POLITIQUE GENERALE DE SECURITE DU SYSTEME D'INFORMATION (PGSSI)

Version 2.0

27/11/2024

Niveau de confidentialité :

Public

SMSI ALMAVIA CX

SOMMAIRE

Lettre de la Direction Générale d'Almavia CX concernant la sécurité du SI

Dans le cadre de son engagement à fournir des services de qualité tout en assurant la protection des informations de nos clients et partenaires, Almavia CX place la sécurité de son Système d'Information (SI) au cœur de sa stratégie. La Direction Générale reconnaît l'importance cruciale de garantir l'intégrité, la disponibilité et la confidentialité des données traitées, en conformité avec la norme ISO 27001, et affirme ainsi son engagement ferme à la mise en œuvre de pratiques de sécurité solides et rigoureuses.

Consciente que la sécurité de l'information représente un investissement stratégique, la Direction s'engage à gérer cet aspect avec une attention particulière pour garantir la pérennité et la confiance dans nos services. Almavia CX s'engage à mettre en place des mesures de sécurité proportionnées aux risques identifiés, en optimisant les ressources et en favorisant des solutions efficientes et adaptées aux besoins de ses activités.

Dans cette perspective, la Direction a procédé à une analyse approfondie des risques afin de cartographier les menaces potentielles pouvant impacter la sécurité et la continuité de nos opérations. Cette analyse a permis d'identifier les vulnérabilités les plus critiques et de mettre en œuvre un Plan de Continuité d'Activité (PCA) adapté, garantissant la résilience de nos services même en cas d'incidents graves. Le PCA est conçu pour anticiper et gérer les interruptions potentielles, minimiser l'impact sur les opérations et assurer la reprise rapide des activités essentielles.

La Direction s'engage également à :

- Allouer les ressources nécessaires pour le maintien et l'amélioration de son Système de Management de la Sécurité de l'Information (SMSI), conformément aux exigences de l'ISO 27001 ;
- Sensibiliser et former l'ensemble des collaborateurs aux bonnes pratiques de sécurité afin de minimiser les risques d'incidents ;
- Assurer une évaluation régulière des risques liés à la sécurité du SI, permettant d'adapter de manière agile et efficace les mesures de protection en fonction des nouvelles menaces et technologies.

Cette politique de sécurité reflète notre volonté d'instaurer un environnement sécurisé pour nos clients, nos partenaires et nos collaborateurs. La Direction Générale s'engage pleinement à conduire Almavia CX vers une amélioration continue de sa posture de sécurité, tout en veillant à maîtriser les coûts associés pour garantir une compétitivité durable et responsable.

Chaque personne travaillant chez Almavia CX est un acteur clé dans la protection de nos informations et systèmes. En adoptant des comportements responsables et en respectant les bonnes pratiques définies dans notre Politique de Sécurité, nous contribuons ensemble à créer un environnement de confiance et de sécurité. La collaboration de tous est essentielle pour atteindre un haut niveau de sécurité et répondre aux attentes de nos clients et partenaires.

À travers cette démarche collective, nous bâtissons une culture de la sécurité qui s'inscrit durablement dans notre façon de travailler et qui constitue un véritable atout compétitif pour notre entreprise.

1 Introduction

1.1 Présentation d'Almavia CX

Almavia CX est une Entreprise de Services Numériques (ESN) qui accompagne la transformation digitale des entreprises et administrations sur toute la chaîne de valeur de l'Expérience Client, en plaçant l'humain au centre des stratégies pour créer des connexions qui ont du sens et de la valeur. Elle propose pour cela des prestations

- De conseil, pour aider à transcrire les idées de business en projets, cadrer ces projets et aider aux choix des fournisseurs et des technologies ;
- D'ingénierie, pour mettre en œuvre les solutions logicielles leaders du marché dans les domaines d'expertise suivants : centres de contact omnicanaux, Gestion de la Relation Client (Customer Relationship Management - CRM), Couplage Téléphonie Informatique (CTI), développement logiciel, plates-formes digitales web et mobiles, architectures complexes, outils de gestion de campagnes marketing et enfin les infrastructures serveurs et réseaux sous-jacentes.

Almavia CX fait partie du Groupe Nextedia qui est spécialisé dans le conseil et les services à forte valeur ajoutée dans les domaines de l'Expérience Client, de la Cybersécurité et de la Gouvernance des Risques de Cybersécurité, du Cloud et du Digital Workspace. De plus, le Groupe Nextedia est coté sur Euronext Growth.

Enfin, Almavia CX est certifiée ISO 27001 sur l'ensemble de ses activités depuis 2017.

1.2 Objet de la PGSSI

La PGSSI est le document qui décrit les grandes orientations en matière de sécurité du SI chez Almavia CX afin d'assurer

- La disponibilité des données et des moyens de les traiter ;
- L'intégrité des données et des moyens de les traiter ;
- La confidentialité des données gérées et des moyens de les traiter.

La PGSSI est le document qui sert de fondation pour définir les mesures de sécurité du SI. Cela signifie que

- Chaque mesure peut être reliée à une orientation de la PGSSI ;
- Aucune mesure ne peut contredire une orientation de la PGSSI.

1.3 Champ d'application de la PGSSI

La PGSSI couvre l'ensemble des données et de leurs traitements (création, stockage, échange, etc.), que le format soit matériel ou immatériel (électronique, imprimé, oral, image, etc.) dans toute l'organisation.

