l



**Rapport d’Audit de la Sécurité du Système d’Information**

**de Imprimerie Officielle de la République Tunisienne**

**pour l’année 2023**



**Expert Auditeur Chargé de la Mission :**

**Signature :**

<Insérer le cachet>

|  |  |  |
| --- | --- | --- |
| **Version du document** | **Date** | **Diffusion** |
| 0.1 | 2023-12-01 | Version de diffusion |

**SOMMAIRE**

[1. Avant-propos 3](#_Toc106872382)

[1.1. Confidentialité du document 3](#_Toc106872383)

[1.2. Historique des modifications 3](#_Toc106872384)

[1.3. Diffusion du document 3](#_Toc106872385)

[2. Cadre de la mission 4](#_Toc106872386)

[3. Termes et définitions 4](#_Toc106872387)

[4. Références 5](#_Toc106872388)

[5. Présentation de Client X 5](#_Toc106872389)

[6. Champ d’audit 6](#_Toc106872390)

[6.1. Périmètre géographique 6](#_Toc106872391)

[6.2. Description des systèmes d’information 6](#_Toc106872392)

[6.3. Schéma synoptique de l’architecture du réseau 9](#_Toc106872393)

[7. Méthodologie d’audit 9](#_Toc106872394)

[8. Synthèse des résultats de l’audit 12](#_Toc106872395)

[9. Présentation détaillée des résultats de l’audit 14](#_Toc106872396)

[9.1. Résultat par domaine de sécurité 14](#_Toc106872397)

[9.2. Vulnérabilités non acceptable enregistrées 40](#_Toc106872398)

[9.3. Les critères d’audit 41](#_Toc106872399)

[9.4. Détails audit technique 41](#_Toc106872400)

[10. Appréciation des risques 41](#_Toc106872401)

[10.1. La démarche d’appréciation des risques adoptée 41](#_Toc106872402)

[10.2. Présentation du processus d’appréciation du risque en sécurité de l’information 41](#_Toc106872403)

[10.3. Evaluation des Risques 42](#_Toc106872404)

[10.4. Identification des menaces, des vulnérabilités et des impacts des processus traités 51](#_Toc106872405)

[11. Plan d’action 52](#_Toc106872406)

[11.1. Le plan d’action 52](#_Toc106872407)

1. Avant-propos
   1. Confidentialité du document

Le présent document est confidentiel et sa confidentialité consiste à :

* Ne pas divulguer des dites informations confidentielles auprès de la tierce partie,
* Ne pas reproduire des informations dites confidentielles, sauf accord de IORT,
* Ne pas profiter ou faire profiter tierce partie du contenu de ces informations en matière de savoir-faire,
* Considérer toutes les informations relatives à la production et au système d’information de IORT déclarées Confidentielles.
  1. Historique des modifications

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Auteur** | **Modifications** |
| 1.0 | 2023-12-01 | Equipe Smart SKILLS | Version initiale |

* 1. Diffusion du document

|  |  |  |  |
| --- | --- | --- | --- |
| **Diffusion (coté *Smart SKILLS*)** | | | |
| Nom  Prénom | Titre | Tél | Mail |
| Ayed AKROUT | Chef de projet | 29961666 | Ayed.akrout@smartskills.tn |
| **Diffusion (coté IORT)** | | | |
| Nom  Prénom | Titre | Tél | Mail |
| Ben Ammar Monji | DSI | 98509854 | mongi@iort.gov.tn |

1. Cadre de la mission

Dans le cadre de la loi N°17-2023, IORT a confié au bureau d’études SMART SKILLS la réalisation d’une mission d’audit réglementaire de la sécurité de son système d’information pour l’année 2023. Le référentiel utilisé lors de cette mission est celui de la norme internationale ISO 27002 en sa version 2022, qui décrit les bonnes pratiques pour la gestion de la sécurité de l’information. Cette norme présente 93 mesures pouvant être mises en place pour gérer la sécurité d’un système d’information, et nous sommes attachés à vérifier l’existence et l’efficacité de chacune de ces mesures au niveau du système d’information de IORT.

1. Termes et définitions

* **Preuves d'audit**

Durant notre mission d’audit, nous avons exploité les différentes preuves d’audit qualitatives et quantitatives :

* La liste des enregistrements
* Les informations qui se rapportent aux critères d'audit et qui sont vérifiables.

Notre audit se base sur les différentes preuves :

* La preuve physique : c'est ce que l'on voit, constate = observation,
* La preuve testimoniale : témoignages. C'est une preuve très fragile qui doit toujours être recoupée et validée par d'autres preuves,
* La preuve documentaire : procédures écrites, comptes rendus, notes,
* La preuve analytique : résulte de calculs, rapprochements, déductions et comparaisons diverses.
* **Critères d’audit**

Ensemble de politiques, procédures ou exigences déterminées par rapport auxquelles la conformité du système est évaluée (contrôles au niveau de la norme ISO/IEC 27002 :2012).

* **Plan d'audit**

Description des activités et des dispositions nécessaires pour réaliser un audit, préparé par le responsable de l'audit en commun accord entre SMART SKILLS et IORT pour faciliter la programmation dans le temps et la coordination des activités d'audit.

* **Champs d'audit**

Étendu et limité d'un audit, le champ décrit généralement les lieux, les unités organisationnelles, les activités et les processus ainsi que la période de temps couverte.

* **Constats d'audit**

Résultats de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.

1. Références

Les documents de référence utilisés pour la réalisation de la présente mission d'audit sont :

* Le référentiel d'audit de l'ANSI v1.4
* La norme ISO 27002 :2012

1. Présentation de IORT

|  |  |
| --- | --- |
| **Nom de l’organisme** | Imprimerie Officielle de la République Tunisienne |
| **Acronyme** | IORT |
| **Statut** | étatique |
| **Secteur d’activité** | Imprimérie officielle |
| **Catégorie** | Imprimérie officielle |
| **Site web** | http://www.iort.gov.tn/ |
| **Adresse Email** | IORT@iort.gov.tn |

|  |  |  |  |
| --- | --- | --- | --- |
| **Désignation du processus** | **Exigences des données traitées en (1)** | | |
| **Confidentialité** | **Intégrité** | **Disponibilité** |
| publication officielle | 3 | 3 | 3 |
| GRI | 3 | 3 | 3 |
| juridique | 3 | 3 | 3 |
| Marché publique | 3 | 3 | 3 |
| Audit | 3 | 3 | 3 |
| GRH et Formation | 3 | 3 | 3 |
| comptabilité | 3 | 3 | 3 |
|  |  |  |  |

**Les principales missions de IORT :**

Les principales missions de l’IORT :
-Publier les textes juridiques de la république tunisienne ;
-Editer les livres juridiques : codes, ensemble de textes et guides spécialisés destinés aux institutions, aux professionnels et tout lecteur intéressé.

**Ci-dessous l’organigramme de IORT**

|  |
| --- |
|  |

1. Champ d’audit
   1. Périmètre géographique

La liste des structures à auditer

|  |  |  |
| --- | --- | --- |
|  | **Structure** | **Lieu d’implantation** |
| **2** | Siége Social | 40, avenue Farhat Hached 2098, Radès ville. Tunisie |

Le choix du périmètre géographique est selon la demande de IORT (Le respect du périmètre de la mission d’audit selon le cahier de charge).

* 1. Description des systèmes d’information
* Les composants du système d'information avec justification des exclusions le cas échéant selon le modèle « Description du SI de IORT »

**Description du SI Siège de IORT**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Applications** | | | | | | | |
| Nom (1) | Modules | Description | Environnement de développement | Développée par /Année | Noms ou @IP des  serveurs d’hébergement | Nombre d’utilisateurs | **Incluse au périmètre d’audit (6)** |
|  |  |  |  |  |  |  | Oui |
| www.iort.gov.tn | www.iort.gov.tn | www.iort.gov.tn |  |  |  |  | Oui |
| www.iort.tn | www.iort.tn | www.iort.tn |  |  |  |  | Oui |
| www.jocl.tn | www.jocl.tn | www.jocl.tn |  |  |  |  | Oui |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Serveurs (par plateforme)** | | | | | |
| Nom (1) | @IP | Type (2) | Système d’exploitation | Rôle/métier (3) | **Inclus au périmètre d’audit (6)** |
|  | 172.18.160.50 |  |  |  | Oui |
|  | 192.168.1.46 |  |  |  | Oui |
|  | 192.168.1.47 |  |  |  | Oui |
|  | 192.168.1.6 |  |  |  | Oui |
|  | 192.168.1.73 |  |  |  | Oui |
|  | 192.168.1.9 |  |  |  | Oui |
|  | 192.168.134.200 |  |  |  | Oui |
|  | 192.168.134.220 |  |  |  | Oui |
|  | 192.168.162.10 |  |  |  | Oui |
|  | 192.168.162.11 |  |  |  | Oui |
|  | 192.168.2.10 |  |  |  | Oui |
|  | 192.168.2.110 |  |  |  | Oui |
|  | 192.168.2.111 |  |  |  | Oui |
|  | 192.168.2.112 |  |  |  | Oui |
|  | 192.168.3.10 |  |  |  | Oui |
|  | 192.168.4.10 |  |  |  | Oui |
|  | 192.168.6.10 |  |  |  | Oui |
|  | 192.168.99.101 |  |  |  | Oui |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Infrastructure Réseau et sécurité** | | | | | |
| Nature (4) | Marque | Nombre | Administré par : | Observations (5) | **Inclus au périmètre d’audit (6)** |
|  | 10.0.0.1 |  |  |  | Oui |
|  | 10.0.0.3 |  |  |  | Oui |
|  | 10.20.1.1 |  |  |  | Oui |
|  | 10.30.1.1 |  |  |  | Oui |
|  | 10.40.1.1 |  |  |  | Oui |
|  | 10.60.1.1 |  |  |  | Oui |
|  | 192.168.17.17 |  |  |  | Oui |
|  | 192.168.17.18 |  |  |  | Oui |
|  | 192.168.17.19 |  |  |  | Oui |
|  | 192.168.17.2 |  |  |  | Oui |
|  | 192.168.17.20 |  |  |  | Oui |
|  | 192.168.17.239 |  |  |  | Oui |
|  | 192.168.17.25 |  |  |  | Oui |
|  | 192.168.17.251 |  |  |  | Oui |
|  | 192.168.17.4 |  |  |  | Oui |
|  | 192.168.17.5 |  |  |  | Oui |
|  | 192.168.17.69 |  |  |  | Oui |
|  | 192.168.17.70 |  |  |  | Oui |
|  | 192.168.2.1 |  |  |  | Oui |
|  | 192.168.255.1 |  |  |  | Oui |
|  | 192.168.3.1 |  |  |  | Oui |
|  | 192.168.4.1 |  |  |  | Oui |
|  | 192.168.6.1 |  |  |  | Oui |
|  | 192.168.99.252 |  |  |  | Oui |
|  | 192.168.99.253 |  |  |  | Oui |

|  |  |  |
| --- | --- | --- |
| **Postes de travail** | | |
| Système d’exploitation | Nombre | **Inclus au périmètre d’audit (6)** |
|  | 0 | Oui |

(1) : **Nomenclature**

(2) : Type du serveur : MV (Machine Virtuelle) ou MP (Machine Physique).

(3) : Rôle/métier : Base de données (MS SQL Server, Oracle, …), messagerie, application métier, Contrôleur de domaine, Proxy, Antivirus, etc.

(4): Nature: Switch, Routeur, Firewall, IDS/IPS, etc.

