RÉPUBLIQUE FRANÇAISE
Liberté – Égalité – Fraternité

Département du Val-de-Marne
Canton d'Orly
Commune d'Orly

Ville d'Orly

N°A- IVP-2024/ 178

ARRÊTÉ DE LA MAIRE

Registre des arrêtés du Maire

Objet : APPROBATION DE L'ANALYSE D'IMPACT A LA PROTECTION DES DONNEES RELATIVES À LA SANTE A LA VILLE D'ORLY

LA MAIRE D'ORLY,

VU le Code général des collectivités territoriales ;

VU le Règlement 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 ;

VU la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

VU le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

VU l'analyse d'impact relative à la protection des données (AIPD) annexée au présent arrêté ;

CONSIDERANT que les traitements de données à caractère personnel susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées implique la réalisation d'analyses d'impact,

CONSIDERANT que la ville d'Orly dispose d'un traitement de données à caractère personnel dont l'objet est la Santé, pour lequel une analyse d'impact à la protection des données a été réalisée ;

CONSIDERANT que le responsable du traitement est la Ville d'Orly dont le représentant est Madame la Maire ;

ARRÊTE:

ARTICLE 1: DIT que la ville d'Orly dispose d'un traitement automatisé de données à caractère personnel dont l'objet est la Santé nécessitant la réalisation d'une analyse d'impact.

ARTICLE 2: APPROUVE l'analyse d'impact à la protection des données relative à la Santé. Le service en charge de la mise en œuvre du traitement ainsi que du plan d'actions et des mesures correctives prévus dans l'analyse d'impact susvisée est le service Santé de la Ville d'Orly.

ARTICLE 3 : DIT que les finalités du traitement cité à l'article 1 sont d'assurer la gestion des consultations médicales des patients, de la prise de rendez-vous jusqu'à la facturation de la consultation, finalités de traitement

qui sont en cohérence avec la législation en vigueur. Le détail des finalités de traitement est contenu dans l'analyse d'impact relative à la protection des données (AIPD) en annexe au présent arrêté.

ARTICLE 4 : PRECISE que l'analyse d'impact à la protection des données relatives à la Santé, telle qu'annexée au présent arrêté, énumère le type de données à caractère personnel et information enregistrées.

ARTICLE 5 : PRECISE que dans le cadre de ces traitements, les données sont accessibles au service Santé de la Ville d'Orly. L'analyse d'impact à la protection des données relatives à la Santé, telle qu'annexée au présent arrêté, précise les personnels compétents ayant accès aux données à caractère personnel utilisées par le présent traitement automatisé de données.

ARTICLE 6 : PRECISE que les personnes concernées sont informées à propos du traitement par le biais des panneaux d'affichage indiquant le numéro de téléphone à contacter pour l'exercice de leurs droits, notamment le droit d'accès.
Les droits d'accès, rectification et de suppression s'exercent auprès du délégué à la protection des données, à l'adresse suivante :

- rgpd@mairie-orly.fr.

ARTICLE 7 : DIT qu'ampliation du présent arrêté sera adressée à Madame la Préfète du Val-de-Marne.

ARTICLE 8 : DIT que la Directrice générale des services de la mairie d'Orly est chargée de l'exécution du présent arrêté.

ARTICLE 9 : DIT que le présent arrêté peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal administratif de Melun dans un délai de 2 mois à compter de sa publication.

Fait à Orly, le 13 JUIN 2024

Imène SOUID

Maire,
Conseillère départementale du Val de Marne

Accusé de réception en préfecture
094-219400546-20240603-AIVP2024178-AR
Date de télétransmission : 03/06/2024
Date de réception préfecture : 03/06/2024

PIA

Analyse d'impact sur la protection des données
Privacy impact assessment

Santé

AESATIS

Ville d'Orly

Présentation

Description de l'analyse

Aperçu de l'analyse

INFORMATIONS GÉNÉRALES

Statut : Validation simple

Saisie : Damien AULANIER
Évaluation : Célia CAMPANA
Validation : Bernadette LEROY

L'analyse est basée sur :

- Une analyse documentaire ;
- Un ensemble d'entretiens, avec :
  - Le service concerné ;
  - Le service informatique de la région BFC ;
  - Le sous-traitant principal ;
- Un ensemble d'échanges par voie électronique avec les différentes parties prenantes.

LISTE DES ANNEXES À L'ANALYSE

- Référentiel des durées de conservation dans le domaine de la santé hors recherche ;
- Référentiel relatif aux traitements de données personnelles pour les cabinets médicaux et paramédicaux ;
- Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire ;
- Plan d'actions.

Présentation

Sommaire de l'analyse

Contexte

Vue d'ensemble

Quel est le traitement qui fait l'objet de l'étude ?

L'étude porte sur un groupement de traitements mis en œuvre par le service Santé de la ville d'Orly.

La CNIL rend obligatoire la création d'une analyse d'impact pour tous les traitements ayant pour finalité l'accompagnement médical des personnes. Entre autres, ces traitements induisent le traitement de données sensibles.

Ainsi, pour la ville d'Orly, le service Santé réalise les traitements suivants, qui entrent potentiellement dans l'analyse :

- Gestion de l'accueil ;
- Gestion des patients ;
- Gestion de la facturation.

Quelles sont les responsabilités liées au traitement ?

Le responsable de traitement faisant l'objet de cette étude est la ville d'Orly, représentée par Madame le Maire.

Le service en charge de la mise en œuvre de ces traitements est le service Santé.

Dans la mise en œuvre de ces traitements, les sous-traitants intervenant sont :

- **SICIO** : **S**yndicat **I**nter **C**ommunal pour l'**I**nformatique et ses **O**utils, qui est le prestataire principal de ville, qui gère et fourni une grande majorité des applications métiers ;
- **Idem Santé :** est le prestataire fournisseur du logiciel Galaxie permettant la gestion de la comptabilité ;
- **Cégédim :** le sous-traitant fournisseur du logiciel Crossway permettant le paramétrage des consultations et la gestion des dossiers patients ;
- **Doctolib :** la plateforme de gestion des rendez-vous médicaux en ligne.

Quels sont les référentiels applicables ?