Cela signifie qu'elle s'applique à l'ensemble

- Du personnel permanent ou temporaire de l'entreprise, travaillant au sein de l'entreprise ou à distance
- Des partenaires de l'entreprise, qu'il s'agisse de personnes physiques ou morales (sous-traitants, prestataires de services, fournisseurs), ayant accès au système d'information d'Almavia CX

- Des équipements et logiciels permettant le traitement des données d'Almavia CX
- Des interfaces entre les applications, ou les services Cloud, permettant le traitement des données d'Almavia CX

1.4 Enjeux

La PGSSI d'Almavia CX est définie en tenant compte d'enjeux externes et internes liés à la sécurité de l'information. Les enjeux sont :

- Acquérir des clients en répondant à leurs attentes en matière de sécurité de l'information
- Conserver les clients en délivrant des prestations dans les règles de l'art en matière de sécurité de l'information
- Maintenir des conditions de travail satisfaisantes pour conserver les salariés
- Maintenir la réputation de l'entreprise sur Internet pour attirer des candidats
- Empêcher que l'entreprise ne soit exposée à des sanctions financières ou pénales
- Intégrer les grands changements externes tels que l'évolution du climat ou le développement rapide de l'Intelligence Artificielle

1.5 Cadre réglementaire

Le cadre réglementaire identifié pour définir la PGSSI d'Almavia CX est composé de plusieurs référentiels issus de la législation française, ainsi que des directives et règlements européens traitant de la sécurité de l'information.

Le tableau ci-dessous recense les domaines à adresser ainsi que les référentiels qu'Almavia CX doit respecter :

Domaine	Référentiel	Contenu concerné
Cybercriminalité	NIS2	Toute la directive
Données à caractère personnel	RPGD	Tout le règlement
Secret des correspondances	Code pénal	Article 226-15 – Interception, divulgation ou détournement de correspondances
Fraude	Code pénal	Article 313-1 – Escroquerie Article 314-1 – Abus de confiance Article 323-1 – Accès frauduleux à un système de traitement automatisé de données (STAD) Article 323-2 – Entrave au bon fonctionnement d'un STAD Article 323-3 – Fraude informatique (modification, suppression ou vol de données) Article 323-4 – Utilisation frauduleuse de données personnelles Article 323-5 – Tentatives d'infractions liées aux systèmes informatiques Article 441-1 – Faux et usage de faux Article 441-2 – Faux en écriture
Propriété intellectuelle	Code de la propriété intellectuelle	Article L335-2 – Contrefaçon de droits d'auteur Article L716-9 – Contrefaçon de marques
Droit à la déconnexion	Code du travail	Article L2242-8 – Droit à la déconnexion Article L6315-1 – Droit à la déconnexion pour les travailleurs mobiles

Droits des salariés en situation de crise	Code du travail	Article L3121-28 – Heures supplémentaires en cas de circonstances exceptionnelles Article L1222-11 – Adaptation du contrat de travail en période de crise
Cryptographie	RGS	Chapitre 4 - Sécurisation des échanges et de la transmission des informations

1.6 Entrée en vigueur de la PGSSI

La PGSSI entre en vigueur à la date de sa validation par la Direction Générale.

1.7 Implémentation de la PGSSI

La Direction Générale confie la définition, l'application et le suivi de la PGSSI au rôle de RSMSI.

1.8 Suivi, modifications et révisions de la PGSSI

La PGSSI est révisée une fois par an, par le RSMSI, et peut évoluer dans les cas suivants :

- Modification majeure du contexte interne d'Almavia CX (changement organisationnel, nouvelles pratiques ou technologies, etc.) ;
- Modification du contexte juridique ou réglementaire (nouvelles lois, etc.) ;
- Evolution des risques.

Toute modification entraine la mise à jour du numéro de la version en respectant les règles suivantes :

- Le nombre affiché à gauche du point correspond au numéro de version majeure. Ce nombre est incrémenté lorsque
  - La structure du plan est modifiée ;
  - Des informations sont ajoutées ou supprimées.
- Le nombre affiché à droite du point correspond au numéro de version mineure. Ce nombre est incrémenté uniquement lorsque des améliorations sont apportées à la mise en forme ou à la qualité d'écriture.

Chaque version majeure est soumise à la Direction Générale pour validation.

2 Parties intéressées par la sécurité du SI

Les parties intéressées sont l'ensemble des personnes ou entités qui peuvent influencer, ou bien être influencées, par le SMSI d'Almavia CX.

Le tableau ci-dessous liste les parties intéressées identifiées par Almavia CX en précisant, pour chacune, le mode de collecte des attentes ainsi qu'une synthèse des attentes.

