**Evaluation du SMSI**

**Copie de travail de l'auditeur**

**Etablissement de référence - 2020**

# 1 Sensibiliser et former

## 1.1 Former les équipes opérationnelles à la cybersécurité

|  |  |
| --- | --- |
| Règle n°1.1.1 | Note |
| Un plan de formation à la cybersécurité au profit des équipes opérationnelles existe et est budgétisé. | 5 - En cours |
| Commentaire | |
| OK pour cette partie | |

|  |  |
| --- | --- |
| Règle n°1.1.2 | Note |
| Le plan de formation des équipes opérationnelles est spécifique à chaque métier (administrateur, chef de projet, développeur,...) | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.1.3 | Note |
| La formation à la cybersécurité des équipes opérationnelles couvre le volet juridique. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.1.4 | Note |
| La formation à la cybersécurité des équipes opérationnelles détaille les principaux risques et menaces. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.1.5 | Note |
| La formation à la cybersécurité des équipes opérationnelles couvre les notions de maintien en condition de sécurité. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.1.6 | Note |
| La formation à la cybersécurité des équipes opérationnelles détaille les principes et règles de l'authentification et du contrôle d'accès. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.1.7 | Note |
| La formation à la cybersécurité des équipes opérationnelle traite du paramétrage et du durcissement des systèmes d'information. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.1.8 | Note |
| La formation à la cybersécurité des équipes opérationnelle traite de l'architecture sécurisé des systèmes et des réseaux. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.1.9 | Note |
| Les contrats d'externalisation et d'infogérance contiennent une clause garantissant la formation à la cybersécurité du personnel. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

## 1.2 Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique

|  |  |
| --- | --- |
| Règle n°1.2.1 | Note |
| Un plan de sensibilisation à la cybersécurité au profit des utilisateurs existe et est budgétisé. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.2.2 | Note |
| La sensibilisation à la cybersécurité des utilisateurs est systématique et renouvelée régulièrement. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.2.3 | Note |
| La sensibilisation à la cybersécurité des utilisateurs détaille les règles de la politique de sécurité des systèmes d'informations. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.2.4 | Note |
| L'entité a élaboré une charte des moyens informatiques précisant les règles et consignes que doivent respecter les utilisateurs. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.2.5 | Note |
| Chaque utilisateur signe la charte des moyens informatiques. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 1.3 Maîtriser les risques de l'infogérance

|  |  |
| --- | --- |
| Règle n°1.3.1 | Note |
| Une liste d'exigences précises a été contractualisée avec le prestataires. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.3.2 | Note |
| La liste d'exigences fixe les modalités de réversibilités du contrat. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.3.3 | Note |
| La liste d'exigence détaille les modalités de réalisation d'audits. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.3.4 | Note |
| La liste d'exigence détaille les modalités de sauvegarde et de restitution des données dans un format ouvert normalisé. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.3.5 | Note |
| La liste d'exigence détaille la mise en œuvre du maintien à niveau de la sécurité dans le temps. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°1.3.6 | Note |
| Pour chaque contrat d'externalisation, le prestataire a fourni un plan d'assurance sécurité (PAS). | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

# 2 Connaître le système d'information

## 2.1 Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau

|  |  |
| --- | --- |
| Règle n°2.1.1 | Note |
| La liste des données sensibles existe et est à jour. | 2 - Inexistant et investissement important |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.1.2 | Note |
| La liste des données sensibles précise sur quels composants elles sont stockées ou traitées. | 3 - Inexistant et investissement faible |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.1.3 | Note |
| Les composants traitants ou hébergeant des données sensibles sont considérés comme critiques. | 2 - Inexistant et investissement important |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.1.4 | Note |
| Des mesures de sécurité spécifiques sont décrites pour les composants critiques (sauvegarde, mise à jour, contrôle d'accès) | 2 - Inexistant et investissement important |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.1.5 | Note |
| Un schéma du réseau existe et est à jour. | 2 - Inexistant et investissement important |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.1.6 | Note |
| Le schéma du réseau précise le positionnement des équipements réseaux et de sécurité. | 3 - Inexistant et investissement faible |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.1.7 | Note |
| Le schéma du réseau identifie les points d'interconnexion avec Internet et avec les partenaires. | 3 - Inexistant et investissement faible |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.1.8 | Note |
| Le schéma du réseau détaille l'emplacement des compsants critiques. | 3 - Inexistant et investissement faible |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.1.9 | Note |
| Le schéma du réseau détaille le plan d'adressage IP. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.1.10 | Note |
| Le schéma du réseau est considéré comme une donnée sensible. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 2.2 Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour

|  |  |
| --- | --- |
| Règle n°2.2.1 | Note |
| La liste des comptes à privilèges existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.2.2 | Note |
| La liste des comptes à privilèges référence les utilisateurs ayant un compte administrateur sur le système d'information. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.2.3 | Note |
| La liste des comptes à privilèges référence les utilisateurs ayant suffisament de droits pour accéder aux données des responsables. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.2.4 | Note |
| La liste des comptes à privilèges référence les utilisateurs utilisant un poste non administré par le service informatique. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.2.5 | Note |
| La revue périodique des droits d'accès au système d'information est effectuée régulièrement. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.2.6 | Note |
| La revue périodique des droits d'accès au système d'information permet de supprimer les comptes obsolètes. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 2.3 Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs

|  |  |
| --- | --- |
| Règle n°2.3.1 | Note |
| Une procédure d'arrivée des utilisateurs existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.3.2 | Note |
| La procédure d'arrivée précise les modalités de création des comptes et des boîtes de messagerie. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.3.3 | Note |
| La procédure d'arrivée précise les modalités d'affectation des équipements informatiques (ordinateur, smartphone, tablette,...). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.3.4 | Note |
| La procédure de d'arrivée est régulièrement mise à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.3.5 | Note |
| Une procédure de départ des utilisateurs existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.3.6 | Note |
| La procédure de départ précise les modalités de fermeture des comptes et des boîtes de messagerie. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.3.7 | Note |
| La procédure de départ précise les modalités de restitution des équipements informatiques (ordinateur, smartphone, tablette,...). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.3.8 | Note |
| La procédure de départ est régulièrement mise à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 2.4 Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés

|  |  |
| --- | --- |
| Règle n°2.4.1 | Note |
| Une politique fixant les règles d'usage des équipements personnels existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.4.2 | Note |
| Une politique fixant les règles d'usage des équipements prestataires et visiteurs externes existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.4.3 | Note |
| Un réseau WiFi dédié aux visiteurs existe. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°2.4.4 | Note |
| Des mesures techniques (802.1x) sont en place pour authentifier les postes de travail. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

# 3 Authentifier et contrôler les accès

## 3.1 Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur

|  |  |
| --- | --- |
| Règle n°3.1.1 | Note |
| Une politique des gestion des comptes existe et est à jour. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.1.2 | Note |
| Chaque utilisateur dispose d'un compte d'accès au système d'information personnel et nominatif. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.1.3 | Note |
| Chaque administrateur du système d'information dispose d'un compte d'administration nominatif différent de son compte d'utilisateur. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.1.4 | Note |
| Les comptes d'administration sont exclusivement dédié aux opérations d'administration du système d'information. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.1.5 | Note |
| Les comptes d'administration sont utilisée sur des environnements dédiés à l'administration. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.1.6 | Note |
| Les actions d'administrations sont journalisées. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 3.2 Attribuer les bons droits sur les ressources sensibles du système d'information

|  |  |
| --- | --- |
| Règle n°3.2.1 | Note |
| Une liste des ressources sensibles existe et est à jour. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.2.2 | Note |
| Pour chaque ressource, la liste des ressources sensibles précise quelle population peut y avoir accès. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.2.3 | Note |
| Les accès aux ressources sensibles sont journalisées. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.2.4 | Note |
| Une revue régulière des droits d'accès aux ressources sensibles est effectuée. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 3.3 Définir et vérifier des règles de choix et de dimensionnement des mots de passe

|  |  |
| --- | --- |
| Règle n°3.3.1 | Note |
| Une politique des mots de passe existe et est à jour. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.3.2 | Note |
| La longueur minimale des mots de passe est définie. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.3.3 | Note |
| Le niveau de complexité des mots de passe est défini. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.3.4 | Note |
| La durée de validité des mots de passe est définie. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.3.5 | Note |
| Les modalités de blocage des comptes à l'issue de plusieurs échecs de connexion sont définies. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.3.6 | Note |
| Les connexions anonymes sont désactivées. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.3.7 | Note |
| La robustesse des mots de passe est audité. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

