REPUBLIQUE DU BURUNDI
MINISTÈRE DE LA COMMUNICATION, DES TECHNOLOGIES DE L'INFORMATION ET DES MÉDIAS
SECRETARIAT EXECUTIF DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (SETIC)

CONCEPT TYPE DES SYSTÈMES D'INFORMATION DES INSTITUTIONS PUBLIQUES

Septembre 2024

Secrétariat Exécutif des Technologies de l'Information et de la Communication

PAGE DE CONTRÔLE DU DOCUMENT

Titre	Concept Type des Systèmes d'Information des Institutions Publiques
Référence	CT-SIIP-2024-001
Version	V1.0
Date de Création	Le 27 / 09 / 2024
Date de Validation	
Statut du document	Mouture
Auteurs	Le SETIC et Les parties prenantes
Validateurs	Autorités compétentes
Destinataires	Institutions publiques et partenaires
Objectif	Mettre en place un cadre standardisé pour les systèmes d'information des institutions publiques, incluant des directives précises en matière de gestion des infrastructures réseaux, de communication, d'administration des systèmes, de cyber sécurité, ainsi que d'applications logicielles et de données.
Classification	Document Publique
Cycle de révision	Chaque année

HISTORIQUE DES RÉVISIONS

Date	Version	Modifications apportées	Auteurs
27 / 09 / 2024	V1.0	Création initiale	1. SETIC 2. Parties prenantes

TABLE DES MATIÈRES

SIGLES ET ABREVIATIONS

Sigles ou Abréviations	Significations
CTSIIP	Concept Type des Systèmes d'Information des Institutions Publiques
TIC	Technologies de l'Information et de la Communication
Mbps	Mégabits par seconde
UPS	Uninterruptible Power Supply ou Alimentation Sans Interruption (ASI)
SFP	Small Form Factor Pluggable ou Module enfichable de petit format
UTP	Unshielded Twisted Pair ou Câble à paires torsadées non blindées
RJ45	Registered Jack 45
FTP	Foiled Twisted Pair ou Câble à paires torsadées blindées
CAT	Category ou Catégorie
GHz	Gigahertz
CDIN	Centre de Données Intégré National
SETIC	Secrétariat Exécutif des Technologies de l'Information et de la Communication
SSD	Solid State Drive ou Disque à état solide
RAM	Random Access Memory ou (Mémoire à accès aléatoire)
Go	Gigaoctet
IP	Internet Protocol
MDM	Mobile Device Management
OS	Operating System ou (Système d'exploitation)
LTS	Long Term Support (Support à Long Terme)
HTTPS	HyperText Transfer Protocol Secure
LAN	Local Area Network
VPN	Virtual Private Network ou Réseau Privé Virtuel

IPsec	Internet Protocol Security
SSL	Secure Sockets Layer
TLS	Transport Layer Security
ACL	Access Control List (Liste de Contrôle d'Accès)
DMZ	Demilitarized Zone (Zone Démilitarisée)
IPS	Intrusion Prevention System (Système de Prévention des Intrusions)
IDS	Intrusion Detection System (Système de détection des Intrusions)
HTML5	HyperText Markup Language, Version 5 (Langage de balisage hypertexte, Version 5.)
VLAN	Virtual Local Area Network (Réseau Local Virtuel)
ATP	Advanced Threat Protection (Protection Avancée contre les Menaces)
MFA	Multi-Factor Authentication (Authentification multi-facteurs)
DNS	Domain Name System
A	Address
CNAME	Canonical Name
MX	Mail Exchange
ASCII	American Standard Code for Information Interchange
ICANN	Internet Corporation for Assigned Names and Numbers
IT	Information Technology (Technologie de l'information)
GED	Gestion Electronique des Documents
RGPD	Règlement Général sur la Protection des Données

GLOSSAIRE DES TERMES TECHNIQUES

Age du mot de passe : Durée d'utilisation d'un mot de passe avant modification ; gestion pour réduire les risques d'accès non autorisé.

ASCII (American Standard Code for Information Interchange) : Système de codage représentant du texte avec des valeurs numériques.

ASHRAE : Organisation qui établit des normes pour les systèmes de chauffage, ventilation et climatisation (HVAC&R : Heating, Ventilation, Air Conditioning and Refrigeration), notamment pour les Datacenters.

Antivirus : Logiciel conçu pour détecter et éliminer les logiciels malveillants.

Boîte à outils informatique : Ensemble de logiciels et matériels utilisés pour diagnostiquer et maintenir les systèmes informatiques.

Bande passante : Capacité d'un canal de communication à transmettre des données, mesurée en bits par seconde (bit/s) ou multiples (Kbit/s, Mbit/s, Gbit/s, etc.).

Coffre-fort à mot de passe : Outil sécurisé pour stocker et gérer des mots de passe, offrant des fonctionnalités de cryptage.

Conception de logiciel : Processus de planification et d'élaboration de la structure d'un logiciel pour répondre à des besoins spécifiques.

Datacenter : Installation large pour héberger une infrastructure informatique, incluant plusieurs serveurs et systèmes de sauvegarde.

DMZ (Demilitarized Zone) : Zone de réseau entre un réseau interne et externe, hébergeant des services accessibles au public.

DNS (Domain Name System) : Système traduisant les noms de domaine en adresses IP pour faciliter l'accès aux sites web.

IDS (Intrusion Detection System) : Système surveillant le réseau pour détecter des activités suspectes, générant des alertes sans bloquer le trafic.

IPS (Intrusion Prevention System) : Système de sécurité détectant et bloquant les activités malveillantes en temps réel.

ICANN (Internet Corporation for Assigned Names and Numbers) : Organisation gérant l'infrastructure d'Internet.

KPIs (Key Performance Indicators) : Métriques mesurant l'efficacité et la réussite d'une organisation par rapport à des objectifs définis.

Large bande : Technologies permettant une transmission de données à haute vitesse sur de grandes distances, capable de gérer simultanément divers types d'informations (voix, données, vidéos).

Logiciels open source : Programmes dont le code source est accessible et modifiable par tous, favorisant la collaboration.

Logiciels propriétaires : Programmes dont le code source est fermé, nécessitant une licence pour être utilisés.

Maintenance du logiciel : Processus de correction et d'amélioration d'un logiciel après son déploiement.

Maintenance préventive : Actions planifiées visant à optimiser le fonctionnement d'un système afin d'éviter la défaillance inattendue à l'avenir.

MFA (Multi-Factor Authentication) : Méthode de sécurité nécessitant plusieurs validations d'identité pour accéder à un système.

Mise à jour applicative : Installation d'une nouvelle version d'un logiciel pour corriger des bugs ou améliorer des fonctionnalités.

Normalisation : Établissement de normes techniques pour garantir l'interopérabilité et la qualité des produits informatiques.

Pare-feu : Dispositif de sécurité contrôlant le trafic de données entrant et sortant d'un réseau, protégeant les réseaux internes des menaces externes.

Pare-feu de nouvelle génération (NGFW) : Pare-feu avancé intégrant des fonctionnalités comme l'inspection approfondie des paquets et la prévention des menaces.

Panneau de brassage : Dispositif centralisant et connectant les câbles réseau, facilitant leur gestion.

Point d'accès (AP) : Dispositif permettant aux appareils sans fil de se connecter à un réseau câblé via Wi-Fi.

RGPD (Règlement Général sur la Protection des Données) : Réglementation européenne encadrant le traitement des données personnelles, entrée en vigueur le 25 mai 2018.

Routeur : Appareil dirigeant le trafic de données entre différents réseaux, connectant un réseau local à Internet.

Salle de communication est un espace plus restreint dédié aux équipements de réseau locaux (serveurs, routeurs, commutateurs) pour gérer les communications internes d'une organisation

Schéma de réseau logique : Représentation des flux de données et des connexions logiques entre composants d'un réseau, sans tenir compte de leur emplacement physique.

Schéma de réseau physique : Représentation de l'agencement matériel et topologique d'un réseau, incluant les équipements réseau et leurs connexions.

SSL (Secure Sockets Layer) : Protocole de sécurité chiffrant les données échangées entre un serveur et un navigateur.

Switch : Appareil connectant plusieurs périphériques dans un réseau local (LAN), permettant la communication entre eux.

TLS (Transport Layer Security) : Protocole successeur du SSL, assurant la sécurité des communications sur Internet.

Version LTS (Long Term Support) : Version d'un système d'exploitation bénéficiant d'un support prolongé pour assurer stabilité et sécurité.

VPN (Virtual Private Network) : Service créant une connexion sécurisée entre un utilisateur et Internet, masquant l'adresse IP.

VLAN (Virtual Local Area Network) : Technologie segmentant un réseau physique en plusieurs réseaux logiques distincts.

I. INTRODUCTION

I.1 Contexte et Justification

Dans un contexte mondial où les Technologies de l'Information et de la Communication (TIC) jouent un rôle central dans la modernisation des services publics, notre pays se trouve à un tournant critique de son développement numérique. Le processus de digitalisation des services publics a débuté, mais il est encore embryonnaire. A ce stade, plusieurs ministères et agences publiques ont lancé des initiatives TIC isolées, souvent sans coordination ni harmonisation. Chaque institution a développé ses propres systèmes, suivant des approches qui varient considérablement en termes de qualité, de sécurité, et de conformité aux normes et standards internationaux.