(5) Observations : des informations complémentaires sur l’équipement par exemple niveau du switch

(6) : Oui/Non. **Si non, présenter les raisons de l’exclusion. En cas où l’élément n’est pas audité pour des raisons d’échantillonnage, indiquer l’élément échantillonné avec, tout en précisant les critères d’échantillonnage adoptés.**

* 1. Schéma synoptique de l’architecture du réseau

Le schéma de réseau de IORT

|  |
| --- |
|  |

1. Méthodologie d’audit

* La méthodologie d’audit adoptée, comporte 4 étapes principales :
* Audit organisationnel et physique
* Audit technique
* Analyse de risque
* Synthèse de l’audit
* Les domaines de la sécurité des systèmes d’information couverts par la méthodologie d’audit sont détaillés dans la partie ci-dessous :
* La maturité des mesures et contrôles de sécurité mise en place est conforme avec les quatorze (04) domaines dudit référentiel :

**A.5 Mesures organisationnelles**

**A.6 Mesures liées aux personnes**

**A.7 Mesures physiques**

**A.8 Mesures technologiques**

**- Les outils d’audit utilisés**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Outils | Version utilisée | License | Fonctionnalités | Composantes du SI objet de l’audit |
| OWASP ZAP | 2.11.1 | Open Source | OWASP ZAP est un outil pour tester le niveau de sécurité des applications Web A | Application Web |
| Subgraph Vega | 1.0 | Open source | Vega est un scanner et une plate-forme pour tester le Niveau de sécurité des applications Web | Application Web |
| Nmap | 7.60 | Open source | Un scanner des ports | Scan des Ports |
| Nipper | 2.9.1 | Version de test | Un scanner des configurations réseau | Scan équipements Réseau |
| Nessus PRO | 10.0.2 | Version Pro | Nessus est un outil de scan des vulnérabilités | Serveur, PC, Application et Réseau |

**- Les check-lists utilisées**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Check List** | **Créer par** | **Equipe** | **Détails** | **Audit** |
| Check List Poste de travail | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit Poste de travail |
| Check List serveur | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit des serveurs |
| Check List applicatif | Créer par SMART SKILLS | Equipe SMART SKILLS | Détails des parties audités | Audit des applications |
| Check List firewall | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit firewall |
| Check List Switch | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit équipements réseau |
| Check List Router | CIS Benchmark | Equipe SMART SKILLS | https://www.cisecurity.org/benchmark | Audit équipements réseau |

**- L’équipe du projet côté SMART SKILLS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nom et Prénom** | **Qualité** | **Qualification** | **Certifié**  **Par l’ANSI** | **Champs d’intervention** |
| AKROUT Ayed | Chef de projet | ISO 27001, 27005, 22301, OSCP, CEH, CISA, CISM, CISSP, 27032 | Oui | AOP, Appréciation des risques |
|  |  |  |  |  |

**- L’équipe du projet côté IORT**

|  |  |  |
| --- | --- | --- |
| **Nom Prénom** | **Qualité** | **Fonction** |
| Ben Ammar Monji | DSI | DSI |

Le planning réel d’exécution de la mission d’audit de la sécurité du SI de IORT

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Composant** | | **Équipe intervenante** | **Date(s) de réalisation** | **Durée en Hommes/jours pour chaque intervenant** | |
| **Phase** | **Objet de la sous phase** | **Sur Site** | **Totale** |
| **Réunion d’ouverture et sensibilisation** | Réunion d’ouverture et sensibilisation |  |  |  |  |
| **AOP** | Audit Org. et Physique |  |  |  |  |
| Audit Org. et Physique |  |  |  |  |
| Audit Org. et Physique |  |  |  |  |
| Audit Org. et Physique |  |  |  |  |
| **AT** | Audit Technique |  |  |  |  |
| Audit Technique (Poste de travail) |  |  |  |  |
| Audit serveurs |  |  |
| Audit applicatif |  |  |  |  |
| Audit réseaux |  |  |  |  |
| **Appréciation des risques** | Appréciation des risques |  |  |  |  |
| **Synthèse et recommandations** | Synthèse et recommandations |  |  |  |  |
| **Réunion de clôture et sensibilisation post audit** | Réunion de clôture et sensibilisation |  |  |  |  |
| **Durée totale de la mission (en Homme/jour)** | | | | |  |

1. Synthèse des résultats de l’audit

* **Les critères et les standards/référentiels par rapport auxquels l’audit a été réalisé,**

D’une façon globale, le niveau de maturité de la sécurité du système d’information de IORT est ${acceptablility} ${raison\_decision}.

Un constat important est que d’après l’appréciation de risque, il y a ${nbr\_risk\_critique} scénarios de risque jugés vitale au niveau de IORT, il y a ${nbr\_risk\_critique} scénarios de risque jugés majeurs.

* **Les critères et les standards/référentiels par rapport auxquels l’audit a été réalisé,**

ISO 27002 / ISO 27005

* **Les types et nature de test réalisés pour établir ces résultats,**

      Scans de vulnérabilités et de configuration, Observations, réunions de travail, interviews, revue    documentaire, workshops.

* **Evaluation du dernier plan d’action**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Projet** | **Action** | **Criticité** | **Chargé de**  **l’action** | **Charge**  **(H/J)** | **Taux de**  **réalisation** | **Evaluation** (**1)** |
| **A.5 Politique de la sécurité de l'information** | **Action .1.1:Le Document Politique de Sécurité des Systèmes d’Information (PSSI) devra être enrichi par certaines politiques et certaines procédures opérationnellestels que: • Politique Cyber Sécurité (PCS), • Procédure de gestion des accès privilégiés, • Procédure de gestion des changements • Politique SIEM • Politique de gestion des patchs/correctifs de sécurit** | **Elévée** | **Comité décisionnel (décideurs) / RSSI** | **2** | **0%** | **Pas encore** |
| **A.6 Organisation de la sécurité de l’information** | **Action .2.1:Elaboration d’une note de décision portant création d’un Comité de Sécurité SI-IORT (CSSI) en précisant les attributions, le rôle et la périodicité de ses réunions et nomination formelle de la fonction RSSI avec élaboration d’une fiche de poste RSSI** | **Elévée** | **Comité décisionnel (décideurs)** | **2** | **0%** | **pas encore** |
| **A.6 Organisation de la sécurité de l’information** | **Action .2.2:Continuation de l’action du lancement du projet d’Assistance et d’Accompagnement à la mise en place d'un SMSI ISO 27001 :2013 (Certification SMSI)** | **Elévée** | **Comité décisionnel (décideurs) /RSSI/RSMSI** | **40** | **0%** | **En cours** |
| **A.7  Organisation de la sécurité de l’information** | **Action .3.1:Mise à jour de la charte IT jour en intégrant un article lié à la politique bureau propre et écran vide ainsi qu’un article lié à la sécurité des prestataires externes et des tiers Cette version de la charte IT devra être signée par les utilisateurs finaux de l’IORT** | **Elévée** | **CSSI/RSSI/RH** | **2** | **0%** | **Pas encore** |
| **A.7  Organisation de la sécurité de l’information** | **Action .3.2:Le plan de formation informatique existant devra être enrichit et améliorée par l’ajout des thèmes : Techniques avancées de sécurisation des environnements Système/base de données + Sessions de formation sur la Sécurité liée aux projets de Développement / Techniques de sécurité Code Source (développement sécurisée) selon l’ISO 27034 + Management de la continuité d’activité SMCA) et Cyber sécurité (ISO 27 032)** | **Moyenne** | **CSSI/RSSI /RH** | **5** | **0%** | **Pas encore** |
| **A.7  Organisation de la sécurité de l’information** | **Action .3.3:Mise en place d’un programme de sensibilisation (annuel) pour les utilisateurs finaux du SI-IORT : intégration des nouveaux enjeux et menaces, scénarios d’attaques expertes et bonnes pratiques de sécurisation SI (les sessions de sensibilisation devront être effectué d’une manière périodique)** | **Moyenne** | **CSSI/RSSI/RH** | **2** | **0%** | **Pas encore** |
| **A.7  Organisation de la sécurité de l’information** | **Action .3.4:Avoir un processus d’échange d’informations formel pour les cas de départ temporaire/définitif ou changement de fonction/poste d'un utilisateur/personnel ceci entre le responsable RH et RSSI** | **Elévée** | **CSSI/RSSI /RH** | **3** | **0%** | **Pas encore** |
| **A8. Gestion des actifs** | **Action .4.1:Mise à jour de l’Analyse des Risques IT et du Plan de Traitement des Risques IT en tenant compte des scénarios de risque d’ordre logique qu’ont été identifiées lors du présent Audit Réglementaire en Sécurité SI-IORT** | **élevée** | **CSSI/RSSI/RSMSI** | **3** | **0%** | **Pas encore** |
| **A9. Contrôle d’accès** | **Action .5.1:Renforcement de la configuration existante de l’Annuaire Active Directory via l'application d’une check-list de sécurité du Rôle Annuaire AD + Instauration d’une politique de gestion des mots de passe d’accès système (principalement la politique de gestion des mots de passe d’accès à l’annuaire AD) + modification dans l’immédiat des mots de passe faible des comptes privilégiés (Administrateur de Domaine)** | **élevée** | **RSSI/Administrateu r Système /Intégrateur de l’Annuaire AD** | **5** | **0%** | **Pas encore** |
| **A9. Contrôle d’accès** | **Action .5.2:Acquisition et Déploiement de la solution Microsoft ATA essentiellement pour la détection des attaques avancées ciblant l’Infrastructure serveurs sous l'Annuaire Active Directory** | **élevée** | **CSSI/RSSI** | **5** | **0%** | **Pas encore** |
| **A9. Contrôle d’accès** | **Action .5.3:Elaborer et implémenter une procédure de gestion des accès privilégiés (avec revue périodique des droits et privilèges d’accès : comptes Administrateurs de Domaine , comptes super\_utilisateur (administration des équipements réseau et sécurité)** | **élevée** | **CSSI/RSSI** | **5** | **0%** | **Pas encore** |
| **A9. Contrôle d’accès** | **Action .5.4:Renforcement des mesures de cloisonnement (segmentation) interne des réseaux locaux du Siège : Application des mesures de filtrage restrictif inter-VLANs/inter-Zones en s’articulant à une nouvelle architecture réseau et sécurité à déployer → un nouveau Système de Filtrage de type NGFW en frontal avec fonctionnalités avancées et services cybersécurité et utilisation du Firewall UTM existant en tant que Firewall de protection interne / Firewall DataCenter (** | **élevée** | **RSSI/Administrateur Réseau /Intégrateur sécurité réseau** | **3** | **0%** | **Pas encore** |
| **A10. Cryptographie** | **Action .6.1:Acquisition d'une solution de cryptage à la volée des disques (chiffrement des disques des PCs sensibles /Serveurs) abritant des données de nature confidentiel et/ou à caractère personnel** | **élevée** | **CSSI/RSSI** | **2** | **0%** | **Pas encore** |
| **A12. Sécurité liée à l’exploitation** | **Action .7.1:Elaborer une procédure de gestion des modifications/changements effectuées au niveau des actifs du SI-IORT** | **élevée** | **CSSI/RSSI/RSMSI** | **5** | **0%** | **Pas encore** |
| **A12. Sécurité liée à l’exploitation** | **Action .7.2:Elaboration d'une politique de gestion des patchs et correctifs de sécurité OS (Patch Management Policy)** | **élevée** | **CSSI/RSSI** | **5** | **0%** | **Pas encore** |
| **A12. Sécurité liée à l’exploitation** | **Action .7.3:Mise à niveau recommandée de la version OS du Serveur Annuaire AD (la version actuelle n’est plus supportée par l’éditeur et elle potentiellement vulnérable) ceci afin de pouvoir exploiter la solution de déploiement des patchs/correctifs OS Windows (Serveur WSUS) déployée** | **élevée** | **RSSI/Administrateur Système** | **10** | **0%** | **Pas encore** |
| **A12. Sécurité liée à l’exploitation** | **Action .7.4:Appliquer dans l’immédiat des patchs et correctifs OS pour les serveurs et postes de travail identifiés comme étant vulnérables : principalement pour le cas du patch/correctif OS MS17-010.** | **élevée** | **Administrateur Système** | **10** | **0%** | **Pas encore** |
| **A12. Sécurité liée à l’exploitation** | **Action .7.5:Consolidation recommandée des Serveurs via une infrastructure virtuelle avec acquisition d’une solution de sauvegarde des machines virtuelles : amélioration de la gestion des actifs de serveurs, dimensionnement/performances, administration et assurance d’une reprise d’activité dans les DMIAs souhaités pour les serveurs de données et d’application** | **élevée** | **CSSI/RSSI** | **10** | **30%** | **En cours** |
| **A12. Sécurité liée à l’exploitation** | **Action .7.6:Elaboration d'une procédure de gestion des vulnérabilités technique prévoyant la périodicité des audits de vulnérabilité et des audits de configuration des actifs de type technique + Traitement des vulnérabilités d’ordre technique identifiées (Plan d’Action VM /Vulnerability Management)** | **élevée** | **CSSI/RSSI** | **5** | **0%** | **pas encore** |
| **A13. Sécurité des communications** | **Action .8.1:Assurance d’un couplage entre le serveur annuaire d'utilisateurs (AD) et le nouveau firewall frontal de type NGFW à acquérir, afin de renforcer les mécanismes d'authentification d'accès aux ressources LAN/WAN du SI-IORT (filtrage par session utilisateur et @IP/@MAC)** | **élevée** | **CSSI/RSSI** | **10** | **0%** | **Pas encore** |
| **A14. Acquisition, développements et maintenance des systèmes d’information** | **Action .9.1:Application dans l'immédiat des mesures techniques correctives recommandées au niveau du Rapport spécifique d’audit de la sécurité des applications, afin de minimiser les risques liés à l'exploitation des faillessignificatives identifiées.** | **élevée** | **RSSI / Développeurs/ Fournisseurs applicatifs** | **5** | **0%** | **Pas encore** |
| **A17. Aspects de la sécurité de l’information dans la gestion de la continuité de l’activité** | **Action .10.1:Elaborer une étude pour la refonte de l’architecture réseau au niveau du site Siège et l’acquisition d’une nouvelle pile des Switchs d’interconnexion permettant d’assurer une bonne qualité et performances des services réseau offerts au niveau du Site central (Siège de l’IORT) et une reprise d’activité dans les DMIAs souhaités [Avoir une architecture réseau et sécurité symétrique permettant ainsi d’assurer la continuité d’activité des services réseau LAN/WAN du SI IORT** | **élevée** | **CSSI/RSSI** | **10** | **0%** | **Pas encore** |
| **A18. Conformité** | **Action .11.1:Formalisation des politiques et procédures d’archivage et de conservation des données en précisant les périodes et modalités de rétention + Se référer à la Norme ISO/CEI 29100 proposant un cadre pour la protection des données à caractère personnel au sein des SI** | **élevée** | **CSSI / RSSI** | **5** | **0%** | **Pas encore** |

