Rapport d'Audit de la Sécurité du Système d'Information

Algérie Télécom

Version: **2.1.1**
Date de l'audit: **27-6-2022.**
Diffusion: **Document Confidentiel**
Auditeurs: **Rahem Hacene** / **Rezal Rabah**

Table des matières

1 - Diffusion

Poste de Résponsabilité	Position
RSSI	DSSI
RRH	DRH

2 - Cadre de la mission

Cadre légal

Respecter la **loi n° 18-07** du 25 Ramadhan 1439 correspondant au 10 juin 2018 en matière de protection des personnes physiques (employées/ parties tierces) dans le traitement des données à caractère personnel au sein de l'entreprise Algérie Télécom.

La présente loi a pour objet de fixer les règles de protection des personnes physiques dans le traitement des données à caractère personnel.

Source: JOURNAL OFFICIEL DE LA REPUBLIQUE ALGERIENNE N° 34 le 25 Ramadhan 1439 10 juin 2018

L'objectif de cette mission d'audit

- Evaluer la conformité de l'entreprise Algérie Télécom par rapport aux exigences du Référentiel National de la Sécurité de l'Information ;

- Proposer des recommandations pour corriger les vulnérabilités et maîtriser les risques liés à ces dernières ;

- Proposer un plan d'action (en terme de projet) pour faire face aux risque enjeux ;

- Mettre en œuvre un Système de Management de la Sécurité de l'Information.

Démarche de conformité

Les résultats de cette mission peuvent être utiles lors de la préparation à la certification ISO 27001

3 - Termes & Définitions

Terme	Définition
RSSI	Responsable de la Sécurité des Systèmes d'Information
DSSI	Direction de la Sécurité des Systèmes d'Information
RRH	Responsable des Ressources Humaines
DRH	Direction des Ressources Humaines
SMSI	Système de Management de la Sécurité de l'Information
RNSI	Référentiel National de la Sécurité de l'Information

4 - Références

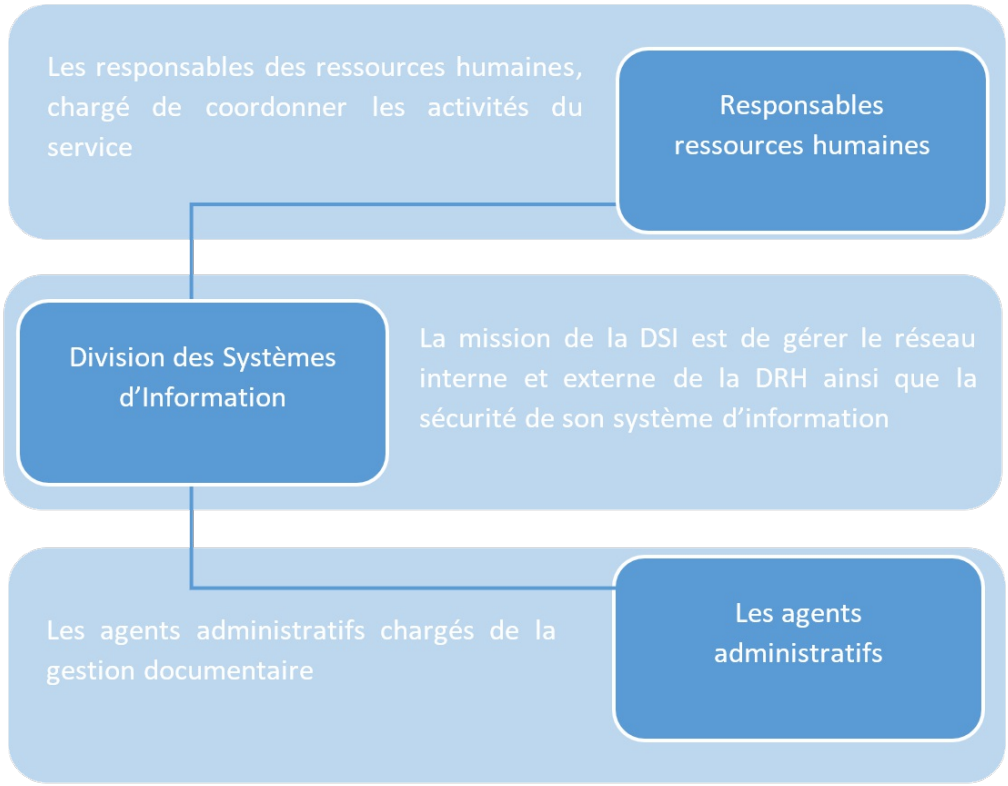
- RNSI 2020;
- RNSI Assesment Tool V1.9.7;
- ISO/CEI 27005 - 2018.

5 - Présentation du RH

Les Ressources Humaines est l'ensemble des pratiques du management, ayant pour objectif de mobiliser et développer les ressources humaines, afin d'obtenir une plus grande productivité et une meilleure qualité de travail, elle vise principalement la valorisation des compétences, de la motivation, l'information et l'organisation

les principales attributions de la direction des ressources humaines DRH porte sur l'administration (fiche de paie) et la gestion du personnel, la gestion des plans de carrière, la formation du personnel, la gestion des prêts et avances au personnel, l'application de la réglementation du travail et du règlement intérieur ainsi que le maintien d'un bon climat social dans l'entreprise Algérie Télécom.

