Politique de Sécurité des Systèmes d'Information du MINFI
Septembre 2021

CARACTÉRISTIQUES DU DOCUMENT

Numéro Version	Date de mise en application	Niveau de confidentialité	Diffusion
00	Immédiate	C0-Aucune confidentialité	Tout public

Cette publication a été réalisée par la Division des Systèmes d'Information
Avec l'appui du Cabinet ITS (…) et en collaboration avec les représentants des Structures du MINFI

ACRONYMES ET ABREVIATIONS

ANTIC	Agence Nationale des Technologies de l'Information et de la Communication
PSSI	Politique de Sécurité des Systèmes d'Information
BCI	Business Continuity Institute
CI-DCP	Cellule Informatique de la Direction de la Comptabilité Publique
CI-DDPP	Cellule Informatique de la Direction de la Dépense de Personnel et des Pensions
CIME	Centre des Impôts des Moyennes Entreprises
COBIT	Control Objectives for Information and related Technology
CRI	Centre Régional des Impôts
CRF	Contrôle Régional des Finances
CSIGIPES	Cellule SIGIPES
DI	Division Informatique
CI-DP	Cellule Informatique de la Division de la Prévision
DI-DGB	Division Informatique de la Direction Générale du Budget
DI-DGD	Division Informatique de la Direction Générale des Douanes
DI-DGI	Division Informatique de la Direction Générale des Impôts
DI-DGTCFM	Division de l'informatique de la Direction Générale du Trésor, de la Coopération Financière et Monétaire
DRH	Direction des Ressources Humaines
DSI	Division des Systèmes d'Information
EPA	Etablissement Publique à caractère Administratif
ISACA	Information Systems Audit and Control Association
ISO	Organisation Internationale de Normalisation
LAN	Local Area Network (réseau informatique local)
MAN	Réseau Métropolitain
MINDEL	Ministre Délégué
MINFI	Ministère des Finances
MINPOSTEL	Ministère des Postes et Télécommunication
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
PGSSI	Politique Générale de Sécurité des Système d'Information
PSSI	Politique de Sécurité des Systèmes d'Information
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
TG	Trésorerie Générale
TIC	Technologie de l'Information et de la Communication
WAN	Réseau étendu

PRÉAMBULE

La Politique de Sécurité des Systèmes d'Information (PSSI) du Ministère des Finances (PSSI-MINFI) jointe est approuvée par Le Ministre des Finances. Sa mise en œuvre sera faite sur le plan opérationnel par les structures techniques du MINFI sous la supervision de la Division des Systèmes d'Information (DSI). Cette première version de la PSSI permettra de mettre en exergue la vision stratégique, l'organisation et les exigences de sécurité à implémenter au sein de toutes les structures du MINFI, afin de protéger le patrimoine informationnel et son système d'information.

Cette PSSI a pour champs d'application les services centraux, déconcentrés, rattachés et extérieurs ainsi que les organismes sous tutelles et les différents partenaires. Les structures opérationnelles procèderont à l'élaboration de leurs PSSI spécifiques, avec pour point d'ancrage la PSSI du Ministère des Finances, qui a elle-même pour ancrage la PSSI Nationale élaborée par le Cabinet ITS, sous la conduite du Ministère des Postes et Télécommunications (MINPOSTEL) en 2018.

La PSSI-MINFI est complétée par un ensemble de politiques détaillées et des politiques spécifiques abordant des thématiques précises et s'adressant à un public cible. Elle sera réévaluée en tant que de besoin en fonction de la survenue d'un facteur exogène, afin de prendre en compte les nouveaux usages et cadres normatifs.

NIVEAU D'ACCÈS AUX DOCUMENTS

L'ensemble des documents produits et diffusés dans ce projet d'élaboration de la PSSI obéiront à l'application de l'un ou plusieurs des niveaux de confidentialité suivants :

- C0 – Public : Informations réputées publiques, notamment celles publiées en ligne via internet.
- C1 – Interne : Informations non sensibles à diffusion interne et vers les usagers/partenaires concernés.
- C2 – Confidentiel : Document contenant des informations nominatives couvertes par les dispositions de la directive CEMAC numéro 08-08 du 19 décembre 2008 relative à la protection des données personnelles.
- C3 – Secret : Document comportant des informations sensibles mais non classifiées, à diffusion limitée à une liste fermée de destinataires ayant droit d'en connaître.
- C4 – Très Secret : Document comportant des informations très sensibles, à diffusion strictement limitée à une liste fermée et contrôlée de destinataires ayant le droit d'en connaître.

CORPUS DOCUMENTAIRE

La présente PSSI est complétée par l'ensemble de documents suivants :

DOCUMENT	DESCRIPTION	NIVEAU DE CONFIDENTIALITÉ	CIBLE
La déclaration d'applicabilité de la PSSI-MINFI	Déclaration signée du Ministre des Finances et rendant applicable l'ensemble des mesures de la PSSI dans le périmètre défini.	C0 - Public	Public
Recommandations de Mise en œuvre de la PSSI	Recommandations détaillées pour la mise en œuvre des règles de sécurités stratégiques au niveau des structures opérationnelles	C2 - Confidentiel	Responsables des structures opérationnelles du MINFI.
Plan d'actions PSSI	Définition des actions prioritaires à mettre en œuvre dans un intervalle de temps défini.	C1- Limitée	Responsables des structures opérationnelles du MINFI.
Politique spécifique (de télétravail, de gestion des mots de passe, de sauvegarde, …)	Ensembles des politiques relatives à des thèmes particuliers édités par la DSI ou les DI des structures opérationnelles.	C2 - Confidentiel	Parties prenantes aux activités couvertes par les politiques spécifiques.

Sommaire

CONTEXTE

Le Ministère des Finances s'est engagé depuis un certain nombre d'années dans un vaste chantier de réforme de son système d'information. Ce chantier a débuté avec l'élaboration de son Schéma Directeur Informatique en 2012, puis avec les multiples projets de dématérialisation des procédures en vue d'améliorer et de faciliter l'accès des services rendus aux usagers.

L'interconnexion des systèmes et leur ouverture au réseau internet appelle le MINFI à mettre un accent particulier sur la sécurité des systèmes d'information aussi bien au niveau central que déconcentré. Il se pose alors désormais un problème de confiance dans les échanges de données, la conformité aux différents cadres règlementaires qui définissent ces échanges ainsi que les besoins de confidentialité avec les fuites constantes d'informations critiques.

Les risques informatiques, les enjeux de la protection du patrimoine informationnel, exigent d'adopter une « **posture permanente de sécurité** », à laquelle la PSSI du MINFI devra fortement contribuer.

La loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité au Cameroun, le décret n°2013/066 du 28 février 2013 portant organisation du MINFI, le schéma directeur informatique du MINFI ainsi que les différents rapports des audits annuels de sécurité conduit par l'ANTIC font de la sécurité du système d'information une préoccupation partagée par tous.

Dans le cadre de l'exécution de sa mission relative à « la conception et le suivie de la mise en œuvre de la politique de sécurité des systèmes d'information du MINFI », la Division des Systèmes d'Information, en liaison avec les structures techniques du MINFI et l'accompagnement du Cabinet ITS expert en sécurité des SI a procédé à l'élaboration de la présente PSSI.

Cette PSSI qui définit le référentiel des règles applicables en matière de sécurité des systèmes d'information traduit la vision globale du MINFI en matière de sécurisation de l'ensemble de ses actifs informationnels. Elle est articulée autour de deux parties à savoir :

- La première partie intitulée « élément stratégique » qui définit le périmètre de la PSSI, les enjeux et orientations stratégiques, les aspects légaux et réglementaires, l'échelle et les besoins de sécurité ainsi que l'origine des menaces.
- La deuxième partie quant à elle intitulée « règles de sécurité », présente l'ensemble des règles de sécurité classées par thèmes. Ces règles sont déclinées en politiques spécifiques relatives à chaque domaine fonctionnel du MINFI.

PARTIE 1 : ELEMENTS STRATEGIQUES

CHAPITRE 1 : Périmètre de la PSSI du MINFI

Ce chapitre décrit le périmètre de la PSSI en indiquant les ressources humaines et matérielles visées. Il peut s'agir d'un secteur d'activité (exécution du budget, traitement de la solde, opérations comptables relatives au paiement des dépenses, etc.), un type de fonction (Directeur, administrateur réseau, programmeur, etc.), un statut d'utilisateur (personnel du MINFI, prestataire de service, partenaire technique et financier, etc.).

Il est également question d'énumérer la clause du domaine d'applicabilité ainsi que les autres politiques gérées par la PSSI (les politiques spécifiques).

Ce chapitre décrit le périmètre d'application de la PSSI qui recouvre les aspects organisationnels, technologiques et physiques.

I. Périmètre organisationnel.

1. Processus métiers.

La PSSI du MINFI s'applique à l'ensemble des activités du MINFI relatives à l'élaboration et la mise en œuvre de la politique du Gouvernement en matière Financière, Budgétaire, Fiscale, Monétaire et Comptable.

En matière Budgétaire et Fiscale, elle s'applique à :

- L'élaboration de la Loi de Règlement et de la Loi des Finances ;
- La préparation, le suivi et le contrôle de l'exécution du budget de fonctionnement de l'État ;
- L'exécution du budget d'investissement ;
- L'opération de dévolution du patrimoine immobilier, mobilier de l'État, des EPA et des sociétés à capital public ;
- Le contrôle financier des organismes dotés d'un budget annexe et des établissements publics autonomes ;
- La mise en œuvre des privatisations et de la réhabilitation des entreprises publiques ;

- Le suivi et contrôle de la gestion des créances et des participations publiques, de l'endettement des personnes morales de droit public et de l'emploi des subventions ;
- La prévision à court terme dans le cadre de l'élaboration du budget.
- Des impôts et des douanes.