(1) Evaluation des mesures qui ont été adoptées depuis le dernier audit réalisé et aux insuffisances enregistrées dans l’application de ses recommandations, avec un report des raisons invoquées par les responsables du système d’information et celles constatées, expliquant ces insuffisances.

* **Etat de maturité de la sécurité du système d’information de IORT**
* **par rapport à la norme ISO 27002 (les détails sont dans la section 9 du présent rapport)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Domaine** | **Critère d’évaluation** | **Valeur attribuée** | **Commentaires** |
| 5.Principes pour les mesures organisationnelles | Appréciation des événements liés à la sécurité de l'information et prise de décision | 1 |  |
| 5.Principes pour les mesures organisationnelles | Fonctions et responsabilités liées à la sécurité de l'information | 0.9 |  |
| 5.Principes pour les mesures organisationnelles | Séparation des tâches | 1 |  |
| 5.Principes pour les mesures organisationnelles | Responsabilités de la direction | 0.4 |  |
| 5.Principes pour les mesures organisationnelles | Intelligence des menaces | 0.4 |  |
| 5.Principes pour les mesures organisationnelles | Sécurité de l'information dans la gestion de projet | 0 |  |

Les valeurs à attribuer pour chaque règle de sécurité invoquée seront entre 0 et 5 :

N/A - Non applicable

0 - Pratique inexistante

1 - Pratique informelle : Actions isolées

2 - Pratique répétable et suivie : Actions reproductible

3 - Processus définis : Standardisation des pratiques

4 - Processus contrôlés : des mesures quantitatives

5 - Processus continuellement optimisés

* **Les indicateurs de sécurité selon le modèle « Indicateurs de sécurité :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Classe/Indicateur** | | **Exp de valeur** | **Valeur** | **Commentaires** |
| **Organisation** | **Nomination officielle RSSI** | 0/1 |  |  |
| **Fiche de poste RSSI** | 0/1 |  |  |
| **Rattachement RSSI** | DG/DSI/Direction Administrative/Direction Audit Interne/Direction Risques |  |  |
| **Existence officielle Cellule Sécurité** | 0/1 |  |  |
| **Existence officielle Comité Sécurité** | 0/1 |  |  |
| **PSSI** | **Existence formelle PSSI** | 0/1 |  |  |
| **Portée** | Partielle/Totale |  |  |
| **Communication** | 0/1 |  |  |
| **Maintien de la PSSI** | 0/1 |  |  |
| **Gestion de la continuité d'activité** | **Existence formelle PCA** | 0/1 |  |  |
| **Existence formelle PRA** | 0/1 |  |  |
| **Maintien du PCA** | 0/1 |  |  |
| **Maintien du PRA** | 0/1 |  |  |
| **Organisation de crise en cas de sinistre** | 0/1 |  |  |
| **Site Secours** | 0/1 |  |  |
| **Gestion des actifs** | **Inventaire complet** | 0/1 |  |  |
| **Procédure formelle de classification** | 0/1 |  |  |
| **Mise en place de la classification** | 0/1 |  |  |
| **Gestion des risques SI Métier** | **Existence formelle de la gestion des risques** | 0/1 |  |  |
| **Couverture totale du Métier** | 0/1 |  |  |
| **Réalisée une seule fois** | 0/1 |  |  |
| **Fréquence Réalisation Périodique** | 0/1 |  |  |
| **En cas de changement majeur** | 0/1 |  |  |
| **Gestion des incidents** | **Procédure formelle de gestion des incidents** | 0/1 |  |  |
| **Existence d'une cellule de gestion des incidents** | 0/1 |  |  |
| **Gestion des sauvegardes** | **Politique formelle de sauvegarde** | 0/1 |  |  |
| **Couverture des données métier** | Absence/Totale/ Partielle |  |  |
| **Couverture des données de serveurs de support** | Absence/Totale/ Partielle |  |  |
| **Couverture des données des PCs utilisateurs sensibles** | Absence/Totale/Partielle |  |  |
| **Couverture des running-config des équipements de sécurité &réseau** | Absence/Totale/Partielle |  |  |
| **Couverture Clonage OS des serveurs** | Absence/Totale/Partielle |  |  |
| **Couverture des codes sources et des paramètres de configuration des applications et des logiciels de base** | Absence/Totale/Partielle |  |  |
| **Maintien de la solution de sauvegarde** | 0/1 |  |  |
| **Tests de restauration périodiques** | 0/1 |  |  |
| **Sécurité physique des copies de sauvegarde** | 0/1 |  |  |
| **Existence des copies à un site distant** | 0/1 |  |  |
| **Contrôle d’accès** | **Politique formelle de contrôle d’accès** | 0/1 |  |  |
| **TdB SSI** | **Existence d'un Tableau de bord SSI** | 0/1 |  |  |
| **Portée : indicateurs opérationnels** | 0/1 |  |  |
| **Portée : indicateurs stratégiques** | 0/1 |  |  |
| **Audit interne de la sécurité** | **Existence de l'Audit interne de la sécurité** | 0/1 |  |  |
| **Réalisation périodique de l'Audit interne** | 0/1 |  |  |
| **Réalisation suite à un incident** | 0/1 |  |  |
| **Réalisation suite à la mise en place d’un nouveau système** | 0/1 |  |  |
| **Portée: uniquement aspects techniques** | 0/1 |  |  |
| **Portée: aspects tech, org et phys** | 0/1 |  |  |
| **Démarche de conformité** | **Existence d'une démarche de conf** | 0/1 |  |  |
| **Nature** | exemples: ISO 27001/ PCI/DSS |  |  |
| **Etape** | certifié/projet en cours/planifié |  |  |
| **Protection antivirale** | **Existence d'une solution antivirale** | 0/1 |  |  |
| **MAJ périodique de la Sol Antivirale** | 0/1 |  |  |
| **Couverture des serveurs** | Absence/Partielle/Totale |  |  |
| **Couverture des PCs** | Absence/Partielle/Totale |  |  |
| **Dépl auto des patchs et correctifs Séc OS** | **Existence Dép auto patchs&cor Séc OS** | 0/1 |  |  |
| **MAJ périodique de la Sol Antivirale** | Absence/Partielle/Totale |  |  |
| **Couverture des serveurs** | Absence/Partielle/Totale |  |  |
| **Couverture des PCs** | 0/1 |  |  |
| **Processus MAJ des firmwares Equips Sécurité** | **Existence** | Absence/Partielle/Totale |  |  |
| **Couverture** | 0/1 |  |  |
| **Processus MAJ des firmwares Equips Réseau** | **Existence** | 0/1 |  |  |
| **Couverture** | Absence/Partielle/Totale |  |  |
| **Remplacement des produits dont la date EoL ou EoS expiré** | **Remp OS Serveurs EoL EoS** | Total/Partiel/Planifié/Absence |  |  |
| **Remp OS PCs EoL EoS** | Total/Partiel/Planifié/Absence |  |  |
| **Remp Produits Sécurité EoL EoS** | Total/Partiel/Planifié/Absence |  |  |
| **Remp Produits Réseau EoL EoS** | Total/Partiel/Planifié/Absence |  |  |
| **Contrôle d'accès logique** | **Utilisation Contrôleur de domaines** | 0/1 |  |  |
| **Utilisation d'une Solution IAM** | 0/1 |  |  |
| **Utilisation Proxy Accès Internet** | 0/1 |  |  |
| **Matrice de Flux Réseau MFR formelle** | 0/1 |  |  |
| **Implémentation règles de filtr -Equips frontaux- cf MFR** | 0/1 |  |  |
| **Implémentation Filtrage inter-VLAN cf MFR** | 0/1 |  |  |
| **Réseau d’administration** | **Existence d'un réseau d'admin** | 0/1 |  |  |
| **Isolé du réseau production et Internet** | 0/1 |  |  |
| **Admin qu’à partir des machines de ce réseau** | 0/1 |  |  |
| **Utilisation protocoles admin chiffrés** | Absence/Partielle/Totale |  |  |
| **Séparation des environnements** | **Sép infras dév, test et exploitation** | 0/1 |  |  |
| **Sécurité des partages** | **Désactiv des partages rés sur les serveurs** | 0/1 |  |  |
| **Désactiv des partages rés sur les PCs** | 0/1 |  |  |
| **Utilisation des serveurs de fichier** | 0/1 |  |  |
| **Système de détection/Prévention d’intrusion** | **Existence** | 0/1 |  |  |
| **Déf politique de détection et de prévention d’intrusion** | 0/1 |  |  |
| **Configuration par défaut des alertes** | 0/1 |  |  |
| **Configuration cf à la politique des IDS/IPS** | 0/1 |  |  |
| **Processus de suivi des alertes générées** | 0/1 |  |  |
| **Solution SIEM** | **Existence** | 0/1 |  |  |
| **Portée: Serveurs** | 0/1 |  |  |
| **Portée: Equips Séc** | 0/1 |  |  |
| **Portée: Equips Rés** | 0/1 |  |  |
| **Synchronisation des horloges** | 0/1 |  |  |
| **Contrats de maintenance** | **Couverture des Serveurs** | Absence/Partielle/Totale |  |  |
| **Couverture des applications métier** | Absence/Partielle/Totale |  |  |
| **Couverture des SGBDs** | Absence/Partielle/Totale |  |  |
| **Couverture des équips sécurité** | Absence/Partielle/Totale |  |  |
| **Couverture des équips réseau** | Absence/Partielle/Totale |  |  |
| **Local Data-center** | **Existence** | 0/1/2/3+ |  |  |
| **Classification** | Non-classé/Tier1/Tier2/Tier3/Tier4 |  |  |
| **Zones d'emplacement** | Forts Risques/Faibles Risques |  |  |
| **Contrôle d’accès au Data-Center** | Exemples: Clé/Carte magnétique/Biométrie |  |  |
| **Secours électrique** | **Couverture onduleurs Serveurs** | Absence/Partielle/Totale |  |  |
| **Couverture onduleurs Equips rés & séc** | Absence/Partielle/Totale |  |  |
| **Couverture onduleurs PCs** | Absence/Partielle/Totale |  |  |
| **Existence Groupe électrogène** | 0/1 |  |  |
| **Test régulier du groupe électrogène** | 0/1 |  |  |
| **Sécurité de la climatisation DC** | **Système de climatisation adéquate** | 0/1 |  |  |
| **Redondance** | 0/1 |  |  |
| **Contrat de maintenance** | 0/1 |  |  |
| **Sécurité Câblage** | **Chemins de câbles dédiés et séparés** | 0/1 |  |  |
| **Etiquetage** | 0/1 |  |  |
| **Plans de chemins de câblage** | 0/1 |  |  |
| **Sécurité périmétrique DC** | **Solution de détection d’intrusion** | 0/1 |  |  |
| **Système de vidéo-surveillance** | 0/1 |  |  |
| **Murs résistants aux intrusions physiques et aux incendies et dépourvus de fenêtres** | 0/1 |  |  |
| **Sécurité Incendie DC** | **Détecteurs de fumée** | 0/1 |  |  |
| **Extincteurs automatiques** | 0/1 |  |  |
| **Porte Data Center Coupe-feu** | 0/1 |  |  |
| **Sécurité contre les dégâts des eaux** | **Détecteurs d’humidité** | 0/1 |  |  |
| **Système d’alerte** | 0/1 |  |  |
| **Dispositif Anti-foudre** | **Dispositif Anti-foudre** | 0/1 |  |  |