Les référentiels applicables sont :

- Référentiel des durées de conservation dans le domaine de la santé hors recherche ;
- Référentiel relatif aux traitements de données personnelles pour les cabinets médicaux et paramédicaux ;
- Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire.

Ces référentiels sont annexés à l'analyse.

Évaluation : **Acceptable**

Quelles sont les données traitées ?

On retrouve plusieurs catégories de données pour la mise en œuvre de ces traitements, dont des données :

- **D'identification :**
  - Civilité ;
  - Nom ;
  - Prénom ;
  - Adresse postale personnelle ;
  - Numéro de téléphone personnel ;
  - Adresse électronique personnelle ;
  - Date de naissance ;
  - Lieu de naissance ;
  - Numéro d'Inscription au Répertoire (NIR) ;
  - Numéro de dossier et Identifiant ;

- **Sur la vie personnelle :**
  - Situation personnelle ;
  - Nombres d'enfants ;
  - Habitudes de vie ;
  - Violences intra familiales ;
  - Addictions ;

- **Sur la vie professionnelle :**
  - Poste occupé ;
  - Formations suivies ;
  - Situation professionnelle ;

- **Économiques et Financières :**
  - Situation financière ;
  - Relevé d'Identité Bancaire;

- **Sensibles :**
  - Données de santé ;
  - Origine raciale ;
  - Données génétiques ;
  - Origine ethnique ;
  - Données biométriques.

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

Les données des personnes concernées peuvent être collectées par divers canaux en fonction de la finalité poursuivie initialement. Les données peuvent être collectées au format papier, par le biais de formulaires, en face à face ou au téléphone. Mais elles peuvent également être collectées au format numérique, par mail ou par formulaires en ligne. Toutefois, la grande majorité des données est traitée au format numérique.

Les données sont ensuite traitées en fonction des finalités, par le traitement de base de données ou l'utilisation des différentes applications métiers.

La nature des traitements mis en œuvre par le service fait que les données sont continuellement transférées vers des destinataires internes mais également vers des destinataires externes.

Comme destinataire interne, on retrouve la direction de la ville, les différents services du centre médical, le service financier, le service informatique, le centre communal d'action sociale (CCAS), les auxiliaires médicaux.

En qualité de destinataires externes, on retrouve le trésor public, la sécurité sociale, le CCAS, les caisses mutuelles, les professionnels de santé extérieurs (hôpitaux / cliniques / libéraux, etc.) et les laboratoires extérieurs.

En ce qui concerne la conservation des données, on retrouve des données stockées dans des dossiers papiers dans le bureau du service, dans la salle des archives, sur le poste de travail (sur l'ordinateur), sur la messagerie, sur un serveur de partage interne, sur les applications métiers et sur les plateformes mises à disposition par les partenaires.

Quels sont les supports des données ?

Les données sont stockées aussi bien au format numérique qu'au format papier.

Évaluation : Acceptable

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

Les finalités des traitements sont **déterminées, explicites** et **légitimes.** Les traitements sont mis en œuvre pour assurer la gestion des consultations médicales des patients, de la prise du rendez-vous jusqu'a la facturation de la consultation.

Évaluation : Acceptable

Quel(s) est (sont) le(s) fondement(s) qui rend(ent) votre traitement licite ?

Les fondements qui rendent les traitements licites sont :

- La sauvegarde d'intérêts vitaux ;
- L'intérêt légitime.

Évaluation : Acceptable

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

Les données collectées dans le cadre de ces traitements sont toutes minimisées au regard des finalités. Les données collectées et traitées permettent la prise de rendez-vous et la réalisation de la consultation médicale mais également la facturation et le remboursement de la consultation.

Évaluation : Acceptable

Les données sont-elles exactes et tenues à jour ?

Les données sont exactes au moment de la collecte et il est possible de les mettre à jour.

Évaluation : **Acceptable**

Quelle est la durée de conservation des données ?

Les durées de conservations ne sont à ce jour pas réellement définies pour l'ensemble des traitements.

Évaluation : **Améliorable**

Plan d'action / mesures correctives :

- Définir des durées de conservation, pour les différentes données récoltées en fonction des finalités poursuivies par les traitements et prendre en compte la réglementation sur les durées de conservation des données de santé ;
- Mettre en place un processus de purge des données dans les applications métiers ;
- S'assurer du respect de ces durées par les prestataires et partenaires ;
- Limiter le doublonnage des données, que ce soit dans le service avec des versions numériques et des versions papiers, mais également avec les autres services lors des transferts de données par mail.

Commentaire d'évaluation :

La définition des durées de conservation est un des fondements du RGPD. Ainsi, pour être conforme à ce dernier, il est nécessaire de définir des durées de conservation, de créer des procédures d'archivage et des procédures de destruction des données afin de maximiser la protection des données des personnes concernées.

Comment les personnes concernées sont-elles informées à propos du traitement ?

Lors de l'analyse des traitements, les récoltes de données ne donnaient pas lieu à une information exhaustive. Les patients ne sont pas donc réellement informés sur la récolte de leurs données et l'utilisation qui en est faite.

Évaluation : Améliorable

Plan d'action / mesures correctives : Informer les personnes concernées sur les données qui sont collectées et le traitement qui en est fait.

- Mettre à jour les formulaires (papier et numérique) de collecte, avec les mentions d'information ;
- Mettre en place des procédures d'information dans les mails ;
- Réaliser des affichages dans les salles où le public est accueilli.

Pour rappel l'information des personnes doit comprendre, a minima :

- Identité et coordonnées de l'organisme responsable de traitement :
- Finalités ;
- Bases légales ;
- Caractère obligatoire ou facultatif du recueil des données ;
- Destinataires ou catégories de destinataires des données ;
- Durée de conservation des données ;
- Droits des personnes concernées ;
- Coordonnées du délégué à la protection des données ;
- Droit d'introduire une réclamation auprès de la CNIL.

Commentaire d'évaluation : L'information des personnes est un des fondements du RGPD. La transparence permet aux personnes concernées :

- de connaître la raison de la collecte des différentes données les concernant ;
- de comprendre le traitement qui sera fait de leurs données ;
- d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits.

Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Dans le cadre de ces traitements, le consentement n'est pas récolté.

Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs :

- **Droit d'accès et droit à la portabilité ?**
- **Droit de rectification et droit à l'effacement ?**
- **Droit de limitation et droit d'opposition ?**

Les personnes concernées ne recevaient pas l'information sur la mise en œuvre de leurs droits au moment de l'analyse.

Évaluation : Améliorable

Plan d'action / mesures correctives : afin de se conformer au RGPD, le service devra :

- Informer les personnes concernées sur leurs droits ;
- Mettre en œuvre des procédures de gestion des droits ;
- Informer l'entièreté du service sur l'existence de ces droits et sur la procédure à respecter pour accéder aux éventuelles demande de droits reçues.

Commentaire d'évaluation : créer des procédures en amont des demandes de droits permet d'assurer une réponse correcte aux attentes de la CNIL. Il est important de rappeler que de plus en plus de personnes sont sensibilisées à la protection des données, ainsi le nombre de demandes pourrait considérablement s'accroître.

Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Une contractualisation et un travail d'amélioration des prestations existe entre la ville et le SICIO. Cependant, des éléments restaient à éclaircir quant aux contrats entre le SICIO et les différents fournisseurs de logiciels.

Évaluation : Améliorable

Plan d'action / mesures correctives : s'assurer que tous les contrats avec les prestataires comportent des clauses RGPD, afin d'assurer une sécurisation de qualité aux personnes ayant fournies leurs données. Intégrer ce niveau de sécurité et ces clauses dans les marchés.

En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Les données n'ont pas vocation à être transférées hors de l'Union européenne.

Évaluation : Acceptable

Authentification des utilisateurs

Les utilisateurs sont authentifiés, dans l'annuaire Active Directory. Ils disposent tous d'un identifiant et d'un mot de passe.

Évaluation : Acceptable

Sauvegarde de données

Des sauvegardes régulières de données sont effectuées et gérées par le SICIO. Toutefois, la mise en place d'une politique de sauvegarde de données est imposée, permettant ainsi une description globale du processus de sauvegarde des données. De plus, cette politique permettra de renforcer la sécurité des données sauvegardées et de constater les éventuels manquements.

Évaluation : Améliorable

Plan d'action / mesures correctives : Il est nécessaire de mettre en place une politique de sauvegarde des données. Les mesures de sécurité à mettre en place doivent assurer la disponibilité et la confidentialité des données sauvegardées. Pour cela, nous vous recommandons a minima de :

- Chiffrer les sauvegardes en prévoyant un stockage dans un lieu sécurisé ;
- Effectuer les sauvegardes sur un disque dur externe sur un site extérieur ;
- Chiffrer le canal de transmission, lorsque les sauvegardes sont transmises via un réseaux externe à l'entreprise ;
- Organiser des tests de restauration ;
- S'assurer que les agents et sous-traitants de la ville savent qui alerter en cas d'incident.

Commentaire d'évaluation : S'assurer que le contrat avec le SICIO inclut des garanties de sécurité des sauvegardes de données effectuées.

Sensibilisation des utilisateurs

Chaque service de la ville a désigné un référent opérationnel RGPD qui a été a minima sensibilisé au RGPD et aux bonnes pratiques. De plus, le DSI de la ville fait partie du COPIL de la mise en conformité au RGPD.

.

Évaluation : Acceptable

Sécurisation des sites Web

Le protocole TLS version 1.2 est utilisé pour le chiffrement des connexions et les ports de communication sont limités au strict nécessaire pour le bon fonctionnement des applications installées. De plus, l'accès aux outils d'interface est limité seulement aux personnes habilitées.

Évaluation : Améliorable

Plan d'action / mesures correctives : Le protocole TLS version 1.2 est utilisé pour le chiffrement des connexions. Toutefois, il serait nécessaire d'utiliser la version TLS 1.3 qui est la plus récente. Nous vous conseillons également la mise en place d'outils de détection des vulnérabilités et la réalisation des tests d'intrusion.

Commentaire d'évaluation : S'assurer que des garanties en termes de sécurités des données sont formalisées avec l'hébergeur sur site et, le cas échéant, les inclure dans le contrat.

Protection des locaux

Mise en place d'un système de Gestion Technique des Bâtiments (GTB) permettant de contrôler et surveiller les différents équipements électriques et mécaniques et les matériels informatiques sont également protégés.

Un contrôle d'accès est mis en place permettant la distinction des zones à risque. Les bureaux sont systématiquement fermés lors de l'absence du personnel. De plus, pour accéder au pôle, il est nécessaire de disposer d'un badge, les visiteurs ne peuvent donc pas y accéder directement. Aussi, l'imprimante partagée est positionnée dans une salle non accessible au public.

Évaluation : Améliorable
Commentaire d'évaluation : D'autres mesures pourraient renforcer cette sécurité, sans que cela n'engendre de dépenses importantes pour la ville :
- Créer un registre des visiteurs ;
- Accompagner les visiteurs lors de leur présence dans les locaux.

Mot de passe

Chaque agent dispose d'un mot de passe personnel. Toutefois, il n'existe pas de règles concernant leur robustesse.

Évaluation : Améliorable

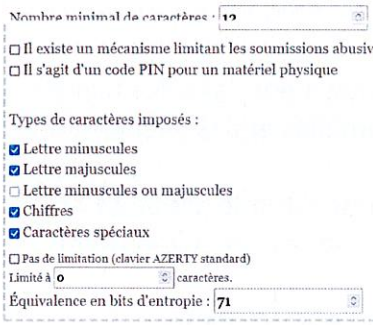
Plan d'action / mesures correctives :

Il serait nécessaire de mettre en œuvre une politique de mot de passe en suivant les nouvelles recommandations de la CNIL. Pour cela :

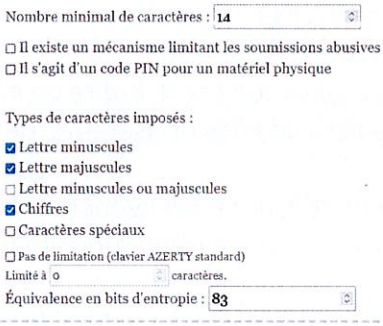
- Définir des règles permettant aux utilisateurs d'avoir des mots de passe sécurisés, exemple un mot de passe de 12 caractères avec des caractères spéciaux, ou un mot de passe comprenant a minima 16 caractères ;
- Interdire certains mots de passe ;
- Pratiquer un renouvellement régulier des mots passe pour les comptes de type administrateur ;
- Formaliser une politique de mot de passe.

