Sécurité physique des sites et contrôle d'accès

Les bureaux du siège social d'Infomaniak Network sont équipés de portes à verrouillage automatique, accessibles uniquement via un système de badges et de reconnaissance faciale : des contrôles d'accès physiques sont effectués régulièrement.

Des caméras de surveillance sont installées dans les couloirs ainsi que dans les zones communes du bâtiment, y compris aux abords des espaces de travail des employés.

12.4. Bureau vide et écran vide

Une politique de bureau vide et écran vide est en place, elle a été communiquée à tous les employés. Elle comprend des instructions détaillées sur le verrouillage des écrans, la gestion appropriée des documents papier et numériques, l'utilisation des tableaux blancs et la destruction sécurisée des documents confidentiels.

13. Sécurité liée à l'exploitation

13.1. Veille cybersécurité

Les informations concernant les menaces en matière de sécurité de l'information sont recueillies, analysées et traitées afin de générer des renseignements relatifs auxdites menaces.

Nous bénéficions d'un service tiers nous offrant la possibilité de superviser les activités et menaces présentes sur le Dark Web.

La recherche de ces menaces potentielles s'effectue au moyen de mots-clés et de termes spécifiques prédéterminés, notamment ceux liés à :

- L'exposition des employés ;
- La surveillance de la marque et des noms de domaine ;
- Le suivi du Darknet ;
- L'exploration du deep web et la découverte des actifs.

13.2. Données

13.2.1. Classification des données

Les informations sont classifiées conformément aux besoins de sécurité de l'information de l'organisation, sur la base des exigences de confidentialité, d'intégrité, de disponibilité, et des exigences importantes des parties intéressées.

13.2.2. Chiffrement des données

Les données sont sécurisées pendant leur transfert entre les postes de travail des collaborateurs, des clients et le système d'information d'Infomaniak Network grâce à l'utilisation de protocoles de chiffrement décrits au chapitre 11 de ce document.

13.2.3. Intégrité des données

Infomaniak Network s'engage à protéger les données de ses clients en mettant en place des procédures, des mesures techniques et des protocoles sécurisés pour prévenir toute altération, qu'elle soit volontaire ou accidentelle. Cela inclut des garanties solides en matière de transmission et de conservation des informations confidentielles.

13.3. Gestion des changements

Notre politique de gestion des changements offre aux utilisateurs un ensemble de procédures opérationnelles bien documentées ainsi que des contrôles rigoureux sur ces derniers. Elle comprend :

- Le cadrage des changements, qui définit clairement leur portée et leurs objectifs ;

- Les directives à suivre pour la mise en œuvre des changements, y compris les critères d'acceptation et les règles de sécurité ;
- La planification détaillée des changements, comprenant l'identification des risques potentiels et des plans de contingence appropriés ;
- Le contrôle strict des changements, avec une traçabilité complète de toutes les modifications apportées au système ;
- Des processus clairs et simples à suivre pour les mises à jour régulières du système, garantissant sa stabilité et sa performance optimales.

13.4. Protection contres les logiciels malveillants

Une protection contre les programmes malveillants est mise en œuvre et renforcée par une sensibilisation appropriée des utilisateurs. Le parc informatique des postes de travail est supervisé par un antivirus centralisé et des contrôles réguliers, des indicateurs sont mis en place et revus pendant les réunions de sécurité.

13.5. Politique de sauvegarde

Une politique de sauvegarde et de sécurité des données est en vigueur, définissant des directives claires pour la sauvegarde et la restauration de l'information conformément aux actifs identifiés dans notre système d'information. Cette politique précise la durée de conservation, la fréquence, le type de chiffrement ainsi que les protocoles de test à suivre.

Grâce à ces mesures, nous pouvons assurer la protection et la récupération efficaces de nos données importantes.

13.6. Journalisation

Des journaux qui enregistrent les activités, les exceptions, les pannes et autres événements pertinents sont générés, conservés, protégés et analysés.

13.7. Synchronisation des horloges

Les horloges des systèmes de traitement de l'information utilisés par l'organisation sont synchronisées avec des sources de temps approuvées.