* **Les vulnérabilités très critiques détectées et jugées être d’un intérêt particulier pouvant affecter la sécurité du cyber espace national :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Vulnérabilité** | **Référence de la vulnérabilité** | **Actifs impactés** | **Impact d’exploitation réussie de la vulnérabilité** | **Probabilité d’exploitation réussie de la vulnérabilité** | **Recommandation / Mesure de traitement** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. Présentation détaillée des résultats de l’audit
   1. Résultat par domaine de sécurité

|  |  |  |  |
| --- | --- | --- | --- |
| **Domaine** | **Critères d’audit** | **Résultats de l’audit (constats)** | **Description des vérifications effectuées (tests, conditions de test, etc)** |
| **5 Mesures de sécurité organisationnelles** | **5.1 Appréciation des événements liés à la sécurité de l'information et prise de décision** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'une politique de sécurité de l'information ainsi des documents plus détaillés de politiques de sécurité par thème |
| **5 Mesures de sécurité organisationnelles** | **5.2 Fonctions et responsabilités liées à la sécurité de l'information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'une structure opérationnelle et de l'organisation de la gestion de la sécurité : RSSI et correspondants ou responsables locaux, rôles et responsabilités respectifs et vis-à-vis des responsables opérationnels. |
| **5 Mesures de sécurité organisationnelles** | **5.3 Fonctions et responsabilités liées à la sécurité de l'information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| La définition des rôles et responsabilités ne garantit plus une séparation des tâches pour des domaines de responsabilité incompatibles avec l'objectif de réduire le risque de fraude, d'erreur et de contournement des mesures de sécurité de l'information. |
| **5 Mesures de sécurité organisationnelles** | **5.4 Fonctions et responsabilités liées à la sécurité de l'information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence de demandes explicites de la part de la direction à tous les salariés et contractants d’appliquer les règles de sécurité conformément aux politiques et aux procédures en vigueur et absence de mesures visant à s'assurer que tout le personnel soit sensibilisé aux responsabilités liées à la sécurité de l'information et qu'il assume ces responsabilités. |
| **5 Mesures de sécurité organisationnelles** | **5.5 Relations avec les autorités** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence de collaboration avec les autorités compétentes afin d'assurer la bonne circulation de l'information à l'égard de la sécurité, et avec lequelles l'organisme peut collaborer avec les autorités légales, réglementaires et de surveillance compétentes. |
| **5 Mesures de sécurité organisationnelles** | **5.6 Relations avec des groupes de travail spécialisés** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence de relations avec des groupes de travail spécialisés ou des forums spécialisés dans la sécurité et avec des associations professionnelles, afin d'assurer la bonne circulation de l'information à l'égard de la sécurité. |
| **5 Mesures de sécurité organisationnelles** | **5.7 Intelligence des menaces** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'un système destiné à recueillir les informations relatives aux menaces pour la sécurité de l'information et de les analyser pour produire une intelligence des menaces. |
| **5 Mesures de sécurité organisationnelles** | **5.8 Sécurité de l'information dans la gestion de projet** | **Bonnes pratiques identifiées** |  |
| Présence d'un procède systématique à une analyse des exigences particulières de sécurité de l'information, dès la phase de spécification de projets de nouveaux systèmes d'information ou de modification de systèmes existants. |
| **Vulnérabilités enregistrées** |
| La prise en considération de la sécurité de l'information n'est pas intégrée aux activités de la gestion de projet. |
| **5 Mesures de sécurité organisationnelles** | **5.9 Inventaire des informations et des autres actifs associés** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.10 Utilisation correcte des actifs** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.11 Restitution des actifs** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.12 Classification de l'information** | **Bonnes pratiques identifiées** |  |
| Présence d'une classification des informations conformément aux besoins de l'organisation en termes de sécurité de l'information sur le plan de la confidentialité, de l'intégrité, de la disponibilité et des exigences des parties intéressées. |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.13 Marquage des informations** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| L'ensemble approprié de procédures pour le marquage de l’information, conformément au plan de classification de l’information adopté par l’organisation n'est plus élaboré ni mis en oeuvre. |
| **5 Mesures de sécurité organisationnelles** | **5.14 Transfert de l'information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.15 Contrôle d'accès** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.16 Gestion des identités** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.17 Informations d'authentification** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.18 Droits d'accès** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.19 Sécurité de l'information dans les relations avec les fournisseurs** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence des processus et des procédures pour la gestion les risques de sécurité de l'information qui sont associés à l'utilisation des produits ou services des fournisseurs. |
| **5 Mesures de sécurité organisationnelles** | **5.20 Prise en compte de la sécurité de l'information dans les accords conclus avec les fournisseurs** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence des exigences applicables liées à la sécurité de l'information dans les accords avec les fournisseurs ayant accès à l'information de l'organisation. |
| **5 Mesures de sécurité organisationnelles** | **5.21 Management de la sécurité de l'information dans la chaîne d'approvisionnement TIC** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence des processus et procédures destinés à traiter les risques de sécurité de l'information associés aux services informatiques et de télécommunication et à la chaîne d'approvisionnement des produits informatiques ou de télécommunication. |
| **5 Mesures de sécurité organisationnelles** | **5.22 Suivi, revue et gestion du changement des services fournisseurs** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence de la surveillance régulière, la revue, l'évaluation et la gestion des changements de pratiques du fournisseur en matière de sécurité de l'information et de prestation de services, afin de maintenir un niveau convenu de sécurité de l’information et de prestation de services, conformément aux accords conclus avec les fournisseurs. |
| **5 Mesures de sécurité organisationnelles** | **5.23 Sécurité de l'information dans l'utilisation de services en Nuage** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.24 Responsabilités et préparation de la gestion des incidents liés à la sécurité de l'information** | **Bonnes pratiques identifiées** |  |
| Présence de planification et de préparation de la gestion des incidents liés à la sécurité de l'information en procédant à la définition, à l'établissement et à la communication des processus, rôles et responsabilités dans le cadre de la gestion des incidents liés à la sécurité de l'information. |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.25 Appréciation des événements liés à la sécurité de l'information et prise de décision** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| L'organisation n' est pas en mesure d'apprécier les événements liés à la sécurité de l'information et de décider s'ils doivent être classés dans la catégorie des incidents liés à la sécurité de l'information (et selon quelle priorité). |
| **5 Mesures de sécurité organisationnelles** | **5.26 Réponse aux incidents liés à la sécurité de l'information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence des procédures documentées pour répondre aux incidents de sécurité de l'information. |
| **5 Mesures de sécurité organisationnelles** | **5.27 Tirer des enseignements des incidents liés à la sécurité de l'information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| L'organisation n'a pas profité des connaissances acquises à partir des incidents liés à la sécurité de l'information pour renforcer et améliorer l'environnement de contrôle et ainsi réduire la probabilité ou les conséquences d'incidents ultérieurs. |
| **5 Mesures de sécurité organisationnelles** | **5.28 Recueil de preuves** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.29 Sécurité de l'information durant une perturbation** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.30 Préparation des TIC pour la continuité d'activité** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence de la planification, des mis en œuvre, de la gestion et du teste de la préparation des TIC (Technologies de l'Information et de la Communication) pour les objectifs de continuité d'activité et des exigences de continuité des TIC. |
| **5 Mesures de sécurité organisationnelles** | **5.31 Identification des exigences légales, statutaires, réglementaires et contractuelles** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'identification, de documentation et de mise à jour les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences. |
| **5 Mesures de sécurité organisationnelles** | **5.32 Droits de propriété intellectuelle** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.33 Protection des enregistrements** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.34 Vie privée et protection des DCP** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **5 Mesures de sécurité organisationnelles** | **5.35 Revue indépendante de la sécurité de l'information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence de recours à des revues indépendantes de l'approche retenue par l'organisation pour gérer et mettre en œuvre la sécurité de l'information, y compris des personnes, processus et technologies. |
| **5 Mesures de sécurité organisationnelles** | **5.36 Conformité aux politiques et normes de sécurité de l'information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence de vérification régulière de la conformité à la politique de sécurité de l'information, aux politiques portant sur des thèmes et aux normes de l'organisation. |
| **5 Mesures de sécurité organisationnelles** | **5.37 Procédures d'exploitation documentées** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Les diverses procédures d'exploitation ne sont pas formellement décrites dans des documents aisément accessibles aux personnes concernées. |
| **6 Mesures de sécurité applicables aux personnes** | **6.1 Présélection** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Les références concernant tous les candidats à l'embauche avant qu'ils n'intègrent l'organisation puis de façon continue, conformément aux lois, aux réglementations et à l'éthique ne sont pas vérifiées. |
| **6 Mesures de sécurité applicables aux personnes** | **6.2 Conditions générales d'embauche** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Les contrats de travail ne précisent pas les responsabilités qui incombent au personnel et à l'organisation en matière de sécurité de l'information |
| **6 Mesures de sécurité applicables aux personnes** | **6.3 Sensibilisation, apprentissage et formation à la sécurité de l'information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Le personnel et les parties intéressées ne sont ni sensibilisés ni suivent un apprentissage et des formations relatives à la sécurité de l'information et ne reçoivent plus régulièrement des mises à jours des politiques et des procédures qui s'appliquent à leurs fonctions. |
| **6 Mesures de sécurité applicables aux personnes** | **6.4 Processus disciplinaire** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'un processus disciplinaire permettant de prendre des mesures à l'encontre du personnel et des autres parties intéressées qui ont commis une violation de la politique de sécurité de l'information. |
| **6 Mesures de sécurité applicables aux personnes** | **6.5 Responsabilités consécutivement à la fin ou à la modification du contrat de travail** | **Bonnes pratiques identifiées** |  |