En matière monétaire, financière et comptable, elle assure :

- La gestion de la dette publique intérieure et extérieure ;
- La gestion du Trésor public ;
- L'élaboration de la balance des paiements ;
- Le contrôle des finances extérieures, de la monnaie et de la réglementation des changes ;
- La promotion de l'épargne et de son emploi pour le développement économique ;
- Le suivi de la coopération monétaire ;
- Le suivi et le contrôle des établissements de crédits, des compagnies d'assurances et des marchés financiers ;
- Le suivi des affaires du Fonds Monétaire International.

2. Les structures impliquées.

La PSSI définit également les règles et mesures applicables à l'ensemble des structures du MINFI à savoir :

- Les Cabinets MINFI et MINDEL,
- Les Inspections Générales des Services ;
- Le Secrétariat Général ;
- La Direction Générale du Budget ;
- La Direction Générale des Douanes ;
- La Direction Générale des Impôts ;
- La Direction Générale du Trésor, de La Coopération Financière et Monétaire ;
- La Direction de La Normalisation et de la Comptabilité Matières ;
- La Division de la Prévision ;

- La Direction des Ressources Humaines ;
- La Direction des Ressources Financières.

Elle s'applique également à l'ensemble des structures et aux personnes qui interagissent avec le système d'information du MINFI, dans le cadre de l'accès en ligne à un service dématérialisé ou d'une prestation de service.

II. Périmètre technologique.

1. Infrastructure matérielle.

La PSSI s'applique à l'ensemble de l'infrastructure de communication du MINFI, notamment les équipements d'interconnexion aux réseaux locaux (LAN), métropolitains (MAN), d'interconnexion (WAN) ainsi qu'au réseau internet. En outre, on pourrait également parler des équipements de sécurité, les serveurs qui hébergent les applications, les postes de travail et les terminaux mobiles.

2. Infrastructure logicielle

Toutes les ressources applicatives utilisées par les différentes structures du MINFI sont également concernées par la présente PSSI, notamment les applications métiers (PROBMIS, CADRE, PATRIOT, FISCALIS, NEXUS, CAMCIS, MESURE, …), les applications support (Messagerie professionnelle, SYGESCA, FUSION, …) et l'ensemble des sites web du MINFI.

III. Périmètre Physique

Le périmètre physique regroupe l'ensemble des bâtiments A et B abritant les services du MINFI au niveau central, ainsi que tous les autres bâtiments abritant les structures du MINFI. Elle concerne particulièrement la protection des bâtiments sensibles et les locaux techniques (salles serveurs).

CHAPITRE 2 : Enjeux et orientations stratégiques

I. Enjeux de la PSSI du MINFI

1. Contexte.

La mise en œuvre de la loi **N° 2018/011 du 11 juillet 2018** portant code de transparence et de bonne gouvernance dans la gestion des Finances Publiques, passe nécessairement par la mise en œuvre des solutions qui utilisent de plus en plus les Technologies de l'Information et de la Communication (TIC).

Ces systèmes d'information sont exposés à des risques et menaces (incidents, erreurs et malveillances) pouvant porter atteinte à la qualité du service rendu à l'usager et à l'image de marque du MINFI. Ces menaces évoluent en permanence alors que l'exposition et la complexité des systèmes d'information ainsi que leur interdépendance ne font que croitre, avec des besoins d'ouverture, d'évolution et de flexibilité toujours plus importants.

La Sécurité des Systèmes d'Information (SSI) a pour finalité de prévenir et de gérer ces menaces, en permettant de répondre à des problématiques opérationnelle, stratégique, juridique et de gestion de risque, ceci dans une démarche adaptée au contexte et aux enjeux du MINFI.

Ainsi le MINFI ambitionne de se doter d'une Politique Générale de Sécurité des Système d'Information (PGSSI), avec comme objectif principal d'assurer la disponibilité, l'intégrité, la confidentialité, l'authenticité et la traçabilité au sein de ses Systèmes d'Information (SI).

2. Terminologie.

La sécurisation vise à encadrer et orienter l'ensemble des actions d'identification puis des actions de traitement des risques de sécurité SI. Un risque de sécurité SI est identifié dès lors qu'il y'a potentiellement atteinte directe ou indirecte (suite à un accident, une erreur ou un acte malveillant) à :

- **La disponibilité**, qui est la propriété pour une information ou un traitement d'être accessible et utilisable à la demande par une entité autorisée ;
- **L'intégrité**, qui est la propriété pour une information ou un traitement d'être non altéré ;
- **La confidentialité**, qui est la propriété pour une information de ne pas être accessible ou divulguée à des entités, personnes ou processus non autorisés ;
- **La traçabilité** qui est la propriété pour une information ou un traitement de permettre la vérification d'un agissement ou d'un événement à des fins d'analyse postérieure et d'en retrouver l'auteur ;
- **L'authenticité**, qui est la propriété pour une information d'être authentique, vrai et pure.

II.Orientations stratégiques de la PSSI du MINFI

Les risques pesant sur les activités du MINFI appellent une réponse claire au travers des lignes directrices, permettant de renforcer le niveau de protection des systèmes d'information et de formaliser une politique de sécurité ad hoc.

1. Accompagner les évolutions du SI du MINFI

La politique de sécurité doit permettre de prévenir les risques sans pour autant figer le système d'information et le rendre inapte à répondre aux nouveaux modes de travail, et aux changements d'organisation nécessaires.

2. Mettre en place une organisation de sécurité transversale et homogène en s'appuyant sur un réseau de correspondants de sécurité de proximité

L'organisation de la sécurité doit assurer la cohérence et la mutualisation au travers d'une chaîne de responsabilité transversale. Ainsi, la Division des Systèmes d'Information (DSI) détermine la stratégie ministérielle en matière de SSI et la mise en œuvre est effectuée sous le pilotage opérationnel des Divisions de l'Informatique (DI) des différentes Directions Générales.

Cette chaîne de responsabilité passe par les responsables hiérarchiques et repose in fine sur les utilisateurs du système d'information et plus particulièrement sur les responsables informatiques de proximité (DI-DGB, DI-DGTCFM, DI-DGI, DI-DGD, CI-DCP, CI-DP, CI-DDPP, CSIGIPES-DRH), qui doivent assurer la diffusion de bonnes pratiques de sécurité et la remontée d'incidents détectés au plus près du « terrain ».

3. Assurer la cohérence du niveau de protection logique et physique

Une protection efficace du système d'information passe nécessairement par la protection physique de celui-ci. Tout accès non maîtrisé au SI est un risque potentiel pour les activités critiques ou pour les informations sensibles du Ministère.

Considérant la nature confidentielle des informations traitées par certaines structures, il est nécessaire d'adopter une protection globale alliant d'une part la protection physique de l'environnement de travail et d'autre part, la protection adéquate des infrastructures systèmes et réseaux.

4. Rendre homogène le niveau de sécurité entre l'administration centrale et les services déconcentrés

L'utilisateur de l'administration centrale ou d'un service déconcentré du MINFI (TG, Recette des Finances, CRF, CDF, CRI, CIME, Secteurs de Douane, …) doit être considéré de la même manière au regard des procédures d'accès et d'habilitation vis-à-vis du système d'information. La fiabilité des données gérées au niveau central est directement liée à la fiabilité des données gérées au niveau local dans les services déconcentrés. Il est donc indispensable de promouvoir une pratique commune et équivalente en tout point en matière de « comportement », sécurité pour tous les utilisateurs et administrateurs, qu'ils soient en administration centrale ou au sein des services déconcentrés.

5. Accompagner le schéma directeur des SI en renforçant la fiabilité et la cohérence du SI

Le Schéma Directeur Informatique (SDI) du MINFI définit les axes majeurs et stratégiques du développement des systèmes d'information. Il se doit d'intégrer la nécessaire mise en œuvre des mesures de sécurité organisationnelles et techniques aptes à réduire les risques pesant sur ce système d'information. Il est donc indispensable que l'urbanisation des systèmes d'information prenne en compte la sécurisation des référentiels et des infrastructures techniques ou fonctionnelles sur lesquelles repose le SI du MINFI.

6. Promouvoir une culture de la sécurité au travers de codes de bonnes pratiques accessible aux utilisateurs et aux prestataires de service

Il est important de rappeler que le rôle d'une maîtrise d'ouvrage (MOA) est de définir le besoin des utilisateurs et notamment le besoin de sécurité vis-à-vis des informations traitées.

La maîtrise d'œuvre (MOE) se doit de développer et mettre en œuvre les mesures de sécurisation permettant de répondre au besoin.

L'exploitant doit prendre en compte les besoins de sécurité définis par les MOA dans ses procédures d'exploitation. Les utilisateurs doivent appliquer les règles de sécurité définies. Cette approche n'est efficace que si elle reste bien comprise par les différents acteurs.

Cette démarche se doit d'intégrer de bonnes pratiques de sécurité permettant de garantir le niveau de protection existant et/ou attendu.

Il est donc essentiel de propager une culture sécurité via une communication adaptée aux différents acteurs.

7. Accompagner le renforcement du niveau de protection des partenaires en développant des standards et la mutualisation des moyens de protection

Le MINFI est de par ses missions, ouvert sur l'extérieur et s'appuie sur un tissu important de partenaires avec qui les échanges et les interconnexions sont multiples et indispensables.