Organigramme du RH

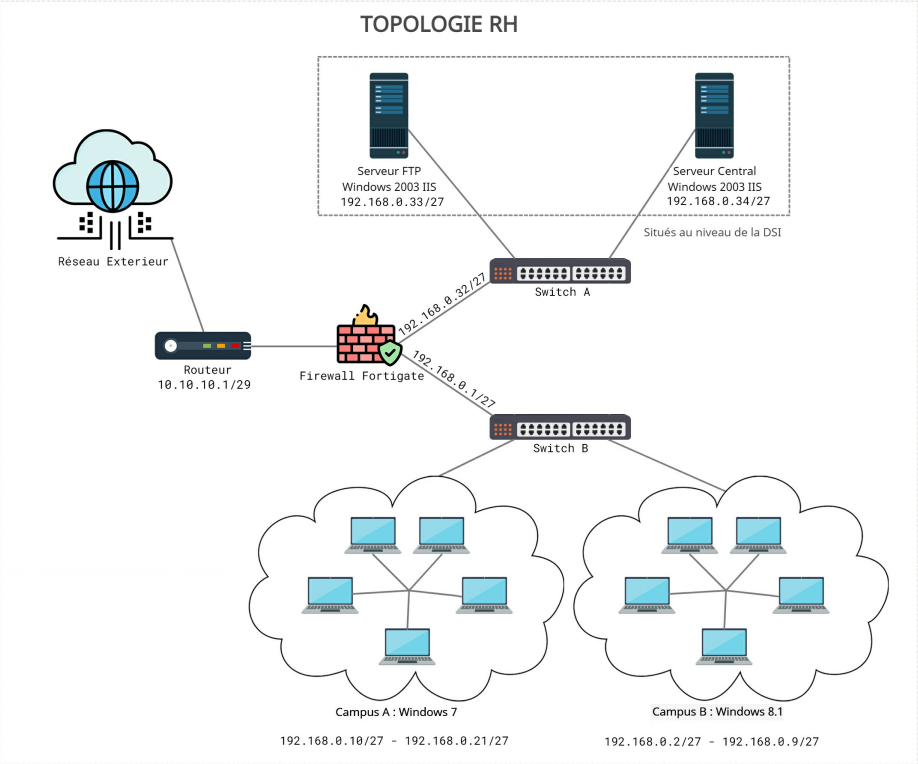


6 - Champ d'audit

Description des systèmes d'information

Actif	Adresse/Plage IP	Localisation
Un routeur	10.10.10.1/29	DRH
Un serveur FTP Windows 2003	192.168.0.33/27	DSI
Un serveur Central Windows 2003	192.168.0.34/27	DSI
8 machines Windows 8.1	192.168.0.2/27 - 192.168.0.9/27	DRH
12 machines Windows 7	192.168.0.10/27 - 192.168.0.21/27	DRH

Schèma synoptique de l'architecture



7 - Outils utilisés

Outil	Version	Fonctionnalités
Nessus	10.2.0.20075	Scanner de vulnérabilités
Nmap	7.91	Scanner du réseau
Questionnaire RNSI	2.0.0	Evaluation de l'entreprise en se basant sur le RNSI 2020
Méthodologie de gestion de risque ISO 27005	2018	Permet de gérer le risque en sécurité de l'information en suivant un schéma bien défini

8 - Vulnérabilités

ID Nessus	57608
Machine(s) Impactée(s)/ID	Windows 8.1, Windows 7, Windows Server 2003
Criticité	Moyenne
Description	Signature SMB non requise
Preuve	Nessus
Recommandation	Appliquer la signature des messages dans la configuration de l'hôte

ID Nessus	97833
Machine(s) Impactée(s)/ID	Windows 8.1, Windows 7, Windows Server 2003
Criticité	Forte
Description	MS17-010 : Mise à jour de sécurité pour Microsoft Windows SMB Server (4013389) (ETERNALBLUE)
Preuve	Nessus
Recommandation	Appliquer le(s) patch(s) nécessaire(s)

ID Nessus	152102
Machine(s) Impactée(s)/ID	Windows Server 2003
Criticité	Moyenne
Description	Élévation de privilège Microsoft Windows EFSRPC NTLM Reflection
Preuve	Nessus
Recommandation	Appliquer les mises à jour fournies par le fournisseur

ID Nessus	90510
Machine(s) Impactée(s)/ID	Windows Server 2003
Criticité	Moyenne
Description	MS16-047 : Mise à jour de sécurité pour les protocoles distants SAM et LSAD
Preuve	Nessus
Recommandation	Appliquer le(s) patch(s) nécessaire(s)

ID Nessus	26920
Machine(s) Impactée(s)/ID	Windows Server 2003
Criticité	Forte
Description	Authentification de session Microsoft Windows SMB NULL
Preuve	Nessus
Recommandation	Appliquer les modifications de registre conformément aux avis Technet

ID Nessus	34477
Machine(s) Impactée(s)/ID	Windows Server 2003
Criticité	Critique
Description	MS08-067 : Traitement de la demande RPC conçue par le service Microsoft Windows Server pour l'exécution de code à distance
Preuve	Nessus
Recommandation	Appliquer le(s) patch(s) nécessaire(s)