Cette situation a conduit à une fragmentation des efforts numériques, avec des solutions qui, dans de nombreux cas, ne sont ni interopérables ni compatibles entre elles. Cette absence de vision stratégique commune limite l'efficacité des investissements TIC et entrave la création d'un écosystème numérique cohérent et intégré au niveau national. De plus, le manque de normes et de protocoles unifiés expose les systèmes d'information publics à des risques accrus en matière de sécurité, de gestion des données, et de continuité des services.

Il devient donc impératif de définir une stratégie claire et unifiée pour le développement et la gestion des systèmes d'information publics. Cette stratégie s'aligne aux objectifs définis dans la « **Vision Burundi pays émergent en 2040 et pays développé en 2060 »** et garantit l'uniformité des pratiques, la conformité aux standards reconnus et l'optimisation des ressources disponibles, tout en assurant une protection adéquate des données et une sécurité renforcée des systèmes. Le Concept Type des Systèmes d'Information des Institutions Publiques (CTSIIP) s'impose ainsi comme un outil essentiel pour orienter la transformation numérique du secteur public, en établissant les principes directeurs, les normes, et les bonnes pratiques à adopter.

I.2 Objectifs et Public cible

I.2.1 Objectif global

Mettre en place un cadre standardisé pour les systèmes d'information des institutions publiques, incluant des directives précises en matière de gestion des infrastructures réseaux, de communication, d'administration des systèmes, de cyber sécurité, ainsi que d'applications logicielles et de données.

I.2.2 Objectifs spécifiques

Les objectifs spécifiques sont :

- Uniformiser les pratiques en établissant des standards communs pour le développement, le déploiement, et la gestion des projets TIC dans l'ensemble des institutions publiques ;
- Assurer l'interopérabilité et l'intégration des systèmes d'information développés, facilitant ainsi la communication et le partage d'informations entre les différentes entités publiques ;
- Mettre en place des politiques robustes de sécurité des systèmes d'information et de protection des données sensibles, conformément aux meilleures pratiques internationales ;
- Maximiser l'efficacité des investissements en TIC en évitant les duplications et en favorisant la mutualisation des ressources technologiques ;
- Renforcer les capacités par le développement des compétences techniques au sein des institutions publiques pour soutenir la mise en œuvre et la gestion durable des systèmes d'information ;
- Prôner la souveraineté numérique en exigeant le transfert des compétences aux techniciens locaux pour pérenniser la gestion des systèmes d'information.

I.2.3 Public cible

Le périmètre du CTSIIP couvre l'ensemble des institutions publiques et leurs partenaires.

I.3 Méthodologie d'Élaboration

L'élaboration de ce Concept Type repose sur une méthodologie collaborative, impliquant une consultation large des parties prenantes au sein des institutions publiques. Cette démarche comprend :

- Analyse des initiatives existantes des projets TIC déjà en cours ou achevés dans les différentes institutions, afin d'identifier les bonnes pratiques et les leçons à tirer ;
- Étude des modèles de CTSIIP et des standards adoptés dans d'autres pays ayant réussi leur transformation numérique, afin d'inspirer les orientations stratégiques ;
- Ateliers de travail et concertations de travail avec les responsables TIC des différents ministères pour harmoniser les visions et définir les priorités communes ;

- Validation de ce Document du CTSIIP rédigé, par des autorités compétentes, avec des ajustements éventuels en fonction des retours reçus ;
- Planification et mise en œuvre du document final qui servira de guide pour le déploiement des projets TIC, avec une feuille de route claire et des indicateurs de suivi pour mesurer les progrès réalisés.

Ce CTSIIP représente une opportunité unique pour notre pays de structurer et d'optimiser ses efforts en matière de digitalisation, en posant les bases d'une administration publique moderne, efficace, et résiliente face aux défis technologiques du futur.
Le chapitre suivant présente la vision stratégique pour une meilleure gestion des systèmes d'information publics.

II. VISION STRATÉGIQUE

II.1 Vision à Long Terme

Le CTSIIP vise à créer un écosystème numérique public intégré, sécurisé et centré sur l'utilisateur. L'objectif est de transformer les institutions publiques en entités modernes, capables de répondre efficacement aux besoins des citoyens et des entreprises.

II.1.1 Système d'Information Intégré

Créer un système d'information national cohérent qui facilite la communication et le partage sécurisé des données entre les différentes entités gouvernementales, assurant ainsi l'interopérabilité et l'accès simplifié aux services publics.

II.1.2 Gouvernance des Données et Sécurité

Traiter les données publiques comme un atout stratégique avec des politiques de sécurité robustes pour protéger les informations sensibles contre les cyber menaces.

II.1.3 Accessibilité et Inclusion Numérique

Garantir l'accessibilité des services numériques à tous les citoyens, en particulier ceux en situation de handicap ou dans des zones reculées, afin de réduire les inégalités.

II.1.4 Transformation Numérique et Innovation

Adopter des technologies émergentes pour réinventer les services publics et encourager l'innovation à tous les niveaux de l'administration.

II.1.5 Durabilité et Responsabilité Environnementale

Intégrer la durabilité dans la conception des systèmes d'information pour minimiser l'impact environnemental, notamment en réduisant la consommation d'énergie.

II.1.6 Renforcement des Capacités et transfert des compétences

Former continuellement le personnel public pour développer une culture numérique au sein des institutions publiques, favorisant l'innovation et l'adoption de nouvelles technologies. Exiger le transfert des compétences aux techniciens locaux pour pérenniser la gestion des systèmes d'information en vue de sauvegarder la souveraineté nationale dans le domaine du numérique.

II.2 Principes directeurs

II.2.1 Interopérabilité

Adopter des standards nationaux pour garantir l'échange fluide des données entre les systèmes publics.

II.2.2 Sécurité et confidentialité

Mettre en place des mécanismes de sécurité robustes pour protéger les données des citoyens.

II.2.3 Centrage sur l'utilisateur

Concevoir des services publics numériques en se concentrant sur l'expérience utilisateur, en impliquant les citoyens dans le processus de conception.

II.2.4 Innovation et agilité

Encourager l'adoption de méthodologies agiles et l'innovation pour répondre rapidement aux évolutions technologiques.

II.2.5 Durabilité

Concevoir des systèmes d'information durables en termes de coût et d'impact environnemental.

II.2.6 Transparence et rendement

Optimiser les ressources investies dans les TIC tout en garantissant la transparence des processus.

II.2.7 Collaboration

Promouvoir la collaboration entre les institutions publiques et les partenariats avec le secteur privé.

II.2.8 Formation continue

Mettre en place des programmes de formation pour développer les compétences en TIC des agents publics.

III. INFRASTRUCTURES RÉSEAUX ET COMMUNICATION

Cette section fournit des lignes directrices et des exigences pour le déploiement de réseaux informatiques dans les institutions pu en trois catégories.

III.1. Conception du réseau

La conception du réseau dans les institutions publiques doit prendre en considération les éléments suivants :

- **Nombre d'utilisateurs dans l'institution** : identifiez le nombre d'utilisateurs du réseau sur place et hors site ;

- **Services consultés ou proposés par l'institution :** les services doivent être définis et catégorisés en fonction des processus et des exigences de disponibilité ;

- **Technologie large bande** : doit être choisie en fonction de l'emplacement, des exigences commerciales institutionnelles et de l'implantation des bureaux. Les réseaux locaux sans fil sont conseillés pour des espaces de travail pratiques et modernisés ;

- **Exigence de bande passante** : l'exigence minimale de bande passante doit être conforme aux besoins des utilisateurs.

A base des recommandations des fournisseurs d'accès internet et de l'expérience utilisateur, le tableau ci-dessous dresse l'exigence minimale en terme de bande passante.

Tableau 1 : Exigence minimale de bande passante dédiée suivant le nombre d'utilisateurs

Nombre d'employés utilisant des Ordinateurs	Bande passante en Mbit/s	Suite	Nombre d'employés utilisant des Ordinateurs	Bande passante en Mbit/s
1-10	2		121-140	28
11-20	4		141-160	32
21-30	6		162-180	36
31-40	8		181-200	40
41-50	10		201-240	48
51-60	12		241-280	56
61-70	14		281-320	64
71-80	16		321-360	72
81-90	18		361-400	80
91-100	20		Au-dessus de 400	Gestion cas par cas
101-120	24			

- **Achat de bande passante Internet**
  - **Services Internet** : les institutions publiques doivent approvisionner tous leurs besoins en services Internet (connexion Internet 4G et Internet par fibre optique).
  - **Capacité de bande passante à acheter** : la bande passante doit être décidée en fonction des besoins de l'utilisateur prévu et de l'objectif d'utilisation, comme détaillé dans le tableau 1.

- **Schéma de réseau physique** : doit prendre en compte le nombre d'utilisateurs en fonction de la structure institutionnelle, de la conception intérieure du bâtiment et de la disposition des sièges (autrement dit si tous les utilisateurs sont assis au même étage ou répartis à des étages différents) ;
- **Schéma de réseau logique** : doit prendre en compte les systèmes, les services et les applications en fonction des processus métier institutionnels.