Ci-après des exemples de **niveau d'entropie en fonction des règles définies** :

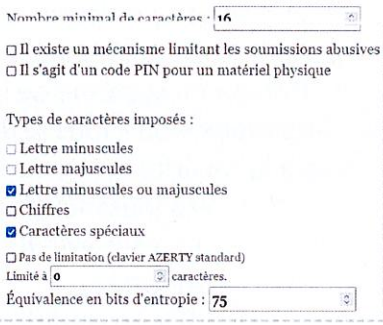
Exemple 1 : minimum de 12 caractères comprenant majuscules, minuscules, chiffres et caractères spéciaux.



Exemple 2 : minimum 14 caractères comprenant majuscules, minuscules et chiffres, **sans** caractère spécial obligatoire.



Exemple 3 : une phrase de passe doit être utilisée et elle doit être composée d'au minimum 7 mots.



Sécurisation des documents papiers

Les documents papiers sont conservés dans des bureaux et salles des archives. Les armoires contenant des documents sont fermées à clés et les bureaux sont systématiquement fermés lors de l'absence du personnel.

Les documents papiers ne sont pas détruits directement. Ils sont déposés dans un conteneur de recyclage fermé à clés. Les agents déposent par la trappe et ne peuvent plus y accéder. Le prestaire détruit directement les éléments sans consultation possible.

Pour l'impression des documents, l'imprimante est partagée dans le pôle mais nécessite un badge afin de l'utiliser.

Évaluation : Acceptable

Gestion des accès

Une gestion des accès est prévue afin que seulement les personnes du service concerné puissent accéder aux données. Toutefois, nous n'avons pas eu accès à une politique formalisée des contrôles des accès.

Évaluation : Améliorable

Plan d'action / mesures correctives : Il serait judicieux de mettre en place un système permettant la traçabilité des accès. Pour cela :

- Prévoir un système de journalisation (c'est-à-dire un enregistrement dans des fichiers « journaux » ou « logs ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité :
    - ces journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important) ;
    - La journalisation doit concerner, a minima, les accès des utilisateurs ;
- Informer les utilisateurs sur la mise en place d'un tel système ;
- Protéger les équipements de journalisation et les informations journalisées.

Commentaire d'évaluation : Formaliser une procédure de gestion des accès par écrit.

Gérer les risques

Tous les traitements faisant l'objet de cette analyse sont recensés dans le registre des traitements.

Un audit de conformité RGPD a été réalisé. Il a permis de déterminer les mesures existantes et a donné lieu à un plan d'actions.

Évaluation : Acceptable

Gestion des postes de travail

Les postes de travail sont sécurisés par des mots de passe. De plus, des antivirus régulièrement mis à jour sont utilisés et font l'objet d'une politique de mise à jour.

Également, les données des utilisateurs sont stockées sur un espace de stockage régulièrement sauvegardé accessible via le réseaux de l'organisme.

Les applications téléchargées ne provenant pas de sources sûres ne sont pas exécutées et l'usage d'applications nécessitant des droits de niveau administrateurs est limité.

Évaluation : Améliorable

Plan d'action / mesures correctives : Il serait judicieux de prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.
Configurer les logiciels pour que leurs mises à jour se fassent automatiquement.

Commentaire d'évaluation : Les risques d'intrusion dans les systèmes informatiques sont importants et les postes de travail constituent un des principaux points d'entrée.

Organisation de la politique de la vie privée

La ville a désigné la société AESATIS comme DPO externalisé, chargée de la mise en conformité au RGPD. De plus, des référents RGPD par service ont été désignés et sont impliqués dans le projet.
La ville dispose d'un corpus documentaire qui est continuellement alimenté. Cette analyse en fera d'ailleurs partie.

Évaluation : Acceptable

Sécurisation du réseau interne

Les accès internet sont limités ; les services non nécessaires sont bloqués.
De plus, les réseaux ouverts aux invités sont séparés du réseau interne et les flux entrants et sortants sur les équipements sont filtrés. Pour l'accès a distance, un VPN est imposé.

Évaluation : Améliorable
Plan d'action / mesures correctives :
Réaliser des tests d'intrusions (recommandé tous les 3 ans) afin de détecter les vulnérabilités et failles de sécurité.
La télémaintenance doit s'effectuer via un VPN.
S'assurer qu'aucune interface réseau n'es accessible depuis internet.

Sécurisation des serveurs

L'accès aux outils interface d'administration est limité aux seules personnes habilitées.
Les habilitations ne sont pas revues régulièrement.

Évaluation : Améliorable
Plan d'action / mesures correctives : Renforcer la sécurité des serveurs :

- Mettre en place une politique spécifique de mots de passe pour les administrateurs ;
- Changement à chaque départ d'administrateur ;
- S'assurer de la sécurité physique des serveurs.

Commentaire d'évaluation : La sécurité des serveurs doit être une priorité car ils centralisent un grand nombre de données. Pour cela, il est nécessaire de renforcer leur sécurité. Cela passe autant par une protection informatique que par une protection physique.

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Sentiment d'atteinte à la vie privée, chantage, harcèlement, refus d'accès à certaines prestations, risques corporels, risques psychologiques, dommages psychologiques, cyberharcèlement, dépression, perte de temps pour réitérer des démarches, diffamation donnant lieu à des représailles.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Acte interne de malveillance, acte externe de malveillance, fuite de données, vol de données, piratage informatique, consultation humaine, interception du flux sur le réseau, accès non autorisé, erreur humaine, vol de matériel, accès non autorisé aux locaux.

Quelles sources de risques pourraient-elles en être à l'origine ?

Attaquant ciblant la structure, attaquant ciblant un utilisateur, employé malintentionné, employé négligeant, personnel de maintenance, tiers malintentionné, entourage d'un utilisateur, tiers négligeant.

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Authentification des utilisateurs, sauvegardes de données, sensibilisation des utilisateurs, sécurisation des sites web, protection des locaux, mot de passe, sécurisation des documents papiers, gérer les risques, gestion des postes de travail, organisation de la politique de la vie privée, sécurisation des serveurs, sécurisation du réseau informatique.