Partie intéressée	Mode de collecte des attentes	Synthèse des attentes
Salariés représentés par le CSE	Interview du CSE	1/ Maintenir les contraintes liées à la sécurité à un niveau acceptable 2/ Assurer la pérennité des activités 3/ Assurer le respect des droits des salariés 4/ Assurer la confidentialité des données des salariés
COMEX	Interview du COMEX	1/ Assurer la capacité de délivrer et facturer les prestations aux clients 2/ Limiter la gravité et la vraisemblance des risques cyber, environnementaux, juridiques et financiers liés au Système d'Information 3/ Renforcer la maitrise des processus
Clients	Collecte dans les documents fournis par les clients (questionnaires de sécurité, plan d'assurance sécurité…)	1/ Assurer que les activités d'Almavia CX ne génèrent pas, ou n'aggravent pas, de risques dans leurs propres SI 2/ Assurer la confidentialité des données qu'ils ont confiées à Almavia CX 3/ Assurer que les incidents de sécurité, survenant dans le SI d'Almavia CX et les impactant, sont traités de manière efficace et transparente
Fournisseurs et sous-traitants	Collecte dans les documents fournis par les fournisseurs et sous-traitants (contrats, conditions générales de vente, plan d'assurance sécurité…)	1/ Assurer qu'Almavia CX utilisent leurs produits (fournisseurs) ou ressources (sous-traitants) en respectant les conditions prévues 2/ Assurer que les activités d'Almavia CX ne génèrent pas, ou n'aggravent pas, de risques dans leurs propres SI 3/ Assurer la confidentialité des données qu'ils ont confiées à Almavia CX 4/ Assurer que les incidents de sécurité, survenant dans le SI d'Almavia CX et les impactant, sont traités de manière efficace et transparente
Candidats	Retours de candidats	Assurer la confidentialité des données personnelles confiées à Almavia CX
CNIL	Veille sur le site cnil.fr et abonnement à la newsletter	Assurer la conformité avec le RGPD
ANSSI	Veille sur le site monespacenis2.cyber.gouv.fr et abonnement à la newsletter	Assurer la conformité avec la directive NIS2

3 Rôles et responsabilités liés à la sécurité du SI

3.1 Responsable du Système de Management de la Sécurité d'Information (RSMSI)

Les responsabilités confiées au rôle de RSMSI sont les suivantes :

- Définition du contexte
- Implication de la direction
- Définition des rôles et responsabilités
- Définition et mise en œuvre des politiques
- Appréciation des risques
- Définition et mise en œuvre des objectifs et indicateurs
- Définition et mise en œuvre du plan de communication interne et externe sur le SMSI
- Définition et contrôle des informations documentées
- Surveillance des objectifs et indicateurs
- Identification des opportunités d'amélioration

Le rôle de RSMSI est porté par une personne dans l'entreprise.

Le rôle de RSMSI peut-être délégué partiellement à des personnes ou des entités, internes ou externes à l'entreprise.

3.2 Responsable de la Sécurité du Système d'Information (RSSI)

Les responsabilités confiées au rôle de RSSI sont les suivantes :

- Définition et mise en œuvre des processus liés à la sécurité
- Participation à l'exécution de certains processus liés à la sécurité, comme la réaction sur incident, l'évaluation de la sécurité des projets ou l'évaluation de la sécurité des fournisseurs
- Définition des moyens opérationnels de sécurité
- Sensibilisation des utilisateurs à la sécurité
- Soutien du business sur les sujets liés à la sécurité

Le rôle de RSSI est porté par une personne dans l'entreprise.

Le rôle de RSSI peut être délégué partiellement à des personnes ou des entités, internes ou externes à l'entreprise.

3.3 Directeur du Système d'Information (DSI)

Les responsabilités confiées au rôle de DSI sont les suivantes :

- Définition de la stratégie SI en alignement avec les objectifs de sécurité
- Gestion des moyens opérationnels de sécurité
- Promotion d'une culture de la sécurité au sein des équipes IT

Le rôle de DSI est porté par une personne dans l'entreprise.

Le rôle de DSI est délégué partiellement à des personnes ou des entités, internes ou externes à l'entreprise (ex : équipe IT, hébergeur, fournisseur de services managés).

3.4 Délégué à la Protection des Données (DPO)

Les responsabilités confiées au rôle de DPO sont les suivantes :

- Surveillance du respect des réglementations en matière de protection des données
- Surveillance du respect de l'exercice des droits des personnes sur leurs données personnelles
- Sensibilisation des utilisateurs sur la protection des données personnelles
- Participation à l'exécution de certains processus liés à la protection des données personnelles, comme la réaction sur incident, l'évaluation de la sécurité des projets ou l'évaluation de la sécurité des fournisseurs

Le rôle de DPO est porté par une personne dans l'entreprise.

3.5 Directeur de Pôle

Les responsabilités confiées au rôle de Directeur de Pôle, dans son périmètre métier, sont les suivantes :

- Intégration des pratiques de sécurité dans les processus de production
- Signalement des vulnérabilités ou incidents constatés dans les activités de production
- Évaluation des impacts de la sécurité sur les activités de production

Le rôle de Directeur de Production Métier est porté par une personne dans chaque périmètre métier.

3.6 Directeur du Pilotage Métier

Les responsabilités confiées au rôle de Directeur du Pilotage Métier, sur l'ensemble des périmètres métiers, sont les suivantes :

- Intégration des pratiques de sécurité dans les processus de pilotage
- Signalement des vulnérabilités ou incidents constatés dans les activités de pilotage
- Évaluation des impacts de la sécurité sur les activités de pilotage

Le rôle de Directeur du Pilotage Métier est porté par une personne dans l'entreprise.

3.7 Directeur Commercial

Les responsabilités confiées au rôle de Directeur Commercial sont les suivantes :

- Intégration des pratiques de sécurité dans les processus de commerce
- Signalement des vulnérabilités ou incidents constatés dans les activités de commerce
- Évaluation des impacts de la sécurité sur les activités de commerce
- Évaluation des impacts des incidents de sécurité sur la confiance des clients

Le rôle de Directeur Commercial est porté par une personne dans l'entreprise.

