Diagnostic

|  |  |
| --- | --- |
| Version : | 1.0 |
| État document : | Brouillon |
| Classification : | confidentiel |
| Société : | Vesperia |
| Document : | Diagnostic |
| Date : | 2016/04/15 |
| Consultant(s) : | Jerome De Almeida |
| Représentant(s) client : | Smile |

Vesperia

Sécurité de l'information

**Informations générales :**

Table des matières

1 Introduction 3

1.1 Avertissement 3

1.2 Interprétation des chiffres et « sensation » de sécurité 3

1.3 Contenu du document 4

1.4 Répartition sectorielle des contrôles 4

1.5 Glossaire 4

2 Synthèse du Diagnostic CASES 5

2.1 Résumé 5

2.2 Tableau des recommandations 6

ANNEXE A : Prise de notes 7

ANNEXE B : Légendes 8

Légende pour l’appréciation des recommandations 8

Légende du tableau d’évaluation détaillé 8

# 1 Introduction

## 1.1 Avertissement

Le Diagnostic CASES, réalisé à la demande du Client, a pour objectif d’apprécier la maturité d’une organisation eu regard aux bonnes pratiques applicables en matière de la sécurité de l'information. Les trois critères pris en compte dans le cadre du Diagnostic sont la confidentialité, l’intégrité et la disponibilité.

Le présent document, basé sur le Diagnostic CASES, est destiné à l’usage exclusif du client. Il est à ce titre confidentiel.

Au vu de la méthodologie employée et de la durée très limitée de l’entretien (2h) tenu pour le Diagnostic, il est entendu par les Parties que l’ensemble des résultats ne peut en aucune manière être exhaustif. À ce titre, l’appréciation du risque réel ou la liste des risques et vulnérabilités détectés sont basées sur les informations fournies par le Client et/ou ses représentants. L’analyse issue de cette appréciation ne peut engager SMILE GIE pour toute omission ou erreur qui seraient due à des tiers ou non.

Le Diagnostic CASES peut éventuellement fournir des recommandations (voir Annexe B, pour explications). Il est entendu par les parties que les recommandations ne sont ni exclusives, ni exhaustives.

## 1.2 Interprétation des chiffres et « sensation » de sécurité

La qualification de la maturité est un exercice qui permet d’apprécier si les mesures de sécurité en place sont à la hauteur du niveau de sécurité à obtenir en fonction des actifs à protéger. Par exemple, un résultat d’appréciation de 100% signifie que des moyens de protection jugés adéquats sont mis en œuvre. Par contre, comme aucune recherche exhaustive de failles n’est effectuée, rien n’affirme que ces moyens de protection soient efficaces et correctement implémentés.

Exemple : Un organisme a mis en place un contrôle d’accès par badge et un gardien à l’entrée de ses bureaux. Toutes les entrées et sorties sont consignées, les visiteurs portent un badge et sont toujours accompagnés.

Cette constatation peut atteindre la note maximum de mise en place de bonnes pratiques de 100%. Ce qui signifie que l’organisme a mis en place un contrôle d’accès en adéquation avec ce qu’il veut protéger. Il est sensible et conscient de son importance. Par contre, cela ne veut pas dire que la sécurité est correctement gérée, car les mesures de sécurité peuvent avoir des failles ou ne traitent pas tous les cas possibles.

**Exemples :**

* Y a-t-il une entrée de service, un fumoir externe ou d’autres accès aux bâtiments (quai de chargement) ?
* Qui autorise les accès, est-il facile de se procurer un badge ?
* Est-ce que les personnes qui quittent la société ont bien leurs accès supprimés ?
* Comment réagit le personnel en présence d’un inconnu seul dans les locaux ?
* Les consignes de sécurité sont-elles connues par l’ensemble du personnel ?
* Les exceptions sont-elles bien gérées ? (ouverture et fermeture des locaux, maladies, congés, pauses du gardien, etc.).
* Seule une analyse des risques permet d’apprécier plus exhaustivement les risques réellement encourus.