La conception de l'infrastructure de réseau physique et logique dans les institutions publiques doit être classée en quatre catégories en fonction du nombre de terminaux :

- **Catégorie 1** : Infrastructure réseau de petite taille pouvant accueillir jusqu'à 50 terminaux ;

- **Catégorie 2** : Infrastructure réseau de taille moyenne pouvant accueillir jusqu'à 100 terminaux ;
- **Catégorie 3** : Infrastructure de réseau de grande taille pour environ 200 terminaux ;
- **Catégorie 4** : Infrastructure réseau pour plus de 400 terminaux.

- **Sécurité des réseaux** : toutes les institutions publiques doivent se conformer aux directives de cyber sécurité adoptées.

III.2. Mise en œuvre du réseau

1) Équipement réseau

Les équipements et périphériques réseau constituant l'infrastructure réseau principale pour fournir des fonctionnalités de connectivité et de sécurité comprennent un rack, un minimum de routeurs, de commutateurs et de points d'accès, ainsi qu'un pare-feu. Tous les équipements devront provenir des fournisseurs mondialement reconnus.

2) Câblage réseau, étiquetage et disposition physique

Toute structure de réseau doit tenir en compte des dernières normes de câblage et d'étiquetage.

3) Salle de communication (salle des serveurs)

Les établissements devraient disposer de salles de communication à leurs locaux lorsque cela s'avère nécessaire et doivent respecter les exigences minimales suivantes :

Localisation	La salle de communication dans les locaux institutionnels doit être située dans un endroit isolé et accessible uniquement aux personnes autorisées.
Taille	Minimum en fonction du nombre d'équipements réseau
Contrôle de la température et de l'humidité	La température à maintenir et l'humidité de l'air doivent être contrôlées à un niveau conforme aux équipements, entre 18 °C à 27 °C (64°F à 81°F) et 20 % à 80 % pour l'humidité selon la norme ASHRAE TC 9.9, définie par ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers).
Considération structurelle (sol, plafond et murs)	Le sol doit être surélevé et bien préparé pour faciliter le nettoyage, le refroidissement à l'intérieur de la pièce et l'installation du câblage, afin de permettre l'élimination des poussières. Carreaux de sol pour faciliter le nettoyage. Les murs ne doivent pas avoir de fenêtres extérieures ni de conduits électriques, doivent avoir un capteur de blocage mural et la taille du cadre de porte devrait être suffisant pour permettre l'entrée /

	sortie facile de l'équipement, les portes doivent s'ouvrir à 180° vers l'extérieur, sur une largeur minimale de 90 cm et 2 m de haut. Seuls les équipements liés à la salle de communication doivent être présents dans la salle.
Système électrique	La salle de communication doit disposer d'au moins deux sources d'alimentation différentes dédiées, non commutées, avec redondance d'alimentation et alimentations de backup. Connecté à des UPS sur des circuits d'alimentation séparés, un interrupteur d'arrêt d'urgence et système de surveillance doit avoir un régulateur de tension automatique avec schéma de circuit et tableau de commutation principal pour tous les services, équipements système de mise à la terre et poteau d'éclairage. Un entretien régulier et des tests doivent être effectués.
Contrôle d'accès et de la sécurité	L'accès physique à la salle de communication doit être limité aux seules personnes ayant des responsabilités légitimes justifiant un tel accès. Le système de contrôle d'accès (carte d'accès ou biométrique) clavier ou porte verrouillable) doit être utilisé à tous les points d'entrée 24h/24 et 7j/7 et procédure claire pour garantir que l'accès est supprimé lorsqu'un individu n'a plus l'autorisation d'entrée. La liste des personnes ayant l'accès doit être révisée en cas de besoin. La salle de communication doit être équipée d'un système de prévention des incidents éventuels (incendies, inondations, rongeurs de câbles, etc.), d'extincteurs, un système de protection électrique automatique. Un système d'alarme et de caméras de vidéosurveillance doivent être installés pour surveiller et enregistrer tous les événements
Système d'armoire de la salle de communication	Les baies de brassage doivent être équipées d'au moins des rails de montage ajustables de 19U ou 24U, avec des points d'accès pour les passages de câbles d'alimentation et de données situés en haut et en bas. Toutes les armoires de brassage doivent être verrouillables et placées dans une zone sécurisée à l'intérieur de la salle de communication.

En plus des exigences minimales ci-dessus, les lignes directrices suivantes concernent les équipements réseau dans la salle de communication :

- **Commutateurs** : il est conseillé aux petites, moyennes et grandes institutions d'utiliser les commutateurs équipés au moins de 24 ports PoE, 10/100/1000 Base-T, avec au moins 4 ports SFP (Small Form Factor Pluggable). Des commutateurs à 48 ports pourront être utilisés par des grandes institutions. Toutefois, les commutateurs doivent être intelligents.
- **Panneaux de brassage (UTP Data Patch Panels)** : doivent être au moins de CAT 6, 24 ports ou plus selon la dernière technologie.
- **Routeurs** : doivent prendre en charge la communication module à module à large bande passante à des vitesses plus élevées en fonction de la plateforme, certains des ports Ethernet 10/100/1000 Base-T peuvent prendre en charge le SFP (Small Form Factor Pluggable) basé sur la connectivité en plus des connexions RJ45, permettant une connectivité à fibre ou cuivre.
- **Pare-feu** : la dernière sécurité du réseau par pare-feu doit être mise en œuvre. (Pour plus de détails sur les exigences, reportez-vous aux directives de cyber sécurité).
- **Points d'accès** : le nombre de points d'accès peut varier en fonction de la configuration architecturale du bâtiment. Les normes sans fil recommandées sont 802.11a/b/g/n/ac (2,4 GHz/5 GHz). Pour tout nouveau bâtiment public, il faut tenir en considération les chemins de câbles réseaux. **Câble Ethernet** : FTP CAT 6 ou types avancés.
- **Documentation** : Cela comprend les schémas du réseau, les informations de connexion et de configuration réseau, les adresses de tous les appareils du réseau avec des adresses IP statiques et les journaux de bord. Les versions des documents doivent être révisées périodiquement et toute modification doit être suivie.

III.3. Gestion du réseau

1) Performances du réseau

La redondance des équipements et liaisons, l'équilibrage de charge, le temps de réponse des applications et la qualité du service doivent être contrôlés et assurés.

2) Maintenance du réseau

Chaque institution doit élaborer un plan de maintenance du réseau, ainsi que le plan de reprise après sinistre et de continuité des activités.

IV. MATÉRIEL ET ÉQUIPEMENT DE L'UTILISATEUR FINAL

Cette partie se focalise sur le matériel informatique, notamment les serveurs, les ordinateurs, les scanners, les imprimantes, etc. Il précise la configuration matérielle recommandée et le système d'exploitation le cas échéant.

IV.1. Serveurs

Les institutions publiques sont tenues d'héberger toutes leurs données et serveurs dans le Centre de Données Intégré National (CDIN) hébergé au SETIC.

Ces serveurs peuvent inclure des serveurs Web, des serveurs de messagerie, un serveur de fichiers (applications), du stockage et d'autres systèmes informatiques.

IV.2. Ordinateurs et appareils de communication

Voici les exigences minimales qui doivent guider les institutions publiques lors de l'acquisition d'ordinateurs et d'appareils de communication à usage de bureau ou à toute autre fin administrative.

1) Ordinateur de bureau/portable

La configuration minimale requise en fonction du but d'utilisation.

- Disque dur : 256 Go SSD ;
- Processeur : Core i5, 10ème Génération, 2 cœurs avec processeurs logiques de vitesse minimum de 2.0 GHz chacun ;
- Mémoire : 4 Go de RAM ;
- Taille de l'écran : 14" ;
- Système d'exploitation : Windows/MacOS/Linux avec Licence valide ;
- Alimentation sans interruption (UPS) pour ordinateur de bureau.

2) Téléphone IP

Il devrait être utilisé lorsque cela est jugé nécessaire.

3) Appareils mobiles personnels

Ils peuvent être utilisés et une politique de « bring your own device » (BYOD) doit être définie pour garantir un accès sécurisé au réseau de l'établissement.

En français, cette politique est traduite « Apportez Votre Propre Appareil » (AVPA) qui est une approche adoptée par les entreprises permettant aux employés d'utiliser leurs appareils personnels (comme des smartphones, tablettes, ou ordinateurs portables) pour accéder aux ressources et aux réseaux de l'entreprise. Cette politique peut offrir des avantages comme la flexibilité et la réduction des coûts pour l'entreprise, mais elle soulève aussi des préoccupations en matière de sécurité, de gestion des données, et de confidentialité, car les appareils personnels peuvent être plus vulnérables aux cyberattaques et aux violations de données.

Pour atténuer ces risques, les entreprises mettent souvent en place des mesures de sécurité spécifiques, comme des protocoles de chiffrement, des applications de gestion des appareils mobiles (MDM) et des directives strictes sur l'utilisation de ces appareils.

IV.3. Alimentation électrique et de secours

L'infrastructure du réseau informatique dans les locaux de l'institution doit disposer d'une alimentation électrique principale et d'une source d'énergie de secours. Les spécifications générales sont fournies dans le contrat cadre qui régit l'acquisition des appareils informatiques et de l'alimentation électrique associée ainsi que des solutions de secours.