3.8 Directeur des Opérations

Les responsabilités confiées au rôle de Directeur des Opérations sont les suivantes :

- Intégration des pratiques de sécurité dans les processus de fonctions support hors DSI
- Signalement des vulnérabilités ou incidents constatés dans les activités de fonctions support hors DSI

- Signalement des vulnérabilités ou incidents constatés dans les activités de fonctions support hors DSI

Le rôle de Directeur des Opérations est porté par une personne dans l'entreprise.

3.9 Comité Exécutif (COMEX)

Le COMEX a les responsabilités suivantes :

- Définition et surveillance des objectifs de sécurité stratégiques
- Allocation des ressources nécessaires pour atteindre et maintenir les objectifs de sécurité stratégiques
- Promotion de la sécurité au sein de l'entreprise
- Engagement des directeurs dans la démarche de sécurité

4 Gouvernance de la sécurité du SI

4.1 Comité de Gestion de la Sécurité (COGESEC)

Le COGESEC comprend l'ensemble des rôles qui gouvernent la sécurité du SI, à savoir :

- Directeur des Opérations
- Directeur du Pilotage Métier
- DSI
- RSMSI
- RSSI
- DPO

Le RSMSI fournit chaque mois un état des lieux sur le fonctionnement du SMSI au COGESEC. Cet état des lieux comprend les indicateurs associés aux objectifs de sécurité.

Le COGESEC se réunit de manière régulière ou bien de manière exceptionnelle à l'initiative du DSI, du RSMSI, du RSSI ou du DPO.

4.2 Appréciation des risques

Almavia CX doit connaître, analyser et évaluer les risques auxquels son SI est exposé, et agir en conséquence.

Des analyses de risques sont réalisées régulièrement en appliquant une démarche inspirée de la méthode EBIOS Risk Manager.

La démarche identifie les risques en s'intéressant aux éléments suivants :

- Valeurs métiers (processus, informations)
- Biens supports sur lesquels reposent les valeurs métiers
- Evènements redoutés sur les valeurs métiers compte tenu des biens supports
- Sources de risques qui pourraient chercher à produire les évènements redoutés
- Parties prenantes qui interviennent directement ou indirectement sur les biens supports (écosystème)
- Scénarios stratégiques qui décrivent comment les sources de risques pourraient produire les évènements redoutés en passant, ou non, par des parties prenantes
- (Si besoin) Scénarios opérationnels qui détaillent les chemins d'attaques

Les risques sont évalués en attribuant une note aux 2 critères suivants :

- Gravité – Importance des conséquences qu'un risque peut avoir sur les informations
- Vraisemblance – Probabilité de déclenchement d'un risque en tenant compte du contexte externe (ex : explosion des cyberattaques dans le monde), des vulnérabilités existantes et des mesures de sécurité en place

Les notes sont utilisées pour classer les risques dans 3 catégories :

- Risques faibles –Pas de traitement requis (acceptation)
- Risques moyens – Traitement ou acception à arbitrer par le COMEX
- Risques forts – Traitement obligatoire

Les risques forts, et les risques moyens non acceptés par le COMEX, sont traités de manière à réduire leur gravité ou vraisemblance. Les options de traitement des risques sont :

- Réduire – Déployer des mesures de sécurité
- Transférer – Déplacer la responsabilité sur un ou plusieurs tiers
- Refuser – Arrêter l'activité concernée ou la modifier

4.3 Objectifs de sécurité

Le COMEX a défini 3 objectifs stratégiques qui lui sont présentés de manière régulière pour lui permettre de surveiller l'efficacité de la sécurité du SI :

- Assurer l'intégrité et la confidentialité des données d'Almavia CX et des données confiées à Almavia CX ;
- Assurer la disponibilité des services d'Almavia CX en adéquation avec les besoins de production métier ;
- Assurer un niveau de sécurité à l'état de l'art dans les activités de production métiers d'Almavia CX.

Chaque objectif stratégique est décliné en plusieurs objectifs opérationnels. A chaque objectif opérationnel est associé plusieurs indicateurs. Les indicateurs sont obtenus en réalisant des mesures dans des outils, et en comparant ces mesures avec des seuils.

Les objectifs opérationnels, les indicateurs et les seuils sont proposés par le RSMSI. Ils sont validés, avant mise en application, puis suivis voire révisés de manière régulière par le COGESEC.

4.4 Plan d'actions

Le RSMI tient à jour le plan d'actions qui sont destinées à traiter les risques, respecter les objectifs de sécurité, mettre en conformité avec les référentiels, corriger les écarts relevés pendant les audits, améliorer le fonctionnement du SMSI, renforcer l'efficacité de la sécurité opérationnelle, etc.

Le plan d'actions est géré dans un outil qui permet de lier chaque action avec un ou plusieurs déclencheurs (risques, objectifs, écarts…) et suivre l'avancement de chaque action, permettant ainsi d'évaluer facilement l'avancement global sur plusieurs axes d'observation (par risque, par référentiel…).

4.5 Informations documentées

Le SMSI est alimenté avec des informations documentées décrites dans le tableau ci-dessous.