Il est donc opportun de veiller et de garantir un niveau de protection cohérent tout particulièrement quand le système d'information s'étend à des locaux hors contrôle direct du MINFI, ou bien lorsqu'il est accessible par des utilisateurs qui ne font pas partie directement du périmètre interne.

La PSSI du MINFI vise la construction d'une vision commune et partagée du niveau minimal indispensable de protection du SI.

CHAPITRE 3 – ASPECTS LEGAUX ET REGLEMENTAIRES DE LA PSSI

I. Bases de la PSSI du MINFI

Les principes et les règles contenus dans la PSSI du MINFI s'appuient sur les textes légaux et règlementaires et reposent sur les normes internationales, les référentiels de bonnes pratiques ainsi que les textes au niveau national.

1. Au niveau International

- La convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel, adoptée par la 23ème Session Ordinaire du sommet de l'Union Africaine à Malabo, le 27 juin 2014 ;
- ISO/CEI 27000 : 2018, Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Vue d'ensemble et vocabulaire ;
- ISO/CEI 27001 : 2013, Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences ;
- ISO/CEI 27002 : 2013 Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information ;
- ISO/CEI 27005 : 2018, Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information ;
- ISO 31000 : 2018, Management du risque – Lignes directrices ;
- ISO 31010 : 2019, Management du risque – Techniques d'appréciation du risque ;
- ISACA, COBIT 5 - Processus facilitants - AP013 Gérer la sécurité :

    - **Description du processus** : Définir, explorer et surveiller un système de management de la sécurité de l'information ;
    - **Objectif du processus :** Maintenir l'impact et l'occurrence des incidents de sécurité de l'information dans les limites de l'appétence de l'entreprise pour le risque.

- BCI (Business Continuity Institute), Guide de bonnes pratiques (de continuité d'activité) 2013, en alignement avec ISO 22301 : 2012.

2. Au niveau national.

Les Lois

- **Loi N° 2019/020 du 24 décembre 2019** modifiant et complétant certaines dispositions de **la loi No 2016/007 du 12 juillet 2016** portant code pénal. Elle définit les sanctions applicables aux actes d'outrage, de diffamation, d'injure ou de menace faites soit par des gestes, paroles, ou écris à l'encontre d'une race ou d'une religion à laquelle appartiennent un ou plusieurs citoyens ou résidents par voie de presse, de radio, de télévision, de réseaux sociaux.
- **Loi n°2018/011 du 11 juillet 2018**, portant code de transparence et de bonne gouvernance dans la gestion des finances publiques au Cameroun ;
- **Loi n°2018/012 du 11 juillet 2018**, portant régime financier de l'État et des autres entités publiques, modifiant et complétant la Loi n° 2007/006 du 26 Décembre 2007 portant régime financier de l'État ;
- **Loi n°2010/012 du 21 décembre 2010** relative à la cybersécurité et la cybercriminalité au Cameroun ;
- **Loi N° 2015/006 du 20 avril 2015** modifiant et complétant certaines dispositions de la loi **N° 2010/013 du 21 décembre 2010** régissant les communications électroniques au Cameroun ;
- **Loi N° 2010/021 du 21 décembre 2010** régissant le commerce électronique au Cameroun ;
- **Loi-cadre N° 2011/012 du 6 mai 2011** portant protection du consommateur au Cameroun.

Les Décrets

- **Décret n° 2000/287 du 12 octobre 2000** modifiant et complétant certaines dispositions du **décret n° 94/199 du 07 octobre 1994** portant Statut Général de la Fonction Publique de l'État ;
- **Décret n°2013/066 du 28 février 2013** portant organisation du Ministère des Finances ;

- **Décret N° 2013/0399/pm du 27 février 2013** fixant les modalités de protection des consommateurs des services de communications électroniques ;
- **Décret N°2012/1643/pm du 14 juin 2012** fixant les conditions et les modalités d'audit de sécurité obligatoire des réseaux de communications électroniques et des systèmes d'information ;
- **Décret N°2012/1640/pm du 14 juin 2012** fixant les conditions d'interconnexion, d'accès aux réseaux de communications électroniques ouverts au public et de partage des infrastructures ;
- **Décret N°2018/366 du 20 juin 2018** portant Code des Marchés Publics ;
- **Décret n° 2000/685/PM du 13 septembre 2000** portant organisation et fonctionnement du conseil permanent de discipline de la fonction publique et fixant les règles de la procédure disciplinaire ;
- **Décret n° 75/769 du 18 décembre 1975** portant statut particulier du corps des Fonctionnaires de l'Information ;
- **Décret n° 78/311 du 31 juillet 1978** portant statut particulier du corps des Fonctionnaires de l'Informatique et de la Téléinformatique ;
- **Décret n° 75/776 du 18 décembre 1975** portant statut particulier du corps des Fonctionnaires des Régies Financières ;
- **Décret n° 75/768 du 18 décembre 1975** portant statut particulier du corps des Fonctionnaires d'Active des Douanes.
- **CIRCULAIRE N° 003 / CAB / PM DU 28 Mars 2018** relative à la gestion des documents et données confidentielles de l'État et des organismes du secteur public. Faisant suite à l'Instruction **n° 013/CAB/PRF du 06 août 1968** sur la protection du secret.

II. Principes fondamentaux de sécurité du SI du MINFI

1. Principes de mise en œuvre de la sécurité du SI

Pour atteindre les objectifs de sécurité du SI, le MINFI s'appuie sur les principes de mise en œuvre suivants :

PRINCIPE 1 : La PSSI du MINFI est conforme aux lois, règlements, et meilleures pratiques en matière de Sécurité des Systèmes d'Information.

La PSSI est élaborée, mise en œuvre, exploitée, surveillée, mise à jour et améliorée en continu conformément aux lois, règlements et meilleures pratiques, notamment celles des normes ISO/CEI 2700x, de COBIT 5, de ISO 22301 et de BCI.

Principe 2 : La gestion des risques en matière de sécurité du SI est régulière, alignée aux objectifs stratégiques du MINFI, et proportionnée.

L'identification, appréciation et traitement des risques sont effectués régulièrement. Les mesures de réduction des risques sont mises en œuvre en s'assurant que leurs coûts sont proportionnels aux bénéfices obtenus. La gestion des risques est revue régulièrement dans une optique d'amélioration continue de la sécurité.

Principe 3 : La mise en œuvre de la sécurité du SI est progressive et pragmatique.

La mise en œuvre des mesures de sécurité (qui découlent de la gestion régulière et proportionnée des risques) est réalisée de manière pragmatique, en traitant en priorité les risques les plus importants, et ce, dans une optique d'amélioration continue.

2. Principes éthiques de la Sécurité du SI

Principe 4 : Moindre privilège (droits d'accès minimum)

Toute personne n'accède qu'aux informations ou ressources strictement nécessaires à l'accomplissement de son travail, en conformité avec les lois, règlements et directives.

Principe 5 : Ségrégation (ou séparation) des tâches

Pour réduire les opportunités de vol, de consultation, d'altération, ou d'usage non autorisés d'informations, les rôles et responsabilités y relatifs sont assignés à des personnes distinctes, permettant ainsi de prévenir les erreurs et les irrégularités dans le traitement des actifs. Cette séparation des tâches évite qu'une même personne puisse avoir le contrôle sur tout le cycle de vie d'un système (depuis son développement ou modification jusqu'à sa mise en production) ou d'une transaction (depuis sa saisie jusqu'à son approbation).

Principe 6 : Renforcement (« hardening ») des systèmes

Pour réduire les vulnérabilités et l'exposition aux menaces, la configuration et l'accès aux différents systèmes (réseaux de télécommunication, serveurs, logiciels, postes de travail) sont limités au strict nécessaire.

Principe 7 : Protection de la sphère privée

Les données du personnel, partenaires ou autres bénéficiaires des prestations du MINFI sont protégées conformément aux lois, règlements et directives.

III. Obligations contractuelles

La sécurité des systèmes d'information du MINFI englobe tous les aspects, notamment organisationnel, technique, physique et environnemental. A ce titre, tous les intervenants qui ont accès aux systèmes d'information du MINFI sont concernés par leur sécurité. Ainsi ; les prestataires de services qui sont amenés à intervenir dans les systèmes d'information, doivent se conformer à la présente PSSI pour garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données.

CHAPITRE 4 – ECHELLE DES BESOINS

Les mesures de sécurité étant souvent coûteuses et contraignantes, leur mise en œuvre doit être adaptée aux réels enjeux du Ministère des Finances. Elle doit ainsi obéir à un principe de gradation des moyens, qui consiste à protéger tous les domaines d'activités selon leurs besoins de sécurité et les menaces qui peuvent les affecter. Il est ainsi nécessaire d'adapter les mesures de sécurité aux enjeux réels, tout en optimisant leur efficacité et les coûts inhérents.

Ce chapitre présente les critères de sécurité pertinents pour le Système d'Information du MINFI ainsi qu'une liste d'impacts pertinents pour le ministère.

I. Les critères de sécurité pris en compte dans l'échelle des besoins

La PSSI du MINFI s'appuie sur les critères de sécurité suivants : **la Confidentialité, la Disponibilité, l'Intégrité**. Pour une meilleure appropriation de ces derniers nous établirons pour chacun de ces critères une échelle de mesure.