| Présence d'une définition des responsabilités et des missions liées à la sécurité de l'information qui restent valables consécutivement à la fin ou à la modification du contrat de travail, avec veille à l'application de ces directives et information du personnel concerné et les autres parties intéressées. |
| **Vulnérabilités enregistrées** |
|  |
| **6 Mesures de sécurité applicables aux personnes** | **6.6 Engagements de confidentialité ou de non-divulgation** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Les engagements de confidentialité ou de non-divulgation ne sont ni identifiés, ni documentés, ni revus régulièrement et ni signés, conformément aux besoins de l'organisme en matière de protection de l'information, afin de gérer la confidentialité de l'information accessible au personnel ou à de tierces parties. |
| **6 Mesures de sécurité applicables aux personnes** | **6.7 Travail à distance** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| L'organisation n'a pas mis en œuvre des mesures de sécurité lorsque le personnel travaille à distance, pour protéger les informations consultées, traitées ou stockées en dehors des locaux de l'organisation |
| **6 Mesures de sécurité applicables aux personnes** | **6.8 Signalement des événements liés à la sécurité de l’information** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'un mécanisme proposé au personnel pour lui permettre de signaler dans les plus brefs délais les événements liés à la sécurité de l'information observés ou suspectés, par le biais des canaux appropriés. |
| **7 Mesures de sécurité physique** | **1. Périmètre de sécurité physique** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Les périmètres de sécurité servant à protéger les zones qui contiennent l'information sensible ou critique et les autres actifs associés ne sont pas définies. |
| **7 Mesures de sécurité physique** | **2. Contrôles physiques des accès** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **7 Mesures de sécurité physique** | **3. Sécurisation des bureaux, des salles et des équipements** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **7 Mesures de sécurité physique** | **4. Surveillance de la sécurité physique** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **7 Mesures de sécurité physique** | **5. Protection contre les menaces extérieures et Environnementales** | **Bonnes pratiques identifiées** |  |
| Présence d'une conception et d'une mis en place d'une protection contre les menaces physiques et environnementales telles que les catastrophes naturelles et autres menaces physiques volontaires ou non liées à l'infrastructure. |
| **Vulnérabilités enregistrées** |
|  |
| **7 Mesures de sécurité physique** | **6. Travail dans les zones sécurisées** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **7 Mesures de sécurité physique** | **7. Bureau propre et écran vide** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'une politique rédigée et concrétisée à l'aide de procédures, pour "bureau propre et à l'écran muet" et au matériel utilisateur laissé sans surveillance afin de réduire les risques d'accès non autorisé, les pertes et l'endommagement de l'information sur les bureaux, les écrans, les autres emplacements et dans les matériels ou équipements accessibles pendant et en dehors des heures normales de travail. |
| **7 Mesures de sécurité physique** | **8. Emplacement et protection du matériel** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Disposition du matériel non sécurisé ni protégé contre les risques liés à des menaces et dangers environnementaux et des possibilités d'accès non autorisé. |
| **7 Mesures de sécurité physique** | **9. Sécurité du matériel et des actifs hors des locaux** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **7 Mesures de sécurité physique** | **10. Supports de stockage** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **7 Mesures de sécurité physique** | **11. Services généraux** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **7 Mesures de sécurité physique** | **12. Sécurité du câblage** | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'une de protection des câbles électriques transportant des données ou supportant les services d'information de façon à empêcher la perte, l'endommagement, le vol ou la compromission de l'information et des autres actifs associés et l'interruption des activités de l'organisation. |
| **7 Mesures de sécurité physique** | 13. Maintenance du matériel | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Le matériel n'est pas entretenu correctement de manière à empêcher la perte, l'endommagement, le vol ou la compromission de l'information et des autres actifs associés et l'interruption des activités de l'organisation. |
| **7 Mesures de sécurité physique** | 14. Mise au rebut ou recyclage sécurisé(e) du matériel | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **8 Mesures de sécurité technologiques** | 1.Terminaux utilisateurs | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'une politique portant sur le thème de la configuration et de la manipulation sécurisées des terminaux utilisateurs finaux, afin de protéger toute information stockée sur un terminal utilisateur final, traitée par ou accessible via ce type d'appareil |
| **8 Mesures de sécurité technologiques** | 2.Privilèges d'accès | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **8 Mesures de sécurité technologiques** | 3.Restriction d'accès à l'information | **Bonnes pratiques identifiées** |  |
| L'accès à l'information et aux autres actifs associés est restreint conformément à la politique ci-dessus (portant sur le thème du contrôle d'accès). |
| **Vulnérabilités enregistrées** |
|  |
| **8 Mesures de sécurité technologiques** | 4.Accès au code source | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **8 Mesures de sécurité technologiques** | 5.Authentification sécurisée | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **8 Mesures de sécurité technologiques** | 6.Dimensionnement | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Absence d'un processus permettant de surveiller l'utilisation des ressources et de l'ajuster conformément au dimentionnement actuel et prévu |
| **8 Mesures de sécurité technologiques** | 7.Protection contre les programmes malveillants | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
| Aucune protection contre les programmes malveillants, appuyée par la sensibilisation des utilisateurs concernés n'est mis en place. |
| **8 Mesures de sécurité technologiques** | 8.Gestion des vulnérabilités techniques | **Bonnes pratiques identifiées** |  |
|  |
| **Vulnérabilités enregistrées** |
|  |
| **8 Mesures de sécurité technologiques** | 9.Gestion de la configuration | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 10.Suppression d'information | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 11.Masquage des données | **Bonnes pratiques identifiées** |  |
| Présence de procédures de masquage des données conformément à la politique de l'organisation portant sur le thème du contrôle d'accès et aux exigences métier, tout en prenant en compte les exigences d'ordre légal. |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 12.DLP | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 13.Sauvegarde des informations | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Absence d'un plan de sauvegarde, couvrant l'ensemble des objets (programmes et données) à sauvegarder et la fréquence des sauvegardes. |  |
| **8 Mesures de sécurité technologiques** | 14.Redondance des moyens de traitement de l'information | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| La criticité des différents éléments de l'architecture (y compris des systèmes périphériques tels que systèmes ou robots de sauvegarde, serveurs d'impression ou équipement central d'impression, etc.) pour mettre en évidence les besoins de continuité de service n'est plus analysée. |  |
| **8 Mesures de sécurité technologiques** | 15.Journalisation | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 16.Activités de surveillance | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 17.Synchronisation des horloges | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 18.Utilisation de programmes utilitaires à privilèges | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 19.Installation de logiciels sur des systèmes en exploitation | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 20.Mesures liées aux réseaux | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Les réseaux sont ni gérés ni contrôlés afin de garantir la protection de l'information contenue dans les systèmes et les applications |  |
| **8 Mesures de sécurité technologiques** | 21.Sécurité des services en réseau | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Absence de la surveillance des mécanismes de sécurité, des niveaux de services et de leurs exigences relatives aux sevices réseaux |  |
| **8 Mesures de sécurité technologiques** | 22.Cloisonnement des réseaux | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Absence de cloisonnement, des groupes de services d'information, d'utilisateurs et de systèmes d'information dans les réseaux |  |
| **8 Mesures de sécurité technologiques** | 23.Filtrage Internet | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 24.Utilisation de la cryptographie | **Bonnes pratiques identifiées** |  |
| Présence des règles relatives à l'utilisation de la cryptographie et à la gestion des clés cryptographiques |  |
| **Vulnérabilités enregistrées** |  |
|  |  |
| **8 Mesures de sécurité technologiques** | 25.Cycle de vie de développement sécurisé | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Absence des règles de développement sécurisé des logiciels et des systèmes, afin de s'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement sécurisé des logiciels et des systèmes. |  |
| **8 Mesures de sécurité technologiques** | 26.Exigences de sécurité des applications | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Absence d'identification et de définition de exigences de sécurité de l'information, lors du développement ou de l'achat d'applications. |  |
| **8 Mesures de sécurité technologiques** | 27.Principes d'ingénierie et d'architecture système sécurisée | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Absence de documentation, de mise à jour et de l'appliquation des principes d'ingénierie de la sécurité des systèmes à toutes les activités de développement de systèmes d'information. |  |
| **8 Mesures de sécurité technologiques** | 28.Codage sécurisé | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Absence d'applicationdes principes de codage sécurisé au développement de logiciels, afin de s'assurer que le logiciel est développé dans un souci de sécurité et réduire ainsi le nombre de vulnérabilités potentielles du logiciel en termes de sécurité de l'information. |  |
| **8 Mesures de sécurité technologiques** | 29.Tests de sécurité dans le développement et l'acceptation | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| L'organisation n'a pas défini des processus pour les tests de sécurité. |  |
| **8 Mesures de sécurité technologiques** | 30.Développement externalisé | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| L'organisation ni dirige , ni contrôle et ni passe en revue les activités liées au développement du système externalisé. |  |
| **8 Mesures de sécurité technologiques** | 31.Séparation des environnements de développement, de test et de production | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Les environnements de développement et de tests ne sont pas séparés de l'environnement de production. |  |
| Absence d'un environnement de développement sécurisé prenant en compte la sensibilité des données qui seront traitées, stockées et transmises par les systèmes ou applications développés. |  |
| **8 Mesures de sécurité technologiques** | 32.Gestion des changements | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Aucun changement n'est soumis à une procédure de gestion des changement afin de préserver la sécurité de l'information lors de l'exécution des changements |  |
| Absence des procédures de contrôle des changements apportés aux moyens de traitement de l'information. |  |
| Le contrôle des versions à chaque mise à jour et une trace de tous les changements et évolutions n'est pas maintenu |  |
| **8 Mesures de sécurité technologiques** | 33.Informations relatives aux tests | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
| Absence de procédures afin de sélectionner, de protéger et de gérer les informations relatives aux tests. |  |
| **8 Mesures de sécurité technologiques** | 34.Protection des systèmes d'information en cours d'audit et de test | **Bonnes pratiques identifiées** |  |
|  |  |
| **Vulnérabilités enregistrées** |  |
|  |  |