Catégorie	Document(s)	Description	Niveau d'accessibilité
Socle	Référentiels réglementaires Référentiels normatifs (ex : ISO 27001) Référentiels de sécurité clients Analyses de risques Déclarations d'applicabilité	Documents décrivant les exigences des différents référentiels ainsi que les états des lieux sur les risques et la maturité	Interne (tous les utilisateurs)
Politiques	PGSSI	Document fondateur décrivant les grandes orientations pour la sécurité du SI	Public

	Politiques thématiques	Documents décrivant de manière détaillée les orientations qui le nécessitent	Interne (tous les utilisateurs)
	Charte informatique	Document décrivant les obligations des utilisateurs quant à l'utilisation des moyens informatiques	
Processus	Procédures	Documents expliquant le fonctionnement des processus, c'est-à-dire qui fait quoi et comment	Restreinte (utilisateurs impliqués dans les procédures)
Opérations	Modes opératoires ; Fiches réflexes ; Registres…	Documents servant à guider les opérations, ou bien produits par les opérations	Restreinte (utilisateurs impliqués dans les opérations)
Enregistrements	Preuves d'efficacité des actions Procès-verbaux de revue Comptes-rendus d'audits Traces techniques Etc.	Documents démontrant que le SMSI fonctionne et est efficace	Restreinte (COGESEC)

4.6 Audits

Almavia CX réalise chaque année au moins 2 audits de sa sécurité opérationnelle et de son SMSI :

- Un audit interne, dont le contenu est proposé par le RSMSI ;
- Un audit de surveillance / renouvellement de la certification ISO 27001, dont le contenu est fixé par l'organisme de certification.

Almavia CX peut accepter qu'un audit soit réalisé sur demande d'un client, à condition

- Que la demande soit cohérente avec les risques que représentent les prestations produites pour le client ;
- Que la demande soit soumise au RSMSI avec un délai de prévenance acceptable ;
- Que la demande n'interfère pas avec l'audit annuel et l'audit de surveillance / renouvellement.

Almavia CX se tient à la disposition de l'ANSSI dans le cas où celle-ci souhaite réaliser un audit.

4.7 Revue de direction

Le SMSI est revu 1 fois par an, par le COMEX, le RSMSI et le RSSI. Cette revue, appelée « revue de direction », a pour objectif de vérifier que le SMSI est toujours approprié, adapté et efficace.

La revue de direction est préparée et conduite par le RSMSI. Les thèmes abordés sont, à minima :

- Actions à l'issue des revues de direction précédentes
- Enjeux externes et internes
- Attentes des parties intéressées
- Résultats des audits
- Indicateurs et objectifs
- Analyse de risque
- Retour des parties intéressées

- Opportunités d'amélioration

4.8 Dérogations

Les orientations de la PGSSI ne peuvent pas faire l'objet de dérogation.

Les dérogations relatives aux orientations des politiques thématiques, ou aux explications des procédures, doivent être documentées et faire l'objet d'une acceptation formelle, avec validation écrite et traçable des risques associés par le RSSI et, si nécessaire, par d'autres avis consultatifs.

Toutes les dérogations, ainsi que les mesures d'atténuation liées, doivent être temporaires. Elles sont et examinées au moins une fois par an par le RSSI.

4.9 Communication

Le RSMSI met en œuvre un plan de communication autour du SMSI afin

- D'informer les parties intéressées internes et externes ;
- D'impliquer les acteurs.

Le plan de communication identifie les informations suivantes pour chaque action de communication :

- Titre
- Mois
- Emetteur
- Destinataires
- Canal (email, réunion, publication…)

Le RSMSI actualise le plan de communication 1 fois par an et le fait valider par le COMEX.

5 Principes retenus pour la sécurité du SI

5.1 Organisation de la sécurité de l'information

5.1.1 Affectation des responsabilités et séparation des rôles

Les responsabilités relatives à la sécurité de l'information sont définies et les rôles sont séparés.

5.1.2 Relations avec les autorités et groupes spécialisés

La relation avec la CNIL et l'ANSSI est entretenue, en s'abonnant aux newsletters et en se déclarant dans les outils disponibles.

Une relation très étroite et régulière est entretenue avec les divisions Cybersécurité et Gouvernance des Risques de Cybersécurité du Groupe Nextedia, afin d'être informé des bonnes pratiques de l'état de l'art en termes de sécurité.

5.1.3 Sécurité dans les projets

Tout projet qui prévoit d'ajouter, remplacer ou supprimer des moyens dans le SI fait l'objet d'une évaluation d'impact sur la sécurité.

5.1.4 Appareils mobiles et télétravail

La gestion des appareils mobiles (ordinateurs et téléphones portables) est organisée : attribution, restitution, contrôle et suivi, sécurité physique, authentification, connectivité, gestion des logiciels, etc.

Le télétravail est possible, et permis, sans dégrader la sécurité.

Les obligations concernant l'utilisation des appareils mobiles, depuis les locaux d'Almavia CX ou en dehors, sont décrites dans la charte informatique.

5.2 Sécurité des ressources humaines

5.2.1 Sélection des personnels, termes et conditions d'embauche

Des vérifications adaptées sont effectuées concernant les candidats à l'embauche ou à la mobilité interne sur les postes sensibles, en accord avec la législation : vérification du CV et confirmation des formations et certifications.

Les responsabilités sont formalisées dans les fiches de postes et sont communiquées aux nouveaux arrivants, et revues lors de chaque entretien annuel d'évaluation, ainsi que les obligations de sécurité y afférant.

Un engagement de confidentialité est systématiquement inséré dans les contrats de travail.

Une vérification à l'embauche, puis annuellement, du casier judiciaire des membres de la DSI est effectuée.