## 3.4 Protéger les mots de passe stockés sur les systèmes

|  |  |
| --- | --- |
| Règle n°3.4.1 | Note |
| L'entité met à disposition de ses utilisateurs un mécanisme de coffre-fort numérique pour protéger leurs mots de passe. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.4.2 | Note |
| Les mots de passe des comptes génériques sont obligatoirement stockés dans un coffre-fort numérique. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 3.5 Changer les éléments d'authentification par défaut sur les équipements et services

|  |  |
| --- | --- |
| Règle n°3.5.1 | Note |
| Les éléments d'authentification par défaut des composants du système d'information sont modifiés dès leur installation. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.5.2 | Note |
| Les éléments d'authentification des composants du système d'information sont stockés dans un coffre-fort numérique. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.5.3 | Note |
| Lorsque les éléments d'authentification par défaut des composants du système d'information ne peuvent pas être modifiés, ces composants font l'objet de mesures de sécurité renforcées. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 3.6 Privilégier lorsque c'est possible une authentification forte

|  |  |
| --- | --- |
| Règle n°3.6.1 | Note |
| L'entité met en œuvre une authentification forte pour ses systèmes sensibles. | 4 - En cours et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.6.2 | Note |
| L'entité met en œuvre une authentification forte pour ses comptes d'administration. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°3.6.3 | Note |
| L'entité met en œuvre une authentification forte pour l'ensemble de ses utilisateurs. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

# 4 Sécuriser les postes

## 4.1 Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique

|  |  |
| --- | --- |
| Règle n°4.1.1 | Note |
| Une politique de sécurisation des postes existe et est à jour. | 3 - Inexistant et investissement faible |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.1.2 | Note |
| Une liste d'applications autorisées sur les postes de travail existe et est à jour. | 3 - Inexistant et investissement faible |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.1.3 | Note |
| Une liste d'applications autorisées sur les smartphones et tablettes existe et est à jour. | 4 - En cours et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.1.4 | Note |
| Une liste des modules autorisés sur les navigateurs web existe et est à jour. | 2 - Inexistant et investissement important |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.1.5 | Note |
| Les postes utilisateurs sont dotés d'un pare-feu local. | 3 - Inexistant et investissement faible |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.1.6 | Note |
| Les postes des utilisateurs sont dotés d'un antivirus à jour. | 4 - En cours et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.1.7 | Note |
| Les disques durs des postes des utilisateurs sont chiffrés. | 1 - Non applicable |
| Commentaire | |
| Pas nécessaire. | |

|  |  |
| --- | --- |
| Règle n°4.1.8 | Note |
| Les espaces de stockages des smartphones et tablettes sont chifrés. | 2 - Inexistant et investissement important |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.1.9 | Note |
| Les fonctions d'exécution automatique (autorun) sont désactivées. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 4.2 Se protéger des menaces relatives à l'utilisation de supports amovibles

|  |  |
| --- | --- |
| Règle n°4.2.1 | Note |
| Le branchement de périphériques amovibles inconnus est interdit. | 3 - Inexistant et investissement faible |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.2.2 | Note |
| Une solution permettant d'interdire l'exécution de programme sur les périphériques amovibles est mises en oeuvre. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.2.3 | Note |
| Le rechargement électrique des smartphones et tabllettes est interdit sur les postes utilisateurs. | 4 - En cours et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.2.4 | Note |
| Les supports amovibles ayant contenus des informations sensibles sont détruit en fin de vie. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 4.3 Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité

|  |  |
| --- | --- |
| Règle n°4.3.1 | Note |
| L'entité met en œuvre un outil de gestion centralisée de type Active Directory. | 4 - En cours et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.3.2 | Note |
| L'ensemble des postes de travail est intégré dans l'outil de gestion centralisé. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.3.3 | Note |
| L'ensemble des serveur est intégré dans l'outil de gestion centralisé. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.3.4 | Note |
| Une politique de durcissement des postes de travail est définie et appliquée via l'outils de gestion centralisé. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.3.5 | Note |
| Une politique de durcissement des serveurs est définie et appliquée via l'outils de gestion centralisé. | 4 - En cours et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