* 1. Vulnérabilités non acceptable enregistrées

|  |  |
| --- | --- |
|  | |
| **${RowNumber#1}** | **Référence de la vulnérabilité:**  1B01-01 |
| **Description :**  Absence d'une structure opérationnelle et de l'organisation de la gestion de la sécurité : RSSI et correspondants ou responsables locaux, rôles et responsabilités respectifs et vis-à-vis des responsables opérationnels. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1B01-01** |
| **Composante(s) du SI impactée(s) :**  5.2 |
| **Recommandation :**  Etablir dans le détail la structure et l'organisation de la gestion de la sécurité : RSSI et correspondants ou responsables locaux, rôles et responsabilités respectifs et vis-à-vis des responsables opérationnels, et cette structure doit etre opérationnelle. |
|  |
| **${RowNumber#2}** | **Référence de la vulnérabilité:**  1B01-08 |
| **Description :**  Absence de relations avec des groupes de travail spécialisés ou des forums spécialisés dans la sécurité et avec des associations professionnelles, afin d'assurer la bonne circulation de l'information à l'égard de la sécurité. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1B01-08** |
| **Composante(s) du SI impactée(s) :**  5.6 |
| **Recommandation :**  Etablir et entretenir des relations avec des groupes de travail spécialisés ou des forums spécialisés dans la sécurité et avec des associations professionnelles, afin d'assurer la bonne circulation de l'information à l'égard de la sécurité. |
|  |
| **${RowNumber#3}** | **Référence de la vulnérabilité:**  1B01-10 |
| **Description :**  Absence d'un système destiné à recueillir les informations relatives aux menaces pour la sécurité de l'information et de les analyser pour produire une intelligence des menaces. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1B01-10** |
| **Composante(s) du SI impactée(s) :**  5.7 |
| **Recommandation :**  Mettre en place un système destiné à recueillir les informations relatives aux menaces pour la sécurité de l'information et de les analyser pour produire une intelligence des menaces. |
|  |
| **${RowNumber#4}** | **Référence de la vulnérabilité:**  1B01-13 |
| **Description :**  La prise en considération de la sécurité de l'information n'est pas intégrée aux activités de la gestion de projet. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1B01-13** |
| **Composante(s) du SI impactée(s) :**  5.8 |
| **Recommandation :**  Intégrer la sécurité de l'information aux activités de gestion de projet de l'organisation. |
|  |
| **${RowNumber#5}** | **Référence de la vulnérabilité:**  1B05-01 |
| **Description :**  Absence de cloisonnement, des groupes de services d'information, d'utilisateurs et de systèmes d'information dans les réseaux |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1B05-01** |
| **Composante(s) du SI impactée(s) :**  8.22 |
| **Recommandation :**  Cloisonné, dans les réseaux de l'organisation, les groupes de services d'information, d'utilisateurs et de systèmes d'information |
|  |
| **${RowNumber#6}** | **Référence de la vulnérabilité:**  1B09-01 |
| **Description :**  Les engagements de confidentialité ou de non-divulgation ne sont ni identifiés, ni documentés, ni revus régulièrement et ni signés, conformément aux besoins de l'organisme en matière de protection de l'information, afin de gérer la confidentialité de l'information accessible au personnel ou à de tierces parties. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1B09-01** |
| **Composante(s) du SI impactée(s) :**  6.6 |
| **Recommandation :**  Elaboration de documents, revus reguliairement et signés pour des engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisation en matière de protection de l'information, afin de gérer la confidentialité de l'information accessible au personnel ou à de tierces parties. |
|  |
| **${RowNumber#7}** | **Référence de la vulnérabilité:**  1C03-01 |
| **Description :**  Le personnel et les parties intéressées ne sont ni sensibilisés ni suivent un apprentissage et des formations relatives à la sécurité de l'information et ne reçoivent plus régulièrement des mises à jours des politiques et des procédures qui s'appliquent à leurs fonctions. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1C03-01** |
| **Composante(s) du SI impactée(s) :**  6.3 |
| **Recommandation :**  Mettre en place une organisation telle que le personnel de l'organisation et les parties intéressées soient sensibilisés et suivent un apprentissage et des formations à la sécurité de l'information adaptés, et qu'ils reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leur fonction. |
|  |
| **${RowNumber#8}** | **Référence de la vulnérabilité:**  1F02-01 |
| **Description :**  Absence des exigences applicables liées à la sécurité de l'information dans les accords avec les fournisseurs ayant accès à l'information de l'organisation. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1F02-01** |
| **Composante(s) du SI impactée(s) :**  5.20 |
| **Recommandation :**  Etablir des exigences applicables liées à la sécurité de l'information dans les accords avec les fournisseurs ayant accès à l'information de l'organisation. |
|  |
| **${RowNumber#9}** | **Référence de la vulnérabilité:**  1F03-01 |
| **Description :**  Absence des processus et procédures destinés à traiter les risques de sécurité de l'information associés aux services informatiques et de télécommunication et à la chaîne d'approvisionnement des produits informatiques ou de télécommunication. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1F03-01** |
| **Composante(s) du SI impactée(s) :**  5.21 |
| **Recommandation :**  Etablir et mettre en oeuvre des processus et procédures destinés à traiter les risques de sécurité de l'information associés aux services informatiques et de télécommunication et à la chaîne d'approvisionnement des produits informatiques ou de télécommunication. |
|  |
| **${RowNumber#10}** | **Référence de la vulnérabilité:**  1F04-01 |
| **Description :**  Absence de la surveillance régulière, la revue, l'évaluation et la gestion des changements de pratiques du fournisseur en matière de sécurité de l'information et de prestation de services, afin de maintenir un niveau convenu de sécurité de l’information et de prestation de services, conformément aux accords conclus avec les fournisseurs. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **1F04-01** |
| **Composante(s) du SI impactée(s) :**  5.22 |
| **Recommandation :**  Mettre en oeuvre un processus de surveillance régulière, de revue, d'évaluation et de gestion des changements de pratiques du fournisseur en matière de sécurité de l'information et de prestation de services, afin de maintenir un niveau convenu de sécurité de l’information et de prestation de services, conformément aux accords conclus avec les fournisseurs. |
|  |
| **${RowNumber#11}** | **Référence de la vulnérabilité:**  2C01-01 |
| **Description :**  Disposition du matériel non sécurisé ni protégé contre les risques liés à des menaces et dangers environnementaux et des possibilités d'accès non autorisé. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **2C01-01** |
| **Composante(s) du SI impactée(s) :**  7.8 |
| **Recommandation :**  Disposer le matériel pour qu'il soit sécurisé et protégé contre les risques liés à des menaces et dangers environnementaux et des possibilités d'accès non autorisé. |
|  |
| **${RowNumber#12}** | **Référence de la vulnérabilité:**  4A01-01 |
| **Description :**  Les diverses procédures d'exploitation ne sont pas formellement décrites dans des documents aisément accessibles aux personnes concernées. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **4A01-01** |
| **Composante(s) du SI impactée(s) :**  5.37 |
| **Recommandation :**  Décrir formellement les diverses procédures d'exploitation dans des documents aisément accessibles aux personnes concernées. |
|  |
| **${RowNumber#13}** | **Référence de la vulnérabilité:**  4A02-01 |
| **Description :**  Aucune protection contre les programmes malveillants, appuyée par la sensibilisation des utilisateurs concernés n'est mis en place. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **4A02-01** |
| **Composante(s) du SI impactée(s) :**  8.7 |
| **Recommandation :**  Mettre en place une protection contre les programmes malveillants, appuyée par la sensibilisation des utilisateurs concernés. |
|  |
| **${RowNumber#14}** | **Référence de la vulnérabilité:**  4A03-01 |
| **Description :**  Absence d'un plan de sauvegarde, couvrant l'ensemble des objets (programmes et données) à sauvegarder et la fréquence des sauvegardes. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **4A03-01** |
| **Composante(s) du SI impactée(s) :**  8.13 |
| **Recommandation :**  Etablir un plan de sauvegarde, couvrant l'ensemble des objets (programmes et données) à sauvegarder et la fréquence des sauvegardes. |
|  |
| **${RowNumber#15}** | **Référence de la vulnérabilité:**  4C01-04 |
| **Description :**  Le matériel n'est pas entretenu correctement de manière à empêcher la perte, l'endommagement, le vol ou la compromission de l'information et des autres actifs associés et l'interruption des activités de l'organisation. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **4C01-04** |
| **Composante(s) du SI impactée(s) :**  7.13 |
| **Recommandation :**  Assurer correctement l'entretient du matériel de manière à empêcher la perte, l'endommagement, le vol ou la compromission de l'information et des autres actifs associés et l'interruption des activités de l'organisation. |
|  |
| **${RowNumber#16}** | **Référence de la vulnérabilité:**  4D02-04 |
| **Description :**  Absence d'un mécanisme proposé au personnel pour lui permettre de signaler dans les plus brefs délais les événements liés à la sécurité de l'information observés ou suspectés, par le biais des canaux appropriés. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **4D02-04** |
| **Composante(s) du SI impactée(s) :**  6.8 |
| **Recommandation :**  Etablir un mécanisme et proposé le au personnel pour lui permettre de signaler dans les plus brefs délais les événements liés à la sécurité de l'information observés ou suspectés, par le biais des canaux appropriés. |
|  |
| **${RowNumber#17}** | **Référence de la vulnérabilité:**  7B01-01 |
| **Description :**  Absence des règles de développement sécurisé des logiciels et des systèmes, afin de s'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement sécurisé des logiciels et des systèmes. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **7B01-01** |
| **Composante(s) du SI impactée(s) :**  8.25 |
| **Recommandation :**  Définir les règles de développement sécurisé des logiciels et des systèmes, afin de s'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement sécurisé des logiciels et des systèmes. |
|  |
| **${RowNumber#18}** | **Référence de la vulnérabilité:**  7B04-01 |
| **Description :**  Absence d'un environnement de développement sécurisé prenant en compte la sensibilité des données qui seront traitées, stockées et transmises par les systèmes ou applications développés. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **7B04-01** |
| **Composante(s) du SI impactée(s) :**  8.31 |
| **Recommandation :**  Etablir un environnement de développement sécurisé prenant en compte la sensibilité des données qui seront traitées, stockées et transmises par les systèmes ou applications développés. |
|  |
| **${RowNumber#19}** | **Référence de la vulnérabilité:**  8A01-01 |
| **Description :**  Absence d'identification, de documentation et de mise à jour les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **8A01-01** |
| **Composante(s) du SI impactée(s) :**  5.31 |
| **Recommandation :**  Identifier, documenter et tenir à jour les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences. |
|  |
| **${RowNumber#20}** | **Référence de la vulnérabilité:**  8C02-01 |
| **Description :**  Absence de vérification régulière de la conformité à la politique de sécurité de l'information, aux politiques portant sur des thèmes et aux normes de l'organisation. |
| **Preuve(s) d’audit :**  Discution concernant le questionnaire MEHARI **8C02-01** |
| **Composante(s) du SI impactée(s) :**  5.36 |
| **Recommandation :**  Vérifier régulièrement la conformité à la politique de sécurité de l'information, aux politiques portant sur des thèmes et aux normes de l'organisation. |
|  |
|  | |

* 1. Détails audit technique

Description dans les Rapports d’audit Technique.

1. Appréciation des risques
   1. La démarche d’appréciation des risques adoptée

Nous nous proposons d’effectuer une analyse des risques menaçant la sécurité du système d’information du **IORT** Méhari.

Méhari est une méthode harmonisée d’analyse de risques, développée par le CLUSIF (Club de la Sécurité de l'Information Français) depuis 1995 et elle est dérivée des méthodes Melissa et Marion. Elle a été initialement conçue pour aider les DSI dans leur tâche de management de la sécurité de l’information. Cette présentation générale leur est ainsi principalement destinée, mais elle s’adresse également aux auditeurs ou aux gestionnaires de risques qui partagent, dans une large mesure, les mêmes préoccupations. L’objectif de Méhari est donc de fournir une gamme d’outils adaptés au management de la sécurité. Or, ceux-ci se concrétisent par un ensemble d’actions qui ont chacune des objectifs particuliers. Parmi les actes de management, nous citons :

* L’élaboration de plans de sécurité, ou de schémas directeurs
* La mise en place de règle ou politiques de sécurité ;
* La conduite de diagnostics, rapides ou approfondis sur l’état de la sécurité ;
* L’évaluation et le management des risques ;
* La gestion de la sécurité dans la conduite de projets de développement ;
* La sensibilisation ((La bonne utilisation des mots des passes, la défense contre l’attaque de phishing, les Ransomwares, le bureau propre et l’écran verrouillé, etc…) et la formation à la sécurité ;
* Le pilotage de la sécurité et le contrôle des actions décidées.

Ces différents actes de management et leurs variantes ne sont pas exclusifs mais au contraire des actions pouvant être menées simultanément ou successivement, par des entités distinctes ou par la même entité, en fonction des besoins ponctuels ou permanents, indépendamment ou faisant partie d’un programme d’ensemble.

En outre, les mêmes actes de management peuvent être conduits différemment selon

* La maturité de l’entreprise de son personnel en termes de sécurité,
* La volonté d’impliquer plus ou moins fortement les managers opérationnels dans les prises de décision concernant la sécurité de l’information
* La culture de l’entreprise : hiérarchique ou, au contraire, décentralisée et responsabilisant.
  1. Présentation du processus d’appréciation du risque en sécurité de l’information

L’appréciation du risque se découpe en deux activités :

L’analyse de risque, elle-même segmentée en deux sous-activités (l’identification et l’estimation des risques) et l’évaluation du risque.

* En premier lieu, l’identification des risques définit les actifs : ceux primaires, c’est-à-dire les activités métier et l’information, et ceux secondaires, comme un serveur, avec pour chacun son propriétaire et sa valeur selon une échelle commune.
* Ensuite, on recherche les menaces, les vulnérabilités et les conséquences, c’est-à-dire les dommages possibles quand une menace exploite une vulnérabilité sur les actifs.
* Enfin, on liste les mesures de sécurité existantes.
* L’estimation des risques consiste à évaluer les conséquences et les probabilités d’occurrence des menaces, analyse - de risques.

L’évaluation du risque correspond à la prise de décision par comparaison des niveaux de risque.



**Processus d’Appréciation du Risque en Sécurité de l’Information**

* 1. Evaluation des Risques

En partant de la méthodologie Méhari stipulant que la sécurité est mise en œuvre à travers de Services de sécurité (Contrôle d’accès par exemple), l’analyse des vulnérabilités consiste alors à faire un diagnostic de la qualité des services de sécurité.