9 - Résultats de l'audit

1 - Gestion des Actifs

Critère	Score	Evaluation
1.2 - Inventaire des actifs ayant accès à des informations au sein de l'organisme	4	Maîtrisé
1.3 - Identification des dépendances entre les différents actifs	4	Maîtrisé
1.6 - Sensibilisation des employés et des partenaires aux exigences de sécurité des informations/actifs	4	Maîtrisé
1.7 - Restitution des actifs de l'organisme en possession des employés lors de la cessation de leur emploi	4	Maîtrisé
1.8 - Destruction de tout équipement disposant d'un support de stockage en cas de réforme	3	Défini
1.9 - Classification des informations de l'organisme et des actifs par rapport aux exigences légales, la valeur, la criticité, la sensibilité, la divulgation ou la modification non autorisée	3	Défini
1.10 - Classification des informations par rapport aux exigences métier de l'organisme	4	Maîtrisé
1.11 - Classification des actifs en conformité avec la classification des informations	3	Défini
1.12 - Association à des procédures de gestion de traitement, inclusion dans le processus de gestion et schématisation des niveaux de classification	3	Défini
1.13 - Indication de la valeur des résultats de classification des actifs par rapport a leur importance	3	Défini
1.14 - Mise en oeuvre, identification, indication sur la localisation et communication aux employés sur les procédures d'étiquetage des actifs	4	Maîtrisé
1.15 - Elaboration et mise en oeuvre des procédures destinées pour la manipulation des actifs conformément aux bonnes pratiques et à la législation et réglementation	3	Défini

2 - Protection des données à caractère personnel

Critère	Score	Evaluation
2.1 - Définition des règles de sécurité lors de la collecte, le traitement, le stockage et la disposition des données personnelles des employés en conformité avec la législation et la réglementation	4	Maîtrisé
2.3 - Exécution d'une analyse DPIA (Data Protection Impact Assessment) des opérations de traitement envisagées, lorsque le traitement génère des risques élevés pour la vie privée	1	Initial
2.4 - Identification des activités principales de l'organisme nécessitant la collecte et le traitement des données personnelles	1	Initial
2.5 - Utilisation des données personnelles pendant la période nécessaire du traitement uniquement	4	Maîtrisé
2.6 - Exactitude, complétude et mise a jour des données personnelles	4	Maîtrisé
2.7 - Respect de la vie privée de la personne concerné lors du traitement de l'information	5	Optimisé
2.8 - Possibilité a la personne concerné de lire et d'approuver toute politique en relation avec le traitement de leurs données personnelles	4	Maîtrisé
2.9 - Application des mesures techniques et organisationnelles pour empêcher la divulgation, la modification et la destruction des données a caractère personnel	3	Défini
2.10 - Avertissement de l'autorité et la personne concerné lors de la divulgation, l'altération ou la destruction des données a caractère personnel sur des réseaux de communication électroniques ouvert au public	3	Défini
2.11 - Mise a jour d'un inventaire des violations et prise de mesures de remédiation des données a caractère personnel	3	Défini
2.12 - Collection des données necessaires seulement, et destruction des informations personnelles identifiable de manière sécurisée	3	Défini
2.13 - Déploiement des mesures pour assurer la sécurité des données personnelles	3	Défini
2.14 - Mise a jour d'un inventaire des violations et prise de mesures de remédiation des données a caractère personnel par les fournisseurs de services	4	Maîtrisé
2.15 - Identification, autorisation et mise en place des mesures de supervision lors de l'envoi de données sensibles à l'étranger	4	Maîtrisé
2.16 - Interdiction de transférer des données susceptibles de porter atteinte à la sécurité publique ou aux intérêts vitaux du pays	3	Défini

3 - Gestion des contrôle des accès

Critère	Score	Evaluation
3.1 - Etablissement d'une politique de contrôle d'accès en determinant les règles, les droits et les restrictions d'accès appropriés aux fonctions de l'utilisateur de ces actifs	3	Défini
3.2 - Mise en oeuvre d'un processus formel de gestion des accès a tout type d'utilisateur, de tous les systèmes et de tout les services d'information	3	Défini
3.3 - Existence d'une politique relative à l'utilisation des réseaux et services	4	Maîtrisé
3.4 - Mise en place des mesures nécessaires pour l'identification, la détection, la protection et la supervision des comptes a privilèges	5	Optimisé
3.5 - Responsabilité de l'utilisation et la protection des informations secrètes d'authentification	5	Optimisé
3.6 - Mise en place des contrôles adéquats pour maitriser les risques liés à tout type d'accès à distance en dehors du périmètre de sécurité	4	Maîtrisé