## 4.4 Activer et configurer le parefeu local des postes de travail

|  |  |
| --- | --- |
| Règle n°4.4.1 | Note |
| Un pare-feu est activé sur les postes de travail. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.4.2 | Note |
| La liste des flux réseaux autorisés existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.4.3 | Note |
| Seuls les ports correspondants aux flux autorisés sont ouverst sur les postes de travail. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.4.4 | Note |
| Les tentatives de connexion sur les ports bloqués par les pare-feu des postes de travail sont journalisées. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 4.5 Chiffrer les données sensibles transmises par voie Internet

|  |  |
| --- | --- |
| Règle n°4.5.1 | Note |
| Les emails transitant via Internet sont transmis en utilisant des protocoles assurant le chiffrement (IMPAS, POPS, SMTPS). | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°4.5.2 | Note |
| Les données transitant via Internet sont transmises en utilisant des protocoles assurant le chiffrement (HTTPS). | 7 - Existant |
| Commentaire | |
| Le site web de la société utilse HTTPS. | |

|  |  |
| --- | --- |
| Règle n°4.5.3 | Note |
| Les données sensibles sont chiffrées avant transmission via Internet. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

# 5 Sécuriser le réseau

## 5.1 Segmenter le réseau et mettre en place un cloisonnement entre ces zones

|  |  |
| --- | --- |
| Règle n°5.1.1 | Note |
| Le réseau de l'entité est segmenté en plusieurs zones matérialisées par des VLAN spécifiques. | 7 - Existant |
| Commentaire | |
| OK | |

|  |  |
| --- | --- |
| Règle n°5.1.2 | Note |
| Un pare-feu assure le filtrage des flux entre les différentes zones du réseau. | 7 - Existant |
| Commentaire | |
| OK | |

|  |  |
| --- | --- |
| Règle n°5.1.3 | Note |
| Un segment du réseau est spécifiquement dédié aux tâches d'administration. | 7 - Existant |
| Commentaire | |
| OK | |

## 5.2 S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages

|  |  |
| --- | --- |
| Règle n°5.2.1 | Note |
| Le réseau Wi-Fi met en œuvre un chiffrement des flux robuste (mode WPA2 avec AES CCMP). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.2.2 | Note |
| Le mot de passe par défaut des points d'accès Wi-Fi est changé lors de l'installation. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.2.3 | Note |
| L'authentification des équipements au réseau Wi-Fi se fait par certificat délivré par une infrastructure de gestion des clefs centralisée. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.2.4 | Note |
| Si l'authentification des équipements au réseau Wi-Fi se fait par mot de passe, celui-ci est robuste et changé régulièrement. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.2.5 | Note |
| Le réseau Wi-Fi est placé dans un VLAN distinct. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.2.6 | Note |
| Le réseau Wi-Fi dédié aux terminaux personnels ou visiteurs est séparé du réseau Wi-Fi des terminaux de l'entité (SSID et VLAN différents). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 5.3 Utiliser des protocoles réseaux sécurisés dès qu'ils existent

|  |  |
| --- | --- |
| Règle n°5.3.1 | Note |
| Sur les serveurs Web de l'entité, le protocole HTTP est désactivé au profit de HTTPS. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.3.2 | Note |
| Sur les serveurs de messagerie de l'entité, les protocoles IMAP, POP3 et SMTP sont désactivés au profit de IMAPS, POP3S et SMTPS. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.3.3 | Note |
| Sur les serveurs de transfert de fichiers de l'entité, le protocole FTP est désactivé au profit de FTPS ou SFTP. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.3.4 | Note |
| Les protocoles TELNET et RLOGIN sont désactivés au profit de SSH. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.3.5 | Note |
| L'implémentation de TLS sur les serveurs de l'entité n'autorise que les versions 1.2 et 1.3 du protocole. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 5.4 Mettre en place une passerelle d'accès sécurisé à Internet

|  |  |
| --- | --- |
| Règle n°5.4.1 | Note |
| L'accès à Internet se fait au travers d'un proxy authentifiant (type Alcasar - www.alcasar.net) | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.4.2 | Note |
| Le proxy d'accès à Internet comporte une fonctionnalité de filtrages des flux réseaux (pare-feu). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.4.3 | Note |
| Le proxy d'accès à Internet comporte une fonctionnalité d'analyse antivirale. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.4.4 | Note |
| Le proxy d'accès à Internet comporte une fonctionnalité de filtrages des URLs. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.4.5 | Note |
| Le proxy d'accès à Internet conserve les journaux d'activité des usagers conformément à la loi française. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.4.6 | Note |
| Un équipement de détection d'intrusion est déployé au point d'interconnexion entre le réseau de l'entité et internet. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 5.5 Cloisonner les services visibles depuis Internet du reste du système d'information