Le niveau de connaissances sécurité requis est défini pour chaque poste (consultant, développeur, etc.). Le personnel affecté à une mission valide ses connaissances au préalable. Un échec déclenche une action de formation.

5.2.2 Sous-traitance

Les sous-traitants sont soumis aux mêmes exigences de sécurité que les personnels internes (signature d'un engagement de confidentialité, sensibilisation à la sécurité, validation des connaissances sécurité requises pour le poste, etc.).

Les sous-traitants qui accèdent au SI d'Almavia CX sont également soumis aux règles suivantes :

- Signature de la charte informatique ;
- Connexion au SI avec un poste Almavia CX , ou depuis un serveur dédié à cet effet
- Utilisation d'identités et accès fournis par Almavia CX.

5.2.3 Charte informatique et règlement intérieur

La charte informatique est un document qui

- Décrit les obligations des utilisateurs quant à l'utilisation des moyens du SI, les responsabilités vis-à-vis de celles-ci ainsi que les conséquences légales et réglementaires en cas de non-respect des obligations de sécurité ;
- Doit être signé par tout nouvel arrivant ;
- Est annexé au règlement intérieur.

Le règlement intérieur rappelle, quant à lui, que tout manquement au respect des obligations de sécurité décrites dans la charte informatique est constitutif d'une faute exposant son auteur à une sanction disciplinaire voire pénale.

5.2.4 Mouvements

Les mouvements de salariés ou sous-traitants sont organisés

- A l'arrivée : préparation en amont, accueil, accompagnement et évaluation de l'intégration
- Sur changement d'affectation
- En cas de départ : préparation en amont, le jour du départ et les suivants

5.2.5 Sensibilisation

Des sessions de sensibilisation à la sécurité sont organisées au fur et à mesure des arrivées et des nécessités de renouvellement.

Un programme de sensibilisation est tenu à jour. Il définit les thèmes, les modes de diffusion, les populations ciblées et les plannings.

Le taux de participation aux sessions de sensibilisation est mesuré de manière régulière. Des actions sont prises rapidement lorsque le taux de participation n'est pas satisfaisant.

5.3 Gestion des actifs

5.3.1 Inventaire des actifs informatiques

Un inventaire des actifs informatiques, achetés par Almavia CX, est établi et mis à jour régulièrement. Les actifs informatiques concernés sont : les applications, les équipements d'infrastructure, les serveurs et les postes de travail. Un propriétaire est identifié pour chacun de ces actifs.

Un inventaire des logiciels installés sur les serveurs, et sur les postes de travail, est également établi et à mis à jour régulièrement.

5.3.2 Classification, marquage et utilisation des actifs

La classification des actifs repose sur l'évaluation d'au moins un besoin de sécurité parmi la disponibilité (D), l'intégrité (I) ou la confidentialité (C). Les besoins de sécurité sont évalués avec des valeurs comprises dans des échelles définies.

Les 3 besoins de sécurité sont établis et mis à jour régulièrement dans l'inventaire des applications, des équipements d'infrastructure et des serveurs.

Le besoin de confidentialité est établi lors de l'enregistrement des documents dans le SMSI. Ces documents sont marqués : le besoin de confidentialité est indiqué dans les nom donnés aux documents.

Des moyens sont mis en œuvre pour assurer la disponibilité, l'intégrité ou la confidentialité des actifs en tenant compte de la classification.

5.3.3 Supports amovibles

L'utilisation de support amovibles, sur des équipements fournis par Almavia CX, est limitée au maximum.

La charte informatique décrit les obligations concernant le stockage, sur des supports amovibles, de données appartenant à Almavia CX ou confiées à Almavia CX.

5.4 Contrôle d'accès et comptes d'accès

5.4.1 Contrôle d'accès

Une matrice de profils et d'accès associés est définie.

Les accès physiques et logiques sont attribués aux salariés, ou aux sous-traitants, à l'arrivée ou sur changement d'affectation, en respectant la matrice de profils.

Les visiteurs ne peuvent pas obtenir d'accès physique. Ils peuvent obtenir des accès logiques avec une durée de fonctionnement limitée, sur demande provenant d'un salarié d'Almavia CX.

En cas de départ, les accès physiques et les accès logiques principaux sont retirés le jour même. Les accès logiques secondaires, s'il y en a, sont retirés dans les jours qui suivent.

5.4.2 Comptes d'accès

Les comptes nominatifs, les comptes partagés, les comptes d'intervenants externes et les comptes fournis par des tiers sont gérés.

Des revues des comptes d'accès sont réalisées plusieurs fois par mois pour détecter les incohérences et les expirations proches. Des revues complémentaires sont également réalisées annuellement ou en cas de situation exceptionnelle.

5.4.3 Mots de passe

Un gestionnaire de mots de passe entreprise est déployé.

Les règles d'utilisation des mots de passe sont définies et communiquées. Exemple de règles concernées : qualité (longueur, complexité, historique…), durée avant expiration, renouvellement périodique et verrouillage sur tentatives infructueuses.

5.5 Cryptographie

Les certificats SSL/TLS, et leurs clés privées, qu'ils soient générés par des équipements du SI ou bien par des entités externes, sont gérés.

Les clés servant à chiffrer les données stockées sur les ordinateurs et serveurs sont gérées.

Les clés servant à chiffrer les données transportées dans les interconnexions réseaux sont gérées.

