cegid

Plan d’assurance sécurité CEGID

23/04/2025

www.cegid.com

À propos de ce document

Le but de ce document est de présenter le Plan d'Assurance Sécurité de Cegid.

Niveau de confidentialité	Public
Dernière mise à jour	23/04/2025

SOMMAIRE

Table des matières

1. EVOLUTION DU DOCUMENT

Les dates figurant dans le tableau suivant sont les dates d'approbation du document.

Date	Auteur	Nature de la modification
03/11/2016	Equipe Sécurité Cegid	Version initiale
02/02/2018	Equipe Sécurité Cegid	Revue du document
30/07/2018	Equipe Sécurité Cegid	Revue du document
23/05/2019	Equipe Sécurité Cegid	Revue du document
07/10/2020	Equipe Sécurité Cegid	Revue du document
08/08/2022	Equipe Sécurité Cegid	Fusion des Plans d'Assurance Sécurité existants au sein de celui de Cegid
03/04/2023	Equipe Sécurité Cegid	Revue du document, ajout des offres concernées et corrections typographiques
11/07/2023	Equipe Sécurité Cegid	Mise à jour de la liste des offres en lien avec le renouvellement de la certification ISO27001 et l'intégration des offres Notilus
04/03/2024	Equipe Sécurité Cegid	Revue du document, ajout des offres concernées et corrections typographiques
06/06/2024	Equipe Sécurité Cegid	Ajout des offres concernées
23/04/2025	Equipe Sécurité Cegid	Revue annuelle du document, mise à jour des offres concernées par le PAS et transition de la version 2013 à la version 2022 de la norme ISO27001.

2. INTRODUCTION

2.1. Objet du document

Le présent document constitue le Plan d'Assurance Sécurité (PAS), celui-ci peut être annexé aux contrats clients. Il décrit les engagements pris par Cegid pour satisfaire aux exigences contractuelles de Sécurité des Systèmes d'Information (SI) visant à :

- Assurer la protection des ressources des SI utilisées pour la réalisation des activités et la fourniture des livrables prévus contractuellement ;
- Préserver le Client des dommages pouvant résulter l'indisponibilité de ces ressources, ainsi que des atteintes à leur intégrité ou à leur confidentialité.

Ce Plan d'Assurance Sécurité (PAS) recense les dispositions relatives à la sécurité, incluant les mesures organisationnelles, applicables aux personnes, physiques et techniques mises en œuvre.

Les mesures décrites dans ce document peuvent être complétées par celles décrites dans le Livret de Service correspondant à l'offre Cegid concernée.

2.2. Domaine d'application

Ce document s'applique aux services SaaS opérés et délivrés par les équipes Cegid Cloud, ainsi qu'aux activités de ces équipes.

2.3. Evolution du PAS

Toute évolution du PAS entraîne la publication d'une nouvelle version de ce document. Les modifications sont enregistrées et datées dans l'historique des versions placé en début de document.

Une modification mineure[1] n'entraînera pas nécessairement de nouvelle version immédiate du PAS. Cette modification sera intégrée dans la prochaine version du document.

Toute évolution du PAS fait obligatoirement partie de celui-ci et engage les parties au même titre.

En cas d'évolution du document, la version publiée sur le site officiel de Cegid fait référence. La version annexée au contrat client permet de vérifier qu'il n'y a pas de régression.

Le PAS est révisé à minima annuellement. Cette révision peut donner lieu à l'édition d'une nouvelle version du présent document.

[1] Modification qui n'entraîne pas d'incidence sur les exigences de sécurité

2.4. Définitions

Actifs : Ensemble des biens ou prestations de services permettant de délivrer les offres de Cegid

ASVS : Application Security Verification Standard

BSIMM : Building Security In Maturity Model

CAB : Change Advisory Board

Client : Client d'une solution couverte par ce document

CMP : Cloud Management Platform

DPO : Data Privacy Officer

GED : Gestion Electronique des Documents

IPS : Système de Prévention d'Intrusion

ITSM : Information Technologie Service Management

Livret Service : Document décrivant les conditions particulières liées à chaque offre SaaS de Cegid

Cegid Cloud : Organisation au sein de Cegid en charge de la conception, de l'exploitation et du support technique de la plateforme SaaS de Cegid (cf. Présentation de Cegid Cloud)

ISO : International Standard Organization (Organisation internationale de normalisation)

OWASP : Open Web Application Security Project

PAS : Plan d'Assurance Sécurité

PAM : Privileged Access Management

PSSI : Politique de Sécurité des Systèmes d'Information

RGPD : Règlement Générale sur la Protection des Données

RPO : Recovery Point Objective ou Point de Rétablissement des données

RSSI : Responsable de la Sécurité des Systèmes d'Information

RTO : Recovery Time Objective ou Temps de Rétablissement du service

SAMM : Software Assurance Maturity Model

SMSI : Système de Management de la Sécurité de l'Information. Cette expression désigne un ensemble de politiques concernant la gestion de la sécurité de l'information

VM : Virtual Machine

VPN : Réseau Privé Virtuel

2.5. Documents de références

CGU : Conditions Générales d'Utilisation de services de Cegid. Elles sont disponibles sur www.cegid.com, site web de Cegid

ISO27001:2022 : Norme d'exigences de Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'information (SMSI)

ISO 27002:2022 : Guide des bonnes pratiques en SMSI

ISO 27005:2018 : Norme de gestion de risques liés à la sécurité de l'information

Livrets Service : Documents décrivant les conditions particulières liées à chaque offre SaaS de Cegid. Ils sont disponibles sur www.cegid.com, site web de Cegid

3. ROLES ET RESPONSABILITES

Dans le cadre de la délivrance de ses services, Cegid s'appuie sur des infrastructures mises à disposition par ses sous-traitants. Le déploiement et la maintenance de ces infrastructures sont à la charge de ces sous-traitants.

4. DESCRIPTION DES SERVICES

Les services spécifiques aux applications délivrés par Cegid et leur description sont fournis dans les livrets de services

5. BONNES PRATIQUES

La sécurité de Cegid est pilotée par une équipe centralisée qui s'inspire de la norme ISO 27001 pour l'ensemble du Groupe. Cegid est certifié ISO 27001:2022 sur les périmètres suivants :

- « Service permettant l'hébergement d'applications contenant des données fournies par les clients dans un environnement Cloud »
  Certificat n° IS 666376 délivré par BSI
  Sites France : Lyon (69), Vénissieux (69), Boulogne Billancourt (92), Nantes (44)
  Services SaaS Cegid concernés par cette certification : Cegid Expert, Cegid Fiscalité (ex-Your Cegid Fiscalité), Cegid HR (Suite Ex-Talentsoft), Cegid HR Sprint, Cegid Loop, Cegid Notilus (Modules Notes de frais et Déplacements), Cegid Optitaxes, Cegid Payroll Ultimate (ex Cegid HR Ultimate), Cegid Portail Etafi, Cegid PMI, Cegid Quadra (ex-Cegid Quadra Expert), Cegid Quadra Entreprise Plus, Cegid Retail, Cegid RHP, Cegid RHPi, Cegid Tax Flex, Cegid Tax Ultimate, Cegid XRP Flex, Cegid XRP Sprint.