1. Confidentialité

Ce critère suppose que seules les personnes autorisées ont accès à l'information et a fortiori peuvent l'utiliser, la modifier ou la divulguer. Ce critère s'applique spécialement aux informations qui pour une raison ou une autre doivent rester secrètes. L'échelle retenue pour le système d'information du Ministère des Finances est la suivante :

Tableau 1 : Échelle des Besoins en Confidentialité

Niveau de Confidentialité	Description de l'expression de besoin	Niveau d'impact redouté
Très Secret	La divulgation de cette information a un impact sur la sécurité nationale, la stabilité économique ou sur la vie des camerounais.	4
Secret	La divulgation de cette information a un impact significatif sur la réalisation des objectifs et missions du ministère.	3
Confidentiel	Information destinée à une liste très restreinte de personnes. Sa divulgation en dehors du périmètre établi causerait un dommage important pour le MINFI.	2
Interne	Information ayant vocation à demeurer au sein du Ministère. Sa communication hors du MINFI peut nuire aux activités.	1
Public	Information qui peut être rendue publique sans impact pour le MINFI	0

2. Intégrité

Ce critère désigne le fait qu'une ressource n'a pas été altérée ou détruite. Ainsi, elle garantit que les ressources sont non corrompues, c'est-à-dire exactes et complètes, et à fortiori, n'être modifiées que par des personnes autorisées et selon un procédé défini. L'échelle suivante peut donc être considérée :

Tableau 2 : Échelle des Besoins en Intégrité

Niveau d'Intégrité	Description de l'expression de besoin	Niveau d'impact redouté
Très Critique	Perte d'intégrité inenvisageable. Toute altération de la ressource aurait un impact très significatif sur la vie des camerounais.	4
Critique	Perte d'intégrité inenvisageable. Toute altération de la ressource aurait un impact significatif sur les activités du Ministère	3
Élevé	Perte d'intégrité intolérable. Toute altération de la ressource aurait un impact élevé sur les activités du MINFI.	2
Moyen	Toute altération de la ressource aurait un impact important sur les activités du MINFI.	1

Faible	Perte d'intégrité tolérée. Toute altération de la ressource aura un impact faible sur les activités du MINFI	0

3. Disponibilité

Ce critère qualifie le fait qu'une ressource peut être accessible et utilisable à la demande par une personne ou une entité autorisée pour rendre le service pour lequel elle a été conçue. L'échelle suivante peut donc être considérée :

Tableau 3 : Échelle des Besoins en Disponibilité

Niveau de Disponibilité	Description de l'expression de besoin	Niveau d'impact redouté
Très Critique	Pas de Tolérance à l'indisponibilité. Si ce besoin n'est pas respecté, l'impact sur les activités du MINFI est très significatif	4
Critique	Tolérance à l'indisponibilité très faible. Si ce besoin n'est pas respecté, le MINFI court un impact significatif.	
Élevé	Tolérance à l'indisponibilité faible. Si ce besoin n'est pas respecté, le MINFI court un impact élevé	3
Moyen	Tolérance à l'indisponibilité moyenne. Si ce besoin n'est pas respecté, le MINFI court un impact important	2
Faible	Tolérance à l'indisponibilité élevée. Si ce besoin n'est pas respecté, l'entreprise court un impact faible	1

II. Liste d'impacts

1. Impacts sur la confidentialité

Impact	Description	Exemple
Perte de confidentialité ayant un impact faible sur les activités du MINFI.	Le sinistre est susceptible de provoquer une diminution des capacités du Ministère des Finances	Ex : données liées aux compétences ou savoir-faire internes, dans un contexte de groupe de confiance, dont vous protégez toutes les traces écrites.
Perte de	Le sinistre est susceptible	Ex : données liées à un

confidentialité entraînant des conséquences dommageables	d'amoindrir les capacités du Ministère, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation	engagement de confidentialité dans un contrat
Perte de confidentialité entraînant des conséquences graves	Sinistre susceptible de provoquer une modification importante dans les structures et la capacité du Ministère comme la révocation de dirigeants, la restructuration du Ministère, des pertes financières.	Ex : données très secrètes

2. Impacts sur l'intégrité

Impact	Description	Exemple
Perte d'intégrité sans conséquence	Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités du Ministère.	Ex : aucune vérification
Perte d'intégrité entraînant des gênes de fonctionnement	Susceptible de provoquer une diminution des capacités du Ministère	Ex : paiement des avantages indus à un agent de l'État
Perte d'intégrité entraînant des conséquences dommageables	Susceptible d'amoindrir les capacités du Ministère, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation	Ex : données qui sont validées et contrôlées par des moyens humains ; double saisie dans le système informatique
Perte d'intégrité entraînant des conséquences graves	Susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières	Ex : données avec au moins deux niveaux de validation et de contrôle différents (techniques ou humains). Corruption de décret de nomination ou des actes pour avoir des avantages financiers colossaux

3. Impacts sur la disponibilité

Impact	Description	Exemple
Délai supérieur à une	Des services qui apportent un	Ex : un climatiseur

semaine	confort supplémentaire mais pas indispensable	
Délai > 8 heures et <= 1 semaine	Ressources pour lesquelles il existe une alternative	Ex : imprimantes.
Délai > 2heures et <= 8 heures	Sans conséquence vitale humainement	Ex : arrêt du réseau, de la messagerie, données non disponibles
Délai : entre temps réel et <= 2 heures	Ressources qui mettent en péril la vie du Ministère	Exemples : les systèmes de télé déclaration et de télépaiement.

CHAPITRE 5 - BESOINS DE SECURITE ET ORIGINE DES MENACES

I. Les besoins de sécurité

1. Protection de l'outil de travail

Les postes informatiques, les réseaux, les applications et les données, constituent « le Système d'Information » du Ministère des Finances. Cet ensemble est indispensable pour l'atteinte des objectifs de performance du MINFI. La disponibilité et l'intégrité de ces outils doivent donc impérativement être placées à l'abri de menaces internes ou externes.

2. Protection des données

Il s'agit des données « classifiées très sécrètes », mais le plus souvent il s'agit de « données sensibles » telles que :

- Les **données de gestion** : authentification, gestion comptable et financière, gestion des ressources humaines, documents contractuels ;
- Les **données nominatives** : liées à la vie privée des personnes, liées aux activités du MINFI ;
- Les **données stratégiques** : informations d'ordre politique ou stratégique ou touchant des questions de défense, informations sécurité etc.

La protection des données sensibles suppose l'identification préalable de ces données, la détermination du type de protection nécessaire (confidentialité, disponibilité, intégrité) et l'évaluation de leur degré de sensibilité (quantification des besoins de sécurité).

La sensibilité des données est appréciée lors d'un inventaire au cours duquel des questions touchant à « la vie de la donnée » doivent être posées :

- Quel est son type ?

- Où réside-t-elle ?
- Par qui est-elle partagée (« besoin d'en connaître ») ?
- Quelle(s) menace(s) est-elle susceptible de subir ?

3. Protection juridique

La mise en œuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire destiné en particulier à protéger les droits de propriété intellectuelle et industrielle et ceux de la vie privée (fichiers nominatifs, cyber surveillance…). Dans ce cadre, la responsabilité administrative et pénale de la hiérarchie et des administrateurs systèmes et réseaux peut être recherchée.

II. Origines des menaces

1. Types de menaces

Le tableau suivant donne des exemples de menaces types. Les menaces peuvent être délibérées, accidentelles ou environnementales (naturelles) et peuvent entraîner, par exemple, des dommages ou la perte de services essentiels. Le tableau suivant indique pour chaque type de menace la codification suivante en fonction de son origine, **D (délibéré), A (accidentel), E (environnemental)**. **D** *est utilisé pour toutes les actions délibérées visant les actifs informationnels*, **A** *est utilisé pour toutes les actions humaines pouvant endommager accidentellement les actifs informationnels* et **E** *est utilisé pour tous les incidents qui ne sont pas d'origine humaines*. Les groupes de menaces ne sont pas classés par ordre de priorité.

Tableau 4: Types de menaces

TYPES	MENACES	ORIGINES
Dommages physiques	Feu	A, D, E
	Dégâts des eaux	A, D, E
	Pollution	A, D, E
	Accident majeur	A, D, E
	Destruction de l'équipement ou des supports	A, D, E

TYPES	MENACES	ORIGINES
	Poussière, corrosion, froid.	A, D, E
Évènements naturels	Phénomène climatique	E
	Phénomène sismique	E
	Phénomène météorologique	E
	Inondation	E
Perte des services essentiels	Défaillance du système de climatisation ou d'approvisionnement en eau	A, D
	Perte de l'alimentation électrique	A, D, E
	Défaillance du matériel de télécommunication	A, D
Compromission des informations	Vol de médias ou de documents	D
	Vol d'équipement	D
	Récupération des supports recyclés ou mis au rebut	D
	Divulgation	A, D
	Données provenant de sources non fiables	A, D
	Altération du matériel informatique	D
	Piratage de logiciels	A, D
Défaillances techniques	Panne d'équipement	A
	Dysfonctionnement de l'équipement	A
	Saturation du système d'information	A, D
	Dysfonctionnement logiciel	A
	Absence de maintenabilité du système d'information	A, D
Actions non autorisées	Utilisation non autorisée de l'équipement	D
	Copie frauduleuse de logiciels	D
	Utilisation de logiciels contrefaits ou copiés	A, D
	Altération des données	D
	Traitement illicite de données	D

TYPES	MENACES	ORIGINES
Compromission des fonctions	Erreur d'utilisation	A
	Abus de droit	A, D
	Falsification de droits	D
	Déni d'actions	D
	Violation de la disponibilité du personnel	A, D, E