## 1.3 Contenu du document

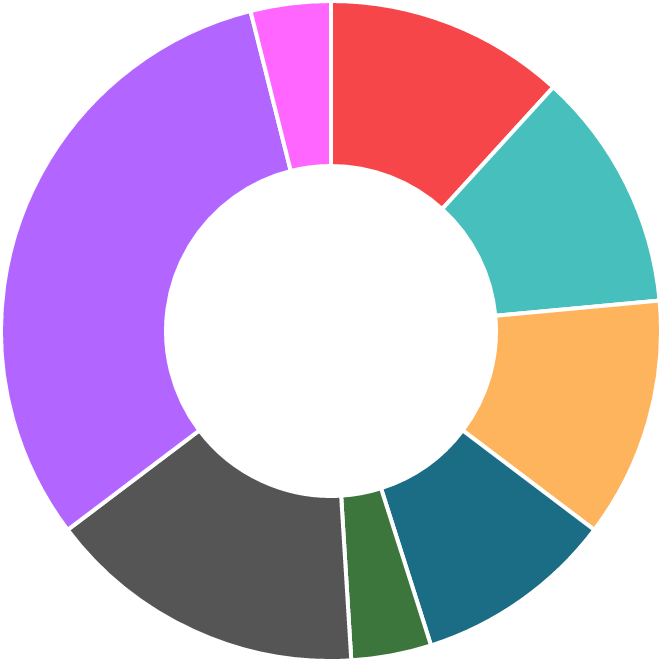
Le chapitre 2 contient la synthèse du Diagnostic.

L’Annexe A contient les notes prises lors de l’interview. Elles permettent, si ce n’est pas le cas de comprendre pourquoi certaines recommandations sont faites.

L’annexe B, contient les légendes nécessaires à la compréhension de ce document.

## 1.4 Répartition sectorielle des contrôles

Le schéma ci-dessous présente les différents secteurs faisant l’objet de l’évaluation. Il faut noter que l’IT « pure » (Système d’information) ne représente qu’un tiers des contrôles.



## 1.5 Glossaire

|  |  |
| --- | --- |
| Terme | Définition |
| Actif | Tout ce qui a de la valeur pour l’organisme (biens et information). |
| Sécurité de l'information | Protection de la confidentialité, de l’intégrité et de la disponibilité de l’information; en outre, d’autres propriétés, telles que l’authenticité, l’imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées. |

# 2 Synthèse du Diagnostic CASES

## 2.1 Résumé

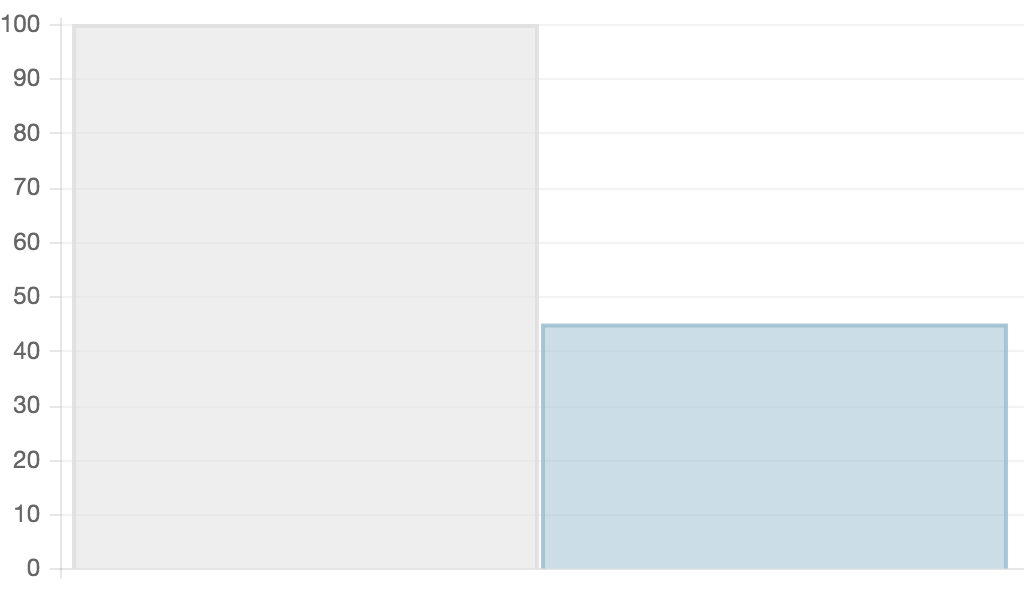
Le niveau de maturité calculé par le Diagnostic est calculé sur xxx points. Le niveau actuel est estimé à environ xxx points. Ce résultat montre que l’administration communale est déjà bien sensibilisée à la thématique de la sécurité de l’information, mais que quelques points peuvent être améliorés.