- « Développement et exploitation de logiciels de gestion des paiements et de la trésorerie en mode SaaS »
  Certificat AFNOR N°2023/106509.3
  Site France : Boulogne Billancourt (92)
  Services SaaS concernés par cette certification : Cegid Exabanque, Cegid Allmybanks, Cegid MesBanques, Cegid Direct-Debits.

- « Services SaaS RH et Paie et Gestion du Temps de Visualtime fournis dans différents modèles de service pour faciliter la gestion des ressources humaines aux clients de Cegid Spain »
  Certificat n° IS 589848 délivré par BSI
  Site Espagne : Madrid and Barcelona
  Services SaaS Cegid concernés par cette certification : Cegid Peoplenet HR, Cegid Peoplenet Payroll et Cegid VisualTime en Espagne

- « Service permettant l'hébergement d'applications pour la gestion et le développement des ressources humaines contenant des données fournies par les clients, dans un environnement Cloud »
  Certificat n° CA09/77186 délivré par SGS
  Site Canada : Montréal
  Site USA : New York
  Site France : Paris (75)
  Services SaaS concernés par cette certification : Cegid Talent

- « Design, delivery, and ongoing support of the StorIQ application »
  Certificat n°20/3244 délivré par CfA
  Site Angleterre : Londres
  Services SaaS Cegid couverts par cette certif cation : Cegid Retail Store Excellence

- « Le système de gestion de la sécurité de l'information qui soutient les activités d'installation, de maintenance et de soutien des systèmes d'hébergement en nuage pour les applications des clients d'Ekon Cloud Computing Solutions SAU, conformément à la version de la déclaration d'applicabilité APL 001/21»
  Certificat n° ES 122286-1 délivré par Bureau Veritas
  Site Espagne : Barcelona
  Services SaaS Cegid concernés par cette certification : Cegid Ekon, Cegid XRP Enterprise

- Rapport ISAE 3402 Type II sur Cegid Tax Ultimate (France uniquement)
- Rapport ISAE 3402 Type II sur Cegid Allmybanks
- Rapport ISAE 3000 Type I en tant que prestataire de Services de Paiement (en anglais Payment Service Provider ou PSP) pour les clients Swift Alliance Lite 2 (SAL2)
- SWIFT Customer Security Controls Framework (CSCF) sur Cegid Allmybanks
- Rapport SOC1 Type II sur Peoplenet Payroll (Argentine et Mexique)
- Rapport SOC2 Type II sur Peoplenet Payroll (Espagne, Portugal, Argentine, Mexique, Colombie et Chili)
- Rapport SOC 1 Type II sur Cegid HR (suite Talentsoft, module Carrière)
- Rapport ISAE 3402 Type II sur PeopleNet France
- SWIFT Customer Security Controls Framework de Cegid Treasury.

Les services SaaS Cegid suivants sont couverts par ce Plan d'Assurance Sécurité bien que n'étant pas dans l'un des périmètres des certifications précédentes : Cegid Assurex, Cegid HR (Module Talent Acquisition Ex-Digitalrecruiters), Cegid ISIE, Cegid Orli, Cegid Payroll Peoplenet en France et en Amérique Latine, Cegid Peoplenet Dedicated, Cegid Peoplenet Enterprise, Cegid Retail UR, Cegid XRP Ultimate, Cegid Treasury.

Si vous ne trouvez pas votre produit dans les listes, n'hésitez pas à contacter notre service commercial pour plus d'informations.

L'objectif est de protéger les fonctions et les informations de toute perte, vol ou altération et de prémunir les systèmes informatiques de toute intrusion ou sinistre.

Le respect d'un Cycle de Vie du Développement Logiciel Sécurisé permet de garantir un niveau de sécurité sur les applications hébergées. Ce cycle de vie est basé sur les principes des référentiel OWASP SAMM, BSIMM et OWASP ASVS.

6. GESTION DES RISQUES

Le processus d'évaluation des risques du Groupe comprend l'identification, l'analyse et la gestion des risques liés au modèle d'entreprise et aux entités utilisatrices.

Cegid reconnaît que la gestion des risques est une composante essentielle de ses activités. La direction a mis en place une cartographie des risques pour Cegid Cloud sur quatre domaines :

Les risques liés aux :

- Risques liés aux ressources humaines.
- Risques stratégiques
- Risques liés à la sécurité de l'information
- Autres risques

Ce processus permet à la Direction de Cegid de comprendre et de suivre les risques pertinents qui pourraient affecter la société et de mettre en place des mesures pour les atténuer.

De plus, des analyses de risque spécifiques aux différents SMSI sont mis en œuvre en se basant les principes de la norme ISO 27005 et méthodes reconnues internationalement (EBIOS 2010, EBIOS RM, MAGERIT,).

L'analyse de risque fait partie intégrante de la sécurité des SI de Cegid. Elle est opérée de manière continue entre les équipes opérationnelles et les équipes sécurité.

7. POLITIQUE DE SECURITE DE L'INFORMATION

Les activités de Cegid sont encadrées par des Politiques de Sécurité de l'Information, mises en place depuis 2008 et révisées chaque année. Ces politiques s'appuient sur les principes et les bonnes pratiques des normes ISO 27001:2022 et ISO 27002:2022.

Ces politiques visent à protéger les informations critiques de Cegid, de ses clients et partenaires. Les politiques sont communiquées aux personnes concernées.

Pour préserver au mieux la sécurité et l'intégrité de ses plateformes, Cegid ne divulgue pas les noms ni les informations relatives aux éléments de sécurité mis en œuvre (fournisseurs, éditeurs, etc.).