2. Origine des menaces

Une attention particulière devrait être accordée aux menaces à sources humaines. Celles-ci sont spécifiquement détaillées dans le tableau suivant :

Tableau 5: Origine des Menaces

ORIGINE DE LA MENACE	MOTIVATION	CONSÉQUENCES POSSIBLES
Hackers	• Défi • Ego • Rébellion • Statut • Argent	• Piratage • Ingénierie sociale • Intrusion dans le système, effractions. • Accès non autorisé au système
Cybercriminels	• Destruction de l'information • Divulgation illégale d'informations • Gain monétaire • Altération non autorisée des données	• Criminalité informatique (Ex : cyber harcèlement criminel) • Acte frauduleux (Ex : usurpation d'identité) • Attaque par usurpation d'identité • Intrusion du système • Corruption d'information
Terroristes	• Chantage	• Bombardement/terrorisme

ORIGINE DE LA MENACE	MOTIVATION	CONSÉQUENCES POSSIBLES
	• Destruction • Exploitation • Vengeance • Gain politique • Couverture médiatique	• Guerre de l'information • Attaque du système (Ex : Attaque par déni de service) • Pénétration du système • Altération du système
Espionnage industriel (renseignement, entreprises, gouvernements étrangers, autres intérêts gouvernementaux)	• Avantage concurrentiel • L'espionnage économique	• Avantage en matière de défense • Avantage politique • Exploitation économique • Vol d'informations • Intrusion dans la vie privée • Ingénierie sociale • Pénétration du système • Accès non autorisé au système (accès à des informations classifiées, exclusives et/ou l'information liée à la technologie)
Menaces internes (Employés mal formés, mécontents, malveillants, négligents, malhonnêtes ou congédiés)	• Curiosité • Ego • Renseignement • Gain financier • Vengeance • Erreurs et omissions involontaires (Ex : erreur de saisie de	• Voies de fait contre un employé • Chantage • Navigation dans les informations confidentielles • Malveillance informatique • Fraude et vol • Corruption d'information • Saisie de données falsifiées et

ORIGINE DE LA MENACE	MOTIVATION	CONSÉQUENCES POSSIBLES
	données, erreur de programmation)	corrompues • Interception • Code malveillant (Ex : virus, bombe logique, cheval de Troie) • Vente de renseignements personnels • Bogues système • Intrusion du système • Sabotage du système • Accès non autorisé au système

PARTIE 2 : RÈGLES DE SÉCURITÉ

Chapitre1– RÈGLES STRATÉGIQUES

Ce chapitre définit un ensemble de règles applicables dans les différentes structures du MINFI. Elles sont basées sur la norme internationale ISO/IEC 27002 qui définit le code de bonne pratique pour le management de la sécurité de l'information. Les règles ainsi évoquées visent la protection des outils de travail (disponibilité), la protection des données (confidentialité, intégrité et disponibilité), ainsi que la protection du personnel des différentes structures.

I. POLITIQUES DE SÉCURITÉ DE L'INFORMATION.

L'objectif recherché est d'apporter à la sécurité de l'information une orientation et un soutien de la part du MINFI conformément aux exigences métier et aux lois et règlements en vigueur.

REG 1-1 : Les règles de la PSSI opérationnelle de chaque structure sont définies après détermination du niveau de couverture des risques applicables.

REG 1-2 : A un niveau inférieur, la PSSI sera étayée par des politiques portant sur des thèmes spécifiques, qui imposent en outre la mise en œuvre des mesures de sécurité de l'information et sont de manière générale structurés pour répondre aux besoins de certains groupes cibles de la structure ou pour englober certains thèmes.

REG 1-3 : les politiques opérationnelles définies à un niveau inférieur par les différentes structures devront être revues à intervalle de temps régulier.

II. ORGANISATION DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DU MINFI

L'objectif recherché est d'établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein du MINFI.

REG 2-1 : Une organisation dédiée à la SSI doit être mise en place au MINFI. Cette organisation doit être établie selon les directives de la norme ISO27001 et conformément à l'organigramme du MINFI. Cette organisation définit les responsabilités

internes à l'égard des tiers, les modalités de coordination avec les autorités externes ainsi que les modalités d'application des mesures de protection. Des procédures d'applications sont écrites et portées à la connaissance de tous.

III. SÉCURITÉ DU PERSONNEL

A. Accueil du personnel

L'objectif est de garantir la confidentialité des données à travers la sensibilisation des personnes nouvellement affectées au sein des structures du MINFI. Ainsi, les personnels qui sont amenés, dans le cadre de leurs activités, à avoir accès aux informations sensibles ainsi qu'aux moyens de traitement de l'information, doivent au préalable faire l'objet de sensibilisation sur la sécurité de l'information et signer une charte de confidentialité, conformément à la réglementation en vigueur.

REG 3-A-1 : A leur arrivée, les personnels doivent être informés, au préalable, de leur rôle sur la sécurité de l'information et leurs responsabilités dans l'application effective des mesures de la PSSI du MINFI.

REG 3-A-2 : Ils doivent s'engager à avoir un comportement responsable qui ne représente aucun risque pour la sécurité de l'information.

REG 3-A-3 : Les personnels qui ont accès à l'information sensible et au système d'information, doivent au préalable signer une charte de confidentialité et de non-divulgation desdites informations. Il doit en être de même pour les prestataires et les partenaires qui interviennent sur le système d'information. L'habilitation est la garantie que ces personnes peuvent, sans risque aussi bien pour elles-mêmes que pour le MINFI, connaître des informations sensibles.

REG 3-A-4 : Les personnels qui ont accès à l'information sensible et au système d'information, doivent être informés de leurs responsabilités en matière de sécurité de l'information et être prévenus des sanctions qui sont prévues en cas de violation des mesures de sécurité prévues dans la PSSI du MINFI (Code pénal, statut général de la fonction publique ; textes particuliers).

REG 3-A-5 : Tout personnel utilisateur d'un système d'information, qui constate un événement susceptible de générer un incident de sécurité informatique, doit le signaler, sans délai au service compétent.

REG 3-A-6 : Les données à caractère personnel doivent être protégées et traitées conformément aux dispositions de la **CIRCULAIRE N° 003 / CAB / PM DU 28 Mars 2018** relative à la gestion des documents et données confidentiels de l'Etat et des organismes du secteur public. Faisant suite à l'Instruction **n° 013/CAB/PRF du 06 août 1968** sur la protection du secret.

B. Affectation du personnel

L'objectif visé est de gérer et limiter les risques liés aux départs et mutations du personnel.

REG 3-B-1 : En cas de mutation, de changement de personnel, de rupture de contrat ou de fin de contrat, tous les aspects relatifs à la sécurité de l'information doivent être pris en compte :

- La gestion et la révocation des comptes et des droits d'accès au système d'information ;
- La gestion du contrôle d'accès aux locaux ;
- La gestion des équipements mobiles ;
- La gestion du principe d'habilitation ainsi que des principes du besoin d'en connaître et d'utiliser.

C. Sensibilisation et formation du personnel à la sécurité du système d'information

Le but recherché est de faire prendre conscience des enjeux de la sécurité du système d'information aux utilisateurs et limiter les risques d'actes malveillants.

REG 3-C-1 : Un programme de sensibilisation et de formation à la sécurité des systèmes d'information doit être élaboré, revu et régulièrement mis à jour. Ce programme doit être cohérent avec la PSSI du MINFI.

REG 3-C-2 : Ce programme doit prendre en compte les différents niveaux de responsabilités du personnel du MINFI.

REG 3-C-3 : Ce programme doit être mis à jour régulièrement afin de prendre en compte les nouveaux personnels et les enseignements tirés des incidents liés à la sécurité de l'information déjà survenus.

REG 3-C-4 : Ce programme doit faire apparaître clairement l'engagement du MINFI sur la problématique de la sécurité du système d'information.

REG 3-C-5 : Un programme de formation continue doit être mis en place pour les personnels qui sont chargés de veiller à l'application effective de la PSSI, afin qu'ils soient informés sur les menaces et vulnérabilités les plus récentes (veille technologique).

IV. ACQUISITION ET DEVELOPPEMENT DES SYSTEMES INFORMATIQUES AU MINFI

L'objectif est d'Intégrer la sécurité durant tout le cycle de vie des systèmes informatiques au MINFI. Il s'agit notamment de spécifier les exigences liées à la sécurité de l'information lors de l'acquisition et/ou du développement puis de la mise en exploitation des nouveaux systèmes informatiques.

A. Acquisition de nouveaux systèmes

Intégrer la sécurité au début de chaque projet d'acquisition de nouveaux systèmes informatiques, en mettant en place une procédure qui permet de réduire les risques.

REG 4-A-1 : Prendre en compte les exigences liées :

- Au contrôle d'accès et à la sensibilisation des utilisateurs sur leurs responsabilités ;

- À la protection pour ce qui concerne la disponibilité, la confidentialité et l'intégrité de l'information et du système d'information ;
- À la journalisation, la surveillance et la détection des fuites de données.

B. Développement de logiciels

Il s'agit d'adopter une méthodologie de développement sécurisé et de veiller à sa mise en œuvre effective en appliquant les mesures suivantes :

REG 4-B-1 : Sécuriser les locaux utilisés pour le développement de logiciels et appliquer les recommandations relatives à la sécurité du langage choisi, notamment dans les phases de conception, du choix des référentiels, du contrôle des versions et de la correction du code source.