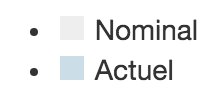
Par contre, l’évaluation décèle des recommandations du type « Risque très important » (●●●), sur-lesquels une attention toute particulière doit être portée. Nous y retrouvons notamment l’absence de mise à jour du système d’exploitation et des logiciels sur les postes locaux, ainsi que le non changement des mots de passe Windows après la première utilisation.

Une série de recommandations est axée sur la mise en place d’une charte de sécurité qui permet de rappeler aux utilisateurs les bonnes pratiques diverses concernant l’utilisation du système d’information, mais également sur une sensibilisation à la thématique désormais disponible dans le catalogue de formations officielles de l’INAP.

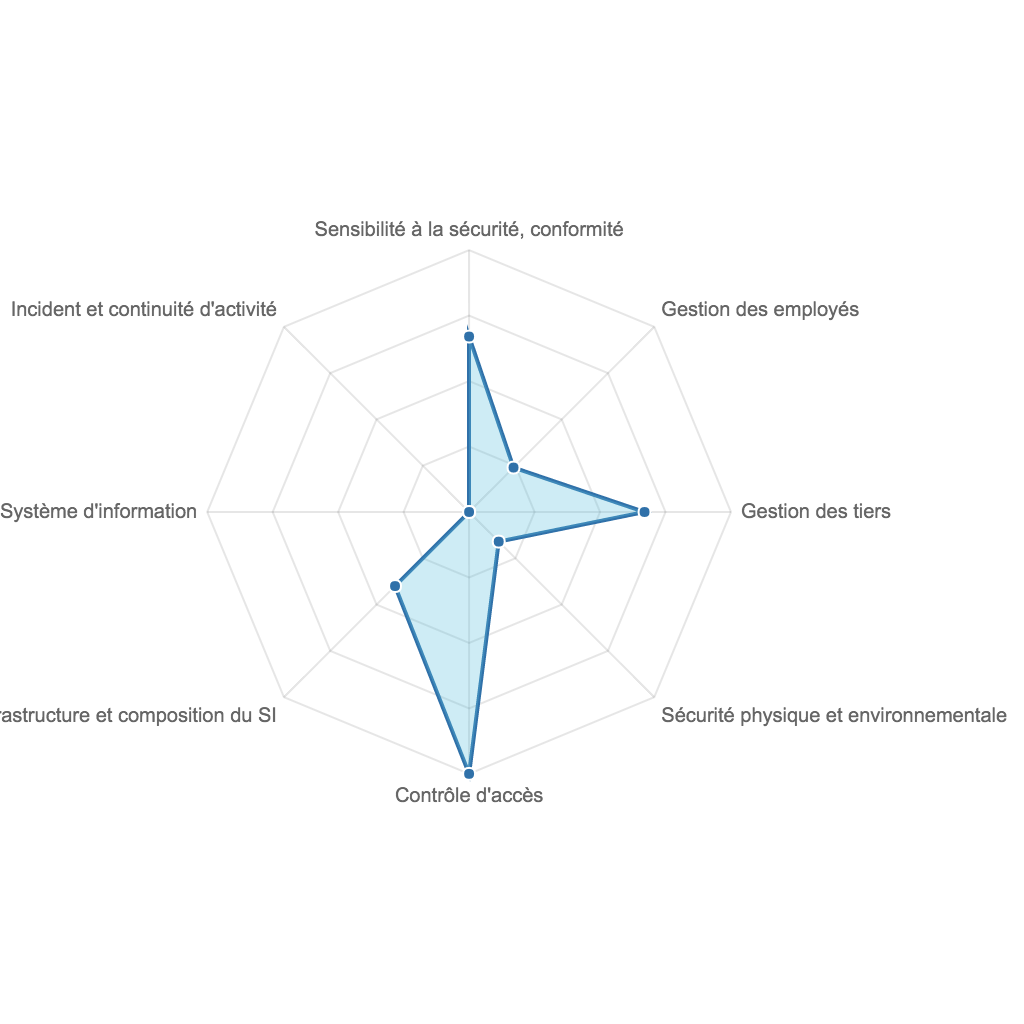
De façon globale, la plupart des mesures de sécurité sont faciles à implémenter et n’ont pas de coût direct.