IV.4. Scanners et imprimantes

Il est recommandé aux institutions publiques d'acquérir des équipements tels que les imprimantes, les scanners et les photocopieurs qui devraient être mis en réseau. La meilleure pratique recommandée consiste à utiliser des équipements multifonction.

IV.5. Équipement d'utilisateur final

1) Appareils utilisateur

Les appareils institutionnels doivent être étiquetés et enregistrés. Une dénomination appropriée doit être effectuée, conformément à la configuration conseillée du réseau.

Ils ne doivent pas être utilisés pour traiter, distribuer ou stocker illégalement des données protégées par le droit d'auteur de la propriété intellectuelle. Ceux-ci ne doivent être utilisés dans aucune activité qui contribuent à diminuer la productivité des employés.

2) Règles d'entretien

Les bureaux avec équipements TIC doivent être fermés à clé pour éviter le vol et d'autres risques :

- Les équipements TIC ne doivent pas être placés à côté de climatiseurs car l'humidité et la chaleur peuvent réduire la durée de vie des composants internes ;

- Les utilisateurs ne doivent pas manger, boire ou fumer à proximité d'équipements TIC car cela peut entraîner des risques pour la sécurité ;
- Seuls des chiffons humides et **des produits de nettoyage** appropriés doivent être utilisés pour nettoyer les claviers d'ordinateur, les écrans, les imprimantes et autres équipements TIC ;
- Dans la mesure du possible, les équipements TIC ne doivent pas être connectés à la même alimentation électrique que d'autres appareils consommateurs d'énergie ;
- Tous les autres équipements TIC introduits dans les locaux gouvernementaux doivent être identifiés et enregistrés au point de contrôle de sécurité à l'entrée.

3) Les équipements informatiques volé

En cas de vol d'un équipement, le responsable doit immédiatement le signaler au superviseur, au bureau chargé d'enquêter et à l'administration responsable ; les règles et règlements internes de l'institution doivent être appliqués.

4) Responsabilités des utilisateurs

Les utilisateurs doivent garantir une utilisation appropriée des équipements TIC conformément à toutes les dispositions de ces lignes directrices :

- Les utilisateurs sont tenus de signaler tout comportement inhabituel des équipements TIC ou d'alerter les responsables informatiques des menaces potentielles pesant sur les équipements TIC ;
- Il est de la responsabilité de l'utilisateur de demander conseils au service informatique ou à toute division connexe du service en cas de doute sur ce qui constitue une utilisation acceptable ou interdite de l'équipement TIC ;
- Bien que la sécurité physique et logique des équipements et des données TIC relève principalement de la responsabilité des institutions concernées, les utilisateurs doivent également prendre note qu'ils partagent cette responsabilité.

5) Responsabilité du service informatique

Les services informatiques de chaque institution publique doivent mettre en œuvre des mécanismes de gestion et de contrôles technologiques pour garantir, surveiller et faire respecter la conformité à la politique TIC et à ces directives.

IV.6. Maintenance du matériel

1) Plan de maintenance

Tous les équipements informatiques doivent être vérifiés une fois par trimestre et entretenus conformément au plan de maintenance élaboré.

2) Contrat de maintenance avec le fournisseur d'équipement

Après la période de garantie, des accords doivent être conclus avec les fournisseurs d'équipements et les prestataires de services et les services de maintenance doivent être fournis au moins tous les trimestres. Les éléments de service étendus tels que la formation, l'assistance téléphonique, les visites de maintenance préventive et les avantages de reprise doivent être pris en compte. Chaque type de contrat doit être examiné et évalué selon son propre mérite, la décision étant prise en compte, s'il est nécessaire de conclure un tel accord avant l'expiration du délai de la garantie.

3) Boîte à outils informatique

L'unité informatique doit être équipée de la boîte à outils informatique pour le matériel informatique et la maintenance du réseau.

V. APPLICATIONS LOGICIELLES ET DONNÉES

V.1. Applications logicielles

1) Modèle architectural pour les applications d'administration électronique

Tous les systèmes doivent être documentés selon cinq points de vue à savoir :

- Le point de vue de l'entreprise (décrit l'objectif, la portée et les processus) ;
- Le point de vue de l'information (détermine la structure et la sémantique des informations du système) ;
- Le point de vue informatique (décrit l'architecture et la fonctionnalité d'un système) ;
- Le point de vue technique (décrit l'approche utilisée,) ;
- Le point de vue technologique (décrit les outils, langages de programmation et frameworks, etc.).

2) Conception de logiciels

Comme principe, toute nouvelle conception de logiciel doit prendre en compte la sécurité dès la conception, la réutilisabilité, l'évolutivité, le partage d'informations, la satisfaction des utilisateurs,

l'amélioration de la productivité, la compatibilité et à travers le système national d'interopérabilité que le Burundi serait amené à mettre en place, le support unifié et la rentabilité.

3) Développement de logiciels

Pour harmoniser le déploiement des différentes applications et logiciels sur le Centre de Données Intégré National, le SETIC doit être consulté pour le choix des exigences technologiques.

L'institution publique peut opter pour le développement dans les cas suivants :

- Les exigences sont très spécifiques et ne peuvent être trouvées sur le marché ;
- Les solutions commerciales ont des prix prohibitifs ;
- Les fournisseurs de solutions commerciales ne fournissent pas de codes sources ;
- Le support est essentiel et ne doit pas être fourni par un fournisseur ; et
- L'institution doit avoir et s'assurer que les capacités de développement et de maintenance du logiciel sont disponibles en interne ou localement par des entreprises burundaises.

4) Acquisition d'un nouveau logiciel

Un Comité TIC compétent (au niveau institutionnel ou sectoriel) doit être consultée afin de déterminer si le nouveau logiciel est nécessaire et d'évaluer s'il doit être développé en interne ou en externe.

L'institution publique peut opter pour l'acquisition dans les cas suivants :

- Le logiciel est facilement et à moindre coût disponible sur le marché ;
- Le délai de livraison est extrêmement court ; ou
- La fiabilité du logiciel est très critique.

Les exigences minimales pour déterminer la meilleure solution entre le développement et l'acquisition d'un logiciel sont :

- **Coût total du cycle de vie** : comprenant le coût initial, l'installation, la formation et le coût récurrent de maintenance et d'assistance.
- **Maintenabilité** : facilité de modification (coût et effort) du logiciel pour corriger les défauts, améliorer les performances ou d'autres attributs ou s'adapter à un environnement modifié.
- **Interopérabilité** : cela inclut le support supplémentaire requis pour s'intégrer aux systèmes existants. Cela inclut également la flexibilité pour s'adapter aux changements au fil du temps et entre plusieurs systèmes.

- **Portabilité :** facilité d'utilisation du même logiciel dans différents environnements. Un environnement informatique peut inclure du matériel, des systèmes d'exploitation et des interfaces avec d'autres logiciels, utilisateurs et programmeurs.
- **Évolutivité** : capacité à prendre en charge la croissance future et un débit accru.
- **Disponibilité et accessibilité** : logiciel robuste et redondant (tolérant aux pannes) pour atteindre le niveau de service requis sans interruption due à une défaillance du logiciel.
- **Réutilisabilité** : capacité à utiliser le logiciel de manière répétée pour des exigences supplémentaires avec un coût supplémentaire minimal.
- **Fonctionnalité/performance** : capacité à répondre aux exigences opérationnelles de manière efficace et efficiente.
- **Sécurité** : capacité à protéger les données du système et l'environnement opérationnel contre toute perte ou compromission.
- **Les critères supplémentaires incluent** : la viabilité du fournisseur, les restrictions de licence, la part de marché du produit, les recommandations des clients, la fréquence des mises à niveau et l'obsolescence potentielle.

5) Logiciels propriétaires et open sources

Doivent être traités de la même manière selon les avantages et bénéfices pour le gouvernement, selon les principes de conception de logiciels définis et en ce qui concerne les besoins et exigences au niveau de l'institution.

6) Licence de logiciel

Seules les licences authentiques sont autorisées dans les institutions publiques. Le choix du mode de licence (basé sur l'utilisateur ou basé sur le serveur) doit tenir compte du rapport coût efficacité. L’acquisition de licences achetées en commun devrait se faire dans un cadre centralisé.

7) Maintenance du logiciel

Il devrait y avoir une équipe focale au niveau de l’institution qui devrait élaborer le plan de maintenance en collaboration avec le SETIC pour des audits périodiques du système, la maintenance, les mises à jour, l'évaluation des vulnérabilités, l'obsolescence de leurs systèmes, afin d'assurer une disponibilité maximale du système.

8) Suppression progressive des systèmes et logiciels

La suppression progressive ou mise à niveau de tout système doit être effectuée en collaboration avec le SETIC. La sécurité et la sauvegarde des données contenues dans ces systèmes doit être prise en compte.

9) Messagerie et collaboration

L'utilisation des emails professionnels doit être renforcée et chaque institution doit se conformer à la politique de sécurité de l'information.