4 - Sécurité des appareils mobiles

Critère	Score	Evaluation
4.1 - Etablissement d'une politique d'utilisation sécurisée des appareils mobiles	3	Défini
4.2 - Existence d'un inventaire détaillé des appareils mobiles qui accèdent aux ressources de l'organisme	3	Défini
4.3 - Identification du niveau de protection nécessaire des appareils mobiles selon le niveau de classification des informations stockées et traitées	3	Défini
4.4 - Approbation de chaque connexion d'un appareil mobile au réseau interne selon sa politique d'utilisation	3	Défini
4.5 - L'utilisation des techniques cryptographiques pour protéger la confidentialité et l'intégrité	4	Maîtrisé
4.6 - Utilisation des mécanismes d'authentification forts	5	Optimisé
4.7 - Etablissement des mesures à suivre en cas de perte des appareils comme la localisation et la suppression des données	4	Maîtrisé
4.8 - Consideration du contrôle technique, procédural, administratif et de la sensibilisation dans le cas d'accès à la messagerie de l'organisme	3	Défini
4.9 - Procedure d'effacement total de données de l'appareil mobile suivant la politique en vigueur, en cas de fin d'usage	3	Défini
4.10 - Sauvegarde des données stockées dans les appareils mobiles dans le cloud, supports de stockage externes	4	Maîtrisé

5 - Sécurité des réseaux

Critère	Score	Evaluation
5.1 - Mise en place d'une politique pour la prise en charge des mécanismes de conception et de gestion sécurisées de l'infrastructure réseau	4	Maîtrisé
5.2 - Elaboration, application et maintenance d'une architecture réseau en prenant en consideration le model de defense multicouches	4	Maîtrisé
5.3 - Établissement d'une politique de segmentation du réseau avec un cloisonnement physique ou logique	4	Maîtrisé
5.4 - Protection des données qui transitent dans le réseau afin de garantir leur intégrité et leur confidentialité	3	Défini
5.5 - Protection de manière appropriée l'information transitant par la messagerie électronique, et mise en place les mesures nécessaires pour maintenir la sécurité du système de messagerie de l'organisme à un niveau acceptable	4	Maîtrisé
5.6 - Sécurisation de communications à caractère confidentiel	4	Maîtrisé
5.7 - Mettre en garde les missionnaires contre les risques de sécurité encourus lors des déplacements à l'étranger	5	Optimisé

6 - Sécurité des systèmes d'information

Critère	Score	Evaluation
6.1 - Existence d'une politique pour la gestion de l'acquisition, et le la mise à jour et le développement des produits et services informatiques	4	Maîtrisé
6.2 - Mise en oeuvre des exigences de sécurité des systèmes d'information	5	Optimisé
6.3 - Suivi d'une procedure de gestion de changement apportés aux logiciels et applications	3	Défini
6.4 - Suivi d'un processus de gestion des mises à jour des systèmes	5	Optimisé
6.5 - Existence des principes d'ingénierie de la sécurité des systèmes d'informations	3	Défini
6.6 - Contrôle de l'installation des logiciels sur les systèmes opérationnels	3	Défini
6.7 - Protection des données de test et du code source des applicatifs	2	Reproductible
6.8 - Utilisation correcte des applications pour éviter les erreurs, la perte, les modifications non autorisées ou l'utilisation abusive d'informations	4	Maîtrisé
6.9 - Surveillance et contrôle du développement externalisé des logiciels	5	Optimisé

7 - Sécurité liée à l'exploitation

Critère	Score	Evaluation
7.1 - Documentation et mise a disposition des procédures d'exploitation du système d'information aux utilisateurs concernés	5	Optimisé
7.2 - Contrôle des changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sr les objectifs de la sécurité de l'information	3	Défini
7.3 - Surveillance et ajustement de l'utilisation des ressources et projections sur les dimensionnements futurs	1	Initial
7.4 - Séparation des environnements de développement, de test et d'exploitation	2	Reproductible
7.5 - Mise en oeuvre des mesures de détection, de prévention et de récupération contre les logiciels malveillants	5	Optimisé
7.6 - Etablissement d'une politique de sauvegarde de l'information et des systèmes d'information	2	Reproductible

8 - Sécurité des Systèmes d'Information Critiques

Critère	Score	Evaluation
8.1 - Elaboration d'une cartographie détaillée des systèmes critiques et designation des personnes en charge de leurs gestion	3	Défini
8.2 - Evaluation régulière des risques et des audits de conformité sur les risques constituant les systèmes d'information critiques	3	Défini
8.3 - Etablissement, documentation et test d'un plan de contingence et de résilience pour les systèmes d'information critiques	3	Défini
8.4 - Organisation des cyber-exercices pour tester le degré de préparation et de réponse aux incidents cybernétiques	4	Maîtrisé
8.5 - Réalisation régulière des tests d'intrusions (réseau et application)	4	Maîtrisé
8.6 - Identification et classification des points de sortie des informations afin de minimiser les risques liés aux fuites d'informations	4	Maîtrisé
8.7 - Surveillances des flux échangés dans le système d'information en analysant les flux de communication transitant sur le réseau pour rechercher les événements susceptible d'affecter la sécurité des SIC	3	Défini
8.8 - Isolation physique de l'infrastructure des systèmes critiques du reste des systèmes dans les centres de données (data center)	4	Maîtrisé
8.9 - Discrétion dans la localisation géographique des infrastructures des systèmes critiques de souveraineté	4	Maîtrisé
8.10 - Réglementation stricte de l'intervention des parties externes sur les systèmes critiques	4	Maîtrisé
8.11 - Stockage des composants de rechange pour assure le fonctionnement pendant les périodes de crise	4	Maîtrisé
8.12 - Utilisation de plusieurs fournisseurs pour l'approvisionnement en matière de composants critiques identifiés	4	Maîtrisé