8. ORGANISATION DE LA SECURITE DE L'INFORMATION

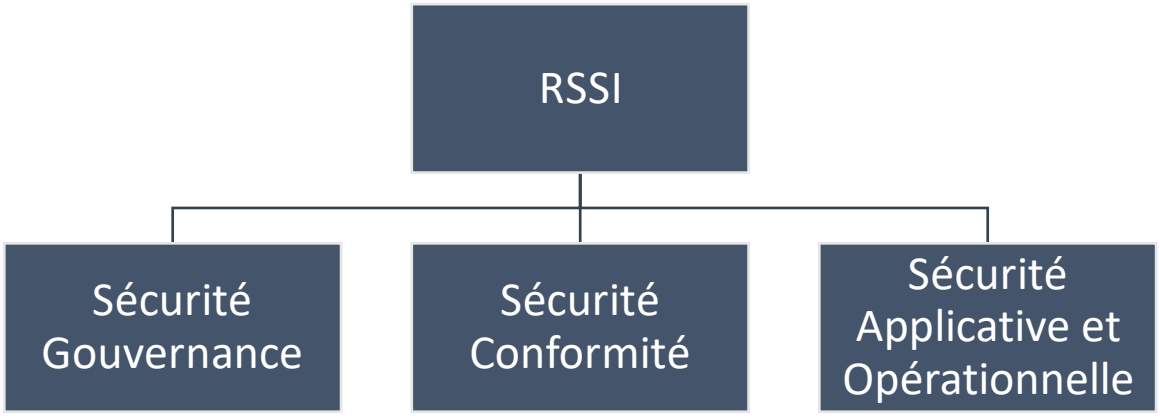
8.1. Organisation interne

8.1.1. Rôles et responsabilités

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

Un RSSI est nommé pour l'ensemble des activités de Cegid. Il a sous sa responsabilité une équipe dédiée à la sécurité.

Les acteurs impliqués dans la sécurité de l'information sont :



8.1.2. Séparation des taches et domaine de responsabilité

Afin de limiter le risque de modification ou d'altération des actifs (non autorisé ou involontaire) les tâches et les domaines de responsabilités des équipes sont séparés.

En particulier, toutes les activités d'hébergement pour nos clients sont séparées du reste des environnements de l'entreprise, tant au niveau organisationnel que technique.

De plus, au sein des activités d'hébergement pour nos clients, un principe de séparation des tâches en mis en place au travers de gestion des droits liés aux besoins métiers.

Une organisation matricielle du Groupe permet de définir les domaines de responsabilité par métier, notamment ceux liés à la responsabilité de la sécurité des données clients, la protection des actifs et des risques associés à la délivrance des services Cloud.

8.1.3. Gouvernance

Les instances de gouvernance sont en place au niveau stratégique et au niveau opérationnel avec des comités dédiés.

Ces instances se réunissent régulièrement pour assurer le suivi des sujets concernant la sécurité des systèmes d'information. Les compte-rendu sont stockés dans le système de gestion documentaire.

8.1.4. Relation avec les organismes et les autorités

Cegid est membre d'associations professionnelles (CLUSIF, CLUSIR, Club ISO 27001, Club de la Continuité d'Activité, Incibe…). Cegid entretient des relations avec les autorités (ANSSI, CNIL, CCN-Cert, AEPD, CERT-MX…) afin de suivre les évolutions dans le domaine de la sécurité de l'information.

8.1.5. Veille de sécurité

Cegid a mis en place une politique de veille de sécurité intégrée, comprenant la veille légale, le renseignement sur les menaces et la veille technique, afin de prévenir les risques et garantir la conformité aux exigences légales.

La veille légale permet d'identifier les évolutions législatives impactant la sécurité, en collaboration avec le département juridique et le DPO, afin de s'assurer que les pratiques de l'entreprise restent conformes aux obligations légales.

Le processus de renseignement sur les menaces, mis en œuvre par Cegid, vise à collecter et analyser les tendances susceptibles d'impacter son système de gestion de la sécurité de l'information, tout en proposant des actions stratégiques pour renforcer les mesures existantes. De plus, des services externes fournissent également des flux d'information continus sur les menaces de sécurité, permettant à Cegid de suivre les vulnérabilités susceptibles de poser des risques pour la sécurité de l'information. La veille technique est assurée par des outils de scan de vulnérabilité, qui détectent et évaluent les failles potentielles au sein des systèmes de Cegid, permettant la mise en place d'actions de protection proactive.

9. SECURITE LIEE AUX RESSOURCES HUMAINES

9.1. Recrutement

Les vérifications des informations des candidats à l'embauche sont effectuées conformément aux réglementations, aux principes éthiques, aux lois, et à toute législation applicable dans la juridiction concernée. Ces vérifications sont adaptées aux exigences du poste, à la classification des informations accessibles, et aux risques identifiés.

Parmi les vérifications en place, on trouve :

- Vérification du curriculum vitæ du candidat ;
- Vérification des compétences en lien avec le poste ;
- Copies des diplômes, des formations et des qualifications professionnelles alléguées dans le CV ;
- Contrôle d'identité indépendant, passeport ou carte d'identité ;
- Vérification de la validité du permis de travail, de la carte de séjour pour les candidats étrangers dans le pays d'exercice.

9.2. Gestion de la confidentialité

Les aspects suivants sont couverts dans les contrats, le règlement intérieur et la charte informatique :

- Respect de la propriété intellectuelle ;
- Respect de la législation sur la protection des données personnelles ;
- Protection des informations, des actifs liés aux informations, des applications de l'entreprise et de ses clients ;
- Protection de l'information provenant des partenaires, d'autres organisations ou tiers.

Des dispositions particulières peuvent s'appliquer dans les situations suivantes :

- Déclenchement d'un processus disciplinaire formel et connu de tous à l'encontre des salariés ayant enfreint les règles de sécurité de l'information. Il constitue un élément dissuasif empêchant les salariés d'enfreindre les politiques et procédures relatives à la sécurité de l'entreprise, ainsi que toute autre règle de sécurité ;
- Responsabilités stipulées dans le contrat de travail continuant à s'appliquer pendant une durée définie après la fin du contrat.

Tous les collaborateurs sont contractuellement tenus à la confidentialité. Toutes les informations fournies par les Clients, que ce soit par le biais de documents ou de réunions sont couverts par cet engagement de confidentialité.

9.3. Gestion de la compétence

9.3.1. Sensibilisation à la sécurité

Les nouveaux collaborateurs suivent un parcours d'intégration qui comprend une sensibilisation à la sécurité et à la confidentialité.

Un plan de sensibilisation et des outils spécialisés permettent un suivi régulier sur les sujets sensibles de la sécurité (campagne de phishing, Safe desk, etc.).

9.3.2. Compétence et formation

Afin de maintenir le savoir-faire, d'identifier les besoins de formation et d'organiser le partage des connaissances des entretiens de performance et d'objectifs sont effectués chaque année par les salariés de Cegid et leurs managers. Lors de ces entretiens, des plans de formations sont discutés. Les RH élaborent un plan de formation annuel à partir de l'expression de ces besoins et de la stratégie de l'entreprise.

10. GESTION DES ACTIFS

10.1. Inventaire

Cegid met en place des inventaires des actifs essentiels et des actifs supports. Ceux-ci sont répertoriés dans les analyses de risque afin de centraliser les risques associés.

Lorsque cela est techniquement faisable et pertinent, un processus automatisé de mise à jour permet de réconcilier l'inventaire avec les actifs présents dans le périmètre SaaS.

10.2. Identification des actifs

L'identification des actifs utilisés dans la fourniture des services fournis par Cegid se base sur des conventions de nommage formalisées. Dans la majorité des cas, et lorsque c'est pertinent, ces conventions de nommage qui ne permettent pas d'établir un lien direct avec les clients.