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Dans le cadre de ces traitements, la gravité du risque d'accès illégitime aux données est évaluée comme maximale.

En effet, une grande quantité de données est traitée. De plus, une grande partie de ces données est recensée comme données sensibles et un accès illégitime pourrait avoir des conséquences redoutables sur la vie privée des personnes concernées.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

La vraisemblance du risque est évaluée comme importante. Le nombre d'intervenants dans l'ensemble de ces traitements rend la vraisemblance à ce niveau. En effet, les échanges en interne et en externe des données dans le cadre de ces traitements sont importants. De plus, l'échange et le stockage de données dans la messagerie ne tendent pas à diminuer cette vraisemblance.

Toutefois, les référents RGPD de chaque service ont été sensibilisés au RGPD et aux bonnes pratiques. De plus, le DSI de la ville fait partie du COPIL de la mise en conformité au RGPD.

Des mesures de protection des échanges sont mises en place (utilisation de protocole garantissant l'authentification et la sécurité du serveur) et une gestion des accès avec habilitations est également mise en place.

Concernant les accès aux locaux, les agents disposent d'un badge permettant la sécurisation des accès physiques. Également, des mesures de sécurité des accès et échanges sont prévues dans le plan d'action, ce qui va tendre à diminuer la probabilité de survenance du risque.

Risques

Accès illégitime à des données

Évaluation : Améliorable

Plan d'action / mesures correctives :

Il est nécessaire de mettre en place des actions sur 2 fronts :

- Se conformer au RGPD en respectant ses grands principes ;
- Proposer un niveau de sécurité important aux données que vous traitez, par la mise en œuvre des actions présentées pour les mesures de sécurité.

Commentaire d'évaluation :

Les données concernées par ce traitement sont très nombreuses et sont sensibles selon leur nature.
Le nombre d'intervenants et de personnes pouvant consulter les informations est également très important.

Prenant en compte le plan d'actions, comment ré-évaluez-vous la gravité de ce risque (Accès illégitime à des données) ? **Importante**
Prenant en compte le plan d'actions, comment ré-évaluez-vous la vraisemblance de ce risque (Accès illégitime à des données) ? **Limitée**

Risques

Modification non désirées de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Sentiment d'atteinte à la vie privée, chantage, harcèlement, refus d'accès à certaines prestations, risques corporels, risques psychologiques, dommages psychologiques, cyberharcèlement, dépression, perte de temps pour réitérer des démarches, diffamation donnant lieu à des représailles.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Acte interne de malveillance, acte externe de malveillance, fuite de données, vol de données, piratage informatique, consultation humaine, interception du flux sur le réseau, accès non autorisé, erreur humaine, vol de matériel, accès non autorisé aux locaux.

Quelles sources de risques pourraient-elles en être à l'origine ?

Attaquant ciblant la structure, attaquant ciblant un utilisateur, employé malintentionné, employé négligeant, personnel de maintenance, tiers malintentionné, entourage d'un utilisateur, tiers négligeant.

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Authentification des utilisateurs, sauvegardes de données, sensibilisation des utilisateurs, sécurisation des sites web, protection des locaux, mot de passe, sécurisation des documents papiers, gérer les risques, gestion des postes de travail, organisation de la politique de la vie privée, sécurisation des serveurs, sécurisation du réseau informatique.

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Dans le cadre de ces traitements, la gravité du risque en cas de modification non désirée des données est évaluée comme maximale.

En effet, une grande quantité de données est traitée. De plus, la plus grande partie de ces données est recensée comme données sensibles et une modification non désirée peut avoir des conséquences redoutables sur la vie privée des personnes concernées.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

La vraisemblance du risque est évaluée comme importante. Le nombre d'intervenants dans l'ensemble de ces traitements rend la vraisemblance à ce niveau. En effet, les échanges en interne et en externe de données dans le cadre de ces traitements sont importants. De plus, l'échange et le stockage de données dans la messagerie et leur dédoublonnage ne tendent pas à diminuer cette vraisemblance.

Toutefois, les référents RGPD de chaque service ont été sensibilisés au RGPD et aux bonnes pratiques. De plus, le DSI de la ville fait partie du COPIL de la mise en conformité au RGPD.

Des mesures de protection des échanges sont mises en place (utilisation de protocole garantissant l'authentification et la sécurité du serveur) et une gestion des accès avec habilitations est également mise en place.

Concernant les accès aux locaux, les agents disposent d'un badge permettant la sécurisation des accès physiques. Également, des mesures de sécurité des accès et échanges sont prévues dans le plan d'action, ce qui va tendre à diminuer la probabilité de survenance du risque.

Risques

Modification non désirées de données

Évaluation : Améliorable

Plan d'action / mesures correctives :

Il est nécessaire de mettre en place des actions sur 2 fronts :

- Se conformer au RGPD en respectant ses grands principes ;
- Proposer un niveau de sécurité important aux données que vous traitez, par la mise en œuvre des actions présentées pour les mesures de sécurité.

Commentaire d'évaluation :

Les données concernées par ce traitement sont très nombreuses et sont sensibles selon leur nature.
Le nombre d'intervenants et de personnes pouvant consulter les informations est également très important.

Prenant en compte le plan d'actions, comment ré-évaluez-vous la gravité de ce risque (Modification non désirée des données) ? **Importante**
Prenant en compte le plan d'actions, comment ré-évaluez-vous la vraisemblance de ce risque (Modification non désirée des données) ? **Limitée**

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Sentiment d'atteinte à la vie privée, chantage, harcèlement, refus d'accès à certaines prestations, risques corporels, risques psychologiques, dommages psychologiques, cyberharcèlement, dépression, perte de temps pour réitérer des démarches, diffamation donnant lieu à des représailles.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Acte interne de malveillance, acte externe de malveillance, fuite de données, vol de données, piratage informatique, consultation humaine, interception du flux sur le réseau, accès non autorisé, erreur humaine, vol de matériel, accès non autorisé aux locaux.

Quelles sources de risques pourraient-elles en être à l'origine ?

Attaquant ciblant la structure, attaquant ciblant un utilisateur, employé malintentionné, employé négligeant, personnel de maintenance, tiers malintentionné, entourage d'un utilisateur, tiers négligeant, incendie, inondation.