L’analyse que nous nous proposons d’effectuer est orientée scénarios. Un scénario de risque est la description d’un dysfonctionnement et de la manière dont ce dysfonctionnement peut survenir. Le dysfonctionnement comprend lui-même un sinistre, c'est-à-dire des détériorations directes et des conséquences indirectes de ce sinistre. Dans notre démarche, nous utilisons la base de connaissance de scénarios de risque proposée par la méthodologie Méhari.

L'objectif de l’analyse d’un scénario de risque est d’évaluer deux paramètres caractéristiques du risque encouru par l’organisme dans l'hypothèse d'occurrence d'un tel scénario. Ces paramètres sont:

* **La potentialité du risque** qui représente, en quelque sorte, sa probabilité d'occurrence, bien que cette occurrence ne soit pas modélisable en termes de probabilité. Cette potentialité est en fonction du contexte et des mesures de sécurité mises en place.
* **L'impact du risque** sur l'organisme, qui représente la gravité des conséquences directes et indirectes qui découlent de l'occurrence du risque. Cet impact est fonction de l'impact maximum ou intrinsèque, défini lors de la classification en termes d'enjeux ou de niveau dans l'échelle de valeurs, éventuellement réduit par la mise en œuvre de mesures de sécurité adaptées.

Afin de quantifier le risque correspondant au scénario analysé, les évaluations de la potentialité et de l’impact seront faites sur une échelle ayant 4 niveaux :

* **Identification des menaces**

Il est important d’identifier les potentielles faiblesses associées à chacun des processus supportant l’information critique de l’organisation. Ces faiblesses peuvent être exploitées par des menaces et avoir un impact négatif sur l’information (divulgation, destruction, etc.).

* **Identification des Impacts**

Le niveau d’impact est défini selon les exigences internes, externes, réglementaires et légales du cadre dans lequel évolue l’organisation. Dans la partie qui suit, nous décrivons ces niveaux d’impacts:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact** | 1 | 2 | 3 | 4 |
| **Gravité** | **Non significatif** | **Important** | **Très grave** | **Vitale** |
| **Description** | A ce niveau les dommages encourus n'ont pratiquement pas d'impact sur les résultats de l'entité ni sur son image, même si certaines personnes sont fortement impliquées dans le rétablissement de la situation d'origine. | Important Il s'agit là de sinistres ayant un impact notable au niveau des opérations de l'entité, de ses résultats ou de son image, mais restant globalement supportables | Il s'agit là d'impact très grave au niveau de l'entité, sans que son avenir soit compromis. En termes financiers, cela peut amputer sérieusement le résultat de l'exercice, sans que les actionnaires se dégagent massivement. En termes d'image, on considérera souvent à ce niveau une perte d'image dommageable qu'il faudra plusieurs mois à remonter, même si l'impact financier ne peut être évalué avec précision. Des sinistres conduisant à une désorganisation notable de l'entreprise pendant une durée de plusieurs mois seront aussi souvent évalués à ce niveau. | A ce niveau l'impact est extrêmement grave et met en danger l'existence même ou la survie de l'entité ou de l'une de ses activités majeures. En cas de survie de l'entreprise ou de l'organisme, les séquelles sont importantes et durables. |
| **Financier** | Perte négligeable | Perte importante | Perte majeure | Perte vitale |
| **Engagement vis à vis parties intéressées** | Faible nuisance | Dégradation du service vis-à-vis parties intéressées | Blocage d’un système ou Perte d’une donnée des parties intéressées | Blocage des systèmes ou Perte de la totalité des données des parties intéressées. |
| **Juridique** | Faible impact | Non-respect de la réglementation nationale | Infraction majeure à la législation | Sanction judiciaire |
| **Sécurité des personnes** | Impact marginal | Inconfort pour un individu | Risque pour la sécurité d’un individu | Risque pour la sécurité d'un groupe de personnes |

* **Identification de la Potentialité**

La gravité du risque ne dépend pas seulement du niveau de son impact sur la Confidentialité, l’Intégrité et la Disponibilité des actifs, mais aussi de sa Potentialité.

**La Potentialité (P):** C’est la probabilité qu'un événement se produise avec un impact indésirable. Si l’événement est très probable, alors le niveau du risque va être plus élevé. Le niveau de potentialité devrait se baser sur l’historique de l'occurrence de l'événement indésirable ou à partir de statistiques disponibles. Ce facteur est essentiel pour la poursuite de l’analyse du risque car il permet de déterminer la gravité du risque.

|  |  |  |
| --- | --- | --- |
| **Description** | **Durée** | **Valeur** |
| **Très peu probable** | 1 fois tous les 5 ans et plus | **1** |
| **Peu probable** | 1 à 2 fois tous les 2 ans | **2** |
| **Probable** | 2 mois < 1 fois < 6 mois | **3** |
| **Très probable** | > 1 fois tous les deux mois | **4** |

* **Maturité des contrôles existants**

Le but de cette phase est d’analyser la maturité des contrôles déjà existants, afin de minimiser la probabilité de l’exploit d’une vulnérabilité ou réduire son impact. Les contrôles existants à analyser doivent couvrir :

Les méthodes organisationnelles et opérationnelles, attestées par un plan d’exploitation, des manuels de procédures, des documents ou des directives de politiques de sécurité.

Les méthodes techniques tels que la segmentation des réseaux par les VLANs, les ACLs sur les routeurs, les Firewalls périmétriques ou de zones, les Systèmes de Détection d’Intrusion (IDS), les techniques cryptographiques et les VPNs, la vidéosurveillance, le contrôle d’accès etc.

Il y a 8 domaines utilisés au niveau de Mehari Standard 2.1 du 10 Aout 2022 à savoir:

1. Organisation de la sécurité
2. Sécurité des Sites
3. Sécurité des systèmes et de leur architecture
4. Exploitation et administration des systèmes
5. Sécurité applicative et continuité de l'activité
6. Protection des postes de travail utilisateurs
7. Sécurité des projets et développements applicatifs
8. Conformité aux exigences légales et contractuelles

* **Calcul de risque**

Avec la méthode Méhari, après avoir calculé l’impact et la potentialité intrinsèques ainsi que la maturité des contrôles existants (pas de formule générale mais pour chaque risque il y aura une formule dédiée suivant le nombre des mesures de réduction de risque possible et leurs type (Dissuasive, Préventive, Confinement, Palliative). Une fois l’impact et la potentialité calculés, le risque sera comme suit :

Risque calculé sera en fonction de deux facteurs I et P calculé suivant la grille suivante :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact** | | |  | |
|  |  | |  | |
| **4** | **2** | **3** | **4** | **4** |
| **3** | **2** | **3** | **3** | **4** |
| **2** | **1** | **2** | **2** | **3** |
| **1** | **1** | **1** | **1** | **2** |
|  | **1** | **2** | **3** | **4** |
|  | **Potentialité** | | | |

* **Résultats globaux de l’appréciation des risques :**

Sur 212 scénarios de risque, on constate :

* ${risk\_4\_nbr} scénarios de gravité 4
* ${risk\_3\_nbr} scénarios de gravité 3
* ${risk\_2\_nbr} scénarios de gravité 2
* ${risk\_1\_nbr} scénarios de gravité 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Panorama des risques** | | | | | |
|  | **Impact** | | |  | |
|  | 4 | ${R41} | ${R42} | ${R43} | ${R44} |
|  | 3 | ${R31} | ${R32} | ${R33} | ${R34} |
|  | 2 | ${R21} | ${R22} | ${R23} | ${R24} |
|  | 1 | ${R11} | ${R12} | ${R13} | ${R14} |
|  | | 1 | 2 | 3 | 4 |
|  | |  | | **Potentialité** | |

* **Panorama des gravités de scénarios par rapport à DIC**

MET ICI screenshot de **Panorama des gravités de scénarios par rapport à DIC**

* **Evaluation des impacts intrinsèques et choix des processus :**

Nous avons sélectionné pour cette appréciation les processus mentionnés dans les tableaux T1 et T2.

Pour chaque processus, on définit l’impact intrinsèque sur les actifs de type données (Tableau T1) utilisées par ce processus puis sur les services (Tableau T2)

MET ICI screenshot de **T1**

Tableau 1: Classifications des données

MET ICI screenshot de **T2**

Tableau 2: Classifications des Services

Ce qui donne le tableau récapitulatif d’impact intrinsèque suivant

MET ICI screenshot de tableau de classification

Tableau 3: tableau récapitulatif des impacts intrinsèques

**Qualité de service de réduction des risques (Vue d’ensemble)**

|  |  |  |
| --- | --- | --- |
| **N°** | **Domaine** | **Note** |
| 1 | Organisation de la sécurité (1 Org) |  |
| 2 | Sécurité physique (2 Phy) |  |
| 3 | Sécurité des systèmes et de leur architecture (3 Sys) |  |
| 4 | Exploitation des systèmes d'information et de communication (4 Ope) |  |
| 5 | Sécurité applicative et continuité de l'activité (5 App) |  |
| 6 | Protection des postes de travail utilisateurs (6 Mic) |  |
| 7 | Sécurité des projets et développements applicatifs (7 Dev) |  |
| 8 | Conformité aux exigences légales et contractuelles (8 CEX) |  |

* **Exposition naturelle aux différents types des événements :**

On adoptera les valeurs de l’exposition naturelle standard de CLUSIQ:

|  |  |  |  |
| --- | --- | --- | --- |
| **Tableau des événements : types et exposition naturelle** | | |  |
| ***Type*** | ***Code type*** | ***Événement*** | ***Exposition naturelle standard CLUSIQ*** |
| Absence de personnel | AB.P | Absence accidentelle de personnel interne ou de partenaire |  |
| Absence ou indisponibilité accidentelle de service | AB.S | Absence de service : Énergie |  |
| Absence de service : défaillance ou indisponibilité du fournisseur d'accès à Internet |  |
| Absence de service : Impossibilité d'accès aux locaux |  |
| Absence de maintenance ou maintenance impossible |  |
| Accident grave d'environnement | AC.E | Incendie, Inondation, foudroiement, … |  |
| Accident matériel | AC.M | Panne d'équipement |  |
| Panne d'équipement de servitude |  |
| Erreur matérielle ou de comportement du personnel | ER.P | Perte ou oubli de document ou de media |  |
| Erreur de manipulation ou dans le suivi d'une procédure |  |
| Erreur de saisie ou de frappe |  |
| Incident dû à l'environnement | IC.E | Dégât dû au vieillissement ou à la pollution |  |
| Dégât externes divers : dégâts des eaux, surcharge électrique, etc. |  |
| Incident logique ou fonctionnel | IF.L | Incident d'exploitation |  |
| Bug bloquant dans un logiciel système, middleware, applicatif ou un progiciel |  |
| Logiciel malveillant ou virus |  |
| Malveillance menée par voie logique ou fonctionnelle | MA.L | Attaque en blocage de comptes |  |
| Effacement volontaire ou pollution massive de configurations systèmes |  |
| Effacement volontaire direct de supports logiques ou physiques |  |
| Falsification logique (données ou fonctions) |  |
| Création de faux (messages ou données) |  |
| Rejeu de transaction |  |
| Saturation malveillante d'équipements informatiques ou réseaux |  |
| Destruction logique totale (fichiers et leurs sauvegardes) |  |
| Détournement logique de fichiers ou données (téléchargement ou copie) |  |
| Malveillance menée par voie physique | MA.P | Manipulation ou falsification matérielle d'équipement |  |
| Terrorisme |  |
| Vandalisme |  |
| Vol physique |  |
| Procédures non conformes | PR.N | Procédures inadéquates |  |
| Procédures inappliquées par manque de moyens |  |
| Procédures inappliquées par méconnaissance |  |
| Procédures inappliquées volontairement |  |

* **Vue détaillée de risques les plus critiques**

MET ICI liste de tableau des scéanrios de risque(max Top 20)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID risque | ***LIBELLÉ*** | **Sélection** | **Type AEM** | **Type DICE** | **Impact Intrins.** | **Exposition** | **Grav. Intrins.** | **Dissuasion** | **Prévention** | **Confinement** | **Palliation** | **I calculé** | **P calculée** | **Gravité calculée** |
|  |  | | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