10.3. Gestion documentaire

Cegid a implémenté des systèmes de gestion documentaire qui prennent en compte les processus et procédures nécessaires au fonctionnement des services destinés aux clients.

10.4. Gestion des supports et matériels affectant les données clients

10.4.1. Stockage

Les supports amovibles contenant des données clients sont stockés dans un emplacement sécurisé quand ils ne sont pas utilisés.

Les supports non-amovibles contenant des données clients sont hébergés dans des datacenters.

10.4.2. Transfert physique

Pour le transfert physique d'un media contenant des données non publiques, Cegid utilise exclusivement des transporteurs reconnus et fiables offrant un suivi et des preuves de livraison. Dans le cadre où Cegid devrait retourner des données sur un media transmis à l'initiative d'un client, alors elles seront transmises en utilisant les mêmes techniques et les mêmes moyens que lors de leur réception.

10.4.3. Mise au rebut

La mise au rebut des actifs est soumise à une procédure particulière de suppression des données confidentielles. Cette procédure impose une suppression sécurisée ou une destruction physique des médias ayant contenu des données confidentielles.

10.4.4. Maintenance

La responsabilité des équipements matériels contenant des données clients incombe aux fournisseurs d'infrastructure de Cegid.

10.5. Gestion des actifs matériels collaborateurs de Cegid

10.5.1. Maintenance du matériel

Les postes collaborateurs de Cegid sont fournis par les services de Cegid (DSI). La maintenance matérielle de ces machines est effectuée par la DSI et ses fournisseurs. Un inventaire de l'affectation de ces postes est maintenu et les collaborateurs sont responsables de leur sécurité physique.

10.5.2. Mise au rebut

Les médias de stockages présents dans les matériels mis au rebut sont détruits de façon sécurisée selon les procédures applicables (logiciel d'effacement de données, suppression des clés de chiffrement des disques…).

10.5.3. Gestion des supports amovibles

Une politique de sécurité des supports amovibles est mise en place et administrée pour les collaborateurs des équipes Cegid Cloud. Cette politique est implémentée par un logiciel de type Endpoint ou par GPO, ce qui permet de limiter l'usage des média amovibles

10.5.4. Mise à jour, antivirus, chiffrement des supports

La DSI est responsable des mises à jour des systèmes et applications de Cegid (Bureautique, applications internes), de la mise à jour des protections contre les logiciels malveillants, ainsi que du chiffrement des supports (Internes et amovibles). Des indicateurs sont régulièrement produits et analysés par l'équipe sécurité.

11. POLITIQUE DE SECURISATION DES SYSTEMES D'EXPLOITATION

Une politique de durcissement destinée à sécuriser les systèmes d'exploitation est mise en place. Il s'agit de réduire la surface d'attaque possible, en désactivant ou supprimant les objets (services, applications, fonctionnalités…) non-essentiels. Cela consiste à mettre en place des options de sécurité particulières et d'assurer les mises à jour logicielles.

11.1. Système d'exploitation des serveurs

Les opérations de durcissement sur les systèmes d'exploitation des serveurs concernent :

- Mise à jour
- Stratégie de compte
- Droits utilisateurs et réseau
- Journalisation
- Protection contre les logiciels malveillants
- Service rôle et fonctionnalité
- Espace utilisateur
- Espace disque

Ces opérations s'inspirent des guides du CIS, de l'ANSSI et du NIST.

12. CONTROLE D'ACCES

12.1. Politique de mot de passe

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

Les mots de passe des utilisateurs ne sont pas stockés en clair dans le système d'information de Cegid.

La règle par défaut pour nos périmètres est d'utiliser des fonctions de chiffrement non réversibles de type « hashage » avec des algorithmes sécurisés.

Pour les périmètres AS400, un chiffrement de Vigenère avec une clé X-OR est en place.

12.1.1. Politique pour les administrateurs techniques de Cegid

La gestion des mots de passe pour les administrateurs techniques de Cegid est soumise à une politique de sécurité stricte :

- Taille minimum : 10 caractères.
- Complexité : lettre, chiffre et symbole
- Fréquence de changement : tous les 60 jours
- Pas de réutilisation des 24 derniers mots de passe
- Verrouillage après 5 tentatives (déverrouillage par un administrateur de Cegid)

Cette politique de sécurité est renforcée pour certaine population telle que celle des administrateurs cloud de Cegid.

12.1.2. Politique pour les clients de Cegid

La politique standard de mot de passe pour les utilisateurs des clients de Cegid est la suivante :

- Taille minimum : 8 caractères.
- Complexité : lettre minuscule et majuscule, chiffre et caractères spéciaux
- Fréquence de changement : tous les 90 jours
- Pas de réutilisation des 24 derniers mots de passe
- Verrouillage après 5 tentatives (déverrouillage par un administrateur de Cegid ou par l'utilisateur via un outil de gestion en ligne des mots de passe)

Certaines applications permettent de déléguer la gestion des identifiants au Client. Lorsque cette fédération des identités est activée, le Client est autonome pour gérer et appliquer sa propre politique de mot de passe. Cegid recommande à ses clients cette option tout en respectant les impératifs liés au RGPD.

12.2. Gestion des droits

La gestion des droits pour les équipes de Cegid se base sur le principe du moindre privilège. Chaque équipe possède les droits nécessaires uniquement en rapport avec l'activité qu'elle réalise.

Des revues des droits d'accès sont effectuées à intervalles réguliers.

Les demandes de droits (ajout, modification, suppression) aux principaux applications et domaines se font au travers de workflows.

Pour des raisons de confidentialité, aucune donnée personnelle relative aux collaborateurs de Cegid ne sera communiquée.

12.3. Gestion des accès aux serveurs

Seules les personnes ayant les autorisations nécessaires peuvent accéder aux serveurs contenant des données clients. Cegid dispose d'annuaires spécifiques aux périmètres de production, séparés du système d'information interne.

12.4. Suppression des accès

La suppression des accès pour le personnel Cegid est liée au processus RH de gestion des départs ou de mobilité interne. Ces actions sont suivies et tracées au travers d'outils de workflows interne.

Concernant les collaborateurs externes, les modification ou suppression de droits sont sous la responsabilité de leur manager.

12.5. Revue des droits

La revue des droits des principaux périmètres et applications est organisée par l'équipe sécurité. Des revues des accès sont effectuées régulièrement sur la base d'une analyse de risque.

13. CRYPTOGRAPHIE

13.1. Transfert de données vers les réseaux publics

Les données sont chiffrées lors des transferts vers les réseaux publics avec des protocoles sécurisés (HTTPS, TLS, SFTP, SSH…)

13.2. Transfert de données vers autres supports

Dans le cas de supports amovibles (ex : clés ou disques USB), les médias doivent être chiffrés par le client, si besoin avec l'aide des équipes support, avant de partir à destination de Cegid. Si ce n'est pas le cas, le client est responsable de la sécurité de ses données durant le transport et la réception chez Cegid. Les médias, après intégration des données, sont effacés avant de repartir chez le client.