9 - Sécurité des Services Cloud

Critère	Score	Evaluation
9.1 - Définition d'une stratégie pour le modèle de déploiement et le type de service et les données qui doivent être ou pas stockés ou traitées dans les services cloud	3	Défini
9.2 - Analyse des risques et mise en oeuvre des mesures de sécurité appropriés avant chaque demande de service cloud	3	Défini
9.3 - Utilisation des canaux de communication sécurisés entre les systèmes internes de l'organisme et les services cloud	3	Défini
9.4 - Compréhension et maintien de l'endroit où l'information soit stockée ou traitée avec les restrictions applicables dans l'environnement cloud	4	Maîtrisé
9.5 - Assurance d'un plan de migration des données et des systèmes après la cessation de relation de service	5	Optimisé
9.6 - Signature des accords de niveau de services avec le fournisseur du service cloud pour chaque service hébergé suivant la matrice de criticité du service fourni	1	Initial
9.7 - Mise en disposition par le fournisseur aux clients des outils nécessaires pour la gestion des services cloud	3	Défini
9.8 - Assurance d'une séparation entre les différents clients des services cloud	2	Reproductible
9.9 - Disposition d'un cadre de gouvernance de la sécurité par le fournisseur de services cloud	4	Maîtrisé

10 - Cryptographie

Critère	Score	Evaluation
10.1 - Développement, implémentation et mise a jour régulière d'une politique d'utilisation des mesures cryptographiques en conformité avec la politique de sécurité générale de l'organisme	4	Maîtrisé
10.2 - Réalisation des audits de conformité pour éviter les violations de la réglementation appliquée en Algérie et de toute exigence de sécurité	3	Défini
10.3 - Déploiement des contrôles cryptographiques en garantissant le respect des exigences légales, réglementaires et contractuelles Algériennes	3	Défini
10.4 - Application des mesures de sécurité cryptographiques sur les actifs de l'organisme en se basant sur le schéma global de classification des données	3	Défini
10.5 - Revue périodique et approbation des exigences de sécurité pour les mesures cryptographiques par la Direction de l'organisme	3	Défini
10.6 - Adoption des algorithmes et normes de cryptages qui ont été testés, approuvés et qui ont atteint une maturité élevée	2	Reproductible
10.7 - En cas d'échange d'informations avec des organismes étrangers hors du pays. Conformité de l'organisme aux exigences liées aux mesures cryptographiques du pays de l'organisme tiers	3	Défini
10.8 - Conformité des fournisseurs ou prestataires de services aux exigences liées à l'usage des mesures cryptographiques de l'organisme	3	Défini
10.9 - Protection des données sensibles ou classifiées au repos et en transit en tenant compte des résultats de l'appréciation des risques	4	Maîtrisé
10.10 - Mise en place des moyens pour la préservation et la restauration des informations cryptées classifiées ou sensibles pour le besoin d'une investigation ou suite a une indisponibilité	4	Maîtrisé
10.11 - Mise en place des mesures procédurales et technique pour la préservation des clés de cryptages lors de la récupération des données	4	Maîtrisé
10.12 - Mise en place des contrôles administratifs, techniques et physiques pour la protection des clés tout au long de leur cycle de vie	4	Maîtrisé
10.13 - Protection physique des clés cryptographiques secrètes et privées dans des Modules de Sécurité Physiques (MSP) ou d'autres dispositifs physiques	3	Défini

11 - Sécurité Physique

Critère	Score	Evaluation
11.1 - Développement et approbation d'une politique de sécurité physique et des procédures associées	4	Maîtrisé
11.2 - Limitation de l'accès aux centres de données, serveurs, équipements réseaux et infrastructure au personnel autorisé uniquement	4	Maîtrisé
11.3 - Définition des périmètre de sécurité pour protéger les zones hébergeant des informations sensibles et les systèmes critiques	4	Maîtrisé
11.4 - Protection des zones sécurisées par des contrôles d'accès adéquats à l'entrée	4	Maîtrisé
11.5 - Conception et application des mesures de sécurité physiques aux bureaux, aux salles et aux équipements	3	Défini
11.6 - Conception et application des mesures de sécurité physiques contre les désastres naturels, les attaques malveillantes ou les accidents	3	Défini
11.7 - Contrôle et isolement des points d'accès par lesquels des personnes non autorisées peuvent pénétrer de façon a éviter les accès non autorisés	3	Défini
11.8 - Localisation et protection du matériel de manière a réduire les risques liés aux menaces et dangers environnementaux et accès non autorisés	3	Défini
11.9 - Protection du matériel des coupure de courant et autres perturbations dues à une défaillance des services généraux	3	Défini
11.10 - Protection des câbles électriques et de télécommunication transportant des données ou supportant les services d'information	3	Défini
11.11 - Entretien correct du matériel pour garantir sa disponibilité permanente et son intégrité	3	Défini
11.12 - Application des mesures de sécurité au matériel utilisé hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site	4	Maîtrisé
11.13 - Protection du matériel non surveillé hors des locaux	4	Maîtrisé

12 - Internet des Objets - Internet Of Things (IoT)