Toutefois, au vu de la durée de l’évaluation (1,5 heure), celle-ci ne peut être exhaustive, et seule une analyse des risques peut déterminer plus en profondeur les risques auxquels l’administration est exposée.





**Vision de la conformité par domaine de la sécurité :**



## 2.2 Tableau des recommandations

La table suivante représente, la liste des recommandations formulées. Elle est ordonnée par gravité, puis par coût direct à prévoir, car certaines mesures organisationnelles ne coûtent que du temps interne de mise en œuvre.

La légende explicitant la lecture de ce tableau se trouve dans l'annexe B. Le détail des notes prises au regard des recommandations se trouve dans l'annexe A.

| **Nr** | **Recommandation** | **Domaine** | **Gravité** | **Maturité actuelle** | **Maturité visée** |
| --- | --- | --- | --- | --- | --- |
| 1 | recommandation 1 | Sensibilité à la sécurité, conformité | Moyen | 3 | 3 |
| 2 | Sécurité des services de l'information | Sensibilité à la sécurité, conformité | Moyen | 2 | 2 |
| 3 | Le chaos | Sensibilité à la sécurité, conformité | Fort | 1 | 2 |
| 4 | Je suis pas concerné | Sensibilité à la sécurité, conformité | Moyen | 0 | 3 |
| 5 | Conforme | Sensibilité à la sécurité, conformité | Moyen | 2 | 3 |
| 6 | Nouvelle recommandation | Sensibilité à la sécurité, conformité | Moyen | 1 | 3 |
| 7 | Formations régulières | Gestion des employés | Moyen | 3 | 3 |
| 8 | Le titre de la fonction est assez explicite | Gestion des employés | Moyen | 1 | 3 |
| 9 | Pas de rotation de personnel dans cette société | Gestion des employés | Fort | 0 | 2 |
| 10 | Les responsabilités IT sont définies | Gestion des employés | Faible | 0 | 2 |
| 11 | Un ordinateur portable ainsi qu'un écran sont fournis à chaque employé | Gestion des employés | Moyen | 3 | 3 |
| 12 | Les salariés ont le droit à un jour par semaine de télétravail | Gestion des employés | Fort | 0 | 2 |
| 13 | On est totalement indépendant, on ne travaille pas avec des fournisseurs de service | Gestion des tiers | Moyen | 2 | 3 |
| 14 | Des NDA ont été signés | Gestion des tiers | Faible | 1 | 2 |
| 15 | Un cahier des charges bien définis leur a été fourni | Gestion des tiers | Fort | 3 | 3 |
| 16 | Les clients n'ont pas accès au système d'information | Gestion des tiers | Fort | 0 | 2 |
| 17 | Le nettoyage des locaux est fait en présence des employés | Gestion des tiers | Faible | 3 | 3 |
| 18 | Aucun badge n'est fourni au non salariés | Gestion des tiers | Faible | 1 | 2 |
| 19 | Les accès physiques sont attribué par les internes | Sécurité physique et environnementale | Moyen | 0 | 3 |
| 20 | Les accès aux locaux sont contrôlés par badge | Sécurité physique et environnementale | Moyen | 2 | 2 |
| 21 | Tout est sous clé | Sécurité physique et environnementale | Fort | 0 | 2 |
| 22 | Non concerné | Sécurité physique et environnementale | Fort | 3 | 3 |
| 23 |  | Sécurité physique et environnementale | Faible | 0 | 2 |
| 24 | Uniquement aux internes | Contrôle d'accès | Faible | 3 | 2 |
| 25 |  | Contrôle d'accès | Faible | 3 | 2 |
| 26 |  | Infrastructure et composition du SI | Moyen | 2 | 3 |
| 27 |  | Infrastructure et composition du SI | Moyen | 2 | 2 |
| 28 | Centraliser les licenses | Infrastructure et composition du SI | Moyen | 0 | 2 |
| 29 |  | Infrastructure et composition du SI | Fort | 0 | 2 |
| 30 |  | Infrastructure et composition du SI | Faible | 0 | 2 |
| 31 | Clé publique et clé privée | Infrastructure et composition du SI | Moyen | 2 | 2 |
| 32 | Les information sensibles sont cryptées | Infrastructure et composition du SI | Moyen | 0 | 2 |

La légende explicitant la lecture de ce tableau se trouve au chapitre 4 « Légendes », le détail des notes prises au regard des recommandations se trouve au chapitre 3.

