



Manuel de politique de sécurité, de disponibilité et de confidentialité

Semana, SAS Mise à

jour précédente : 5/07/2022

Révision : Nicolas Cosme et Albert Reynaud

Point de contact : Nicolas Cosme - nicolas@semana.io

Évolution du document	3
Champ d'application	3
Référence normative	3
Politiques de sécurité de l'information	3
Organisation de la sécurité de l'information	4
Sécurité des ressources humaines	5
Sécurité physique et environnementale	6
Information et gestion des actifs	6
Politique de contrôle d'accès	9
Politique de cryptage	12
Politique de sauvegarde/restauration	12
Sécurité des opérations	13
Développement et maintenance du système	13
Relations avec les fournisseurs	14
Gestion des incidents de sécurité de l'information	15
Aspects de la sécurité de l'information dans le cadre de la gestion de la continuité des activités	16
Conformité	16

1. Évolution du document

Date de la dernière révision	Auteur
05/04/2022	Nicolas Cosme

2. Champ d'application

Semana a établi le document suivant pour la mise en œuvre, le maintien et l'amélioration continue d'un système de gestion de la sécurité de l'information dans le contexte de notre organisation. Ce document comprend également les exigences en matière d'évaluation et de traitement des risques liés à la sécurité de l'information, adaptées aux besoins de l'organisation.

Cette politique s'applique à toutes les données et à tous les équipements détenus et exploités par Semana.

3. Référence normative

Le présent document et nos politiques de sécurité internes sont conformes à la norme ISO/IEC 27001:2013, reconnue sur le marché pour les technologies de l'information, les techniques de sécurité et les systèmes de gestion de la sécurité de l'information.

4. Politiques de sécurité de l'information

Sécurité de l'information Politiques

Semana met en œuvre une politique de sécurité des systèmes d'information (PSSI). Nous avons mis en place un ensemble de procédures et de politiques afin que chaque membre de l'entreprise prenne conscience de l'importance de la sécurité de l'information. L'attention des employés et des tiers est attirée sur l'importance de respecter les procédures, au moment de l'engagement, mais aussi de façon régulière,

par le biais d'une formation générale. Notre programme de sécurité vise à assurer la protection des données de nos clients et à répondre aux préoccupations en matière de protection de la vie privée.

Examen des politiques en matière de sécurité de l'information

Notre PSSI est un document interne confidentiel de Semana. Notre processus de révision comprend l'évaluation des possibilités d'amélioration des politiques de l'organisation et de l'approche de la gestion de la sécurité de l'information en réponse aux changements de l'environnement organisationnel, des circonstances commerciales, des conditions juridiques ou de l'environnement technique. L'approbation de la direction pour une politique révisée est nécessaire et enregistrée. Il s'agit de notre documentation la plus récente. **Des mises à jour sont effectuées au fur et à mesure que des changements importants se produisent et sur une base annuelle.**

5. Organisation de la sécurité de l'information

Rôles et responsabilités en matière de sécurité de l'information

Nicolas COSME, notre directeur technique, est le propriétaire qui a approuvé la responsabilité de gestion pour le développement, l'examen et l'évaluation des politiques. Il dirige les efforts de Semana en matière de sécurité de l'information.

Séparation des tâches

Aucune personne ne peut accéder, modifier ou utiliser les actifs sans autorisation ou détection. D'autres contrôles, tels que la surveillance des activités, les pistes d'audit et la supervision de la direction, sont en place pour éviter toute utilisation non autorisée ou abusive des actifs de Semana.

Sécurité de l'information dans la gestion de projet

Nicolas COSME, notre CTO, a une formation d'ingénieur en informatique et plus de 15 ans d'expertise dans le développement de logiciels.

Semana applique les principes du "privacy by design", ce qui signifie que l'impact sur la collecte et le stockage des données est pris en compte à tous les stades du développement. En particulier, les développements web appliquent les meilleures pratiques de l'OWASP. En outre, les membres de notre personnel sont régulièrement (au moins une fois par an) formés aux outils et processus de sécurité, y compris à la gestion des données à caractère personnel. Les programmes de formation passés et futurs sont disponibles sur demande.

Contact avec les autorités

Notre procédure de gestion des incidents définit les rôles et les responsabilités en matière de communication en cas d'incident et précise les responsabilités en matière de contact avec les autorités (par exemple, les services d'urgence, les organismes de réglementation, les autorités de contrôle et les services publics) et de signalement de ces incidents en temps utile.