|  |  |
| --- | --- |
| Règle n°5.5.1 | Note |
| Dans le cas d'un hébergement interne de services accessibles sur internet, ces services sont isolés des autres systèmes d'information de l'entité. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.5.2 | Note |
| Dans le cas d'un hébergement interne de services accessibles sur internet, les flux liés à ces services sont filtrés (pare-feu). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.5.3 | Note |
| Dans le cas d'un hébergement interne de services accessibles sur internet, les flux entrants passent par un serveur mandataire (proxy). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.5.4 | Note |
| Dans le cas d'un hébergement externe, l'entité s'assure que son prestataire est conforme à ses exigences de sécurité (plan d'assurance sécurité). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 5.6 Protéger sa messagerie professionnelle

|  |  |
| --- | --- |
| Règle n°5.6.1 | Note |
| La redirection de messages professionnels vers une messagerie personnelle est interdite. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.6.2 | Note |
| Afin de se prémunir des escroqueries aux faux ordres de virement, des mesures organisationnelles sont décrites et appliquées. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.6.3 | Note |
| L'entité dispose d'un système d'analyse antivirus des boîtes de messagerie des utilisateurs. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.6.4 | Note |
| L'entité dispose d'un service anti-spam. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 5.7 Sécuriser les interconnexions réseau dédiées avec les partenaires

|  |  |
| --- | --- |
| Règle n°5.7.1 | Note |
| Les interconnexions réseaux avec une entité externe se font au travers d'un réseau privé virtuel de site à site (VPN). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.7.2 | Note |
| Les réseaux privés virtuels (VPN) mis en œuvre utilisent le standard IPSEC. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.7.3 | Note |
| Un filtrage IP à l'aide d'un pare-feu est mis place au plus près de l'entrée des flux VPN sur le réseau de l'entité. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.7.4 | Note |
| La matrice des flux (entrants et sortants) circulant au travers du VPN existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.7.5 | Note |
| Un point de contact à jour chez le partenaire est identifié pour pouvoir réagir en cas d'incident de sécurité. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 5.8 Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

|  |  |
| --- | --- |
| Règle n°5.8.1 | Note |
| Les accès aux salles serveurs et aux locaux techniques sont contrôlés à l'aide de serrures ou de mécanismes de contrôle d'accès par badge. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.8.2 | Note |
| Les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont interdit. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.8.3 | Note |
| Une revue des droits d'accès est réalisée régulièrement afin d'identifier les accès non autorisés. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.8.4 | Note |
| Lors du départ d'un collaborateur ou d'un changement de prestataire ses droits d'accès sont supprimés. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°5.8.5 | Note |
| Les prises réseau se trouvant dans des zones ouvertes au public (salle de réunion, hall d'accueil, couloirs, placards, etc.) sont désactivées. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

# 6 Sécuriser l'administration

## 6.1 Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information

|  |  |
| --- | --- |
| Règle n°6.1.1 | Note |
| Les postes utilisés pour l'administration des systèmes d'information de l'entité sont physiquement déconnecté d'internet. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°6.1.2 | Note |
| Les administrateurs de l'entité disposent d'un deuxième poste de travail pour les activités hors administration. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°6.1.3 | Note |
| Les mises à jour des équipements administrés se font via une zone d'échange sécurisée ou en mode déconnecté (via un support amovible). | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 6.2 Utiliser un réseau dédié et cloisonné pour l'administration du système d'information

|  |  |
| --- | --- |
| Règle n°6.2.1 | Note |
| L'entité utilise un réseau dédié aux activités d'administration de ses systèmes d'information. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°6.2.2 | Note |
| L'entité met en œuvre un cloisonnement logique ou physique de son réseau d'administration. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°6.2.3 | Note |
| Dans le cas d'un cloisonnement logique, un filtrage IP (pare-feu) contrôle les flux réseaux. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 6.3 Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail

|  |  |
| --- | --- |
| Règle n°6.3.1 | Note |
| Par défaut, les utilisateurs ne dispose pas de privilèges d'administration sur leur poste de travail. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°6.3.2 | Note |
| L'entité met en œuvre un magasin d'applications validées du point de vue de la sécurité. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°6.3.3 | Note |
| Seuls les agent chargés de l'administration des postes disposent de ces droits lors de leurs interventions. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°6.3.4 | Note |
| Si une délégation de privilèges sur un poste de travail est nécessaire elle est tracée, limitée dans le temps et retirée à échéance. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