10) Mise à jour applicative

Les applications installées au niveau des différentes institutions pourront être directement mises à jour à partir d'un serveur local des mises à jour. Le serveur de mise à jour reçoit automatiquement des mises à jour à partir des fournisseurs de mises à jour des applications

11) Antivirus

Le logiciel antivirus doit prendre en charge le serveur de licences local et le serveur de mise à jour applicative et une mise à jour automatique du serveur de licences local doit être fournie à partir du serveur du fournisseur et en cas de non disponibilité du serveur applicatif locale d'antivirus doit être capable d'obtenir les mises à jour directement auprès du fournisseur en cas de non disponibilité du serveur de mise à jour. L'antivirus doit prendre en charge toutes les versions disponibles des systèmes d'exploitation sur le marché et doit être indépendant du navigateur et de sa version. La fonctionnalité de déploiement réseau doit inclure les virus, l'état des mises à jour, l'utilisation des licences, l'état du client et les machines installées.

12) Sites Web

Tout site web d'une institution publique doit être conçu selon le modèle officiel. Il doit être hébergé dans le Centre de Données Intégré National et le contenu du web doit être mis à jour en temps opportun et doit être surveillé.

V.3. Données

1) Disponibilité des données

Les données doivent être disponibles 24 heures sur 24 pour un accès depuis différents fuseaux horaires.

2) Source de données

Doit être unique pour éviter la duplication des données autant que possible

3) Normalisation des données partagées

Doit être conforme à tout cadre d'interopérabilité défini au niveau institutionnel ou sectoriel.

4) Identificateurs de données

Chaque objet de données partagé doit être reconnu par un identifiant unique global.

5) Sauvegarde et récupération des données

Les institutions publiques sont tenues d'héberger tous les systèmes et applications informatiques qui traitent, stockent et fournissent les données et informations critiques du gouvernement dans le Centre de Données Intégré National (CDIN).

6) Catégories de données à protéger

Les données à protéger sont notamment des applications et bases de données, sites web, systèmes de messagerie, systèmes d'exploitation, données sur les ordinateurs personnels des institutions.

Les directives pour chaque catégorie de données sont les suivantes :

- Pour les systèmes et applications informatiques critiques hébergés dans le CDIN, l'institution doit s'assurer qu'ils souscrivent à un plan d'hébergement minimum comprenant des sauvegardes quotidiennes et des services de reprise après sinistre ;
- Pour les systèmes et applications informatiques critiques hébergés au sein de l'institution ou à l'étranger, l'institution publique doit adresser une demande officielle au Ministère ayant les TIC dans ses attributions pour la migration vers le Centre de Données Intégré National ;
- En attendant la migration complète des systèmes et applications informatiques critiques vers le CDIN, les institutions publiques sont tenues de se conformer au calendrier détaillé de sauvegarde des données indiqué dans la section précédente ;
- Pour les autres systèmes et applications informatiques jugés non critiques et conservés sur site, les institutions publiques sont tenues de se conformer à un calendrier de sauvegarde détaillé ;
- Pour les données gouvernementales se trouvant sur des ordinateurs personnels (ordinateurs portables et de bureau), les institutions publiques sont tenues de configurer un serveur de fichiers local qui se synchronise automatiquement avec les ordinateurs personnels des utilisateurs pour conserver des copies de tous les fichiers de données créés/mis à jour par les utilisateurs ;
- Les ordinateurs personnels doivent également être installés avec une version à jour d'Antivirus/Anti Malware et aucun utilisateur ne devrait être autorisé à conserver des

données gouvernementales sur un ordinateur personnel n'ayant pas d'Antivirus reconnu par l'institution ;

- Les Ordinateurs personnels, tablettes et serveurs installés avec les systèmes d'exploitation Windows/ Linux / Mac OS/Android/ iOS doivent être mis à niveau vers Windows/Linux/MacOS/Android/ iOS avec une version LTS (Support à Long Terme) valable pour deux ans minimum (pour les Ordinateurs de bureau, tablettes et portables) et au moins vers Windows Server / Linux / Unix valable pour deux ans minimum (pour les serveurs) nouvellement achetés. En attendant, les équipes techniques d'informaticiens appliqués doivent s'assurer qu'aucun ordinateur n'exécute encore du système d'exploitation obsolète dans aucune institution et que tous les systèmes en place sont mis à niveau.

VI. ADMINISTRATION SYSTÈME

L'administration système est une fonction essentielle dans la mise en œuvre des TIC. Elle implique une gamme d'activités allant de l'installation, du support de serveurs ou de systèmes informatiques à la réponse aux pannes de service et à d'autres problèmes connexes. Dans cette section, nous allons nous concentrer sur la gestion des utilisateurs, les utilitaires généraux de gestion du réseau, les politiques de mots de passe et les conventions de numérotation IP. Les mécanismes par lesquels les données stockées sur les systèmes informatiques appartenant à chaque institution publique et utilisées par les employés du gouvernement sont définies.

VI.1. Protection par mot de passe

- Le mot de passe ne doit pas être écrit sur papier ;
- Le mot de passe ne doit pas être envoyé par courrier électronique ;
- Le mot de passe ne doit pas être inclus dans un document stocké non crypté ;
- Le mot de passe ne doit pas être révélé par téléphone ;
- Le mot de passe ne doit pas être révélé ou suggéré sur un formulaire sur Internet ;
- Le mot de passe ne doit pas être « mémorisé » si la fonction « Mémoriser le mot de passe » dans le programme d'application tel qu'Internet Explorer, Google Chrome, Safari et Mozilla Firefox est utilisée ;
- Le mot de passe ne doit pas être utilisé sur un compte sur Internet qui ne dispose pas d'une connexion sécurisée (https) ;
- Le mot de passe ne doit pas contenir d'acronymes courants ;
- Le mot de passe ne doit pas avoir une orthographe inversée ;

- Le mot de passe ne doit pas utiliser une partie de votre nom de connexion ;
- Le mot de passe ne doit pas contenir de chiffres faciles à retenir, tels que anniversaires, numéros de téléphone, etc.

VI.2. Comptes de messagerie

Les employés officiels du gouvernement burundais ainsi que les visiteurs administratifs des départements doivent demander un compte utilisateur générique pour faciliter les opérations et les communications. Une demande doit-être faite auprès des services informatiques.
Les comptes génériques créés ne doivent pas être liés à un compte personnel (c'est-à-dire Gmail, Yahoo mail, etc.). Les comptes de messagerie seront vérifiés afin de ne pas inclure de noms associés à d'autres départements, par exemple : helpdesk (services informatiques) ; Tous les comptes de messagerie appartenant aux institutions publiques doivent avoir un domaine avec le suffixe gov.bi, par exemple @setic.gov.bi.

VI.3. Accès au système

1) Connexion au réseau local (LAN)

Les ordinateurs qui ont été en dehors de l'institution seront automatiquement mis à jour avec le dernier fichier de signature antivirus par un serveur.

2) Ordinateurs

Les utilisateurs doivent mettre fin aux sessions actives ou se déconnecter de leurs ordinateurs lorsqu'ils s'éloignent du poste de travail, à moins qu'ils ne verrouillent l'ordinateur, auquel cas ils devront ressaisir le mot de passe. Les bureaux, les salles informatiques et les installations de stockage doivent toujours être verrouillés lorsqu'ils sont sans surveillance. Le fait de ne pas appliquer la protection nécessaire à l'équipement constitue une négligence et l'utilisateur peut être tenu responsable de la perte. De plus, tous les utilisateurs doivent être responsables de la sécurité et de la garde de l'ordinateur portable au bureau et à l'extérieur du bureau.

3) Normalisation du matériel et des logiciels

Les administrateurs informatiques doivent normaliser les logiciels et le matériel informatique pour les utilisateurs en fonction, mais sans s'y limiter, de la fonction professionnelle, de la division et du principe du moindre privilège.

4) Exigence de mot de passe

- La longueur minimale recommandée du mot de passe est de 8 caractères ;

- La complexité minimale du mot de passe doit utiliser des minuscules, des majuscules, des chiffres et des caractères spéciaux ;
- Les mots de passe doivent être créés en gardant à l'esprit la sensibilité ;
- L'âge maximum du mot de passe ne doit pas dépasser 60 jours ;
- Un coffre-fort à mot de passe doit être utilisé pour conserver les mots de passe dans un endroit sécurisé ;
- Les ordinateurs doivent être verrouillés lorsque les utilisateurs sont loin de ces derniers ou en cas d'inactivité ;
- Les règles appliquées au mot de passe doivent également s'appliquer aux phrases secrètes utilisées pour l'authentification par clé publique/privée, comme un VPN ou tout autre système.

5) Fonctionnement des imprimantes et des scanners

Les utilisateurs devront partager les imprimantes sur le réseau en fonction de la proximité physique et de la division afin d'optimiser les ressources au cas échéant. Les administrateurs des réseaux informatiques doivent s'assurer que toutes les interfaces de gestion des imprimantes sont protégées par un mot de passe pour empêcher toute utilisation ou configuration non autorisée.

Les utilisateurs doivent veiller à une gestion efficace des ressources d'impression en n'imprimant que lorsqu'une copie papier est nécessaire. Les documents imprimés sensibles ou classifiés doivent être immédiatement retirés de l'imprimante après impression afin d'éviter toute divulgation d'informations indésirables. Seul le personnel de maintenance autorisé doit effectuer les réparations de l'imprimante.