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Authentification des utilisateurs, sauvegardes de données, sensibilisation des utilisateurs, sécurisation des sites web, protection des locaux, mot de passe, sécurisation des documents papiers, gérer les accès, gérer les risques, gestion des postes de travail, organisation de la politique de la vie privée, sécurisation des serveurs, sécurisation du réseau informatique.

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Dans le cadre de ces traitements, la gravité du risque de disparition des données est évaluée comme importante, les conséquences pourraient être contraignantes en cas de disparition de données.

En effet, une grande quantité de données est traitée. De plus, une partie de ces données est recensée comme données sensibles.

Toutefois, des sauvegardes régulières sont effectuées, permettant la récupération des données en cas de disparition.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

La vraisemblance du risque est évaluée comme importante.

Les accès physiques sont contrôlés. De plus, un système de gestion technique des bâtiments est mis en place et les équipements informatique sont protégés.

Également, les référents RGPD de chaque service sont sensibilisés aux bonnes pratiques, permettant ainsi de diminuer la probabilité d'une erreur humaine.

Des mesures sont également prévues dans le plan d'actions, ce qui va tendre à diminuer la vraisemblance d'une disparation de données.

Risques

Disparition de données

Évaluation : Améliorable

Plan d'action / mesures correctives :

Il est nécessaire de mettre en place des actions sur 2 fronts :

- Se conformer au RGPD en respectant ses grands principes ;
- Proposer un niveau de sécurité important aux données que vous traitez, par la mise en œuvre des actions présentées pour les mesures de sécurité.

Commentaire d'évaluation :

Les données concernées par ce traitement sont très nombreuses et sont sensibles selon leur nature.
Le nombre d'intervenants et de personnes pouvant consulter les informations est également très important.

Prenant en compte le plan d'actions, comment ré-évaluez-vous la gravité de ce risque (Disparition des données) ? **Importante**
Prenant en compte le plan d'actions, comment ré-évaluez-vous la vraisemblance de ce risque (Disparition des données) ? **Limitée**

Risques

Vue d'ensemble des risques

Impacts potentiels

- Sentiment d'atteinte à la vie privée
- Chantage
- Harcèlement
- Refus d'accès à certaines prestations
- Risques corporels
- Risques psychologiques
- Dommages psychologiques
- Cyberharcèlement
- Dépression
- Perte de temps pour réitérer des démarches
- Diffamation donnant lieu à des représailles

Menaces

- Acte externe de malveillance
- Acte interne de malveillance
- Fuite de données
- Vol de données
- Piratage informatique
- Consultation humaine
- Interception de flux sur le réseau
- Accès non autorisé
- Erreur humaine
- Vol de matériel
- Accès non autorisé aux locaux

Sources

- Attaquant ciblant la structure
- Attaquant ciblant un utilisateur
- Employé malintentionné
- Employé négligeant
- Personnel de maintenance
- Tiers malintentionné
- Entourage d'un utilisateur
- Tiers négligeant
- Incendie
- Inondation

Mesures

- Authentification des utilisateurs
- Sauvegardes de données
- Sensibilisation
- Sécurisation des sites WEB
- Protection des locaux
- Mot de passe
- Sécurisation des documents papiers
- Gérer les accès
- Gérer les risques
- Gestion du poste de travail
- Organisation de la politique de la vie privée
- Sécurisation du réseau interne
- Sécurisation des serveurs

Accès illégitime à des données	Gravité : **Maximale**	
	Vraisemblance : **Importante**	
Modification non désirée des données	Gravité : **Maximale**	
	Vraisemblance : **Importante**	
Disparition des données	Gravité : **Importante**	
	Vraisemblance : **Importante**	

Validation

Avis du DPD et des personnes concernées

Nom du DPD

Société AESATIS, représentée par sa dirigeante Madame Bernadette LEROY

Statut du DPD

Les traitements pourraient être mis en œuvre.

Opinion du DPD

Les mesures proposées pour sécuriser les traitements sont suffisantes pour leur bonne mise en œuvre.

Recherche de l'avis des personnes concernées

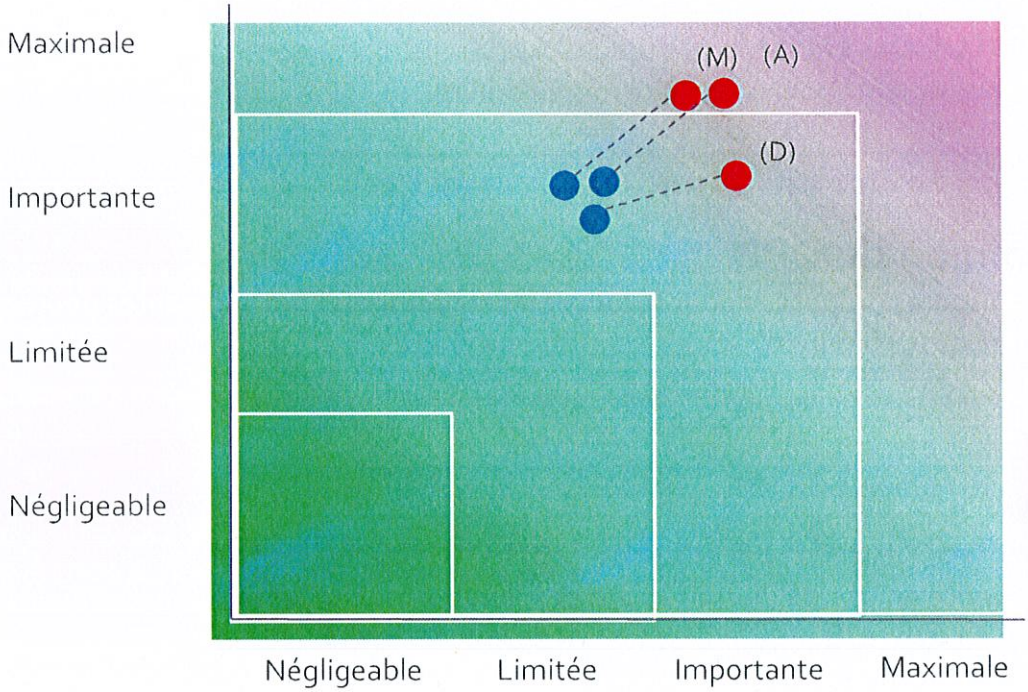
Le service en charge du traitement et son responsable de traitement valident la mise en œuvre des traitements au vu de leur nécessité.