Critère	Score	Evaluation
12.1 - Possession des autorisations nécessaires auprès des autorités concernées pour l'acquisition et l'exploitation de l'IoT	2	Reproductible
12.2 - Assurance du fonctionnement de l'IoT avec la dernière version stable de son système d'exploitation et de son micrologiciel(firmware)	2	Reproductible
12.3 - Assurance de l'absence des vulnérabilités ou défauts connus en exigeant la fourniture éventuelle d'un document de conformité avec les standards	3	Défini
12.4 - Assurance de la réception des mises à jour logicielles régulières	3	Défini
12.5 - Assurance de la non inclusion des informations d'authentification fixées ou codées en dur utilisées pour l'administration à distance, la fourniture de mises à jour ou la communication	2	Reproductible
12.6 - Assurance de l'utilisation des protocoles et technologies standards non obsolètes par l'IoT	4	Maîtrisé
12.7 - Changement de la configuration par défaut de l'IoT, cela inclut le nom du compte et le mot de passe	2	Reproductible
12.8 - Démilitarisation(DMZ) de la mise en place des IoT sur réseau	2	Reproductible
12.9 - Assurance de la protection physique des objets	3	Défini
12.10 - Activation de toutes les fonctionnalités de journalisation d'alertes ou de notification sur les événements de sécurité	2	Reproductible
12.11 - Désactivation des services et protocoles inutiles	2	Reproductible

13 - Surveillance et Journalisation

Critère	Score	Evaluation
13.1 - Définition et mise en oeuvre d'une politique et procédures de gestion et d'analyse des journaux ainsi que la surveillance des infrastructures et des systèmes d'information	2	Reproductible
13.2 - Arrêt d'une liste d'évènements et d'activités qui doivent être créés, tenus à jour, vérifiés régulièrement et archivés	2	Reproductible
13.3 - Mise en place d'un système de gestion de la journalisation permettant d'enregistrer, maintenir et analyser périodiquement les évènements liés à la sécurité de l'information	2	Reproductible
13.4 - Conservation des journaux d'évènements durant une période préalablement définie afin de faciliter les opérations d'audit et d'investigations	4	Maîtrisé
13.5 - Protection de la disponibilité, la confidentialité et l'intégrité des journaux d'évènement	4	Maîtrisé
13.6 - Veille à ce que le système de journalisation ne soit accessible que par les personnes autorisées	3	Défini
13.7 - Synchronisation automatique des horloges de l'ensemble des systèmes de traitement de l'information dans une source de référence temporelle unique	4	Maîtrisé

14 - Gestion des Incidents de sécurité

Critère	Score	Evaluation
14.1 - Etablissement d'une politique pour gérer la réponse aux incidents de sécurité de l'information incluant des procédures d'identification, de signalement, d'enregistrement, d'intervention et d'escalade d'incidents	2	Reproductible
14.2 - Création d'une équipe de réponse aux incidents de sécurité(CERT) pour une meilleure prise en charge des incidents	3	Défini
14.3 - Définition des lignes directrices pour aider les utilisateurs à identifier et signaler les incidents, ainsi que les données pertinentes à collecter avant, pendant et après un incident	5	Optimisé
14.4 - Signalement immédiat par les utilisateurs du SI de toute atteinte à la sécurité, tentative de violation et tout faille de sécurité soit à l'entité responsable de la gestion des incidents de l'organisme, soit aux autorités externes	4	Maîtrisé
14.5 - Enregistrement des incidents déclarés avec un identifiant unique pour faciliter le suivi	4	Maîtrisé
14.6 - Présentation des informations conformément aux dispositions légales relatives à la présentation de preuves auprès des juridictions compétentes	1	Initial
14.7 - Evaluation des incidents par rapport a la catégorie, l'impact et la fréquence	1	Initial
14.8 - Reprise d'activité par l'ensemble du personnel et l'équipe de sécurité de l'information en fonction de la nature de l'incident et du plan d'action élaboré	4	Maîtrisé
14.9 - Réalisation d'une analyse détaillée pour identifier les points forts et faibles de l'infrastructure une fois la reprise des activités est terminée	3	Défini
14.10 - Considération de contrôles préventifs pour éviter la récurrence de l'incident	3	Défini
14.11 - Identification des exigences légales et réglementation applicables pour la collecte des preuves en enquêtes d'investigation	3	Défini

15 - Gestion de la continuité des activités

Critère	Score	Evaluation
15.1 - Etablissement d'une politique et d'un plan de continuité et de reprise des activités basé sur les scénarios de risques	3	Défini
15.2 - Alignement de la gestion des risques liés à la continuité avec les politiques et procédures de gestion des risques de l'organisme	3	Défini
15.3 - Définition des catégories de désastres en fonction de leurs gravités et localisation par le plan de continuité des activités	4	Maîtrisé
15.4 - Inclusion des exigences en matière de la sécurité de l'information et des mesures de protection appropriées	3	Défini
15.5 - Formation des parties prenantes et du personnel au fonctionnement du plan et des processus opérationnels connexes	3	Défini
15.6 - Etablissement d'une procédure de test du plan de continuité et de reprise des activités après sinistre(DRP)	2	Reproductible
15.7 - Utilisation d'une variété de techniques et de tests ainsi que des indicateurs de performance afin de s'assurer de l'efficacité du plan	4	Maîtrisé
15.8 - Participation de toutes les parties prenantes impliquées dans le plan de continuité et de reprise des activités aux tests de plan	4	Maîtrisé
15.9 - Revue périodique ou suite à un changement majeur du plan de continuité et de reprise des activités	3	Défini