REG 4-B-2 : Appliquer les normes et standards en vigueur sur le développement sécurisé des applications (*ISO, IEC, OWAPS*, ...).

REG 4-B-3 : En cas d'externalisation du développement des logiciels, le maître d'œuvre doit se conformer aux exigences de sécurité citées supra, mais aussi considérer les problèmes relatifs aux licences d'utilisation, à la qualité du développement et aux tests sécurité à réaliser pendant le développement.

V. GESTION DES ACTIFS

Les actifs du MINFI, notamment en matière de système d'information, doivent être identifiés et affectés à des responsables qui doivent en assurer la protection.

A. Inventaire et responsabilités relatifs aux actifs

REG 5-A-1 : Procéder à un inventaire précis des actifs du MINFI afin de les identifier et les mettre à jour.

REG 5-A-2 : Affecter les actifs à des responsables désignés qui sont chargés d'assurer leur sécurité (classification, protection et contrôle d'accès).

REG 5-A-3 : Identifier, documenter, et mettre en œuvre des règles d'utilisation correcte de l'information, des actifs associés à l'information et des moyens de traitement de l'information.

REG 5-A-4 : Veiller à la restitution effective des actifs dans leur totalité, en cas de fin de contrat ou de mission.

REG 5-A-5 : Procéder à une classification des informations suivant leur sensibilité et leur criticité

B. Manipulation des supports d'information

REG 5-B-1 : Les informations stockées sur des supports amovibles doivent être protégées contre toute divulgation, modification ou destruction.

REG 5-B-2 : Pour les matériels qui doivent être mis au rebut, il faut procéder à un effacement sécurisé des données qui y sont stockées.

VI. RELATION AVEC LES FOURNISSEURS

Il est question de garantir la protection des actifs du MINFI accessibles aux fournisseurs. La sécurité des systèmes d'information du MINFI englobe tous les aspects, notamment organisationnel, technique, physique et environnemental.

A ce titre, tous les intervenants qui ont accès au système d'information sont concernés par sa sécurité. Ainsi, les fournisseurs de service, qui sont amenés à intervenir au sein du système d'information, doivent se conformer à la PSSI pour assurer la confidentialité, l'intégrité et la disponibilité des données de l'information et du système d'information.

A. Sécurité de l'information dans la relation avec les fournisseurs

REG 6-A-1 : Mettre en place une politique de sécurité applicable aux différents fournisseurs (logistique, finance, informatique, . . .).

REG 6-A-2 : Mettre en place des procédures permettant de surveiller la conformité aux exigences de sécurité de l'information pour chaque fournisseur.

REG 6-A-3 : Mettre en place un programme de sensibilisation du personnel, en contact avec les fournisseurs sur les règles de sécurité applicables à ces derniers, ainsi que sur le niveau d'accès au système d'information.

REG 6-A-4 : Mettre en place une charte de sécurité signée par les différentes parties qui doivent s'engager à en respecter scrupuleusement les clauses.

REG 6-A-5 : Rappeler les exigences légales et réglementaires sur les lois relatives à la protection des données à caractère personnel, sur les droits d'auteur et sur la propriété intellectuelle, et veiller à leur respect.

REG 6-A-6 : Mettre en place un point focal qui sera chargé de communiquer sur les questions de sécurité avec les fournisseurs.

B. Prestations de service et sécurité de l'information

REG 6-B-1 : Tous les intervenants doivent être pris en compte, notamment les sous-traitants qui travaillent pour le compte des fournisseurs.

REG 6-B-2 : Les clauses contractuelles entre les fournisseurs et le MINFI doivent intégrer toute la chaîne d'approvisionnement informatique à savoir ; (i) conformité avec les normes relatives à la sécurité des produits informatiques et (ii) publication des exigences de sécurité satisfaites par leurs produits et en fournir la preuve.

REG 6-B-3 : Mettre en place des procédures d'audit sur les prestations effectuées par les fournisseurs ainsi que sur la qualité de ces prestations.

VII. SÉCURITÉ PHYSIQUE

A. Zones sécurisées

L'objectif est d'empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information du MINFI.

REG 7-A-1 : Tous les centres de traitement des données, les salles des serveurs, les salles d'exploitation, les installations de stockage, les salles de service et les salles des équipements réseau doivent être considérées comme des zones sécurisées.

REG 7-A-2 : L'accès à ces zones doit être autorisé et contrôlé.

REG 7-A-3 : Tous les droits d'accès doivent être immédiatement révoqués en cas de départ à la retraite de l'agent, de démission, de suspension, de mutation ou de congé de longue durée.

REG 7-A-4 : Les enregistrements d'accès doivent être régulièrement sauvegardés et conservés pendant une période déterminée.

REG 7-A-5 : Les équipements-clés doivent être installés dans un emplacement non accessible au public. Ils doivent être configurés de manière à empêcher toute fuite d'information sensible, notamment par rayonnement électromagnétique.

REG 7-A-6 : Les répertoires et les annuaires téléphoniques internes, identifiant les emplacements des moyens de traitement de l'information sensible ne doivent pas être accessibles sans autorisation.

REG 7-A-7 : Le personnel doit être informé de l'existence des zones sécurisées et n'avoir accès que sur la base des principes du besoin d'en connaître et d'utiliser.

REG 7-A-8 : Le travail sans surveillance dans les zones sécurisées doit être évité pour des raisons de sécurité.

REG 7-A-9 : Les zones sécurisées inoccupées doivent être physiquement verrouillées et contrôlées périodiquement.

REG 7-A-10 : L'utilisation d'équipements photo, vidéo, audio ou d'autres dispositifs tels que les caméras intégrées à des appareils mobiles, doit être interdite, sauf autorisation.

REG 7-A-11 : Désigner la zone d'approvisionnement pour les matières entrantes (accès restreint au personnel de livraison).

REG 7-A-12 : Inspecter les matières entrantes, par des équipements appropriés, pour vérifier la présence éventuelle de substances dangereuses (substances explosives, chimiques, ou autres) avant qu'elles ne quittent la zone de livraison et de chargement.

REG 7-A-13 : Enregistrer les matières entrantes dès leur arrivée sur le site conformément aux procédures d'enregistrement des actifs.

B. Sécurité des matériels

L'objectif est d'empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités du MINFI.

REG 7-B-1 : Les installations sensibles doivent être équipées des systèmes d'alarme périodiquement contrôlés.

REG 7-B-2 : Tout le matériel doit être installé dans des salles sécurisées. Les portes et les fenêtres ne doivent pas être des moyens d'accès ou de connexion au matériel de l'extérieur de la zone sécurisée. Des issues de secours doivent être prévues sur tous les sites.

REG 7-B-3 : Dans tous les sites sensibles, des dispositifs de détection et de lutte contre l'incendie tels que les détecteurs de fumée et les extincteurs, doivent être installés, contrôlés et testés régulièrement.

REG 7-B-4 : faire inspecter et tester régulièrement les installations électriques pour s'assurer de leur bon fonctionnement (systèmes d'éclairage, interrupteurs, câbles électriques, générateur de secours, . . .).

REG 7-B-5 : Tous les équipements sensibles doivent disposer d'une alimentation électrique permanente.

REG 7-B-6 : Le matériel doit être installé sur un support surélevé et des systèmes de détection de fuite d'eau doivent être installés dans les sites sensibles.

REG 7-B-7 : Des systèmes de climatisation, de ventilation, d'alimentation en gaz et d'évacuation des eaux usées doivent être installés, entretenus et vérifiés régulièrement pour empêcher d'éventuels endommagements des actifs et l'interruption des activités de l'entité. Des appareils de mesure de l'humidité et de la température doivent être prévus.

REG 7-B-8 : Les sites de reprise après sinistre et de stockage de données doivent être installés à des endroits très éloignés du site principal.

REG 7-B-9 : Le matériel ou le support de stockage défectueux et les pièces de rechange, mis au rebut, doivent être stockés dans une pièce séparée qui doit être en permanence verrouillée.

REG 7-B-10 : Les équipements doivent être nettoyés régulièrement pour éviter la présence de poussière.

REG 7-B-11 : Il doit être strictement interdit d'effectuer des activités autres que celles prévues dans les salles abritant des équipements sensibles.

REG 7-B-12 : Il doit être strictement interdit de manger, de boire et de fumer à l'intérieur de la zone sécurisée.

REG 7-B-13 : Les câbles électriques doivent être séparés des câbles de télécommunication pour empêcher les interférences.

REG 7-B-14 : Tous les câbles de télécommunication doivent être fiables et installés dans des conduits. Des câbles redondants doivent être installés pour assurer une reprise rapide de services.

REG 7-B-15 : Les panneaux de brassage et les salles des câbles doivent être isolés des zones d'accueil du public avec un accès contrôlé.

REG 7-B-16 : Les panneaux de répartition électrique ainsi que les chambres de câblage doivent être strictement contrôlés et l'accès limité au personnel autorisé.

REG 7-B-17 : Les activités de maintenance doivent être effectuées sous une surveillance étroite et adéquate. En cas d'intervention d'un prestataire, un représentant du MINFI doit toujours être présents et veiller à ce qu'aucun fichier ou programme de données ne soit copié.

REG 7-B-18 : Les dossiers de maintenance doivent être conservés pour suivi.

REG 7-B-19 : En cas de remise d'un équipement pour réparation, les données qui y sont contenues doivent être sauvegardées dans d'autres supports et être supprimées de manière sécurisée.