Avis des personnes concernées n'a pas été demandé

Les personnes concernées n'ont pas été consultées car les traitements sont déjà en œuvre.

Validation

Cartographie des risques



- Mesures prévues ou existantes
- Avec les mesures correctives mises en œuvre
- (A)ccès illégitime à des données
- (M)odification non désirée de données
- (D)isparition de données

Validation

Plan d'action

Vue d'ensemble

Principes fondamentaux

- Finalités
- Fondement
- Données adéquates
- Données exactes
- Durée de conservation
- Information des personnes
- Droit d'accès et à la portabilité
- Droit de rectification et d'effacement
- Droit de limitation et d'opposition
- Sous-traitance
- Transferts

Mesures existantes ou prévues

- Authentification des utilisateurs
- Sauvegardes de données
- Sensibilisation
- Sécurisation des sites WEB
- Protection des locaux
- Mot de passe
- Sécurisation des documents papiers
- Gestion des accès
- Gérer les risques
- Gestion du poste de travail
- Organisation de la politique de la vie privée
- Sécurisation du réseau informatique
- Sécurisation des serveurs

Risques

- Accès illégitime à des données
- Modification non désirée de données
- Disparition de données

Mesures Améliorables
Mesures Acceptables

Principes fondamentaux

Durée de conservation

Évaluation : Améliorable

Plan d'action / mesures correctives :

- Définir des durées de conservation, pour les différentes données récoltées en fonction des finalités poursuivies par les traitements et tenir en compte la réglementation sur les durées de conservation des données de santé ;
- Mettre en place un processus de purge des données dans les applications métiers ;
- S'assurer du respect de ces durées par les prestataires et partenaires ;
- Limiter le doublonnage des données, que ce soit dans le service avec des versions numériques et des versions papiers, mais également avec les autres services lors des transferts de données par mail

Commentaire d'évaluation :

La définition des durées de conservation est un des fondements du RGPD, ainsi pour être conforme à ce dernier, il est nécessaire de définir des durées de conservation , de créer des procédures d'archivage et des procédures de destruction des données, afin de maximiser la protection des données des personnes concernées.

Principes fondamentaux

Information des personnes

Évaluation : Améliorable

Plan d'action / mesures correctives : Informer les personnes concernées sur les données qui sont collectées et le traitement qui en est fait.

- Mettre à jour les formulaires (papier et numérique) de collecte, avec les mentions d'information ;
- Mettre en place des procédures d'information dans les mails ;
- Réaliser des affichages dans les salles où le public est accueilli.

Pour rappel l'information des personnes doit comprendre, a minima :

- Identité et coordonnées de l'organisme responsable de traitement :
- Finalités ;
- Bases légales ;
- Caractère obligatoire ou facultatif du recueil des données ;
- Destinataires ou catégories de destinataire des données ;
- Durée de conservation des données ;
- Droits des personnes concernées ;
- Coordonnées du délégué à la protection des données ;
- Droit d'introduire une réclamation auprès de la CNIL.

Commentaire d'évaluation : L'information des personnes est un des fondements du RGPD. La transparence permet aux personnes concernées :

- de connaître la raison de la collecte des différentes données les concernant ;
- de comprendre le traitement qui sera fait de leurs données ;
- d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits.

Principes fondamentaux

Droits des personnes

Évaluation : Améliorable

Plan d'action / mesures correctives : afin de se conformer au RGPD, le service devra :

- Informer les personnes concernées sur leurs droits ;
- Mettre en œuvre des procédures de gestion des droits ;
- D'informer l'entièreté du service sur l'existence de ces droits et sur la procédure à respecter pour accéder aux éventuelles demandes de droits reçues.

Commentaire d'évaluation : créer des procédures en amont des demandes de droits permet d'assurer une réponse correcte aux attentes de la CNIL. Il est important de rappeler que de plus en plus de personnes sont sensibilisées à la protection des données, ainsi le nombre de demandes pourrait considérablement accroître.

Sous-traitants

Évaluation : Améliorable

Plan d'action / mesures correctives : s'assurer que tous les contrats avec les prestataires comportent des clauses RGPD, afin d'assurer une sécurisation de qualité aux personnes ayant fourni leurs données. Intégrer ce niveau de sécurité et ces clauses dans les marchés.

Mesures existantes ou prévues

Sauvegarde des données

Évaluation : Améliorable

Plan d'action / mesures correctives : Il est nécessaire de mettre en place une politique de sauvegarde des données. Les mesures de sécurité à mettre en place doivent assurer la disponibilité et la confidentialité des données sauvegardées. Pour cela, nous vous recommandons a minima de :

- Chiffrer les sauvegardes en prévoyant un stockage dans un lieu sécurisé ;
- Effectuer les sauvegardes sur un disque dur externe sur un site extérieur ;
- Chiffrer le canal de transmission, lorsque les sauvegardes sont transmises via un réseaux externe à l'entreprise ;
- Organiser des tests de restauration ;
- S'assurer que les agents et sous-traitants de la ville savent qui alerter en cas d'incident.

Commentaire d'évaluation : S'assurer que le contrat avec le SICIO inclut des garanties de sécurité des sauvegardes de données effectuées.

Sécurisation des sites WEB

Évaluation : Améliorable

Plan d'action / mesures correctives : Le protocole TLS version 1.2 est utilisé pour le chiffrement des connexions. Toutefois, il serait nécessaire d'utiliser la version TLS 1.3 qui est la plus récente. Nous vous conseillons également la mise en place d'outils de détection des vulnérabilités et la réalisation de tests d'intrusion.

Commentaire d'évaluation : S'assurer que des garanties en termes de sécurité des données sont formalisées avec l'hébergeur sur site et, le cas échéant, les inclure dans le contrat.

Protection des locaux

Évaluation : Améliorable

Commentaire d'évaluation : D'autres mesures pourraient renforcer cette sécurité, sans que cela n'engendre de dépenses importantes pour la ville :

- Créer un registre des visiteurs ;
- Accompagner les visiteurs lors de leur présence dans les locaux.