# ANNEXE A : Prise de notes

| Information à collecter | Information collectée | Évaluation de la maturité | | | | | Recommandation | Maturité visée |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | R | **½** | **** | Q |
| Sensibilité à la sécurité, conformité | | | | | | | | |
| Quels sont les mécanismes de sécurité existants (autres que techniques) ? | note 1 | Mécanismes de sécurité existants ? |  |  |  | X | recommandation 1 | 3 |
| Quel est le cœur de métier ? Processus/informations les plus sensibles ? | note 2 | Conscience des actifs importants ? |  |  | X |  | Sécurité des services de l'information | 2 |
| Quel est l'impact redouté (divulgation, modification, perte d'information) ? | note 3 | Conscience de l'impact de la non-sécurité ? |  | X |  |  | Le chaos | 2 |
| Quelles sont les obligations de conformité induites par le métier ? | note 4 | Conscience et respect des aspects de conformité ? | X |  |  |  | Je suis pas concerné | 3 |
| Conformité avec la législation sur les données à caractère personnel ? | note 5 | En ligne avec les exigences (CNPD) ? |  |  | X |  | Conforme | 3 |
| Nouvelle question ? | note 6 | Nouvelle question |  | X |  |  | Nouvelle recommandation | 3 |
| Gestion des employés | | | | | | | | |
| Le personnel a-t-il suivi des formations récemment ? | note 7 | Culture de la formation ? Sensibilité à la sécurité ? |  |  |  | X | Formations régulières | 3 |
| Existe-t-il des descriptions de fonction ? | note 8 | Job description pour les employés ? |  | X |  |  | Le titre de la fonction est assez explicite | 3 |
| Gestion de la rotation de personnel ? | note 9 | Gestion des employés ? | X |  |  |  | Pas de rotation de personnel dans cette société | 2 |
| Les responsabilités IT et éventuellement sécurité sont-elles définies ? | note 10 | Responsabilités IT ? | X |  |  |  | Les responsabilités IT sont définies | 2 |
| Du matériel est-il fourni à certains employés pour accomplir leur mission ? | note 11 | Bonne gestion des mouvements de personnel ? |  |  |  | X | Un ordinateur portable ainsi qu'un écran sont fournis à chaque employé | 3 |
| Le télétravail est-il pratiqué ? | note 12 | Pas de télétravail, ou bonne gestion de l'environnement de télétravail ? | X |  |  |  | Les salariés ont le droit à un jour par semaine de télétravail | 2 |
| Gestion des tiers | | | | | | | | |
| Qui sont les principaux fournisseurs de service ? Partenaires critiques ? | note 13 | Qui sont les principaux fournisseurs de service ? Partenaires critiques ? |  |  | X |  | On est totalement indépendant, on ne travaille pas avec des fournisseurs de service | 3 |
| Les fournisseurs de services ont-ils signé des engagements de confidentialité ? | note 14 | NDA signés ? |  | X |  |  | Des NDA ont été signés | 2 |
| Les fournisseurs de services s'engagent-ils formellement sur la qualité des prestations ? | note 15 | Signature de SLA sur les prestations vitales ? |  |  |  | X | Un cahier des charges bien définis leur a été fourni | 3 |
| Les clients ont-ils un accès au système d'information ? | note 16 | Pas d'accès client ou bonne gestion des accès ? | X |  |  |  | Les clients n'ont pas accès au système d'information | 2 |
| Comment s'organise l’entretien (nettoyage) des locaux ? | note 17 | Accès restreint aux zones sensibles |  |  |  | X | Le nettoyage des locaux est fait en présence des employés | 3 |
| Les visiteurs peuvent-ils circuler librement dans les bâtiments ? | note 18 | Circulation accompagnée, badge ou autres moyens ? |  | X |  |  | Aucun badge n'est fourni au non salariés | 2 |
| Sécurité physique et environnementale | | | | | | | | |