6. Sécurité des ressources humaines

Sensibilisation, éducation et formation à la sécurité de l'information

Tous les ingénieurs suivent un programme de formation à la sécurité dans le cadre de leur intégration, notamment en ce qui concerne la gestion des clés, la sécurité des points d'accès et d'autres sujets. Une formation annuelle permet de s'assurer que tous les employés et les sous-traitants connaissent et comprennent leurs responsabilités avant de se voir accorder l'accès à des informations confidentielles et à des systèmes d'information. Ils sont également informés des attentes en matière de sécurité de l'information liées à leur rôle au sein de l'organisation.

Filtrage et vérification des antécédents

Tous les employés et sous-traitants de Semana font l'objet d'une vérification rigoureuse de leurs antécédents avant qu'une offre d'emploi ne leur soit faite. Tous les employés font l'objet d'une vérification de leur emploi et de leur formation.

Conditions d'emploi

Nos contrats comportent des clauses spécifiques relatives à la confidentialité des données afin de protéger nos actifs informationnels, et prévoient les responsabilités des employés et des sous-traitants en matière de sécurité de l'information.

Licenciement et changement d'emploi

L'accès des employés licenciés est examiné et ajusté si nécessaire. Les comptes des employés licenciés sont désactivés lors de leur transfert ou de leur licenciement, à compter du dernier jour de travail et avant la fin de la journée. Étant donné qu'il peut y avoir des retards dans la notification des changements de responsabilités des utilisateurs, des examens périodiques de l'accès des utilisateurs sont effectués par Nicolas COSME.

Procédure disciplinaire

Un employé ayant enfreint cette politique peut faire l'objet de mesures disciplinaires pouvant aller jusqu'au licenciement.

7. Sécurité physique et environnementale

Périmètre de sécurité physique et contrôles d'entrée

L'accès physique à Semana est contrôlé par des cartes d'accès individuelles.

Les employés doivent être conscients de l'environnement physique - l'accès aux zones sécurisées de Semana est restreint, et les situations auxquelles il faut faire attention sont les suivantes :

- Personnel non autorisé dans les zones sécurisées

- Utilisateurs inconnus sur un ordinateur
- Matériel manquant ou déplacé
- Portes ouvertes ou déverrouillées alors qu'elles sont normalement sécurisées

Sécurité des centres de données

Semana héberge l'infrastructure de ses produits chez des fournisseurs d'infrastructure de premier plan, actuellement Google Cloud Platform, qui fournit des niveaux élevés de disponibilité physique et de réseau et maintient divers niveaux de sécurité vérifiés, y compris SOC 2 Type II et la conformité ISO 27001.

Nos fournisseurs d'infrastructure mettent à disposition leurs documents de conformité sur leurs sites. Veuillez consulter les sites suivants : Google Cloud Platform : <https://cloud.google.com/security/compliance>.

8. Gestion de l'information et des actifs

Inventaire des actifs

Semana tient un inventaire de tous les actifs associés aux installations d'information et de traitement de l'information. Cet inventaire couvre à la fois les actifs physiques (par exemple les postes de travail) et les actifs non physiques (infrastructure, données, etc.). Pour chacun des actifs identifiés, la propriété de l'actif est attribuée et la classification est identifiée (voir la classification de l'information).

Classification des informations

Rôles et responsabilités

Semana définit trois rôles et responsabilités pour le traitement des informations.

Propriétaire des données

La personne qui est en fin de compte responsable des données et des informations collectées et gérées par son équipe. Il s'agit généralement du PDG ou du directeur technique.

Dépositaires de données

Les conservateurs de données sont responsables de la maintenance et de la sauvegarde des systèmes, des bases de données et des serveurs qui stockent les données de l'organisation. En outre, il est responsable du déploiement technique de toutes les règles définies par les propriétaires de données et doit s'assurer que les règles appliquées dans les systèmes fonctionnent. Le gardien des données est généralement le directeur technique de Semana (Nicolas COSME).

Utilisateur de données

Personne, organisation ou entité qui interagit avec les données, y accède, les utilise ou les met à jour dans le but d'effectuer une tâche autorisée par le propriétaire des données. Les utilisateurs de données doivent utiliser les données d'une manière conforme à l'objectif visé et se conformer à la présente politique et à toutes les politiques applicables à l'utilisation

des données.