Mesures existantes ou prévues

Mot de passe

Évaluation : Améliorable

Plan d'action / mesures correctives :

Il serait nécessaire de mettre en œuvre une politique de mots de passe en suivant les nouvelles recommandations de la CNIL. Pour cela il convient de :

- Définir des règles permettant aux utilisateurs d'avoir des mots de passe sécurisés, exemple un mot de passe de 12 caractères avec des caractères spéciaux, ou un mot de passe comprenant a minima 16 caractères ;
- Interdire certains mots de passe ;
- Pratiquer un renouvellement régulier des mots passe pour les comptes de type administrateur ;
- Formaliser une politique de mot de passe.

Ci-après des exemples de **niveau d'entropie en fonction des règles définies** :

Exemple 1 : minimum de 12 caractères comprenant majuscules, minuscules, chiffres et caractères spéciaux.

Nombre minimal de caractères : 12

☐ Il existe un mécanisme limitant les soumissions abusives
☐ Il s'agit d'un code PIN pour un matériel physique

Types de caractères imposés :

☑ Lettre minuscules
☑ Lettre majuscules
☐ Lettre minuscules ou majuscules
☑ Chiffres
☑ Caractères spéciaux

☐ Pas de limitation (clavier AZERTY standard)
Limité à 0 caractères.

Équivalence en bits d'entropie : 71

Exemple 2 : minimum 14 caractères comprenant majuscules, minuscules et chiffres, **sans** caractère spécial obligatoire.

Nombre minimal de caractères : 14

☐ Il existe un mécanisme limitant les soumissions abusives
☐ Il s'agit d'un code PIN pour un matériel physique

Types de caractères imposés :

☑ Lettre minuscules
☑ Lettre majuscules
☐ Lettre minuscules ou majuscules
☑ Chiffres
☐ Caractères spéciaux

☐ Pas de limitation (clavier AZERTY standard)
Limité à 0 caractères.

Équivalence en bits d'entropie : 83

Exemple 3 : une phrase de passe doit être utilisée et elle doit être composée d'au minimum 7 mots.

Nombre minimal de caractères : 16

☐ Il existe un mécanisme limitant les soumissions abusives
☐ Il s'agit d'un code PIN pour un matériel physique

Types de caractères imposés :

☐ Lettre minuscules
☐ Lettre majuscules
☑ Lettre minuscules ou majuscules
☐ Chiffres
☑ Caractères spéciaux

☐ Pas de limitation (clavier AZERTY standard)
Limité à 0 caractères.

Équivalence en bits d'entropie : 75

Mesures existantes ou prévues

Gestion des accès

Évaluation : Améliorable

Plan d'action / mesures correctives : Il serait judicieux de mettre en place un système permettant la traçabilité des accès. Pour cela, il convient de :

- Prévoir un système de journalisation (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « logs ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité :
    - ces journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important) ;
    - La journalisation doit concerner a minima les accès des utilisateurs ;
- Informer les utilisateurs sur la mise en place d'un tel système ;
- Protéger les équipements de journalisation et les informations journalisées.

Commentaire d'évaluation : Formaliser une procédure de gestion des accès par écrit.

Gestion du poste de travail

Évaluation : Améliorable

Plan d'action / mesures correctives : Il serait judicieux de prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.
Configurer les logiciels pour que ces mises à jours se fassent automatiquement.

Commentaire d'évaluation : Les risques d'intrusion dans les systèmes informatiques sont importants et les postes de travail constituent un des principaux points d'entrée.

Sécurisation du réseau interne

Évaluation : Améliorable
Plan d'action / mesures correctives :
Réaliser des tests d'intrusions (recommandé tous les 3 ans) afin de détecter les vulnérabilités et failles de sécurité.
La télémaintenance doit s'effectuer via un VPN.
S'assurer qu'aucune interface réseau n'est accessible depuis internet.

Mesures existantes ou prévues

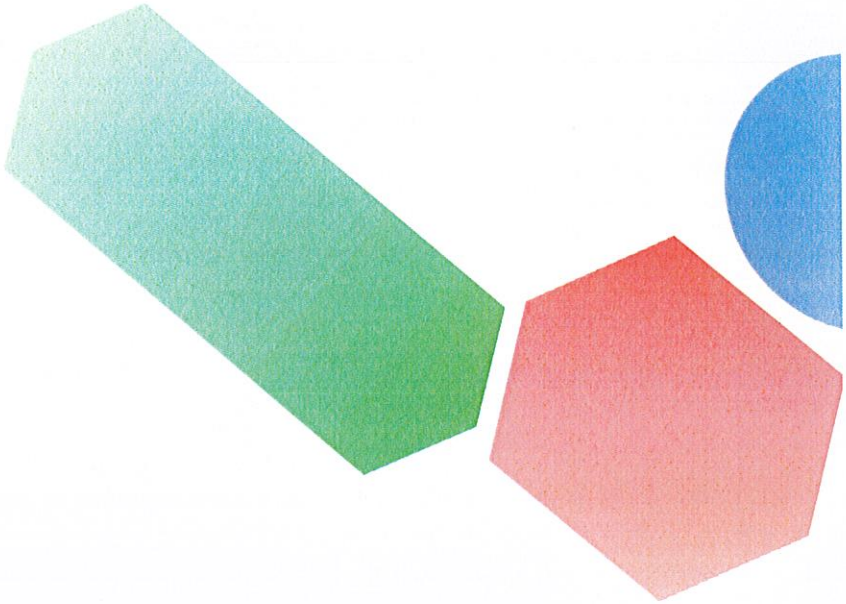
Sécurisation des serveurs

Évaluation : Améliorable

Plan d'action / mesures correctives : Renforcer la sécurité des serveurs :

- Mettre en place une politique spécifique de mots de passe pour les administrateurs ;
- Changement à chaque départ d'administrateur ;
- S'assurer de la sécurité physique des serveurs.

Commentaire d'évaluation : La sécurité des serveurs doit être une priorité car ils centralisent un grand nombre de données. Pour cela, il est nécessaire de renforcer leur sécurité. Cela passe autant par une protection informatique que par une protection physique.



AESATIS