16 - Ressources humaines

Critère	Score	Evaluation
16.1 - Développement d'une politique et des procédures associées pour intégrer les exigences de sécurité avant, pendant et après le contrat de travail	3	Défini
16.2 - Etablissement d'un règlement intérieur et vérification que les employés, fournisseurs ou tierces parties doivent accepter et signer le contrat de travail et le règlement intérieur	4	Maîtrisé
16.3 - Définition des rôles et responsabilités en termes de la sécurité de l'information dans le contrat d'embauche et dans le règlement intérieur	4	Maîtrisé
16.4 - Etablissement d'une procédure pour la vérification des antécédents(l'historique du travail, casier judiciaire, certificats et diplômes)	4	Maîtrisé
16.5 - Signature d'un accord de confidentialité et de non divulgation avant d'avoir accès aux ressources de l'organisme	4	Maîtrisé
16.6 - Etablissement d'un plan de communication et un mécanisme de sensibilisation pour informer les employés des politiques et procédures de sécurité auxquelles ils doivent se conformer	3	Défini
16.7 - Test et évaluation de l'efficacité du programme de formation et sensibilisation pour identifier les points à améliorer	4	Maîtrisé
16.8 - Définition d'un processus disciplinaire formel pour les violations de la sécurité de l'information conformément aux exigences légales et réglementaires	2	Reproductible
16.9 - Restitution des actifs et révocation des droits d'accès des utilisateurs lors de la cessation de l'emploi	2	Reproductible

17 - Sécurité liée a l'usage des Réseaux Sociaux

Critère	Score	Evaluation
17.1 - Etablissement et revue d'une politique d'usage des réseaux sociaux pour être conforme aux lois et exigences en matière de régulation et de sécurité	3	Défini
17.3 - Identification et classification des comptes réseaux sociaux de l'organisme, seul les utilisateurs autorisés ont accès aux comptes	4	Maîtrisé
17.4 - Mise en place d'un mécanisme de prédiction, détection et de protection contre les bots qui sont utilisés pour influencer l'opinion publique sur un sujet particulier	4	Maîtrisé
17.5 - Revue régulière et implémentation des contrôles pour détecter les contenus inappropriés et contenant du code malveillant	3	Défini
17.7 - Interdiction aux employés ayant des comptes personnels sur les réseaux sociaux d'utiliser le même profil pour communiquer directement ou indirectement au nom de l'organisme	4	Maîtrisé
17.8 - Responsabilité sur la sécurité, la confidentialité et les risque inhérent à l'envoi de contenu sur les réseaux sociaux	3	Défini
17.9 - Protection des comptes des réseaux sociaux avec des mécanismes d'authentification forts	4	Maîtrisé
17.10 - Interdiction aux employés de mettre dans leurs profils les détails de leur fonction, le nom de leur employeur et les équipements qui sont en train de gérer	3	Défini
17.11 - Interdiction d'utiliser les emails de l'organisme pour créer des comptes sur les réseaux sociaux	2	Reproductible
17.12 - Méfiance des liens partagés ou des pièces jointes via des services de messagerie des réseaux sociaux	3	Défini

18 - Intégration de la sécurité durant le cycle de vie de développement des logiciels

Critère	Score	Evaluation
18.1 - Etablissement et revue régulière d'une politique de développement sécurisée des applications	1	Initial
18.4 - Réalisation d'une analyse de risques dans le cadre du traitement des informations compte tenu de leur catégories dès le commencement de tout projet	3	Défini
18.5 - Conformité du code source aux bonnes pratiques de codage	4	Maîtrisé
18.6 - Considération des points faibles de sécurité inhérents aux langages de programmation lors du développement des applications	3	Défini
18.7 - Prise de mesures maximales pour éviter les canaux de communication et les malwares dans les logiciels développés	4	Maîtrisé
18.8 - Utiliser des données de tests spécialement prévues à des fins de développement	2	Reproductible
18.9 - Développement et maintenance d'une documentation tout au long de la vie du projet	4	Maîtrisé
18.10 - Etablissement d'une communication efficace entre les différentes parties concernées par le projet	4	Maîtrisé

19 - Exigences de Sécurité pour les projets de technologie de l'information (TIC)

Critère	Score	Evaluation
19.1 - Considération de la sécurité de l'information dans toutes les phases de la gestion des projets	3	Défini
19.3 - Intégration des exigences de sécurité de l'information dès les premières phases des projets	2	Reproductible
19.6 - Identification et attribution des rôles et responsabilités en matière de sécurité de l'information à des fonctions spécifiques définies dans les méthodes de gestion de projet	2	Reproductible