Infomaniak Network dispose de ses propres serveurs de référence temporelle, qui permettent à tous les appareils et serveurs de bénéficier d'une synchronisation temporelle précise. Ce service est également accessible au public et mis à la disposition des clients comme des non-clients.

13.8. Supervision

13.8.1. Principes

L'intégralité des services et systèmes administrés par Infomaniak Network font l'objet d'une surveillance attentive. Nos outils de supervision s'appuient sur des protocoles standard ainsi que sur des automates conçus spécialement pour collecter des données auprès de toutes les sources de contrôle.

En cas de défaillance, des alertes en temps réel sont émises pour tous les services surveillés.

Ces alertes peuvent également être envoyées sous forme de SMS aux équipes d'astreinte pendant les heures hors service.

13.8.2. Astreintes

L'équipe d'astreinte assure une surveillance et une intervention continues 24 heures sur 24, 7 jours sur 7, sur le système d'information (SI) d'Infomaniak Network. Cette équipe est structurée en différents niveaux et regroupe des spécialistes issus de diverses équipes de production, couvrant ainsi l'ensemble des domaines de compétences.

14. Sécurité des communications

14.1. Architecture technique

L'infrastructure prenant en charge les services d'Infomaniak Network est compartimentée et structurée en plusieurs zones de sécurité distinctes. Cette conception offre une sécurité renforcée, évolutive et adaptée aux exigences actuelles et futures. Les groupes de services d'information, d'utilisateurs et de systèmes d'information sont isolés au sein des réseaux internes à l'organisation, garantissant ainsi un haut niveau de protection contre d'éventuelles menaces externes ou internes.

14.2. Internet

Infomaniak Network dispose de ses propres adresses IP publiques ainsi que de plusieurs connexions Internet provenant de fournisseurs différents. Cela permet à l'entreprise de garantir un niveau de service optimal à ses clients et employés, même en cas de défaillance d'un fournisseur. De plus, toutes les prestations gérées par Infomaniak bénéficient d'une redondance, assurant leur continuité.

14.3. Réseaux wifi

Les réseaux Wi-Fi chez Infomaniak sont segmentés en fonction de leurs utilisations spécifiques telles que les réseaux Wi-Fi invités, employés, pré-production, etc., avec un

contrôle d'accès basé sur la gestion des droits. En outre, les points d'accès Wi-Fi sont sécurisés pour empêcher tout accès non autorisé.

14.4. Equipements de sécurité

14.4.1. Pare-feu

Chez Infomaniak, des firewalls sont installés entre chaque zone de sécurité et chaque zone applicative. Ainsi, les flux entrants en provenance de l'extérieur doivent traverser plusieurs niveaux de firewall avant d'atteindre le service sollicité, ce qui assure une protection renforcée contre les menaces potentielles.

14.4.2. IDS

Des sondes IDS ont été déployées à des endroits clés du réseau Infomaniak afin d'analyser les flux entrants et sortants du système d'information. Ces sondes sont chargées de détecter les activités suspectes ou anormales, ainsi que le trafic malveillant, et d'en informer immédiatement les équipes de production. Pour cela, les sondes reçoivent régulièrement des mises à jour de signatures d'attaques depuis notre prestataire spécialisé en cybersécurité. L'installation et la maintenance de ces dispositifs relèvent de la responsabilité de l'équipe de sécurité de production.

14.4.3. Anti DDoS

Infomaniak met en place une protection anti-DDoS appropriée pour chacune des technologies qu'elle exploite, assurant ainsi la défense de toutes ses plates-formes et infrastructures face à ce type de cybermenace. Ce faisant, elle entend maintenir un niveau élevé de disponibilité et de résilience pour ses services, au profit de sa clientèle et de son personnel.

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

15.1. Cycle de vie de développement sécurisé

Des règles de sécurité, de bonnes pratiques et de bon sens sont établies et mises en œuvre pour assurer un développement sûr des logiciels et des systèmes. Parmi ces principes figurent :

- L'audit et l'enregistrement des actions
- La formation des développeurs à la sécurité
- La lutte contre les programmes malveillants
- Les tests de sécurité des applications
- Les tests de conformité du système
- La sécurité des applications Web côté client et serveur

- La sécurité des applications mobiles
- La cryptographie

Le personnel du service de développement est sensibilisé aux risques liés à la sécurité des applications et aux normes édictées par l'OWASP (Open Web Application Security Project).