Le propriétaire des données est chargé d'attribuer à chaque donnée une étiquette de classification basée sur le niveau d'impact global :

Niveau d'impact global	Niveau de classification
Haut	Restreint
Modéré	Confidentiel
Faible	Public

Sur la base de cette classification, les détenteurs de données appliquent des contrôles de sécurité appropriés pour protéger chaque donnée en fonction de l'étiquette de classification.

Informations collectées et stockées par Semana

Toutes les informations relatives aux clients sont classées comme restreintes/à fort impact global. Pour l'instant, les seuls utilisateurs autorisés sont le CEO (Albert REYNAUD), le CTO (Nicolas COSME) et 2 développeurs seniors (à des fins de support) de Semana.

Voici une liste de toutes les informations relatives aux clients collectées/stockées par Semana.

Collecté / stocké	
Information du public	Semana ne stocke que les informations publiques de base relatives à ses clients (nom de l'entreprise, logo et/ou URL du site web).
Informations confidentielles	Semana ne recueille et ne stocke que les informations nécessaires à des fins commerciales et opérationnelles : - Conditions spécifiques et contrats - Informations sur Billings - Contacts et rôles - Adresses et plans des bureaux - Liste des collaborateurs -
Informations personnelles identifiables (IPI)	Semana ne recueille pas et ne stocke pas d'informations personnelles identifiables (PII) : - les informations de connexion et de contact des utilisateurs (courriel et nom d'utilisateur) - Planification du statut (bureau, à

	distance)
	-Emplacement dans le bureau
Non collecté / Non stocké	
Propriété intellectuelle	Semana ne recueille ni ne stocke la propriété intellectuelle du client.
Informations à diffusion restreinte (numéros de sécurité sociale, etc.)	Non collecté / stocké
Informations sur les cartes de paiement (PCI)	Non collecté / stocké
Informations de santé protégées (PHI)	Non collecté / stocké

Stockage des données

Toutes les données de l'application sont stockées sur les services gérés de GCP :

- Google Cloud SQL (Postgres 13) : Base de données Postgres répliquée et gérée par GCP
- Google Storage : Service de stockage de fichiers répliqué et hautement disponible

Ces services fournissent une couche supplémentaire de sécurité et de services opérationnels, notamment :

- Chiffrement au repos et en transit
- Protection du réseau (restriction des adresses IP, etc.)
- Sauvegardes automatisées, périodiques et cryptées

Pour plus d'informations, voir l'**accès aux bases de données** dans la **politique de contrôle d'accès**.

Politique de conservation des données

Toutes les données des clients stockées sur la plate-forme Semana peuvent être supprimées sur demande.

Les données supprimées par les utilisateurs sont effacées en toute sécurité de toutes les bases de données, à l'exception des sauvegardes. Les sauvegardes sont automatiquement effacées après 8 jours. Les sauvegardes mensuelles sont conservées pendant 30 jours.

Postes de travail

Les postes de travail sont protégés par un mot de passe.

Tous les services et toutes les données dont ont besoin les employés et les contractants sont disponibles via des solutions Saas (à l'aide d'un navigateur web). Aucune donnée sensible n'est stockée sur le poste de travail.

Les accès à distance sont basés sur un protocole sécurisé (HTTPS) ou un tunnel (SSH).

Tous les accès sont nominatifs et nécessitent une authentification forte (clé de chiffrement nominative ou MFA).

Supports amovibles

L'utilisation de supports amovibles (y compris, mais sans s'y limiter, les clés USB, les DVD, les cartes SD, les disques durs externes, etc : clés USB, DVD, cartes SD, disques durs externes, etc.) est **strictement interdite** au sein de l'organisation Semana.

9. Contrôle d'accès

Contrôle d'accès Politique

Semana a établi une politique de contrôle d'accès pour définir comment le contrôle d'accès aux systèmes et services d'information couvre toutes les étapes du cycle de vie de l'accès des utilisateurs : de l'enregistrement des nouveaux utilisateurs à la désinscription des utilisateurs qui n'ont plus besoin d'accès. Dans la mesure du possible, les politiques d'utilisation sont appliquées par le système d'exploitation ou d'autres logiciels. Semana peut partager sa politique de contrôle d'accès sur demande, moyennant la signature d'un accord de confidentialité.