* 1. Identification des menaces, des vulnérabilités et des impacts des processus traités

Le tableau suivant fournit :

* L’impact/conséquences d’exploitation des vulnérabilités associées
* La complexité d’exploitation des vulnérabilités associées
* La probabilité d’occurrence des menaces associées
* Une estimation de la gravité du risque (la gravité du risque étant une résultante des facteurs suscités)

|  |
| --- |
| **Scénario du risque :** |
| **Description :** |
| **Référence(s) de(s) la vulnérabilité(s) :** |
| **Composante(s) du SI impactée(s) :** |
| **Impact(s)/Conséquence(s) d’exploitation des vulnérabilités associées :** |
| **Complexité d’exploitation de(s)s vulnérabilité(s) :** |
| **Gravité du risque :** |
| **Recommandation :** |
| **Complexité de mise en œuvre de la recommandation :** |

1. Plan d’action

Durant le reste de ce rapport, nous allons préparer et de mettre en œuvre une stratégie de sécurité cohérente et ciblée. Ce rapport sera mis à jour lors des audits de la seconde et de la troisième année tenant compte du taux de réalisation des mesures qui ont été adoptées depuis le dernier audit réalisé et des insuffisances enregistrées dans l’application de ses recommandations, ainsi que des résultats de l’audit de l’année en cours,

**Plan d’action cadre s’étalant sur trois (03) années**

Nous allons présenter dans cette partie les actions à mener en urgence pour la sécurisation du SI de l’ XXXXX

|  |  |
| --- | --- |
| Très urgente | A réaliser dans la 1ère année |
| Urgente | A réaliser dans la 2ème année |
| Normale | A réaliser dans la 3ème année |

* 1. Le plan d’action

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Projet** | **Action** | **Priorité** | **Responsable de l’action** | **Charge (H/J)** | **Planification** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.1 :Etablir dans le détail la structure et l'organisation de la gestion de la sécurité : RSSI et correspondants ou responsables locaux, rôles et responsabilités respectifs et vis-à-vis des responsables opérationnels, et cette structure doit etre opérationnelle.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.2 :Etablir des exigences applicables liées à la sécurité de l'information dans les accords avec les fournisseurs ayant accès à l'information de l'organisation.** | **Trés Urgent** | **Responsable SSI** | **10** | **Fin de 2024** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.3 :Etablir et mettre en oeuvre des processus et procédures destinés à traiter les risques de sécurité de l'information associés aux services informatiques et de télécommunication et à la chaîne d'approvisionnement des produits informatiques ou de télécommunication.** | **Trés Urgent** | **Responsable SSI** | **10** | **Fin de 2024** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.4 :Mettre en oeuvre un processus de surveillance régulière, de revue, d'évaluation et de gestion des changements de pratiques du fournisseur en matière de sécurité de l'information et de prestation de services, afin de maintenir un niveau convenu de sécurité de l’information et de prestation de services, conformément aux accords conclus avec les fournisseurs.** | **Trés Urgent** | **Responsable SSI** | **10** | **Fin de 2024** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.5 :Assurer que l'organisation soit en mesure d'apprécier les événements liés à la sécurité de l'information et de décider s'ils doivent être classés dans la catégorie des incidents liés à la sécurité de l'information (et selon quelle priorité).** | **Normal** | **DSI** | **14** | **Fin de 2026** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.6 :Etablir des procédures documentées pour répondre aux incidents de sécurité de l'information.** | **Normal** | **DSI** | **14** | **Fin de 2026** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.7 :Assurer aue l'organisation tire profit des connaissances acquises à partir des incidents liés à la sécurité de l'information pour renforcer et améliorer l'environnement de contrôle et ainsi réduire la probabilité ou les conséquences d'incidents ultérieurs.** | **Normal** | **DSI** | **14** | **Fin de 2026** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.8 :La définition des rôles et responsabilités doit garantit une séparation des tâches pour des domaines de responsabilité incompatibles avec l'objectif de réduire le risque de fraude, d'erreur et de contournement des mesures de sécurité de l'information.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.9 :Identifier, documenter et tenir à jour les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.10 :Procèder à des revues indépendantes de l'approche retenue par l'organisation pour gérer et mettre en œuvre la sécurité de l'information, y compris des personnes, processus et technologies.** | **Trés Urgent** | **CISO** | **4** | **Fin de 2024** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.11 :Vérifier régulièrement la conformité à la politique de sécurité de l'information, aux politiques portant sur des thèmes et aux normes de l'organisation.** | **Trés Urgent** | **CISO** | **4** | **Fin de 2024** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.12 :Décrir formellement les diverses procédures d'exploitation dans des documents aisément accessibles aux personnes concernées.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.13 :Maintenir des contacts avec les autorités compétentes afin d'assurer la bonne circulation de l'information à l'égard de la sécurité, entre l'organisation et les autorités légales, réglementaires et de surveillance compétentes.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.14 :Etablir et entretenir des relations avec des groupes de travail spécialisés ou des forums spécialisés dans la sécurité et avec des associations professionnelles, afin d'assurer la bonne circulation de l'information à l'égard de la sécurité.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.15 :Mettre en place un système destiné à recueillir les informations relatives aux menaces pour la sécurité de l'information et de les analyser pour produire une intelligence des menaces.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 1 : Organisation de la sécurité** | **Action 1.16 :Intégrer la sécurité de l'information aux activités de gestion de projet de l'organisation.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 2 : Améliorer des mesures de sécurité liées aux personnes** | **Action 2.1 :Mettre en place une organisation telle que le personnel de l'organisation et les parties intéressées soient sensibilisés et suivent un apprentissage et des formations à la sécurité de l'information adaptés, et qu'ils reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leur fonction.** | **Urgent** | **DRH** | **17** | **Fin de 2025** |
| **Projet 2 : Améliorer des mesures de sécurité liées aux personnes** | **Action 2.2 :Formaliser et communiquer un processus disciplinaire permettant de prendre des mesures à l'encontre du personnel et des autres parties intéressées qui ont commis une violation de la politique de sécurité de l'information.** | **Urgent** | **DRH** | **17** | **Fin de 2025** |
| **Projet 2 : Améliorer des mesures de sécurité liées aux personnes** | **Action 2.3 :Elaboration de documents, revus reguliairement et signés pour des engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisation en matière de protection de l'information, afin de gérer la confidentialité de l'information accessible au personnel ou à de tierces parties.** | **Urgent** | **DRH** | **17** | **Fin de 2025** |
| **Projet 2 : Améliorer des mesures de sécurité liées aux personnes** | **Action 2.4 :Mettre en œuvre des mesures de sécurité lorsque le personnel travaille à distance, pour protéger les informations consultées, traitées ou stockées en dehors des locaux de l'organisation** | **Urgent** | **DRH** | **17** | **Fin de 2025** |
| **Projet 2 : Améliorer des mesures de sécurité liées aux personnes** | **Action 2.5 :Etablir un mécanisme et proposé le au personnel pour lui permettre de signaler dans les plus brefs délais les événements liés à la sécurité de l'information observés ou suspectés, par le biais des canaux appropriés.** | **Urgent** | **DRH** | **17** | **Fin de 2025** |
| **Projet 3 : Améliorer des mesures physiques** | **Action 3.1 :Protéger les câbles électriques transportant des données ou supportant les services d'informationde façon à empêcher la perte, l'endommagement, le vol ou la compromission de l'information et des autres actifs associés et l'interruption des activités de l'organisation.** | **Trés Urgent** | **CISO** | **4** | **Fin de 2024** |
| **Projet 3 : Améliorer des mesures physiques** | **Action 3.2 :Assurer correctement l'entretient du matériel de manière à empêcher la perte, l'endommagement, le vol ou la compromission de l'information et des autres actifs associés et l'interruption des activités de l'organisation.** | **Trés Urgent** | **CISO** | **4** | **Fin de 2024** |
| **Projet 3 : Améliorer des mesures physiques** | **Action 3.3 :N/A** | **Trés Urgent** | **DG** | **9** | **Fin de 2024** |
| **Projet 3 : Améliorer des mesures physiques** | **Action 3.4 :Etablir une politique rédigée et concrétisée à l'aide de procédures , relative au "bureau propre et à l'écran muet" et au matériel utilisateur laissé sans surveillance afin de réduire les risques d'accès non autorisé, les pertes et l'endommagement de l'information sur les bureaux, les écrans, les autres emplacements et dans les matériels ou équipements accessibles pendant et en dehors des heures normales de travail.** | **Trés Urgent** | **DG** | **9** | **Fin de 2024** |
| **Projet 3 : Améliorer des mesures physiques** | **Action 3.5 :Disposer le matériel pour qu'il soit sécurisé et protégé contre les risques liés à des menaces et dangers environnementaux et des possibilités d'accès non autorisé.** | **Trés Urgent** | **CISO** | **4** | **Fin de 2024** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.1 :Elaboration d'une politique portant sur le thème de la configuration et de la manipulation sécurisées des terminaux utilisateurs finaux, afin de protéger toute information stockée sur un terminal utilisateur final, traitée par ou accessible via ce type d'appareil** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.2 :Etablir un plan de sauvegarde, couvrant l'ensemble des objets (programmes et données) à sauvegarder et la fréquence des sauvegardes.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.3 :Effectuer une analyse de la criticité des différents éléments de l'architecture (y compris des systèmes périphériques tels que systèmes ou robots de sauvegarde, serveurs d'impression ou équipement central d'impression, etc.) pour mettre en évidence les besoins de continuité de service.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.4 :Appliquer une gestion et un contrôle des réseaux afin de garantir la protection de l'information contenue dans les systèmes et les applications** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.5 :Identifier, mettre en œuvre et placer sous surveillance les mécanismes de sécurité, les niveaux de service et les exigences de services des services en réseau** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.6 :Cloisonné, dans les réseaux de l'organisation, les groupes de services d'information, d'utilisateurs et de systèmes d'information** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.7 :Définir les règles de développement sécurisé des logiciels et des systèmes, afin de s'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement sécurisé des logiciels et des systèmes.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.8 :Assurer l'identification et la définition de exigences de sécurité de l'information, lors du développement ou de l'achat d'applications.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.9 :Etablir, documenter, tenir à jour et appliquer les principes d'ingénierie de la sécurité des systèmes à toutes les activités de développement de systèmes d'information.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.10 :Appliquer les principes de codage sécurisé au développement de logiciels, afin de s'assurer que le logiciel est développé dans un souci de sécurité et réduire ainsi le nombre de vulnérabilités potentielles du logiciel en termes de sécurité de l'information.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.11 :L'organisation doit définir des processus pour les tests de sécurité.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.12 :N/A** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.13 :Assurer que l'organisation dirige, contrôle et passe en revue les activités liées au développement du système externalisé.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.14 :Etablir un environnement de développement sécurisé prenant en compte la sensibilité des données qui seront traitées, stockées et transmises par les systèmes ou applications développés.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.15 :séparer les environnements de développement et de tests, de l'environnement de production.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.16 :Définir des procédures pour contrôler les changements apportés aux moyens de traitement de l'information.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.17 : Assurer que tout changement soit soumis à une procédure de gestion des changements afin de préserver la sécurité de l'information lors de l'exécution des changements.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.18 :Maintenir le contrôle des versions à chaque mise à jour et une trace de tous les changements et évolutions est maintenu** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.19 :Définir des procédures afin de sélectionner, de protéger et de gérer les informations relatives aux tests.** | **Normal** | **RSI** | **8** | **Fin de 2026** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.20 :Mettre en place un processus permettant de surveiller l'utilisation des ressources et ajuster le conformément au dimensionnement actuel et prévu.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |
| **Projet 4 : Améliorer des mesures de sécurité technologiques** | **Action 4.21 :Mettre en place une protection contre les programmes malveillants, appuyée par la sensibilisation des utilisateurs concernés.** | **Urgent** | **RSSI** | **12** | **Fin de 2025** |