VII. CYBERSÉCURITÉ

VII.1. Minimiser l'exposition des systèmes aux réseaux externes

- Installer et configurer le pare-feu de passerelle, le VPN IPsec et SSL/TLS et le sans-fil ;
- Configurer la liste de contrôle d'accès (ACL) entrante et sortante pour contrôler uniquement le trafic requis et légitime uniquement pour être autorisé à entrer et sortir du réseau ;
- Fermez tous les ports et ouvrez uniquement le port requis ;
- Evitez de mettre en place des règles « n'importe quelle » dans toutes les configurations ;

- Toutes les règles doivent être configurées pour garantir qu'aucune des services « indésirables » ou « hôtes » sont exposés à Internet, à la protection web contre les logiciels malveillants, à la visibilité, au contrôle et à la protection du web et des applications ;
- Mettre en œuvre la ségrégation du réseau en créant une zone démilitarisée (DMZ) pour les serveurs publics, la zone serveur et la zone utilisateur ;
- Veiller à ce que le réseau soit sécurisé en séparant les différentes tâches administratives ;
- Envisagez les systèmes de protection du réseau comme IPS, IDS, HTML5 VPN, ATP et Security Pulsation.
- Tous les accès à distance à l'infrastructure TIC doivent se faire via VPN.

VII.2. Mettre en œuvre la segmentation des réseaux

1) Contrôle d'accès

Le contrôle d'accès doit commencer par la classification des actifs informatiques, des données et du personnel en groupes spécifiques et restreindre l'accès associé via VLAN.

2) Gestion des accès

L'accès aux VLAN doit être restreint en les isolant les uns des autres et en répartissant les ressources dans différents VLAN, afin qu'un système compromis dans un segment ne se traduise pas par l'exploitation de l'ensemble du réseau.

3) Utilisation de méthodes d'accès à distance sécurisées

Tout accès à distance au réseau ou au système de l'institution doit être sécurisé via VPN pour tout accès à distance requis.

L'accès à distance devrait être encore renforcé en limitant le nombre d'adresses IP autorisées à se connecter à distance pour des raisons de sécurité.

VII.3. Établir des contrôles d'accès basés sur les rôles et mettre en œuvre la journalisation du système

1) Contrôle d'accès basé sur les rôles

L'accès aux ressources du réseau doit être accordé ou refusé en fonction des fonctions professionnelles. Les autorisations doivent être définies en fonction du niveau d'accès nécessaire pour exécuter les fonctions professionnelles et les tâches connexes.

2) Des procédures opérationnelles standard

Doivent être établies pour permettre le retrait de l'accès au réseau des anciens employés et sous-traitants.

3) Capacité de journalisation pour chaque système

La journalisation doit être implémentée pour chaque utilisateur et pour chaque activité.

VII.4. Mettre en œuvre une politique de mots de passe

- Utilisez strictement des mots de passe forts comportant au minimum 8 caractères alphanumériques. Les caractères numériques et spéciaux, comme décrit à la section 6.3 ;
- Les utilisateurs doivent avoir des mots de passe différents pour différents comptes ;
- Tous les mots de passe par défaut doivent être modifiés lors de l'installation d'un nouveau logiciel ou d'un nouveau Système d'exploitation (OS);
- Les tentatives de connexion infructueuses doivent être limitées à trois fois, puis verrouiller l'utilisateur. La durée du verrouillage du compte doit être d'au minimum 20 minutes et d'au maximum 1 heure ;
- Une authentification à plusieurs facteurs (MFA) doit être mise en place pour les applications et/ou systèmes critiques.

VII.5. Conscientisation à la cyber sécurité au niveau des institutions

Les institutions publiques doivent planifier et mener régulièrement des sensibilisations internes à la cyber sécurité pour conscientiser les utilisateurs finaux au moins 3 fois par an en collaboration avec le Secrétariat Exécutif des Technologies de l'Information et de Communication.

VII.6. Effectuer régulièrement des évaluations de vulnérabilités et des tests d'intrusion

1) Maintenance préventive

Les institutions publiques doivent planifier et réaliser une évaluation des vulnérabilités de l'infrastructure informatique et des tests de pénétration au moins une fois par an.

2) Réponse aux incidents

Les institutions publiques doivent être prêtes à atténuer ou à réagir le plus rapidement possible à un cyber-incident susceptible de toucher l'institution. Un **plan de reprise après sinistre** approprié doit également être mis en place pour assurer la continuité des activités tout en se remettant d'un tel incident.

VIII. COMMUNICATION INTERNE ET EXTERNE

La communication, tant interne qu'externe, est un pilier essentiel pour assurer le succès de la mise en place et du fonctionnement des systèmes d'information au sein des institutions publiques. Une stratégie de communication bien définie permet non seulement de garantir une collaboration efficace entre les différentes parties prenantes, mais aussi de renforcer la transparence, la confiance, et la cohérence dans la mise en œuvre des initiatives technologiques.

VIII.1 Politique de communication interne

La communication interne joue un rôle crucial dans l'intégration et l'adoption des systèmes d'information au sein des institutions publiques. Une politique de communication interne bien structurée assure que toutes les parties prenantes, à tous les niveaux de l'institution, sont informées des objectifs, des changements, des défis et des progrès relatifs aux projets TIC. Cette politique favorise un environnement où l'information circule librement, où les employés se sentent impliqués, et où les initiatives sont alignées sur les objectifs stratégiques de l'institution.

VIII.1.1 Objectifs de la politique de communication interne

Les objectifs principaux d'une politique de communication interne dans le cadre des systèmes d'information sont les suivants :

- **Informer et sensibiliser** : S'assurer que tous les employés sont informés des projets en cours, des objectifs stratégiques, des nouvelles procédures, et des outils technologiques mis en place. La sensibilisation inclut la formation des utilisateurs sur les nouveaux systèmes et la diffusion d'informations sur les avantages et les implications des changements.
- **Renforcer la cohésion et la collaboration** : Promouvoir un esprit de collaboration entre les différents départements et services, en brisant les silos de communication. Une bonne communication interne facilite le partage de connaissances, la résolution de problèmes, et l'harmonisation des pratiques à travers l'institution.
- **Encourager l'adoption** : La politique doit inclure des stratégies pour encourager l'adoption des nouvelles technologies, en mettant en avant leurs avantages et en répondant aux préoccupations des utilisateurs. Cela peut inclure des campagnes internes, des formations, et des sessions de feedback pour s'assurer que les utilisateurs sont à l'aise avec les nouveaux systèmes.
- **Assurer la transparence** : Garantir que toutes les actions, décisions et changements liés aux systèmes d'information sont communiqués de manière transparente.

La transparence renforce la confiance des employés et favorise un climat institutionnel où chacun se sent impliqué et valorisé.

VIII.1.2 Canaux de communication

Les canaux de communication sont les moyens par lesquels l'information est diffusée au sein de l'institution. Il est essentiel de choisir des canaux adaptés aux besoins de l'institution et à la nature des informations à transmettre. Les canaux peuvent inclure :

- **Intranet** : Un intranet institutionnel est un outil central pour la diffusion d'informations internes, y compris les annonces de projets, les documents stratégiques, les manuels d'utilisation et les forums de discussion. Il permet un accès facile à l'information et une communication rapide à travers l'ensemble de l'institution.
- **Réunions et séminaires** : Les réunions régulières, qu'elles soient en présentiel ou virtuelles, sont essentielles pour discuter des progrès, des défis et des prochaines étapes des projets de systèmes d'information. Les séminaires et les ateliers de formation offrent des occasions de sensibilisation et de formation pour les utilisateurs.
- **Bulletins et newsletters** : Les bulletins électroniques et les newsletters sont des moyens efficaces pour partager des mises à jour régulières sur les projets TIC, les nouvelles procédures et les histoires de succès au sein de l'institution.
- **Tableaux d'affichage et affiches** : Les affiches physiques dans les lieux de travail peuvent servir à rappeler les utilisateurs des initiatives en cours, des dates importantes, et des informations essentielles sur les systèmes d'information.
- **Emails et circulaires** : Les emails restent un canal de communication direct et personnel permettant d'envoyer des informations ciblées à des groupes spécifiques ou à l'ensemble de l'institution. Les circulaires peuvent formaliser les annonces importantes et les directives officielles.

VIII.1.3 Stratégies de mise en œuvre

La mise en œuvre d'une politique de communication interne nécessite une planification minutieuse et l'implication de différents acteurs clés de l'institution :

- **Implication du leadership** : Le leadership doit être fortement impliqué dans la communication interne pour montrer l'exemple et motiver les équipes. Les dirigeants doivent participer activement aux campagnes de communication, aux réunions et aux formations pour souligner l'importance des projets TIC.

- **Définition des responsabilités** : Les responsabilités en matière de communication doivent être clairement définies. Un comité ou une équipe dédiée à la communication interne peut être créé pour superviser l'exécution de la politique, assurer la cohérence des messages et coordonner les efforts de communication.
- **Feedback et amélioration continue** : La communication interne ne doit pas être unidirectionnelle. Il est essentiel de créer des boucles de feedback où les employés peuvent exprimer leurs préoccupations, poser des questions et donner leur avis sur les systèmes d'information et les processus de communication. Ce feedback doit être analysé et utilisé pour améliorer continuellement la politique de communication interne.
- **Mesure de l'efficacité** : L'efficacité de la politique de communication interne doit être régulièrement évaluée. Des indicateurs tels que la participation aux formations, l'engagement des employés et la satisfaction utilisateur peuvent être utilisés pour mesurer l'impact de la communication. Les résultats doivent être utilisés pour ajuster les stratégies et améliorer les processus.