Exigences de l'entreprise et granularité de l'accès

L'accès aux systèmes d'information est régi par les principes du "besoin de savoir" et du "moindre privilège". Les propriétaires des actifs (jusqu'à présent uniquement le PDG et le directeur technique) ont la responsabilité de définir le niveau d'accès requis par chaque collaborateur. L'accès à l'infrastructure et aux données des clients est détaillé ci-dessous (voir Accès aux **bases de données** et **Accès à l'infrastructure**).

Exigence SSO

L'accès aux ressources et aux outils de Semana est basé sur le SSO Google Workspace. Chaque employé de Semana dispose d'un compte Google Workspace individuel et nominatif. L'accès à ce compte est protégé par un mot de passe fort et une authentification multifactorielle (MFA).

Tous nos logiciels et ressources en ligne sont configurés pour utiliser Google Workspace SSO. Cela permet de révoquer immédiatement tous les accès en cas de cessation d'emploi et d'imposer l'utilisation d'une authentification à plusieurs facteurs.

Si un logiciel, un tiers ou une ressource ne prend pas en charge le SSO ou nécessite un niveau de sécurité plus élevé, le propriétaire du bien doit le faire :

1. Obtenir l'amélioration de la gestion
2. Si possible, activez l'authentification multifactorielle pour ce logiciel.
3. Maintenir une liste cohérente et actualisée de tous les utilisateurs et des droits d'accès qui leur sont associés.
4. En cas de licenciement ou de changement d'emploi, révoquer tous les accès associés.
5. Examiner régulièrement les droits d'accès et les mettre à

jour si nécessaire Jusqu'à présent, les seules ressources qui

n'utilisent pas le SSO sont :

- Accès aux bases de données (voir accès aux bases de données ci-dessous)

Gestion de l'accès des utilisateurs

Les propriétaires de chaque bien/ressource sont tenus de tenir à jour une liste de tous leurs utilisateurs et des droits d'accès qui leur sont associés.

Comme indiqué ci-dessus, les accès sont immédiatement révoqués après la cessation d'emploi en déprovisionnant le compte Google de l'employé.

Les droits d'accès sont régulièrement revus afin de correspondre aux besoins des employés et à leurs missions au sein de l'entreprise.

Politique en matière de mots de passe et utilisation d'informations d'authentification secrètes

Tous les employés de Semana (y compris les sous-traitants et les fournisseurs ayant accès aux systèmes de Semana) sont tenus de prendre les mesures appropriées, comme indiqué ci-dessous, pour sélectionner et sécuriser leurs mots de passe.

Complexité du mot de passe

Les utilisateurs sont tenus d'utiliser des mots de passe forts (plus de 8 caractères, y compris des caractères spéciaux et des chiffres). La complexité des mots de passe des employés est régie par les règles de l'espace de travail Google.

Utilisation de mots de passe et d'informations secrètes d'authentification

Les mots de passe ne doivent jamais être partagés, envoyés par courrier électronique ou stockés en clair dans un fichier. Les mots de passe/accréditations ne doivent jamais être écrits dans le code source.

Suivi des incidents et des activités suspectes

Si un compte ou un mot de passe est suspecté d'avoir été compromis, signalez l'incident et changez tous les mots de passe.

Accès au réseau

L'accès au réseau Wifi de l'entreprise est réservé aux employés (nous n'avons pas de réseau Wifi pour les invités et nous ne donnons pas accès au réseau Wifi à nos visiteurs).

Accès à l'application Semana

Nous utilisons Google Cloud Identity Platform pour gérer l'authentification à l'application Semana. Il n'a accès qu'aux informations de connexion des utilisateurs. Il nous permet de fournir une procédure de connexion sécurisée et de prendre en charge le SSO.

Accès au code source de l'application

La source du code est gérée à l'aide d'un flux de travail git standard, y compris les revues de code obligatoires avant le déploiement. Nous utilisons Github pour héberger le code. Les accès sont immédiatement supprimés en cas de licenciement.