# 7 Gérer le nomadisme

## 7.1 Prendre des mesures de sécurisation physique des terminaux nomades

|  |  |
| --- | --- |
| Règle n°7.1.1 | Note |
| Les utilisateurs sont sensibilisés aux risques spécifiques liés aux équipements informatiques lors d'un déplacement. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.1.2 | Note |
| Les terminaux nomades de l'entité sont équipés d'un filtre de confidentialité. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.1.3 | Note |
| Les terminaux nomades de l'entité ne portent pas de signe distinctifs liés à l'entité. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 7.2 Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable

|  |  |
| --- | --- |
| Règle n°7.2.1 | Note |
| Les données stockées sur supports amovibles (disques durs externes, clefs USB) de l'entité sont chiffrées. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.2.2 | Note |
| Les supports de stockages des terminaux nomades (ordinateurs, tablettes, smartphones) de l'entité sont chiffrés. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 7.3 Sécuriser la connexion réseau des postes utilisés en situation de nomadisme

|  |  |
| --- | --- |
| Règle n°7.3.1 | Note |
| L'entité met en œuvre un réseau privé virtuel (VPN) entre son système d'information et les terminaux nomades. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.3.2 | Note |
| Le VPN à destination des terminaux nomades utilise le standard IPSEC. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.3.3 | Note |
| Le tunnel VPN est automatiquement activé et non débrayable dès que le terminal est en situation de nomadisme. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.3.4 | Note |
| Une procédure de révocation identificants de connexion en cas de perte de vol existe et est à jour. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.3.5 | Note |
| Une plainte est systématiquement déposée en cas de vol d'un terminal nomade. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.3.6 | Note |
| L'entité met en œuvre un mécanisme d'authentification forte pour les ordinateurs nomades. La démarche est formalisée dans une procédure interne à l'entité. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 7.4 Adopter des politiques de sécurité dédiées aux terminaux mobiles

|  |  |
| --- | --- |
| Règle n°7.4.1 | Note |
| L'entité met en œuvre une solution de gestion centralisée de sa flotte de terminaux nomades. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.4.2 | Note |
| La configuration de sécurité des terminaux nomades est homogène. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°7.4.3 | Note |
| L'entité déploie un magasin d'applications limitant l'accès à des applications validées du point de vue de la sécurité. | 6 - Existant et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

# 8 Maintenir le système d'information à jour

## 8.1 Définir une politique de mise à jour des composants du système d'information

|  |  |
| --- | --- |
| Règle n°8.1.1 | Note |
| L'entité dispose d'un dispositif de veille concernant les vulnérabilités et les mises à jours des composants de son système d'information. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°8.1.2 | Note |
| Une procédure de mise à jour des composants du système d'information existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°8.1.3 | Note |
| La procédure de mise à jour des composants du SI précise les sources d'information relatives à la publication des mises à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°8.1.4 | Note |
| La procédure de mise à jour des composants du SI précise les outils utilisés pour déployer les correctifs de sécurité. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 8.2 Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles

|  |  |
| --- | --- |
| Règle n°8.2.1 | Note |
| L'entité assure un suivi des mises à jour et des dates de fin de support des logiciels. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°8.2.2 | Note |
| L'entité dispose d'un plan de renouvellement des composants matériels et logiciels obsolètes. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°8.2.3 | Note |
| Les contrats avec les prestataires et fournisseurs intègrent des clauses garantissant le suivi des correctifs de sécurité et la gestion des obsolescences | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