13.3. Certificats

Dans l'optique de garantir le meilleur niveau de sécurité, les certificats HTTPS utilisés par Cegid proviennent d'autorités de certifications publiques et reconnues. La gestion de ces certificats est encadrée par des procédures couvrant leur cycle de vie.

13.4. Chiffrements

Les règles concernant la longueur des clés de chiffrement sont :

- Chiffrement asymétrique : supérieur ou égal à 2048 bits
- Chiffrement symétrique : supérieur ou égal à 256 bits

Cegid utilise des logiciels de chiffrement s'appuyant sur l'AES256 pour créer des archives sécurisées.

Concernant le chiffrement des protocoles de connexion pour nos sites externes sont au minimum en TLS 1.2.

13.5. Mobilité

Les équipes d'administration de Cegid utilisent uniquement leurs ordinateurs portables pour se connecter à distance).

14. SECURITES PHYSIQUES ET ENVIRONNEMENTALES

14.1. Localisation

Les datacenters utilisés par Cegid sont implantés à travers le monde pour répondre aux contraintes réglementaires des clients. Cegid veille à la conformité de ses fournisseurs, tant au niveau technique que sécuritaire. Le choix des datacenters est effectué avant mise en production, en fonction des offres de Cegid.

14.2. Datacenters

14.2.1. Sécurité physique des sites et contrôle d'accès

Pour garantir un niveau de sécurité optimal, les datacenters utilisés par Cegid sont tous certifiés ISO 27001. La visite des datacenters n'est autorisée que par les personnes habilitées.

14.2.2. Sécurité des matériels

Un ensemble de mesures et de principes ont été intégrés dans la conception de l'infrastructure pour assurer le niveau de disponibilité et d'intégrité optimal des services de Cegid.

La règle principale est d'éviter tout point de défaillance unique ('Single Point Of Failure' en anglais) au niveau du matériel ou des liens. Par exemple :

- Redondance au niveau des serveurs physiques
- Redondance au niveau du réseau
- Redondance au niveau du stockage
- Virtualisation

14.3. Locaux de Cegid

14.3.1. Sécurité des sites

Les locaux de Cegid sont soumis à minima aux règles suivantes :

- Fourniture d'énergie avec contrat particulier + onduleur
- Détecteurs d'incendie, extincteurs
- Fourniture des services CCV (Climatisation, Chauffage, Ventilation).

14.3.2. Contrôle des accès

Les accès aux locaux sont sécurisés par des lecteurs de badges. Chaque collaborateur dispose d'un badge programmé lui permettant l'accès total ou partiel à certaines parties du bâtiment.

Les contrôles des accès physiques font partie de la gestion des droits décrite au paragraphe 12.2.

14.3.3. Bureau propre

Une politique de bureau propre est en place dans les locaux des équipes de Cegid. Les documents, médias ou tout autre support pouvant contenir des informations confidentielles sont rangés quand ils ne sont pas utilisés.

15. SECURITE LIEE A L'EXPLOITATION

15.1. Sécurité des Données

15.1.1. Classification des données

La norme ISO 27001 impose une classification des biens et des informations essentiels. Cette classification est établie sur au moins trois niveaux :

- Public
- Limité
- Confidentiel

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

15.1.2. Sécurité sur les fichiers

Les fichiers de données sont stockés dans des répertoires dédiés à chacun de nos clients. Ces répertoires sont protégés avec les mécanismes de sécurité fournis par les systèmes d'exploitation sous-jacents.

Cela permet de garantir la sécurité, le cloisonnement et l'étanchéité entre chaque client.

15.1.3. Sécurité sur les bases de données

Cegid utilise pour ses bases de données des systèmes standards et connus de type Microsoft SQL, Oracle, MySQL, MongoDB. DB2…

La sélection d'acteurs majeurs du domaine permet à Cegid de s'appuyer sur des éditeurs confirmés et une communauté très active pour maintenir toujours au niveau optimal ses systèmes de gestion de base de données.

15.1.4. Chiffrement des données

Les données sont sécurisées lors de leurs transferts entre le poste de travail des clients et le SI de Cegid en utilisant des protocoles de chiffrement décrits en 13.1.

15.1.5. Intégrité des données

Cegid s'engage par l'intermédiaire de procédures, de mesures techniques et de protocoles sécurisés sur la transmission et la conservation des données de ses clients afin de se prémunir contre l'altération (volontaire ou accidentelle).

15.1.6. Fin de contrat

Les modalités de conservation et de suppression des données client après la résiliation d'un contrat sont spécifiées dans les documents contractuels.

15.2. Gestion des changements

Les changements suivent le processus de ci-dessous :

Changements applicatifs :

- Les changements standards et normaux sont autorisés après validation en comité. A titre d'exemple, parmi ces changements, on trouve : les mises à jour de portail standard, les mises à jour de fiscalité, les évolutions de paramétrage, les corrections de bugs et vulnérabilités…

Changements Infrastructures et systèmes :

- Autorisés après validation en comité : changements infrastructure ayant un impact direct sur la production, résolution d'incidents, gestion de capacité, sécurité.
- Autorisés sans validation en comité : gestes d'exploitation courants servant à maintenir la production en condition opérationnelle.

Périodes spéciales :

- En fonction de la saisonnalité des produits et métiers de nos clients, les changements sont limités sur certaines périodes, généralement appelées « périodes de freeze »

Changements URGENTS :

- Les changements urgents sont à déployer rapidement et ne peuvent pas attendre le prochain cycle de validation.
- Cette catégorie de changement est réservée à la résolution d'une crise ou d'un risque critique imminent (e.g. faille de sécurité, incident majeur).
- Cette catégorie de changement est traitée dans un comité réuni en urgence (e.g. eCAB / Emergency CAB).

15.3. Protection contre les logiciels malveillants

L'ensemble des infrastructures serveurs est protégé par des solutions antivirus et antimalware centralisées. Les serveurs pivots contrôlent au minimum quotidiennement la présence des mises à jour chez l'éditeur, puis les diffusent sur l'ensemble des serveurs.

15.4. Sauvegarde

15.4.1. Politique de sauvegarde

Les données clients sont au cœur de l'attention des équipes de Cegid. Afin d'en assurer l'intégrité et la disponibilité, Cegid opère un système de sauvegarde performant.

Le principe retenu par Cegid est celui de la double sauvegarde :

- Une première sauvegarde est réalisée depuis les systèmes de production sur une première infrastructure dédiée.
- Une duplication est ensuite effectuée sur une deuxième infrastructure dédiée.

Les infrastructures de sauvegarde ne sont pas localisées dans le même Datacenter que les systèmes de production. Cette organisation permet de garantir un niveau de disponibilité et d'intégrité optimal tout en assurant nos exigences de RTO et RPO (cf chapitre 20.3).