Accès aux bases de données

Nous utilisons Google Cloud SQL comme base de données transactionnelle. L'accès à la base de données est très restreint :

- Les connexions aux bases de données ne sont possibles que dans un réseau restreint.
- Les connexions à des bases de données distantes ne sont autorisées qu'avec le proxy SQL fourni par Google, à l'aide d'un tunnel crypté.
- Le tunnel crypté nécessite une clé individuelle qui fait l'objet d'une rotation fréquente et qui est révoquée en cas de cessation d'emploi.
-
- Les développeurs n'ont accès qu'à une base de données de développement et d'essai qui ne contient que des données de test fictives ou anonymisées.
- L'accès aux bases de données de production est limité aux applications et aux administrateurs. Les serveurs de production utilisent des clés individuelles qui font l'objet d'une rotation régulière. Les administrateurs utilisent un login dédié avec un mot de passe fort et une authentification à 2 facteurs. Pour l'instant, les seuls administrateurs sont le CTO et deux développeurs seniors.
- GCP fournit également une piste d'audit et des enregistrements de journaux. L'accès aux journaux est limité et les journaux ne peuvent pas être modifiés, même par les administrateurs.

Accès à l'infrastructure GCP

Nous suivons les meilleures pratiques du GCP en termes de sécurité :

- Le compte root est sécurisé par un mot de passe fort dédié, MFA et je ne l'ai jamais utilisé sauf pour des tâches nécessitant un accès root.
- Nous utilisons un accès IAM séparé pour chaque tâche en suivant la règle du moindre privilège en termes d'autorisation.
- Nous imposons des mots de passe forts pour la connexion des utilisateurs
- Seuls les administrateurs ont accès aux environnements de production
- Nous utilisons GCP Logging and Monitoring pour surveiller les activités et les vulnérabilités de notre infrastructure.

10. Politique de cryptage

Nous exigeons l'utilisation de schémas de cryptage sécurisés. Pour ce faire, nous n'utilisons que des protocoles et des programmes de cryptage dont la sécurité a été prouvée, tels que HTTPS et Google SQL Proxy.

Tous les schémas et clés de cryptage sont fournis par le GCP. [Voir](https://cloud.google.com/security/)
<https://cloud.google.com/security/>

11. Politique de sauvegarde/restauration

Sauvegarde des bases de données

Nous effectuons quotidiennement des sauvegardes automatisées sur Google SQL. Les sauvegardes sont conservées pendant 8 jours.

Création d'une sauvegarde

Notre workflow git nous permet de restaurer la version précédente de l'application si des problèmes surviennent après une mise à jour.

Supports de sauvegarde

Semana n'utilise pas de sauvegarde sur bande. Toutes les sauvegardes des données opérationnelles sont effectuées à l'aide de sauvegardes automatisées Cloud SQL. Tous les jeux de sauvegarde sont cryptés.

Essais

La capacité à restaurer des données à partir de sauvegardes est testée au moins une fois par an à l'aide de restaurations réelles.

12. Sécurité des opérations

Anti-malware

Les postes de travail doivent être équipés de logiciels antivirus à jour.

Tous les autres appareils sont gérés par les services gérés de GCP, qui comprennent une solide politique de mise à jour des systèmes.

Enregistrement

Nous utilisons Google Logging and Monitoring pour enregistrer l'activité de notre infrastructure et surveiller les changements importants.

Contrôles du réseau

Notre infrastructure GCP est protégée par un système VPC et un pare-feu.

Gestion des vulnérabilités

Nous utilisons des gestionnaires de paquets pour détecter les correctifs de sécurité à chaque version de l'application.

Les mises à jour des vulnérabilités mineures et moyennes sont effectuées sur une base hebdomadaire. Les vulnérabilités élevées et critiques sont corrigées dans les 48 heures.

Gestion des capacités

Notre infrastructure GCP est évolutive et utilise des équilibrateurs de charge pour supporter les pics de charge.

13. Développement et maintenance du système

Politique de développement des logiciels

Semana a mis en place une politique de développement de logiciels. Cette politique vise à garantir que les logiciels sont développés de manière sûre en créant un environnement de développement sécurisé, en intégrant la sécurité à chaque étape du développement des logiciels et en gérant de manière appropriée les changements dans le processus de développement.

Semana communique ces règles et a mis en place des contrôles et des procédures appropriés pour s'assurer que les exigences sont respectées.

Semana peut partager sa politique de développement de logiciels sur demande avec la signature d'un accord de confidentialité.

Développement sécurisé

Pour toutes les applications, le pipeline CI/CD applique les éléments suivants avant le déploiement en production :

- Examen du code statique
- Tests unitaires, d'intégration et de bout en bout

Nos développeurs suivent les 10 principales recommandations de l'OWASP.

Gestion du changement

Nous utilisons un workflow git standard pour gérer notre SDLC. Les commits sont revus avant d'être poussés avec des tests unitaires et des revues de code manuelles. Les applications sont testées dans l'environnement d'essai avant d'être mises en production.