Les signatures de code sont gérées.

5.6 Sécurité physique et environnementale

5.6.1 Zones et accès

Les locaux d'Almavia CX sont découpés en plusieurs zones.

Les contrôles d'accès associés aux zones sont définis.

Les équipements d'infrastructures, hébergés dans les locaux d'Almavia CX, sont placés dans des zones à accès restreint.

5.6.2 Protection des locaux

Un système de vidéosurveillance est mis en place dans les locaux les plus sensibles (salle serveur, entrée des locaux).

5.6.3 Services généraux

Les accès Internet des locaux d'Almavia CX sont redondés.

5.6.4 Maintenance des équipements d'infrastructure

Toute opération de maintenance effectuée par un prestataire sur les équipements d'infrastructure donne lieu à un bon d'intervention. Ces interventions sont planifiées et supervisées.

Les accès en salle serveur sont enregistrés.

5.6.5 Sortie des équipements et utilisation hors site

Seuls les utilisateurs autorisés et disposant d'équipements adéquats peuvent sortir des sites Almavia CX avec leurs équipements.

Les obligations sont décrites dans la charte informatique. Les bonnes pratiques sont décrites dans la sensibilisation.

5.6.6 Mise au rebut des équipements

Des moyens sont mis en œuvre pour envoyer les équipements obsolètes au rebut.

5.6.7 Equipements laissés sans surveillance et bureau propre

Les tablettes et téléphones laissés sans surveillance dans les locaux d'Almavia CX sont rangés.

Les obligations sont décrites dans la charte informatique. Les bonnes pratiques sont décrites dans la sensibilisation.

5.6.8 Localisation des serveurs

Les serveurs hébergeant des données clients de production sont hébergés dans des datacenters certifiés ISO 27001.

Les serveurs hébergés dans les locaux d'Almavia CX sont placés dans les zones à accès restreint.

5.6.9 Maintenance des éléments de sécurité

Les éléments ci-dessous sont révisés annuellement :

- Climatisations
- Extincteurs
- Blocs de secours
- Plans d'évacuation
- Détecteurs de fumée

5.7 Sécurité liée à l'exploitation

5.7.1 Procédures d'exploitation

Les procédures d'exploitation sont tenues à jour et communiquées.

Les personnes qui appliquent les procédures d'exploitation sont formées, ou accompagnées, afin d'avoir le niveau de compétences requis.

L'exécution des procédures d'exploitation ne dépend pas d'une seule personne.

5.7.2 Changements

Les changements sont qualifiés puis planifiés.

Les changements sont contrôlés après réalisation.

5.7.3 Sauvegardes

Les serveurs hébergés par Almavia CX, ainsi que les serveurs hébergés dans des datacenters, sont sauvegardés.

La bonne exécution des sauvegardes est surveillée.

La viabilité des sauvegardes est vérifiée régulièrement avec des tests de restauration.

5.7.4 Journalisation

Des traces d'activités sont conservées dans un journal centralisé ou des journaux locaux, ce qui est désignée par journalisation.

La journalisation cible les traces liées, ou pouvant être liées, aux activités

- Suspectes, volontaires ou involontaire
- Indésirables, volontaires ou involontaires
- Susceptibles d'être demandées par une autorité judiciaire en cas d'enquête
- Réalisées par les administrateurs du SI

Les traces sont récupérées depuis

- Les postes de travail fournis par Almavia CX
- Les équipements d'infrastructure hébergés par Almavia CX
- Les serveurs hébergés dans les datacenters lorsque cela est possible
- Les applications SaaS lorsque cela est possible

5.7.5 Maintien en conditions de sécurité

Les alertes émises par le CERT-FR sont vérifiées de manière régulière. Chaque alerte fait l'objet d'une évaluation de l'impact sur le SI d'Almavia CX.

Les correctifs de sécurité, qualifiés d'importants et critiques par les éditeurs, sont déployés tous les mois et de manière automatique sur les serveurs et les postes de travail.

Les serveurs et les postes de travail sont équipés d'un EDR capable de détecter et bloquer les malwares ainsi que les comportements malveillants. Les alertes remontées par l'EDR sont surveillées et analysées en 24/7.

5.7.6 Supervision

La stabilité, la capacité et les performances des serveurs, et des équipements d'infrastructure, sont supervisés

- Par Almavia CX lorsqu'ils sont hébergés par Almavia CX
- Par les hébergeurs lorsqu'ils hébergés dans des datacenters

5.8 Sécurité des communications

5.8.1 Cloisonnement et filtrage

Les locaux d'Almavia CX, ainsi que les infrastructures hébergées dans des datacenters, sont protégés par des pares-feux.

Le réseau global est cloisonné en différents VLAN et des règles de filtrage sont appliquées.

Les serveurs qui publient des applications, ou services exposés sur Internet, sont isolés dans des DMZ.

L'architecture réseau et les matrices de flux sont documentés, et revus régulièrement.

5.8.2 Connexion au réseau local d'Almavia CX

La connexion au réseau interne d'Almavia CX est restreinte aux seuls équipements fournis par Almavia CX.

Les équipements des visiteurs peuvent se connecter à un réseau dédié qui ne permet que de sortir sur Internet.

5.8.3 Administration des équipements d'infrastructure réseau

Les équipements d'infrastructure réseau (routeur, commutateur, pare-feu, etc.) sont durcis conformément aux préconisations des constructeurs. Les correctifs de sécurité et les mises à jour sont installés dès lors qu'ils permettent de corriger des vulnérabilités.