En outre, nous avons mis en place une politique de surveillance et de contrôle du développement externe qui recommande les modalités d'exécution, les mesures de sécurité existantes ainsi que des instructions impératives relatives à la gestion des journaux, la gestion des accès, la gestion du code source et les tests de sécurité au cours du cycle de développement.

15.2. Séparation des environnements de développement, de test et opérationnels

Nos réseaux et infrastructures de développement sont isolés aussi bien physiquement que logiquement en fonction des services fournis. Nous mettons également en place une séparation distincte entre les divers environnements applicatifs tels que ceux consacrés au développement, aux tests, à la préproduction et à la production.

Plus précisément, l'environnement de développement est strictement restreint et uniquement accessible aux développeurs via notre réseau interne hautement sécurisé.

16. Relation avec les fournisseurs

Nous avons instauré des processus et des procédures visant à gérer les risques potentiels relatifs à la sécurité de l'information découlant de l'utilisation de nos produits ou services auprès de fournisseurs donnés.

De plus, nous veillons scrupuleusement à mettre en place et à convenir des exigences adéquates en matière de sécurité de l'information avec chacun de nos fournisseurs.

Par ailleurs, nous effectuons régulièrement une révision, une évaluation et une gestion proactive des modifications apportées aux pratiques de sécurité de l'information de nos fournisseurs et prestataires de services respectifs.

17. Gestion des vulnérabilités et des incidents

17.1. Gestion des vulnérabilités

Un workflow a été mis en place du côté des équipes de production pour la gestion des vulnérabilités de type CVE à l'aide d'outils internes et de veilles technologiques.

Différents outils internes permettent un suivi, une surveillance et un balayage automatisé des faiblesses susceptibles d'affecter nos systèmes d'information.

Une SLA (Service Level Agreement) interne a été mise en place pour traiter les signalements de vulnérabilités, avec un délai d'intervention fixé en fonction de la gravité des failles identifiées.

17.2. Scanner de vulnérabilités

Des analyses sont régulièrement réalisées sur plusieurs plages d'adresses IP Infomaniak que nous avons spécifiées. Nous sommes alertés via un tableau de bord en cas de détection de vulnérabilités et programmons des plans d'actions pour corriger rapidement les failles découvertes.

17.3. Programme de bug bounty

Nous collaborons activement avec une communauté composée de chercheurs et d'éthiques "hackers" afin d'offrir à nos clients le niveau de sécurité optimal. Un programme publique est disponible ainsi que des programmes privés afin de tester tous les services proposés à nos clients.

Les lanceurs d'alerte bénéficient d'une protection adéquate, tandis que nos employés ont la possibilité de rapporter toute irrégularité suspectée de façon confidentielle et anonyme à tout moment.

17.4. Gestion des incidents de sécurité

Une procédure bien établie de gestion des incidents de sécurité définit clairement les rôles, les responsabilités, le processus de triage, la communication, la réponse et l'atténuation, ainsi que l'ensemble du flux de travail nécessaire pour assurer une résolution complète de l'incident.

Selon la gravité et la nature de l'événement, Infomaniak Network peut collaborer activement avec les autorités compétentes et coordonner le processus de traitement de l'incident afin d'assurer sa résolution rapide et efficace.

17.5. Gestion de crise

Une procédure de gestion de crise spécifique est formalisée. Cette procédure présente les différentes étapes à suivre pour résoudre l'incident de manière la plus efficace possible et pour communiquer au mieux en interne et en externe sur la cause et les impacts.

18. Gestion de la continuité d'activité

18.1. Continuité du pilotage

Un plan de continuité est défini pour le management et le pilotage des services et actifs de l'infrastructure de nos centres de données.

18.2. PCA et Résilience

La continuité d'activité est prise en compte dès la phase de conception et d'architecture des services gérés par Infomaniak Network.