VIII.2 Communication externe

La communication externe est un aspect crucial de la gestion des systèmes d'information dans les institutions publiques. Elle englobe toutes les interactions entre l'institution et ses parties prenantes externes, y compris les citoyens, les autres institutions publiques, les partenaires privés, les médias et la communauté internationale. Une politique de communication externe bien définie permet de renforcer la transparence, de gagner la confiance du public, de promouvoir l'image de l'institution et de garantir une diffusion cohérente et stratégique des informations essentielles.

VIII.2.1 Objectifs de la politique de communication externe

Les objectifs principaux d'une politique de communication externe pour les systèmes d'information des institutions publiques sont les suivants :

- **Transparence et responsabilité** : Une communication transparente avec les parties prenantes externes est essentielle pour établir et maintenir la confiance dans les systèmes d'information des institutions publiques. Cela inclut la diffusion d'informations sur les projets en cours, les résultats obtenus, les budgets et les défis rencontrés. La transparence contribue à renforcer la responsabilité des institutions vis-à-vis du public.
- **Promotion de l'image institutionnelle** : La communication externe joue un rôle clé dans la promotion de l'image de l'institution en tant qu'acteur moderne, efficace et engagé dans

l'amélioration des services publics à travers la technologie. Elle contribue à façonner la perception du public et à renforcer la légitimité de l'institution.

- **Engagement des citoyens** : Une communication efficace avec les citoyens est essentielle pour leur engagement dans les initiatives numériques. Cela peut inclure la sensibilisation sur les nouveaux services en ligne, la sollicitation de leur feedback et l'encouragement à utiliser les plateformes numériques pour interagir avec l'institution. L'engagement des citoyens est un facteur clé pour le succès des projets TIC dans le secteur public.
- **Gestion des crises** : En cas de crises ou d'incidents tels que des violations de données, des interruptions de service ou des failles de sécurité, la communication externe doit être rapide, claire et rassurante. Une gestion de crise efficace à travers une communication bien structurée peut minimiser les impacts négatifs et restaurer la confiance des parties prenantes.

VIII.2.2 Canaux de communication externe

Les canaux de communication externe sont les moyens par lesquels l'institution interagit avec ses parties prenantes externes. Les choix des canaux dépendent de l'audience cible, du message à transmettre, et des objectifs de communication. Les principaux canaux comprennent :

- **Site web institutionnel** : Le site web de l'institution est un outil central pour la communication externe. Il doit être conçu pour être accessible, informatif, et interactif, offrant un accès facile aux informations sur les systèmes d'information, les projets TIC, et les services en ligne disponibles pour les citoyens et les autres parties prenantes.
- **Médias sociaux** : Les plateformes de médias sociaux tels que Facebook, X/Twitter, LinkedIn, Instagram, Telegram, etc. sont des canaux puissants pour atteindre un large public et pour engager directement les citoyens. Elles permettent une interaction en temps réel, la diffusion rapide d'annonces et la réponse aux questions et préoccupations du public.
- **Communiqués de presse et médias traditionnels** : Les communiqués de presse sont utilisés pour diffuser des informations officielles sur les projets TIC, les réalisations et les politiques. Les médias traditionnels comme la télévision, la radio, les journaux restent des canaux efficaces pour atteindre un public plus large, notamment dans les régions où l'accès à l'internet est limité.
- **Événements publics et conférences** : Les événements publics, tels que les conférences, les forums et les journées portes ouvertes sont des occasions importantes pour communiquer directement avec les citoyens, les experts et les partenaires sur les initiatives

technologiques de l'institution. Ces événements permettent de présenter les avancées, de recueillir des retours et de renforcer les partenariats.

- **Rapports annuels et publications** : Les rapports annuels et autres publications institutionnelles sont des moyens de communiquer de manière détaillée et formelle sur les activités et les performances des systèmes d'information. Ils sont souvent utilisés pour rendre compte aux parties prenantes, y compris les instances de régulation et les partenaires au développement.

VIII.2.3 Stratégies de mise en œuvre

La mise en œuvre d'une politique de communication externe nécessite une stratégie bien définie, avec des étapes claires et une coordination entre les différents services de l'institution :

- **Segmenter l'audience** : Il est essentiel de segmenter l'audience pour s'assurer que les messages sont adaptés aux besoins et aux attentes des différentes parties prenantes. Par exemple, les messages destinés aux citoyens seront différents de ceux destinés aux partenaires privés ou aux autres institutions publiques.
- **Élaborer des messages clés** : La communication externe doit être construite autour de messages clés qui reflètent les valeurs, les objectifs, et les réalisations de l'institution. Ces messages doivent être cohérents à travers tous les canaux de communication et être répétés de manière à renforcer leur impact.
- **Coordination interdépartementale** : La communication externe ne doit pas être l'apanage d'un seul service. Une coordination étroite entre les départements TIC, le service de communication, et les autres services concernés est nécessaire pour s'assurer que les messages diffusés sont précis, pertinents, et alignés avec la stratégie globale de l'institution.
- **Utilisation de porte-parole officiels** : Les porte-parole officiels jouent un rôle crucial dans la diffusion des messages de l'institution. Ils doivent être bien formés pour représenter l'institution lors des interactions avec les médias et les autres parties prenantes pour répondre de manière efficace aux questions et préoccupations.

- **Surveillance et réaction** : La communication externe nécessite une surveillance constante pour évaluer son efficacité et réagir rapidement aux développements. Cela inclut le suivi des mentions de l'institution dans les médias et sur les réseaux sociaux ainsi que la gestion proactive des crises potentielles.

VIII.3. Enregistrement du domaine

Chaque institution doit avoir son propre nom de domaine lié à son site web. Les Ministères en premier, puis les départements et/ou Directions.

VIII.3.1. Processus d'enregistrement

1) Démarches administratives

Soumettre une demande officielle d'enregistrement de domaine auprès du Secrétariat Exécutif des Technologies d'Information et de la Communication (SETIC) à travers le Ministère ayant les TIC dans ses attributions, incluant toutes les informations requises (nom de domaine souhaité, informations de contact, etc.).

2) Validation et approbation

Processus de vérification pour s'assurer que le domaine est disponible et respecte les normes et règlements en vigueur.

3) Configuration technique

Une fois approuvé, on procède à la configuration des enregistrements DNS pour que le domaine soit opérationnel (enregistrements A, MX, CNAME, etc.).

VIII.3.2. Nomenclature pour l'enregistrement de domaine

Lors de la proposition d'un domaine pour l'enregistrement, il est crucial de suivre une nomenclature claire et standardisée pour garantir la cohérence et la gestion efficace des ressources numériques.

L'équipe technique du SETIC peut intervenir pour des ajustements si le nom proposé n'est pas conforme. Voici les principes de nomenclature à respecter :

- **Format du nom de domaine**

  Utilisation de caractères ASCII standard (lettres d'A à Z, chiffres de 0 à 9 et le trait d'union "-"). Les noms de domaine doivent commencer et se terminer par un caractère alphanumérique.

- **Longueur maximale du nom de domaine**

  Généralement 63 caractères, conformément aux standards de l'ICANN (Internet Corporation for Assigned Names and Numbers).

- **Structure du nom de domaine**

Il faut adopter une structure logique et significative qui reflète l'entité ou le service associé. Exemple : **setic** (nom de domaine en même temps nom de l'institution).

Utilisation de sous-domaines pour organiser et hiérarchiser les services ou les départements au sein de l'institution publique.

Exemple : **departement.nominstitution.gov.bi** (où "département" pourrait être remplacé par un nom spécifique de département ou de service, "nominstitution" est le nom de l'institution et "bi" est le domaine de premier niveau).

VIII.3.3. Normes de conformité et sécurité

1) Conformité réglementaire

Assurer que l'enregistrement du domaine et son utilisation respectent toutes les lois et régulations locales et internationales ;

2) Protocoles de sécurité

Les mesures de sécurité strictes pour protéger l'intégrité du domaine sont mises en œuvre au niveau du CDIN.

VIII.4. Gestion des emails professionnels

VIII.4.1. Création et enregistrement des comptes email

VIII.4.1.1. Procédure de création des comptes

- Chaque institution doit disposer d'une liste de tous ses employés ;
- L'enregistrement collectif des emails professionnels de tous les employés sur le domaine est fait par le SETIC en collaboration avec les équipes IT des institutions bénéficiaires ;
- Un module de formation sur la création et la configuration des emails professionnels est disponible pour les gestionnaires des sites web dans chaque institution ;
- L'équipe IT crée le compte email professionnel en utilisant le système de gestion des utilisateurs. Les informations de connexion (identifiant et mot de passe temporaire) sont ensuite communiquées au nouvel utilisateur.
- L'utilisateur doit se connecter pour la première fois et changer le mot de passe temporaire. Une formation initiale sera fournie par l'équipe IT dans chaque institution pour familiariser les utilisateurs avec les outils de messagerie professionnelle.