Les équipements d'infrastructure réseau sont administrés au travers d'outils intégrant un chiffrement des flux et une authentification.

5.9 Acquisition, développement et maintenance

5.9.1 Sécurité des applications exposées sur Internet

Les applications hébergées par Almavia CX, ou dans des datacenters, et exposées sur Internet sont construites en respectant les règles suivantes :

- Protection des données au niveau infrastructure avec le chiffrement des supports de stockage

- Protection des données au niveau réseau avec le chiffrement des communications
- Protection des données au niveau applicatif avec déploiement d'architectures n-tiers, répartition des tiers dans zones réseaux distinctes et filtrage des flux entre les zones

5.9.2 Sécurité des serveurs

Les serveurs hébergés par Almavia CX, ou dans des datacenters, sont durcis au moment de leur installation ou lors de l'ajout d'un composant.

5.9.3 Développement sécurisé

Les équipes sont formées sur l'intégration de la sécurité dans les pratiques de développement.

Les sources des développements sont gérées.

Les librairies tierces inclues dans les développements sont gérées.

Le déploiement des nouvelles versions est réalisé en intégration continue.

La qualité et la sécurité des développements est contrôlée de manière régulière.

La sécurité des développements est surveillée avec des métriques.

5.9.4 Données de test

Les accès à l'environnement et aux données de test sont restreints aux seules personnes présentant un besoin d'en connaitre. Les jeux de données sont détruits dès lors qu'ils ne sont plus utiles.

Les jeux de données personnelles sont anonymisés dès lors qu'ils sont sortis d'un environnement maîtrisé.

5.10 Relations avec les fournisseurs

Une échelle d'importance des fournisseurs est définie. Les clauses contractuelles et obligations de sécurité sont définies pour chaque valeur de l'échelle d'importance.

Un registre des fournisseurs est tenu à jour. Ce registre précise l'importance attribuée à chaque fournisseur.

La contractualisation avec de nouveaux fournisseurs est précédée par l'évaluation de leur importance puis la vérification du respect des clauses contractuelles et obligations de sécurité.

Les fournisseurs avec une importance élevée font l'objet d'une revue annuelle. Cette revue consiste à vérifier que les clauses contractuelles et obligations de sécurité sont toujours respectées.

5.11 Gestion des incidents de sécurité

Les sources de signalement des incidents de sécurité sont identifiées.

La méthode de qualification de la gravité des incidents de sécurité est définie. La répartition des rôles et responsabilités, en fonction de la gravité, est également définie.

Les conditions justifiant de notifier la CNIL, ou des personnes, en cas d'incident impactant des données personnelles, sont définies. Les responsabilités liées à ces notifications sont également définies.

La méthode de recherche de la cause racine est définie.

Les incidents de sécurité sont suivis par le COGESEC.

5.12 Continuité des activités

5.12.1 Organisation

Le dispositif de pilotage des incidents de sécurité critiques est appelé cellule de crise.

Les critères d'activation de la cellule de crise, les rôles et les responsabilités dans la cellule de crise ainsi que les moyens de communication utilisés par la cellule de crise sont définis. Ils sont également révisés et diffusés de manière régulière. Enfin, la diffusion est faite de façon que les informations soient utilisables en cas d'indisponibilité de tout ou partie du SI d'Almavia CX.

Un exercice de simulation de crise est réalisé au moins une fois tous les 3 ans.

5.12.2 Incidents critiques dans les locaux d'Almavia CX

Des moyens de secours informatiques assurent la continuité des activités dans les locaux d'Almavia CX.

Les sauvegardes des applications hébergées dans les locaux d'Almavia CX sont externalisées.

5.12.3 Incidents critiques dans les datacenters

La mise en œuvre et la maintenance des moyens de secours, permettant d'assurer la continuité, sont confiées aux hébergeurs.

Des plans de test sont définis en collaboration avec les hébergeurs.

L'efficacité des moyens de secours, et des mécanismes de résilience aux pannes, est testée au moins une fois par an.

5.13 Conformité

5.13.1 Veille règlementaire

Une veille règlementaire est assurée afin d'identifier les exigences applicables aux activités Almavia CX et adapter les actions de mise en conformité.

5.13.2 Conformité règlementaire et contractuelle

Les exigences légales règlementaires et contractuelles applicables, ainsi que l'approche adoptée pour satisfaire à ces exigences, sont documentées.

6 Annexes

6.1 Historique du document

Version	Date
2.0	Novembre 2024
1.0	Octobre 2017

6.2 Table des abréviations

Abréviation	Définition
ANSSI	Agence Nationale pour la Sécurité des Systèmes d'Information
CNIL	Commission Nationale de l'Informatique et des Libertés
CSE	Comité Social Entreprise
DPO	Data Protection Officer – Délégué à la Protection des Données
DSI	Directeur du Système d'Information
CODIR	Comité de Direction
COGESEC	Comité de Gestion de la Sécurité
NIS2	Network & Information Security (version 2)
PGSSI	Politique Générale de Sécurité du Système d'Information
RGPD	Règlement pour la Protection des Données
RSMSI	Responsable du Système de Management de la Sécurité d'Information
RSSI	Responsable de la Sécurité du Système d'Information
SI	Système d'Information
SMSI	Système de Management de la Sécurité d'Information