REG 7-B-20 : Les supports amovibles de stockage de données sensibles tels que les disques durs, les disquettes, les bandes magnétiques, les CDROM, les DVD, les Blu-ray, les clés USB, les cartes SD, les cartes à puces ..., doivent être conservés dans un coffre ou une armoire au même titre que les documents et correspondances sensibles sur support papier.

REG 7-B-21 : Toute sortie de clé doit être contrôlée, et les personnes autorisées doivent être désignées par l'autorité responsable.

REG 7-B-22 : Les fichiers contenant des informations classifiées et qui sont périmées doivent être effacés. Cette destruction ne doit pas être uniquement logique mais elle doit être accompagnée d'un effacement physique pour prévenir toute possibilité de lecture.

REG 7-B-23 : Les documents contenant des informations sensibles ou classifiées doivent être immédiatement retirés des imprimantes, des photocopieuses, des scanneurs, des appareils de télécopie après leur utilisation.

REG 7-B-24 : En l'absence de leurs utilisateurs, les ordinateurs et les terminaux doivent être déconnectés ou protégés par un verrouillage automatique (délai court) de l'écran ou du clavier contrôlé par un mot de passe ou tout autre mécanisme d'authentification.

VIII. SÉCURITÉ LOGIQUE

L'objectif est de protéger le système d'information contre toute intrusion et d'assurer la confidentialité des données. La sécurité logique est composée de la sécurité des accès, de la sécurité des applicatifs et de la sécurité des échanges.

A. Sécurité des accès

REG 8-A-1 : Spécifier les mesures de sécurité pour les applications métiers.

REG 8-A-2 : Appliquer le principe du besoin d'en connaître : « Nul ne peut, du seul fait de son grade ou son titre, avoir accès aux informations sensibles s'il n'est pas habilité et s'il n'a pas besoin d'en connaître pour réaliser ses tâches ».

REG 8-A-3 : Appliquer le principe du besoin d'en utiliser : « Nul ne peut, du seul fait de son grade ou son titre, avoir accès aux moyens de traitement des informations

sensibles, s'il n'est pas habilité et s'il n'a pas besoin de les utiliser pour accomplir son travail ».

REG 8-A-4 : Effectuer un cloisonnement des rôles pour le contrôle des accès.

REG 8-A-5 : Mettre à jour régulièrement les droits d'accès attribués aux utilisateurs.

REG 8-A-6 : Revoir régulièrement les privilèges et les droits d'accès en cas de changement de poste de travail.

B. Sécurité des applicatifs

REG 8-B-1 : Un mécanisme permettant de contrôler l'accès aux fonctions des applications doit être mis en place.

REG 8-B-2 : Les droits d'accès des utilisateurs doivent être contrôlés (lecture, écriture, suppression, . . .).

REG 8-B-3 : Une technologie d'authentification forte doit être utilisée lorsque les données sont classifiées.

REG 8-B-4 : Il faut limiter le nombre de connexions non autorisées aux applications.

REG 8-B-5 : Il ne faut pas afficher d'informations qui peuvent fournir des indications lors d'une tentative de connexion non autorisée.

REG 8-B-6 : Les mots de passe par défaut doivent être impérativement changés.

REG 8-B-7 : Il faut mettre en place un système de contrôle des tentatives de connexion automatique et fermer les sessions inactives au bout d'un certain temps d'inactivité. Toutes les tentatives de connexion doivent être journalisées.

REG 8-B-9 : Les mots de passe doivent être robustes. Ils ne doivent pas être transmis en clair. Il faut les changer régulièrement suivant une périodicité définie.

REG 8-B-10 : Il faut prévenir rigoureusement et interdire formellement l'installation de logiciels sans l'autorisation du responsable de la Sécurité des Systèmes d'Information.

REG 8-B-11 : Les applications ou utilitaires non indispensables doivent être désinstallés.

REG 8-B-12 : L'accès au code source des applications doit être contrôlé afin d'en assurer l'intégrité.

C. Sécurité des échanges

REG 8-C-1 : Il faut mettre en place une politique d'accès aux réseaux du MINFI, qui précise les exigences d'authentification des utilisateurs.

REG 8-C-2 : Il faut définir les responsabilités et les procédures de gestion des équipements réseaux.

REG 8-C-3 : Les moyens de transmission de l'information doivent être conformes à la réglementation en vigueur.

REG 8-C-4 : Il faut mettre en place un mécanisme de surveillance et de journalisation de toutes les activités dans le réseau.

REG 8-C-5 : Les services de réseau doivent, en accord avec le fournisseur de services, être sécurisés par des fonctions de sécurité : l'authentification, l'intégrité, le chiffrement, la non répudiation et les contrôles de connexion réseau.

REG 8-C-6 : Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifiques.

REG 8-C-7 : Il faut effectuer un cloisonnement, physique et/ou logique des réseaux informatiques, suivant un critère bien défini pour séparer les réseaux : par service administratif, par niveau de sécurité, etc.

REG 8-C-8 : Dans le cas d'une interconnexion avec une autre administration ou lors de la mutualisation des moyens de traitement de l'information, il faut effectuer une analyse des risques afin de protéger les systèmes contenant des informations sensibles.

REG 8-C-9 : Il faut sensibiliser le personnel sur les risques de divulgation des informations classifiées.

REG 8-C-10 : Les données transmises par le biais d'équipements électroniques doivent respecter la législation sur les transactions électroniques et les différents décrets d'application.

REG 8-C-11 : Chiffrer une ou plusieurs parties des disques durs des systèmes informatiques contenant les informations sensibles.

REG 8-C-12 : Lorsque le matériel ou le système informatique est mis hors service, en plus de l'effacement sécurisé des disques, l'intégralité de ces disques doit être chiffrée pour réduire le risque de divulgation de l'information sensible.

REG 8-C-13 : Il faut mettre en place une politique rigoureuse de gestion des clefs de chiffrement afin d'en assurer la protection, sans faille, durant tout leur cycle de vie.

REG 8-C-14 : Il faut former les utilisateurs à l'emploi correct des matériels et des logiciels de chiffrement.

IX. SÉCURITÉ DE L'EXPLOITATION

Cette partie vise la protection du système d'information des différentes menaces liées à la mauvaise exploitation des applications métiers ou utilitaires.

A. Responsabilités liées à l'exploitation

REG 9-A-1 : les procédures d'installation et de configuration des systèmes doivent être établies et documentées.

REG 9-A-2 : Les procédures de redémarrage et de récupération de chaque système, en cas de défaillance doivent être définies et documentées.

REG 9-A-3 : Les procédures de sauvegarde et de maintenance, pour chaque système, doivent être définies et documentées.

REG 9-A-4 : Les contacts du support technique doivent être disponibles et tenus à jour, pour faire face notamment aux difficultés d'exploitation.

REG 9-A-5 : Les normes de sécurité de l'équipement doivent être documentées et suivies.

REG 9-A-6 : L'installation de logiciels n'ayant aucun rapport avec les activités du MINFI doit être prohibée.

REG 9-A-7 : L'utilisation de logiciels sans une licence authentique, doit être strictement interdite.

REG 9-A-8 : Les procédures d'exploitation doivent être régulièrement auditées, contrôlées et mises à jour.

REG 9-A-9 : Les changements significatifs survenus dans le système doivent être consignés.

REG 9-A-10 Les changements et les phases de test doivent être planifiés.

REG 9-A-11 : Les changements ayant un impact sur la sécurité doivent faire l'objet d'une appréciation particulière.

REG 9-A-12 : Une procédure d'autorisation formelle des changements proposés doit être mise en œuvre.

REG 9-A-13 : Les exigences de sécurité de l'information doivent être formellement respectées.

REG 9-A-14 : Les informations détaillées sur les changements apportés doivent être transmisses à toutes les personnes concernées.

B. Séparation des environnements de développement, de test et d'exploitation

REG 9-B-1 : Les règles concernant le passage des logiciels du stade de développement au stade d'exploitation doivent être définies et documentées.

REG 9-B-2 : Les systèmes informatiques en cours de développement doivent être exécutés dans un environnement totalement distinct des environnements de production.

REG 9-B-3 : Toute modification à apporter au système et aux applications doit être au préalable exécuté dans un environnement de test avant application au système en exploitation.

REG 9-B-4 : Les activités de développement doivent être séparées des activités de test.

REG 9-B-5 : Les compilateurs, les éditeurs et les autres outils de développement ou les utilitaires systèmes ne doivent pas être accessibles depuis les systèmes en exploitation lorsqu' ils ne sont pas nécessaires.

REG 9-B-6 : Les utilisateurs doivent utiliser des profils différents pour les systèmes en exploitation et les systèmes de test, et les menus doivent afficher les messages d'identification adéquats pour réduire le risque d'erreur.

REG 9-B-7 : Il est recommandé de ne pas copier les données sensibles dans l'environnement du système de test, à moins qu'il ne soit doté de mesures de sécurité équivalentes.

C. Protection contre les logiciels malveillants

REG 9-C-1 : Un outil de protection contre les logiciels malveillants doit être installé et maintenu à jours sur tous les serveurs, les ordinateurs fixes et les terminaux mobiles.

REG 9-C-2 : Des anti-spams doivent être installés sur les serveurs de messagerie. Des listes noires en temps réel doivent être utilisées pour bloquer les spams.

REG 9-C-3 : Des filtres de contenus doivent être installés pour empêcher l'utilisation de sites web malveillants ou suspectés en tant que tels.

REG 9-C-4 : Des procédures de continuité d'activités doivent être établies dans chaque structure après une attaque par logiciels malveillants, comprenant les sauvegardes de tous les logiciels et données nécessaires ainsi que les dispositions de sauvegarde.