Les mises à jour de l'environnement de production (mises à jour d'applications, mises à niveau du système, correctifs de sécurité mineurs, etc.) et les autres tâches de maintenance sont généralement effectuées pendant le week-end et/ou en dehors des heures de bureau (22h heure d'Europe/Paris).

Environnements séparés

Nous disposons de trois environnements différents : le développement, la mise en scène et la production. Ces environnements sont séparés logiquement et physiquement. L'accès à la production est réservé aux administrateurs. Les données des environnements de développement et de mise à l'essai sont fictives ou anonymes.

Développement externalisé

Nous ne sous-traitons le développement d'aucune partie de notre logiciel.

14. Relations avec les fournisseurs

Politique de sécurité de l'informatique en nuage

Les activités de Semana dépendent fortement de l'utilisation de l'informatique en nuage et des logiciels en nuage. Si l'informatique en nuage apporte une plus grande souplesse et réduit les délais de rentabilité, elle s'accompagne de ses propres risques et exigences en matière de sécurité. Semana reconnaît que l'utilisation de l'informatique en nuage et des logiciels en nuage requiert de la prudence et s'engage à documenter, à mettre en œuvre et à diffuser les procédures nécessaires dans l'ensemble de l'organisation.

C'est pourquoi Semana a mis en œuvre une politique de sécurité dans l'informatique dématérialisée. Cette politique vise à garantir que l'utilisation des solutions Cloud se fait de manière sécurisée, afin de préserver la confidentialité, l'intégrité et la disponibilité des informations de Semana. Cette politique décrit les principaux domaines de sécurité concernant les solutions Cloud, et décrit comment les différents aspects de la sécurité sont pris en compte tout au long du cycle de vie des solutions Cloud.

Semana peut partager sa politique de sécurité dans le nuage sur demande avec la signature d'un accord de confidentialité.

Sécurité de l'information dans les relations avec les fournisseurs

Semana tient à jour une liste de fournisseurs et veille à ce que les meilleures pratiques en matière de sécurité (telles que 2FA) soient appliquées lors de l'utilisation de logiciels tiers. Nous n'exigeons pas de conformité en matière de sécurité dans notre contrat, mais tous nos fournisseurs tiers répondent à nos exigences internes en matière de sécurité.

Suivi et examen des services des fournisseurs

Des mesures de protection appropriées sont mises en œuvre avec nos fournisseurs de services et sont gérées dans le cadre de notre relation contractuelle avec eux. Notre équipe de sécurité, qui est responsable de chaque contrat, coordonne les considérations uniques pour nos fournisseurs avant que les contrats ne soient mis en place ou renouvelés.

15. Gestion des incidents de sécurité de l'information

Plan de réponse aux incidents

Semana a mis en place un plan d'intervention en cas d'incident afin de guider les employés ou les personnes chargées d'intervenir en cas d'incident qui pensent avoir découvert un incident de sécurité ou qui sont en train d'y remédier. Semana peut partager son plan de réponse aux incidents sur demande et avec la signature d'un accord de confidentialité.

Gestion des incidents et des améliorations en matière de sécurité de l'information

En fonction de leur gravité, les vulnérabilités découvertes sont traitées comme un incident de sécurité réel. Les vulnérabilités SEV-1 sont traitées immédiatement. Les vulnérabilités de moindre gravité sont ajoutées au backlog de l'équipe avec l'objectif d'être résolues lors de la prochaine analyse mensuelle. Le MTTR (Mean Time To respond) des incidents de sécurité est activement suivi et contrôlé par Nicolas COSME.

Nous informerons nos clients de toute atteinte confirmée à la sécurité ou à la vie privée dans les meilleurs délais. Nous fournissons des rapports d'évaluation et d'atténuation dans les délais impartis :

- 24 heures pour les événements critiques.
- 2 jours ouvrables pour les événements non critiques.

Les réponses à des incidents spécifiques peuvent inclure

Évaluation et réponse aux incidents

- Vérifier tous les systèmes pour les comptes nouveaux ou modifiés
- Examiner les fichiers journaux pour y déceler des entrées anormales ou des périodes manquantes.
- Recherchez les modifications apportées au logiciel du système et/ou aux fichiers de configuration.
- Recherche de nouveaux binaires dans le système (y compris dans les répertoires des utilisateurs)
- Vérifier les autres systèmes locaux et les systèmes distants connexes
- Modifier le(s) mot(s) de passe du système
- Nettoyer et/ou reformater le système le cas échéant

Rapport d'incident

- Créer une nouvelle carte Notion avec l'étiquette "Incident".
- Contactez immédiatement support@semana.io pour discuter de la nature de l'incident.