La fréquence des sauvegardes et la durée de rétention est propre à chaque offre et détaillée dans le Livret de Service de l'offre concernée.

15.4.2. Contrôles et restauration

Un contrôle des tâches de sauvegarde est réalisé par les outils de reporting. En cas d'incident lors d'une sauvegarde, une alerte est émise automatiquement et celle-ci est traitée par les équipes de Cegid.

Dans le cadre de son activité régulière d'exploitation, Cegid effectue au quotidien des restaurations. Celles-ci permettent de valider le bon fonctionnement des sauvegardes ainsi que les processus de restauration associés.

15.4.3. Principes de rétention

En tant qu'éditeur spécialisé, Cegid connait bien les métiers et les besoins de ses clients. Cette caractéristique a permis de mettre en place des durées de rétention de sauvegarde spécifiques à chaque offre proposée.

Les principes de rétention sont détaillés dans le Livret Service de chaque offre.

15.5. Gestion des traces

15.5.1. Collecte des traces

La traçabilité sur le SI de Cegid est assurée grâce à des outils de concentration et de corrélation des journaux d'évènements (logs). Ceux-ci sont conservés à des fins techniques et d'exploitation pour une durée adaptée en fonction des contraintes légales, contractuelles et opérationnelles.

Ces outils permettent d'uniformiser la durée de rétention des informations collectées et d'en garantir la sécurité.

Les informations collectées sont par exemple le nom de l'utilisateur, son heure de connexion, de déconnexion, l'application utilisée, l'adresse IP source…

Les logs sont accessibles aux équipes Cegid et ne sont pas exportables pour le Client. Ces logs pourront être communiqués au Client uniquement sur demande légitime comme dans le cas de

résolution d'un incident. Certaines offres Cegid proposent des logs applicatifs disponibles directement à partir de l'application.

15.5.2. Politique d'accès aux outils

Les outils sont accessibles par les collaborateurs de Cegid Cloud pour les besoins spécifiques à l'exploitation de la plateforme et avec des droits adaptés à leurs fonctions (voir chapitre 12).

15.5.3. Usage des traces

Exemples d'usages des informations collectées :

- Répondre aux contraintes réglementaires et contractuelles liées aux métiers de Cegid.
- Suivre l'état de santé des systèmes gérés par Cegid Cloud et pouvoir détecter au plus tôt tout évènement pouvant entrainer une dégradation du service.
- Produire des informations statistiques rendues anonymes concernant la fourniture du service.

L'usage des statistiques et des informations issues des traces est régi par les Conditions Générales d'Utilisation.

15.6. Supervision

15.6.1. Principes

Tous des services et des systèmes gérés par Cegid Cloud sont supervisés. Les outils de supervision utilisent soit le protocole SNMP, soit des automates développés spécifiquement pour récupérer les informations de tous les points de contrôle.

Une salle de télésurveillance permet aux équipes de Cegid Cloud de suivre en permanence l'état de santé de certains services. Des alertes en temps réels sont déclenchées en cas de dysfonctionnement pour tous les services supervisés.

Les outils sont également couplés à des systèmes d'envoi de SMS vers les équipes d'astreinte durant les heures non ouvrées (HNO).

15.6.2. Astreinte

L'astreinte se charge de surveiller et d'intervenir sur le SI de Cegid 24h sur 24 et 7 jours sur 7. Elle est composée de spécialistes représentant tous les domaines de compétence de Cegid.

15.7. Gestion des mises à jour

15.7.1. Gestion des logiciels installés

Cegid utilise logiciels permettant d'inventorier et maitriser l'ensemble des logiciels présents sur le système d'information ainsi que sur les postes d'administration.

15.7.2. Mise à jour système

Les mises à jour des systèmes sont effectuées via des consoles centralisées. Cegid applique le principe suivant les mises à jour critiques et de sécurité : les mises à jour sont déployées sur un cycle mensuel sur un ensemble d'environnements témoins dès la sortie d'un patch, afin de vérifier qu'il n'affecte pas l'intégrité ou de disponibilité du service délivré aux clients. Si aucun problème n'est détecté, le déploiement est ensuite réalisé sur l'ensemble de la plateforme de production. En cas d'indisponibilité d'un patch, une solution de contournement est mise en place pour maintenir la sécurité du service proposé.

15.7.3. Mise à jour applicative

Cegid a mis en place une gestion industrialisés des changements (voir chapitre 15.2) permettant de gérer les mises à jour applicatives conformément aux engagements définis dans les Livrets de Service de ses solutions SaaS.

16. SECURITE DES COMMUNICATIONS

16.1. Architecture technique

L'infrastructure supportant les services de Cegid est cloisonnée et organisée en zones de sécurité et en zones applicatives. Ce principe permet de proposer une sécurité en profondeur adaptée aux besoins actuels et futurs.

16.2. Accès télécom

16.2.1. Internet

Cegid possède des adresses IP publiques en propre ainsi que plusieurs accès internet auprès de fournisseurs différents pour palier toute défaillance d'un fournisseur et ainsi fournir à ses clients le niveau de service attendu.

L'ensemble des communications proposées par Cegid est sécurisé et utilise les protocoles mentionnés au chapitre 13.1

16.2.2. Réseaux wifi

Les réseaux wifi sont compartimentés en fonction de leurs fonctions (wifi invités, employés, mobile, etc.) et leur accès dépend de la gestion des droits. Les points d'accès wifi sont protégés.

Dans les datacenters, le réseau wifi est prohibé.

16.3. Equipements de sécurité

16.3.1. Pare-feu

Des pares-feux sont présents entre chaque zone de sécurité et chaque zone applicative.

Les flux en provenance de l'extérieur traversent plusieurs couches de pare-feu avant d'atteindre le service demandé.

Les flux directs vers les zones de confiance ne sont pas autorisés, ils doivent obligatoirement passer par les zones démilitarisées (DMZ).

16.3.2. IDS/IPS

Des sondes IDS/IPS ont été mises en place dans certains emplacements réseaux stratégiques pour analyser les flux entrants et sortants du SI de Cegid. Leur rôle est de détecter les flux anormaux et le trafic malveillant, puis de les bloquer.

Les sondes récupèrent les mises à jour de signatures d'attaque auprès des experts sécurité de l'éditeur et sont déployées sous la responsabilité de l'équipe sécurité de Cegid.

Ces données sont ensuite corrélées et présentées sous forme de tableaux de bords et indicateurs.

16.3.3. Anti DDoS

Toutes les plateformes et infrastructures bénéficient d'une protection anti DDoS adaptée aux différentes technologies opérées.