20 - Relation avec les tierces parties

Critère	Score	Evaluation
20.1 - Etablissement et documentation des exigences de sécurité liées à l'accès des prestataires de services aux actifs de l'organisme	1	Initial
20.2 - Conformité des cahiers des charges d'acquisition des solutions matérielles ou logicielles avec le RNSI	3	Défini
20.3 - Evaluation des risques pour identifier les exigences de sécurités avant d'accorder l'accès à une partie externe	3	Défini
20.4 - Respect des objectifs, des politiques, des normes et des procédures de sécurité adoptés par l'organisme	2	Reproductible
20.5 - Etablissement d'un plan de communication avec les tierces parties en cas d'un incident de sécurité	2	Reproductible
20.6 - Limitation des informations partagées avec les fournisseurs	3	Défini
20.7 - Surveillance régulière des accès des tierces parties aux informations et aux systèmes d'information de l'organisme	3	Défini
20.8 - Elaboration et signature d'une charte fournisseur par l'intervenant du prestataire avant chaque intervention sur site ou à distance	3	Défini
20.9 - Signature d'un accord individuel de confidentialité par chaque personne concernée par le fournisseur	3	Défini
20.10 - Limitation et contrôle de l'accès au système d'information de l'organisme au personnel de l'organisme externe	4	Maîtrisé
20.11 - Conservation d'une visibilité sur les activités de la sécurité telles par le fournisseur de services	4	Maîtrisé
20.12 - Communication des modifications apportées à la fourniture des services et produits par les tierces parties à l'organisme impacté	3	Défini

10 - Recommandations

Suivant les analyses des scans et le calcul des résultats, nous pouvons donner des recommandations afin d'augmenter la sécurité.

Chaque direction de la DSI (DSSI,DII,DDSI) doit suivre les fiches techniques, manuels de politique, normes et procédures servant à la planification, l'organisation, le contrôle et à l'évaluation de la DSI concernant :

- Le référentiel national de la sécurité des systèmes d'information.

- Les procédures de la mise à jour des applications informatiques et l'élaboration d'un guide de sécurité aux utilisateurs.

- Vérifier l'existence de toute documentation relative aux politiques et normes informatiques. Les responsabilités de la DSI doivent être justifiées par une définition claire des responsabilités et un équilibrage entre les pouvoirs et les responsabilités.

- Une procédure de gestions des patch doit être élaborée et validée par la DSSI afin d'assurer le bon fonctionnement des logiciels, applications et les OS.

- Effectuer des scans des vulnérabilités en mode DAST pour s'assurer de la qualité des applications développées par l'entreprise (AT) en terme de sécurité.

- Désactiver l'authentification anonyme (anonymous login) de serveur FTP.

- Planifier un processus de migration des machines sous Windows 7 (fin de support le 14 janvier 2020) vers Windows 10 graduellement.

- Procéder à la planification de migration des machines sous Windows 8.1 vers Windows 10 avant la fin du support étendu prévue par l'éditeur pour le 10 janvier 2023.

- Activation de la fonctionnalité IDS/IPS dans le Firewall FortiGate.

Selon le besoin métier de chaque département RH, nous recommandons la création de trois VLANs :

VLAN1 : Responsables ressources humaines.
VLAN2 : Départements gestion des carrières, relations sociales, recrutements, formations.
VLAN3 : Département administration et système de paie.

11 - Plan d'action

L'organisme devrait intégrer les exigences en matière de sécurité de l'information dans ses processus de gestion des ressources humaines, et veiller à ce que les parties prenantes soient conscientes des menaces de sécurité de l'information ainsi que leurs rôles et responsabilité avant, pendant et après le contrat de travail. [RNSI 2020 page 67]

En effet, après avoir compléter notre mission, il ressort que le réseau de la division des ressources humaines au sein d'Algérie Télécom présente des failles en terme de sécurité. Les risques liés à l'activité du service des ressources humaines, sont maîtrisés, mais comme on ne peut connaitre à l'avance toutes les menaces et toutes les vulnérabilités, nous tenons à proposer les recommandations suivantes pour les prendre en considération lors de la mise en œuvre du plan d'action 2023.

Gouvernance :

- Une politique et des procédures associées doivent être développées pour intégrer les exigences de sécurités dans les processus de gestion des ressources humaines avant, durant et après le contrat de travail ;

- Améliorer le plan de communication et de sensibilisation pour s'assurer que tous les employés, les fournisseurs et les tierces parties sont conscients des politiques et procédures de sécurité de l'organisme

auxquelles ils doivent se conformer ;

- Revoir les procédures de restitution des actifs et révocation des droits d'accès des utilisateurs lors de la cessation de l'emploi.

Organisationnel :

- Identifier et classifier les points de sortie des informations afin de minimiser les risques liés aux fuites d'informations, pour ce faire nous recommandons d'implémenter une solution DLP (Data Leak Prevention) ;

- Définir et documenter un processus de gestion de patch avec un environnement de test identique à l'environnement réel, afin d'éviter les disfonctionnements des applications métiers critiques lors de l'application des nouveaux patchs.

Techniques :

- Acquisition d'une solution PAM (Privileged Access Management) pour appliquer un processus de gestion des privilèges à haut risque sur les systèmes nécessitant un traitement spécial afin de minimiser les risques pouvant découler d'une mauvaise utilisation des droits.

- Elaborer et lancer un cahier des charges pour procéder à l'acquisition des licences Windows 10 et Windows server 2016 avec support.
Conduire à un intervalle régulier des audit réseaux et applicatifs pour surveiller l'état du système d'Information RH.