| Comment sont attribués les accès physiques ? | note 19 | Gestion des autorisations mature ? | X |  |  |  | Les accès physiques sont attribué par les internes | 3 |
| Les accès aux locaux sont-ils contrôlés ? | note 20 | Contrôle d'accès mature ? |  |  | X |  | Les accès aux locaux sont contrôlés par badge | 2 |
| Les locaux à accès restreints sont-ils protégés ? La salle informatique ? salle d'archive ? cave ? Coffre-fort ? | note 21 | La sécurité est-elle suffisante ? | X |  |  |  | Tout est sous clé | 2 |
| Quel est le système de contingence en cas d'une chute électrique ? | note 22 | Contingence électrique? |  |  |  | X | Non concerné | 3 |
| Les locaux à accès restreints sont-ils protégés ? La salle informatique ? | note 23 | La sécurité est-elle suffisante ? | X |  |  |  |  | 2 |
| Contrôle d'accès | | | | | | | | |
| Comment sont attribués les accès logiques ? | note 24 | Gestion des autorisations mature ? |  |  |  | X | Uniquement aux internes | 2 |
| Quelles sont les règles concernant les mots de passe ? | 8 caractères minimum, une majuscule, un chiffre et un caractère spécial obligatoire | Bonne gestion des mots de passe ? |  |  |  | X |  | 2 |
| Infrastructure et composition du SI | | | | | | | | |
| Partie Hardware et réseau ? Comment est construit le réseau interne (LAN) ? | note 26 | Bonne architecture réseau ? |  |  | X |  |  | 3 |
| Comment est géré le réseau Wifi ? | 2 bornes; une pour les visiteurs et une pour les employés | Bonne gestion du Wifi? |  |  | X |  |  | 2 |
| Partie software : Logiciels spécifiques ? | note 28 | Bonne gestion des logiciels ? | X |  |  |  | Centraliser les licenses | 2 |
| Des fournisseurs ont-ils la possibilité d'effectuer de la télémaintenance ? | Aucune télémaintenance est possible | Pas ou bonne gestion de la télémaintenance ? | X |  |  |  |  | 2 |
| Certains services à distances passent par des réseaux non sécurisés | Aucun service à distance de passe par un réseau non sécurisé | Pas de données en transit ou bonne gestion ? | X |  |  |  |  | 2 |
| Autres services et utilisation de la cryptographie | note 31 | Bonne gestion de la Cryptographie ? |  |  | X |  | Clé publique et clé privée | 2 |
| Des informations sensibles sont transmises par des réseaux non sécurisés ? | note 32 | Pas de données en transit ou bonne gestion ? | X |  |  |  | Les information sensibles sont cryptées | 2 |
| Système d'information | | | | | | | | |
| Incident et continuité d'activité | | | | | | | | |

# ANNEXE B : Légendes

## Légende pour l’appréciation des recommandations

Chaque recommandation comporte une indication du degré d'importance:

 : Risque très important qui doit être traité en urgence.

 : Risque important nécessitant une attention particulière.

 : Risque mineur/suggestion qui permettrait l’amélioration du niveau de la sécurité.

## Légende du tableau d’évaluation détaillé

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Information à collecter** | **Information collectée** | **Évaluation de la maturité** | | | | | **Recommandation** | **Maturité visée** |
| **Sujet** | **** | **½** | **** | **** |

**Information à collecter** : Question posée pendant l’interview, sujet à traiter.

**Information collectée** : Informations diverses collectées suite à la question posée.

**Évaluation de la maturité** :

**Sujet**  : Point de sécurité à évaluer

****: La (ou les) mesure de sécurité est correctement implémentée.

**½ **: La (ou les) mesure de sécurité est partiellement implémentée.

****: L’implémentation de la (ou les) mesure de sécurité est planifiée.

****: La (ou les) mesure de sécurité ne sont pas en place.

**Recommandation** : Formulation de ce qu’il faudrait idéalement faire pour contrer le risque.

**Mat visée** : Maturité visée après mise en place de la mesure.