16.3.4. Haute disponibilité et tolérance de panne

La disponibilité des services de Cegid est assurée grâce à la redondance des systèmes permettant de pallier tout dysfonctionnement, défaillance de composant ou indisponibilité temporaire. Parmi les technologies utilisées, on retrouve :

- Virtualisation des serveurs,
- Redondance du stockage des données,
- Équilibrage de charge en cluster sur les équipements réseaux et Telecom,
- Gestion de capacité avec extension à chaud (VM et Pare-Feu),
- Équilibrage de charge applicative sur les fermes de serveurs.

17. ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION

La sécurité dans les développements est un enjeu majeur chez Cegid.

Cegid a mis en place une démarche visant à intégrer la sécurité tout au long du cycle de vie des applications développées. Cette démarche s'inspire des bonnes pratiques et recommandations des frameworks OWASP SAMM, OWASP ASVS et BSIMM.

17.1. Cycle de vie de développement sécurisé

Un volet gouvernance regroupe les activités liées à l'organisation du cycle de vie de développement sécurisé incluant la définition de politiques, d'objectifs de mesure, ainsi qu'un programme de formation et sensibilisation associé.

Un volet conception englobe les activités liées à la collecte des exigences de sécurité, aux spécifications d'architecture de haut niveau et à la conception détaillée.

Un volet implémentation couvre les activités et processus de construction et déploiement des composants logiciels (voir chapitre 15.2), ainsi que ceux liés à la gestion des défauts.

Un volet vérification comprend les activités liées aux tests de bon fonctionnement, de non-régression et de sécurité, permettant de s'assurer de la qualité des logiciels développés.

La démarche, dans son ensemble, vise à améliorer la qualité et la sécurité des produits livrés, avec, entre autres :

- Une communauté de développeurs référents dans le domaine de la sécurité au sein de chaque équipe de développement.
- Des outils dédiés à la revue de sécurité du code
- Un référentiel commun (OWASP) qui permet de capitaliser sur les sujets de la sécurité et d'assurer la diffusion et la mise en œuvre des bonnes pratiques.
- Une veille sécurité spécifique, incluant des bulletins d'information, des mises à jour, et des améliorations envoyés aux équipes.

17.2. Cloisonnement des environnements

Les réseaux et infrastructures de Cegid sont séparés physiquement et logiquement selon les services.

La plateforme applique en outre une séparation des différents environnements applicatifs (développement, test, préproduction et production). L'environnement de développement est exclusivement réservé et accessible aux développeurs et ne comprend aucune donnée de production sauf accord particulier contractualisé avec le client.

Les équipements sont accessibles via bastion d'administration ou machine virtuelle de rebond pour les équipes bénéficiant des privilèges nécessaires.

17.3. Acquisition

Lors de l'acquisition de nouveaux systèmes, les besoins de sécurité sont pris en compte dans le processus de sélection pour garantir la protection des données et la conformité aux normes de sécurité.

18. RELATION AVEC LES FOURNISSEURS

Afin d'élaborer une politique cohérente avec ses activités, Cegid établit une classification de ses fournisseurs en fonction de la criticité vis-à-vis de la fourniture des services clients. En fonction de leur criticité différents contrôles sont mis en place, par exemple :

- Analyse leurs certifications en sécurité,
- Mise en place de comités de suivi avec indicateurs d'efficacité et de conformité en sécurité,
- Audits techniques ou organisationnels,
- Mise en place et suivi de SLA en sécurité,
- Mise en place de clauses de sécurité spécifiques dans les contrats,
- Clarification des rôles et responsabilités dans la gestion des incidents de sécurité.

Dans le cadre de la délivrance de ses services, Cegid s'appuie sur des infrastructures mises à disposition par ses sous-traitants. Le déploiement et la maintenance de ces infrastructures sont à leur charge.

19. GESTION DES VULNERABILITES ET DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

19.1. Gestion des vulnérabilités

Les vulnérabilités sont échelonnées suivant le CVSS V3.1 et traitées par défaut suivant le tableau suivant :

Type de vulnérabilité	Score CVSS	Engagement de plan d'action
Low	0,1 – 3,9	Selon analyse
Medium	4,0 – 6,9	Selon analyse
High	7,0 – 8,9	7 jours à partir de la détection
Critical	9,0 - 10	7 jours à partir de la détection

Certains produits ou services peuvent avoir des engagements supérieurs mentionnés dans les livrets de service.

19.2. Scanner de vulnérabilités

Des scans sur l'ensemble du périmètre Internet du SI de Cegid sont lancés régulièrement, et au minimum mensuellement, via un scanner de vulnérabilités managé par l'équipe sécurité de Cegid.

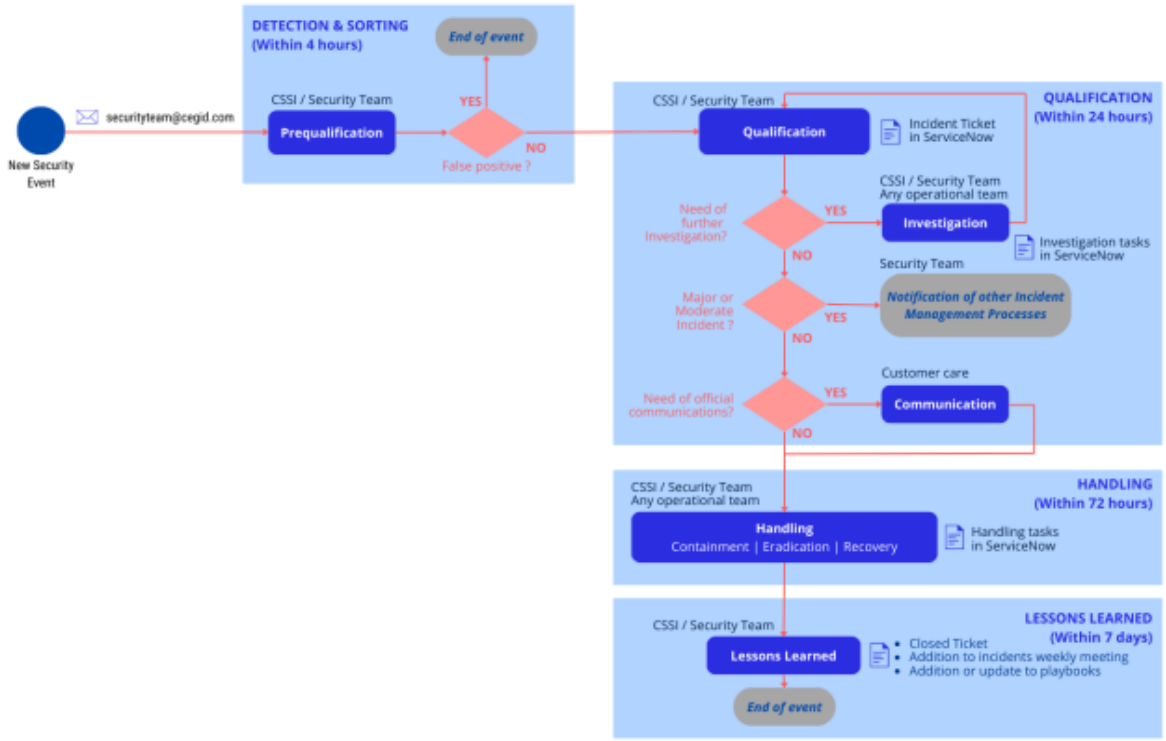
Ces scans permettent de contrôler la bonne configuration des matériels et des logiciels dans le but de détecter l'apparition de vulnérabilité.