La redondance entre nos différents centres de données, ainsi que la sauvegarde sur plusieurs supports et dans plusieurs de nos centres de données contribuent à assurer la continuité d'activité pour nos clients.

Les solutions de reprise après sinistre de nos services gérés dépendent des architectures techniques et logicielles et sont adaptées au niveau de chaque offre métier, en fonction des contraintes spécifiques et des équipes de production.

18.3. Bilan d'impacts sur l'activité

Un Bilan d'Impacts sur l'Activité (BIA) a été mis en place dans le but de collecter des données afin de planifier et gérer efficacement les incidents de sécurité affectant les actifs de notre système d'information.

Ce BIA permet d'identifier les activités et les ressources clés de l'entreprise, ainsi que différents niveaux de gravité associés. Des mesures spécifiques ont également été définies pour assurer la continuité de l'activité en cas d'incident.

18.4. RPO et RTO

Infomaniak Network a établi une stratégie de continuité en prenant en considération trois facteurs clés :

- Le Temps maximal d'interruption admissible (TMA), également connu sous le nom d'Objectif de temps de rétablissement (OTR) ou Recovery Time Objective (RTO) en anglais ;
- La perte maximale acceptable de données (PMAD), aussi appelée Objectif de point de récupération (OPR) ou Recovery Point Objective (RPO) en anglais ;
- Les impacts financiers et commerciaux potentiels.

Lorsque ces éléments sont pertinents, ils sont consignés dans le Bilan d'Impacts sur l'Activité (BIA).

18.5. Plan de tests

Un plan de tests, qui tient compte des situations à risque, est établi et mis en œuvre chaque année. Il permet ce qui suit :

- En amont : de mesurer l'efficacité du plan par rapport aux objectifs de continuité, grâce à des indicateurs, des audits, etc.
- Durant une crise : de surveiller les niveaux de service effectivement atteints et le fonctionnement des procédures opérationnelles prévues dans le cadre du PCA.
- A posteriori : de mettre en place un plan d'amélioration.

19. Conformité

19.1. Normes et réglementations

19.1.1. ISO 27001

Les équipes d'Infomaniak Network s'appuient sur les normes de sécurité internationalement reconnues, telles que l'ISO 27001:2022 et l'ISO 27002:2022, comme références pour élaborer et gérer les services qu'elles proposent à leurs clients.

Ces normes constituent un cadre robuste pour garantir la confidentialité, l'intégrité et la disponibilité des données sensibles, ainsi que pour assurer une gestion efficace des risques liés à la sécurité de l'information.

19.1.2. LPD et RGPD

Infomaniak Network a mis en place une politique de confidentialité des données, consultable sur son site Internet à l'adresse suivante :
https://www.infomaniak.com/fr/cgv/politique-de-confidentialite

De plus, la politique d'utilisation des cookies est accessible via ce lien :
https://www.infomaniak.com/fr/cgv/politique-dutilisation-des-cookies

19.2. Audit

19.2.1. Audit interne

Le contrôle des activités de sécurité dans les périmètres de certification d'Infomaniak Network est assuré par des consultants qualifiés, qui travaillent sous la supervision de l'équipe de conformité.

Ces consultants effectuent régulièrement un examen des éléments associés aux périmètres certifiés, conformément au plan d'audit et à la déclaration d'applicabilité d'Infomaniak Network.

Les documents relatifs aux audits internes sont confidentiels et ne peuvent être divulgués.

19.2.2. Audit externe

Dans le cadre de la certification ISO 27001:202, Infomaniak Network est auditée annuellement par les organismes certificateurs.

19.2.3. Audit technique

Infomaniak Network fait appel à des experts qualifiés pour effectuer des audits techniques réguliers sur son système d'information et selon les besoins et mise en production de nouveaux services.

19.2.4. Audit client

Les clients ont la possibilité d'effectuer des tests d'intrusion (pentests) sur les services qu'ils utilisent, dans le strict respect des conditions spécifiées dans leur contrat.

Ils doivent également prendre en compte les contraintes des équipes internes, telles que la réalisation des pentests uniquement pendant les heures de bureau et en informant les équipes de production à l'avance.