16. Aspects de la sécurité de l'information dans la

gestion de la continuité des activités

Plan de continuité des activités

Semana a mis en place un plan de continuité des activités afin d'assurer la poursuite de ses activités en cas de catastrophe.

Semana héberge l'infrastructure de ses produits chez un fournisseur d'infrastructure de premier plan, actuellement Google Cloud Platform, qui fournit des niveaux élevés de disponibilité physique et de réseau et maintient divers niveaux de sécurité vérifiés, y compris SOC 2 Type II et la conformité ISO 27001.

Semana peut partager son plan de continuité des activités sur demande, moyennant la signature d'un accord de confidentialité.

Plan de reprise après sinistre

Semana a mis en place un plan de reprise d'activité ("DRP"). Ce plan établit des procédures visant à rétablir les activités de Semana à la suite d'une interruption résultant d'une catastrophe. Les types de catastrophes envisagées par ce plan comprennent les catastrophes naturelles, les troubles politiques, les catastrophes d'origine humaine, les menaces humaines externes et les activités malveillantes internes. Ce plan est tenu à jour par l'équipe informatique et peut être communiqué sur demande.

Semana tire parti de son infrastructure en nuage et de ses stratégies de sauvegarde. Comme Semana dispose d'une image logicielle et d'une sauvegarde de la base de données, le redéploiement de l'application peut être effectué très rapidement.

Licenciements

Nos principaux fournisseurs nous garantissent un temps de disponibilité des installations compris entre 99,95 % et 100,00 %, et les deux fournisseurs assurent une redondance minimale de N+1 pour tous les services d'alimentation électrique, de réseau et de chauffage, ventilation et climatisation.

Les données sont répliquées et sauvegardées dans plusieurs entrepôts de données durables répartis dans des centres de données afin d'ajouter un niveau supplémentaire de protection hors site géographiquement dispersé. Les applications dorsales sont exploitées dans 3 zones de disponibilité de notre fournisseur d'hébergement.

Vérifier, examiner et évaluer la continuité de la sécurité de l'information

Les tests de continuité des activités font partie du processus normal de Semana. Nos processus de récupération sont validés en permanence dans le cadre des processus normaux de maintenance et d'assistance. Nous utilisons des services gérés qui nous permettent de mettre rapidement en place des environnements. Nous utilisons exactement les mêmes procédures dans un scénario de reprise, ce qui nous permet de pratiquer notre processus de reprise tous les jours.

17. Conformité

Respect des politiques et des normes de sécurité

Nous avons modelé nos contrôles sur la norme ISO-27001 et nous hébergeons nos produits chez des fournisseurs de centres de données de confiance qui détiennent les certifications SOC 2 Type II, ISO 27001 et bien d'autres certifications de sécurité. Nos fournisseurs d'infrastructure publient leurs documents de conformité sur leurs sites. Veuillez consulter les sites suivants : Google Cloud Platform : <https://cloud.google.com/security/compliance>

Nous prévoyons d'effectuer un test de boîte grise externe au quatrième trimestre 2022.

Identification de la législation applicable et des exigences contractuelles

Notre directeur juridique ainsi que les membres de l'équipe de sécurité se tiennent au courant des modifications apportées aux lois sur la cybersécurité et la protection de la vie privée dans les régions où nous exerçons nos activités. Les modifications pertinentes des exigences ou des orientations sont intégrées dans des mises à jour itératives de nos politiques, de nos processus et de nos produits. Notre procédure logicielle garantit la conformité avec les exigences législatives, réglementaires et contractuelles.

Vie privée et protection des informations personnelles identifiables

Semana ne collecte ni ne stocke d'informations personnelles identifiables (PII) en dehors de celles qui sont strictement nécessaires au fonctionnement du service Semana.

Nous disposons d'une boîte aux lettres : security@semana.io pour soumettre des demandes relatives au GDPR et au CCPA. Les demandes sont traitées dans un délai conforme à la réglementation.

Pour de plus amples informations concernant les politiques et les contrôles de sécurité de Semana, veuillez contacter security@semana.io.