Les résultats sont revus et font l'objet de plans d'actions spécifiques.

19.3. Gestion des incidents de sécurité

Le traitement des incidents de sécurité est opéré par un workflow dans les outils ITSM de Cegid. Le principe est inspiré des bonnes pratiques présentes dans les normes ISO 27001 et ISO 27002.

Il est établi comme suit :



Une communication est effectuée au maximum dans les 72 heures auprès des clients et/ou partenaires concernés une fois que le périmètre impacté est évalué.

En fonction de la nature du plan d'action, Cegid peut également communiquer avec les entités concernées de Cegid pour organiser le traitement de l'incident.

19.4. Gestion de crise

Des plans de gestion de crise spécifiques sont formalisés, incluant des scénarios de crise encadrés par une organisation et des processus définis. Les annuaires de gestion de crise sont maintenus à jour, permettant d'améliorer la coordination des actions nécessaires en cas de crise. Ces mesures permettent également d'apporter une réponse structurée face aux situations de crise chez Cegid.

20. GESTION DE LA CONTINUITE D'ACTIVITE

20.1. Continuité du pilotage

Un plan de continuité est défini pour le management et le pilotage des services (infrastructure, applications, etc.) des équipes de Cegid.

La continuité de ces activités repose à la fois sur la mise en place d'architectures résilientes des systèmes de pilotage que sur la sécurité des ordinateurs portables. Cela permet à tout collaborateur ou administrateur des équipes Cegid d'accéder, de manière sécurisée à distance, et en adéquation avec les droits qui lui sont octroyés, aux ressources et aux outils permettant d'assurer le service.

20.2. PCA & Résilience

La continuité d'activité est intégrée dès la phase de conception des services délivrés par Cegid.

Le plan de continuité d'activité (PCA) est défini de façon globale, incluant des aspects humains, organisationnels et techniques. Il est décliné et adapté au niveau de chaque offre métier, en tenant compte des contraintes métiers et des architectures techniques.

Les ressources critiques (ressources humaines, infrastructures, Système d'information, ressources immatérielles) sont identifiées pour chaque offre métier.

Le PCA est conçu pour répondre aux besoins de continuité en matière de disponibilité des services.

En plus de la conception de la résilience des architectures techniques et logicielles, les processus opérationnels et organisationnels du PCA sont définis et testés dans une démarche d'amélioration continue.

20.3. RPO & RTO

20.3.1. RPO

RPO : Recovery Point Objective ou Point de Rétablissement des données

Le RPO est indiqué dans les livrets de service. Par défaut, il est de 24 heures.

20.3.2. RTO

RTO : Recovery Time Objective ou Temps de Rétablissement du service

En standard, Cegid ne définit pas de RTO dans les Livrets Services. Cependant, pour certaines offres particulières, un RTO est garanti (voir contrat ou livret de service).

En cas de sinistre grave entrainant une interruption prolongée du service, Cegid s'engage à restaurer le service dans les meilleurs délais, en utilisant la sauvegarde la plus appropriée.

21. CONFORMITE

21.1. Normes et réglementations

21.1.1. ISO 27001

Les équipes de Cegid se réfèrent à la norme ISO 27001 pour concevoir et exploiter les services SaaS fournis aux clients. Les certifications et périmètres couverts sont détaillés au chapitre 5

Afin de proposer une architecture et une infrastructure conformes aux standards en matière de sécurité, Cegid s'appuie sur des datacenters et des services associés certifiés ISO 27001.

21.1.2. RGPD et protection des données à caractère personnel

Cegid a mis en place une Politique de confidentialité et cookies disponible sur son site internet : https://www.cegid.com/fr/politique-de-confidentialite/

21.1.3. Sécurité concernant l'Intelligence Artificielle

L'intelligence artificielle est intégrée de manière native dans plusieurs applications de Cegid, conformément à la stratégie de l'entreprise pour les prochaines années. Chez Cegid, nous accordons la priorité à la sécurité et à l'intégrité lors de nos projets d'implémentation d'IA, en veillant à ce qu'elles respectent les normes les plus strictes en matière de sécurité et de conformité.

En alignement avec l'Acte sur l'Intelligence Artificielle de l'Union Européenne (EU AI Act, https://artificialintelligenceact.eu/the-act/) publié le 12 juillet 2024, nous avons adopté un cadre permettant d'intégrer les technologies de l'IA de manière responsable et sécurisée dans nos applications.

Notre engagement est renforcé par notre participation active au Pacte IA (https://digital-strategy.ec.europa.eu/en/policies/ai-pact#ecl-inpage-Signatories-of-the-AI-Pact), par lequel nous nous engageons à respecter les meilleures pratiques et les lignes directrices éthiques dans le déploiement de l'IA. Cela inclut la réalisation d'évaluations de risque approfondies, la mise en œuvre de mesures de protection des données, et la surveillance continue des systèmes d'IA afin de protéger contre les vulnérabilités.

21.1.4. Audit

21.1.4.1. Audit interne

Le contrôle des activités de sécurité dans les périmètres de certification de Cegid est assuré par des consultants qualifiés sous la supervision du service sécurité.

Ceux-ci réalisent à intervalle planifié une revue des éléments en lien avec les périmètres certifiés conformément au plan d'audit de Cegid.

Les documents concernant les audits internes sont confidentiels et ne sont pas communicables. Cegid s'engage, en cas de non-conformité entrainant atteinte à la sécurité, à communiquer avec le(s) client(s) concerné(s) dans le périmètre impacté (cf. § Gestion des incidents de sécurité).

21.1.4.2. Audit externe

Dans le cadre des certifications listées aux Chapitre 5, Cegid est auditée annuellement par les organismes certificateurs sur les périmètres de chacune de ces certifications.

21.1.4.3. Audit technique

Cegid fait réaliser également des audits techniques réguliers sur son SI avec des experts qualifiés.

Une planification régulière de ces audits techniques est effective et permet de tester chaque application stratégique sur un cycle de trois ans

21.1.4.4. Audit client

Les clients souscripteurs peuvent effectuer des pentests sur les services qu'ils utilisent dans les conditions précisées au contrat.

Des audits organisationnels peuvent également être réalisés à l'initiative des clients. Ils sont soumis à certaines conditions d'éligibilité et nécessitent la signature de clauses contractuelles particulières.