REG 9-C-5 : Les utilisateurs doivent veiller à se protéger de l'introduction de logiciels malveillants qui peuvent contourner les mesures de protection habituelles, lors des opérations de maintenance et de dépannage.

REG 9-C-6 : Il est nécessaire de s'assurer que les bulletins d'alerte concernant les logiciels malveillants sont exacts et informatifs, et proviennent des sources qualifiées (publications réputées, sites internet fiables, éditeurs de logiciels contre les logiciels malveillants) pour distinguer les canulars des menaces réelles.

REG 9-C-7 : Les utilisateurs doivent être informés de l'existence de canulars et de la démarche à suivre s'ils en découvrent.

REG 9-C-8 : Une procédure de sauvegarde sur site et/ou hors site ou sur support de stockage amovible doit être définie et incluant la sauvegarde des données des utilisateurs, les configurations, les fichiers système et les messages électroniques.

REG 9-C-9 : Le stockage en ligne gratuit, offert par certains prestataires privés, doit être interdit.

REG 9-C-10 : Il est recommandé de protéger les données sensibles sauvegardées en les chiffrant avec des moyens de chiffrement labellisés par l'ANTIC.

REG 9-C-11 : Les locaux de stockage des données sensibles doivent être sécurisés.

REG 9-C-12 : Les supports de stockage des données sauvegardées doivent être étiquetés selon une convention standard applicable au MINFI.

REG 9-C-13 : Un test de restauration des données doit être effectué périodiquement pour vérifier l'intégrité des données sauvegardées. La fréquence de ces tests doit être proportionnelle au degré de sensibilité des systèmes.

REG 9-C-14 Les archives des données sauvegardées doivent être conservées pendant une durée déterminée, conformément aux lois et règlements en vigueur. Pour empêcher la perte des données archivées, à cause de l'obsolescence des moyens utilisés, celles-ci doivent être réécrites en utilisant les techniques modernes d'archivage.

REG 9-C-15: Les journaux d'événements doivent contenir les informations suivantes: les identifiants des utilisateurs ; les activités du système ; la date, l'heure et les détails relatifs aux événements significatifs (exemple: ouvertures et fermetures de sessions) ; l'identité ou l'emplacement du terminal si possible et l'identifiant du système ; les enregistrements des tentatives d'accès au système réussies ainsi que celles avortées ; les enregistrements des tentatives d'accès aux données et autres ressources, réussies ou avortées; les modifications apportées à la configuration du système ; l'utilisation des privilèges ; l'emploi des utilitaires et des applications ; les

fichiers qui ont fait l'objet d'un accès et la nature de l'accès ; les adresses et les protocoles du réseau ; les alarmes déclenchées par le système de contrôle d'accès.

REG 9-C-16 : Les moyens de journalisation de l'information doivent être protégés contre les risques de falsification et les risques d'accès non autorisés.

REG 9-C-17 : Il est indispensable de journaliser les activités de l'administrateur système et les activités de l'opérateur système, protéger et revoir régulièrement les journaux.

REG 9-C-18 : Un système de détection des intrusions hors du contrôle des administrateurs système et réseau doit être utilisé pour vérifier la conformité des activités d'administration système et réseau.

REG 9-C-18 : Tous les événements majeurs doivent être enregistrés sur n'importe quel ordinateur ou système manipulant des données sensibles y compris, mais sans s'y limiter, les échecs de connexion, les modifications de données, l'utilisation de comptes privilégiés, les changements de mode d'accès, les modifications apportées aux logiciels installés ou au système d'exploitation et les modifications apportées aux autorisations accordées aux utilisateurs.

REG 9-C-19 : Toutes les horloges système, les horloges des ordinateurs et des périphériques réseau doivent être synchronisées à un serveur de temps central protégé des accès non autorisés.

D. Installation de logiciels sur les systèmes en exploitation

REG 9-D-1 : La mise à jour des logiciels en exploitation, des applications et des bibliothèques des programmes doit être effectuée par des administrateurs qualifiés après autorisation du responsable de l'entité.

REG 9-D-2 : Les correctifs doivent être appliqués sur un site de test, et si aucune anomalie n'est constatée, ils sont appliqués sur le site de production. Les correctifs critiques doivent avoir une haute priorité et être immédiatement installés.

REG 9-D-3 : Les responsables des processus dépendants d'un logiciel doivent être informés avant l'application d'un correctif critique.

REG 9-D-4 : Une sauvegarde complète doit être effectuée avant l'application d'un correctif.

REG 9-D-5 : Les correctifs doivent être installés manuellement sur les systèmes qui ne sont pas connectés à internet.

REG 9-D-6 : Les ordinateurs qui sont connectés à internet doivent être configurés pour télécharger automatiquement les mises à jour recommandées.

REG 9-D-7 : Les mises à niveau, mises à jour et correctifs doivent être journalisés par l'administrateur système dans un registre.

REG 9-D-8 : Si l'application automatique d'un correctif ou d'une mise à jour affecte négativement les systèmes, il faut rétablir les systèmes originaux à partir des sauvegardes.

X. CLOUD COMPUTING, APPAREILS MOBILES ET TELE TRAVAIL

REG 10-1 : Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

REG 10-2 : L'hébergement des données sensibles du MINFI sur le territoire national est obligatoire, sauf dérogation dûment motivée et précisée dans une décision d'autorisation.

REG 10-3 : Sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'information, notamment les risques encourus dans le cadre du télétravail et de l'utilisation des terminaux mobiles dans les lieux publics, les salles de congrès, de réunions, de conférences et dans d'autres zones non sécurisées.

REG 10-4 : Les appareils mobiles doivent être physiquement protégés contre le vol, en cas de déplacement des utilisateurs. Ils doivent être mis sous clé et dotés de systèmes de verrouillage spéciaux.

REG 10-5 : Il est indispensable de mettre en place une politique de contrôle d'accès, protéger les appareils mobiles contre les logiciels malveillants, effectuer des sauvegardes et éviter l'installation d'applications non approuvées.

REG 10-6 : Il est indispensable d'empêcher la compromission et la divulgation des informations sensibles stockées et traitées par les appareils mobiles en utilisant les algorithmes de chiffrement labellisés par l'ANTIC.

REG 10-7 : Il est indispensable de veiller à ce que les appareils mobiles du MINFI ne soient utilisés que pour des usages professionnels.

REG 10-8 : Mettre en place un mécanisme d'effacement des données, en cas de perte d'appareils mobiles.

REG 10-9 : Éviter de se connecter au réseau du MINFI par l'intermédiaire de réseaux sans fil non sécurisés.

REG 10-10 : procéder au contrôle des appareils mobiles durant tout leur cycle de vie.

XI. MESURES CRYPTOGRAPHIQUES

REG 11-1 : Mettre en œuvre des procédures devant permettre l'usage des mesures cryptographiques et des moyens de la block Chain dans l'administration.

REG 11-2 : Les solutions de collecte des fonds par le biais des cryptoactifs doivent être étudiées et encadrées.

XII. GESTION DES INCIDENTS

REG 12-1 : Mettre en œuvre des procédures de surveillance, de détection, d'analyse et de signalement des événements et des incidents concernant les activités des réseaux.

REG 12-2 : Mettre en place, au sein du MINFI, une structure d'alerte et de réaction rapide à tout incident relatif à la sécurité des systèmes d'information, composée d'un personnel qualifié avec un point focal qui sert d'interlocuteur dans chaque structure.

REG 12-3 : Tout incident lié à la sécurité des systèmes d'information du MINFI doit être immédiatement remonté à la structure d'alerte et de réaction rapide. Les actions à mener doivent être coordonnées afin d'enrayer les attaques et d'assurer la continuité du fonctionnement des systèmes d'information.

REG 12-4 : Il est indispensable de revoir régulièrement le plan de continuité d'activités pour prendre en compte les changements intervenus dans le système d'information, afin d'en maintenir la validité et l'efficacité.

REG 12-5 : Les utilisateurs doivent être formés à la détection des actions suspectes ou anormales pouvant présager un incident lié à la sécurité des systèmes d'information (dysfonctionnements ou comportements anormaux du système d ' information)

REG 12-6 : La procédure de réponse aux incidents doit comprendre : une phase de recueil et d'analyse des preuves, une communication détaillée sur l'incident survenu, la méthode de traitement utilisée, etc.

REG 12-7 : La procédure relative au recueil de preuves doit prendre en compte les éléments suivants :

- La chaîne de traçabilité ;
- Les aptitudes et la sécurité du personnel pour effectuer la collecte des preuves numériques ;
- Les fonctions et les responsabilités du personnel ;
- La documentation ;
- Les séances d'information.

Il est indispensable d'appliquer la norme **ISO/CEI 27037** qui fournit les lignes directrices concernant l'identification, l'acquisition et la protection des preuves numériques.

REG 12-8 : Il est indispensable de déterminer la typologie des incidents de sécurité, et en tirer tous les enseignements nécessaires.

XIII. AUDIT ET CONFORMITÉ

REG 13-1 : Il est indispensable d'effectuer des audits pour s'assurer que les objectifs de sécurité sont atteints et que les politiques de sécurité sont conformes aux normes de sécurité en vigueur. Les rapports d'audit doivent être communiqués à l'ANTIC.

REG 13-2 : Les auditeurs des systèmes d'information du MINFI doivent être compétents.

REG 13-3 : Des rapports complets doivent être communiqués au MINFI, de telle sorte que des mesures puissent être prises lors de la planification des futurs projets sur la base de l'expérience actuelle.