# 9 Superviser, auditer, réagir

## 9.1 Activer et configurer les journaux des composants les plus importants

|  |  |
| --- | --- |
| Règle n°9.1.1 | Note |
| Les journaux des pare-feu sont activés et intègrent notamment la liste des paquets bloqués. | 2 - Inexistant et investissement important |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.1.2 | Note |
| Les journaux des applications métiers sont activés et contiennent notamment les informations d'authentifications et d'autorisations (échecs et succès). | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.1.3 | Note |
| Les journaux des systèmes d'exploitation des postes de travail sont activés et contiennent notamment les informations d'authentifications et d'autorisations (échecs et succès). | 4 - En cours et demande un ajustement |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.1.4 | Note |
| L'entité dispose d'un serveur de temps (NTP) utilisé pour synchroniser les horloges des composants critiques du son système d'information. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.1.5 | Note |
| L'entité dispose d'une collecte centralisée des journaux d'activités des composants critiques de son système d'information. | 5 - En cours |
| Commentaire | |
| Pas de commentaire | |

## 9.2 Définir et appliquer une politique de sauvegarde des composants critiques

|  |  |
| --- | --- |
| Règle n°9.2.1 | Note |
| Une politique de sauvegarde existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.2.2 | Note |
| La politique de sauvegarde précise la liste des données jugées vitales pour l'entité et les serveurs concernés. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.2.3 | Note |
| La politique de sauvegarde précise le type et le fréquence des sauvegardes. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.2.4 | Note |
| La politique de sauvegarde précise la procédure d'administration et d'exécution des sauvegardes. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.2.5 | Note |
| La politique de sauvegarde précise les procédures de test et de restauration. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.2.6 | Note |
| Un exercice de restauration des données est planifié au moins une fois par an. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 9.3 Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées

|  |  |
| --- | --- |
| Règle n°9.3.1 | Note |
| Un audit interne de la sécurité du système d'information est réalisé au moins une fois par an. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.3.2 | Note |
| Un audit externe de la sécurité du système d'information est réalisé régulièrement. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.3.3 | Note |
| Les actions correctives, identifiées lors des audits internes et externes, sont planifiée et des points de suivi organisés à intervalles réguliers. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 9.4 Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel

|  |  |
| --- | --- |
| Règle n°9.4.1 | Note |
| L'entité a formellement désigné un référente en sécurité des systèmes d'information. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.4.2 | Note |
| Le référent en sécurité des systèmes d'information dispose d'une lettre de mission validée par la direction de l'entité. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.4.3 | Note |
| Le référent en sécurité des systèmes d'information est connu de tous les utilisateurs. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.4.4 | Note |
| Le référent en sécurité des systèmes d'information est en charge de la définition des règles de sécurité et de la vérification de leur application. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.4.5 | Note |
| Le référent en sécurité des systèmes d'information est en charge de la sensibilisation des utilisateurs. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

## 9.5 Définir une procédure de gestion des incidents de sécurité

|  |  |
| --- | --- |
| Règle n°9.5.1 | Note |
| Une procédure de gestion des incidents de sécurité existe et est à jour. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.5.2 | Note |
| Le référent en sécurité des systèmes d'information centralise et traite les incidents de sécurité. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.5.3 | Note |
| La procédure de gestion des incidents de sécurité impose la déconnexion du réseau du composant concerné. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.5.4 | Note |
| La procédure de gestion des incidents de sécurité impose le maintien sous tension du composant concerné. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.5.5 | Note |
| La procédure de gestion des incidents de sécurité fixe les modalités d'information de la hiérarchie et du référent en sécurité des systèmes d'information. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.5.6 | Note |
| La procédure de gestion des incidents de sécurité précise les modalités de collecte des informations sur le composant concerné. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

|  |  |
| --- | --- |
| Règle n°9.5.7 | Note |
| La procédure de gestion des incidents de sécurité précise les modalités de plainte aurès du service judiciaire compétent. | 0 - Pas de réponse |
| Commentaire | |
| Pas de commentaire | |

# 10 Gérer la sécurité par les risques

## 10.1 Mener une analyse de risques formelle

|  |  |
| --- | --- |
| Règle n°10.1.1 | Note |
| L'entité met en œuvre une démarche d'analyse des risques informationnels (EBIOS). | 7 - Existant |
| Commentaire | |
| OK | |

|  |  |
| --- | --- |
| Règle n°10.1.2 | Note |
| Une analyse des risques est réalisée pour chaque système d'information critique de l'entité. | 7 - Existant |
| Commentaire | |
| OK | |

|  |  |
| --- | --- |
| Règle n°10.1.3 | Note |
| L'analyse des risques permet d'exprimer les besoins de sécurité, d'identifier les objectifs de sécurité et de déterminer les exigences de sécurité. | 7 - Existant |
| Commentaire | |
| OK | |