VIII.4.1.2. Nomenclature des adresses emails professionnels

1) Format des adresses

Les adresses email doivent suivre un format standardisé pour faciliter la reconnaissance et la gestion. Le format adopté est le prénom suivi d'un point et puis le nom avec le suffixe @institution.gov.bi Exemple **:** prenom.nom@institution.gov.bi

Pour les mails professionnels liés aux postes, il faut commencer par la fonction suivie d'un tiret suivi du nom du département. **Exemple** : directeur-finances@institution.gov.bi

Si le nom du poste et/ou de la fonction est très long, il faut les abréger.

Exemple : dg-tic@institution.gov.bi

2) Noms uniques

Pour éviter les doublons, une numérotation est ajoutée pour les noms communs dans une même institution (ex. : prenom.nom1@institution.gov.bi).

Si c'est le nom et prénom qui sont identiques dans une même institution, on fera la numérotation sur le nom et le prénom (ex. : *prenom1.nom1@institution.gov.bi*)

VIII.4.2. Configuration et utilisation des comptes mails

VIII.4.2.1. Paramètres de configuration

- La Configuration des clients de messagerie est faite par l'équipe IT chargée de gérer les sites web dans les institutions publiques en collaboration avec le SETIC ;
- L'équipe IT doit veiller à ce que les protocoles de sécurité comme SSL/TLS sont activés pour le chiffrement des emails en transit ;
- L'équipe IT peut paramétrer la synchronisation avec les appareils mobiles en utilisant des outils sécurisés en cas de besoin.

VIII.4.2.2. Bonnes pratiques d'utilisation

- On encourage l'utilisation de dossiers et de règles pour organiser les e-mails et maintenir la boîte de réception propre ;
- Utilisation des filtres anti-spam et anti-phishing. Les utilisateurs doivent être informés sur la reconnaissance des emails suspects ;
- Mise en place des politiques d'archivage pour conserver les e-mails importants et des systèmes de sauvegarde réguliers pour éviter la perte de données ;

- Formation des utilisateurs sur l'importance de la confidentialité et les bonnes pratiques pour protéger les informations sensibles (ex. : ne pas partager de mots de passe, vérifier les destinataires avant d'envoyer des emails confidentiels).

VIII.5. Normes et formats de communication

VIII.5.1. Format uniforme de communication

VIII.5.1.1. Modèles de documents

1) Lettre officielle

Mise à disposition de modèles de lettres officielles avec en-têtes et pieds de page standardisés incluant le logo de l'institution, l'adresse et les informations de contact.

2) Mémos internes

Modèles pour les mémos internes avec sections pour l'objet, les destinataires, le corps du message et la signature.

3) Rapports

Formats standardisés pour les rapports internes et externes incluant des sections pour le titre, le résumé, le contenu détaillé, les conclusions et les annexes.

VIII.5.1.2. Signatures liées aux emails professionnels

Format des signatures

Les signatures liées aux emails professionnels doivent inclure le nom complet, le titre, le département, l'institution, et les coordonnées de contact.

VIII.5.2. Groupes de communication et nomenclature

Les groupes de communication sont des groupes constitués par des emails professionnels qui seront créés dans chaque institution.

VIII.5.2.1. Types de groupes (Fonctionnels, Hiérarchiques, Projet, etc.)

La mise en place des groupes de communication respecte les formats suivants :

1) Groupes fonctionnels

Groupes basés sur les fonctions ou départements (ex. : departement@institution.gov.bi) ;

2) Groupes hiérarchiques

Groupes basés sur les niveaux hiérarchiques (ex. : managers@institution.gov.bi) ;

3) Groupes de projet

Groupes temporaires ou permanents pour des projets spécifiques (exemple :

projet-abc@institution.gov.bi).

VIII.5.2.2. Nomenclature des groupes par institution

1) Convention de nommage

La nomenclature se base sur les départements, les fonctions et les projets (Ex. dg@institution.gv.bi, it@institution.gov.bi, ged@institution.gov.bi) ;

2) Gestion des groupes

Le processus de création, modification et suppression des groupes est géré par l'équipe IT en coordination avec les responsables des départements et du SETIC.

VIII.5.3. Identification des institutions par communication

VIII.5.3.1. Codes instituts

1) Attribution des codes

Chaque institution publique ayant un nom très long se voit attribuer un code unique pour faciliter l'identification (ex. : INST1, INST2).

2) Utilisation des codes

Les codes doivent être utilisés dans les adresses emails, les groupes de communication et les documents officiels pour une identification rapide et claire.

VIII.5.3.2. Formats de référence

1) Références documentaires

Inclure le code de l'institution et un identifiant unique dans les références des documents (ex. : INST1-2024-001).

2) Références dans les communications

Utilisation des codes et formats de référence dans les sujets d'emails et les titres de documents pour une traçabilité optimale.

VIII.6. Outils de communication interne

VIII.6.1. Plateformes et logiciels de communication

VIII.6.1.1. Logiciels de messagerie instantanée

1) Sélection des outils

Choisir des outils de messagerie instantanée sécurisés et conformes aux normes de sécurité de l'institution.

2) Configuration et déploiement

Configuration des outils pour une utilisation institutionnelle avec des groupes prédéfinis et des permissions d'accès contrôlées.

VIII.6.1.2. Outils de collaboration et partage de fichiers

1) Plateformes de collaboration

Utilisation de plateformes de Gestion Électronique de Documents (GED).

2) Gestion des Accès

Contrôle des permissions pour garantir que seuls les utilisateurs autorisés peuvent accéder et modifier les documents partagés.

VIII.6.2. Intégration des systèmes de communication

VIII.6.2.1. Intégration avec les systèmes d'information existants

1) Interopérabilité

Assurer que les systèmes de communication sont compatibles avec les autres systèmes d'information utilisés par l'institution.

2) Automatisation des processus

Mise en place de workflows automatisés pour intégrer les communications dans les processus métiers (ex. : notifications automatiques pour les approbations).

VIII.6.2.2. Automatisation des processus

1) Automatisation des réponses

Utilisation de règles et de scripts pour automatiser les réponses aux emails courants ou routages d'emails.

2) Intégration des bots

Implémentation de chat bots pour les réponses aux questions fréquentes et l'assistance utilisateur.

IX. FORMATION ET RENFORCEMENT DES CAPACITÉS

Le développement des compétences au sein des institutions publiques est un facteur clé pour assurer la réussite des initiatives liées aux systèmes d'information. Alors que la transformation numérique se poursuit, il devient impératif de renforcer les capacités des employés à tous les niveaux de sorte qu'ils puissent non seulement utiliser les nouvelles technologies de manière efficace, mais aussi contribuer à leur mise en œuvre, gestion et évolution.

Le renforcement des capacités englobe à la fois la formation technique et le développement des compétences de gestion, garantissant que les équipes puissent naviguer dans un environnement technologique complexe et en perpétuelle mutation. Une stratégie de formation bien définie est essentielle pour aligner les compétences des employés avec les exigences des systèmes d'information modernes.

IX.1 Plan de formation

Un plan de formation structuré est essentiel pour doter les employés des compétences nécessaires à l'exercice de leurs fonctions dans un environnement de plus en plus numérique. Ce plan doit être élaboré en tenant compte des besoins spécifiques de l'institution, des compétences existantes, des écarts à combler et des objectifs stratégiques globaux.

IX.1.1 Identification des besoins en formation

Le processus de formation commence par une évaluation approfondie des besoins en compétences. Cette évaluation permet de déterminer les domaines où il existe des lacunes et où une intervention est nécessaire.

1) Analyse des compétences actuelles

Il s'agit d'évaluer les compétences actuelles des employés en ce qui concerne les systèmes d'information. Cela peut inclure une évaluation des connaissances en matière de logiciels, de réseaux, de gestion des données, de cyber sécurité et d'autres domaines pertinents.

2) Identification des écarts

Une fois les compétences actuelles évaluées, l'étape suivante consiste à identifier les écarts par rapport aux compétences nécessaires pour atteindre les objectifs de l'institution. Ces écarts peuvent

être liés à l'introduction de nouvelles technologies, à des processus métiers spécifiques ou à des exigences réglementaires.

3) Priorisation des besoins

Tous les besoins en formation ne peuvent pas être comblés en même temps. Il est donc important de prioriser les domaines critiques qui auront le plus grand impact sur la performance et la sécurité des systèmes d'information.

IX.1.2 Conception des programmes de formation

Sur la base de l'évaluation des besoins, des programmes de formation spécifiques doivent être conçus pour répondre aux exigences identifiées.

1) Programmes techniques

Ceux-ci doivent se concentrer sur le développement de compétences techniques spécifiques telles que l'administration des systèmes, la gestion des réseaux, la sécurité des données, le développement de logiciels et l'utilisation d'applications spécifiques. Les programmes doivent être adaptés aux niveaux de compétence des participants, avec des options pour les débutants, les intermédiaires et les experts.

2) Programmes de gestion et gouvernance

En plus des compétences techniques, il est crucial de former les cadres et gestionnaires à la gouvernance des systèmes d'information, à la gestion des risques, à la conformité réglementaire et à la stratégie de transformation numérique. Ces programmes doivent préparer les leaders à prendre des décisions éclairées et à superviser la mise en œuvre et l'évolution des systèmes d'information.

3) Formation en cyber sécurité

La cyber sécurité est un domaine critique qui nécessite une attention particulière. Les programmes de formation doivent couvrir des sujets tels que la protection contre les cyberattaques, la gestion des incidents, la sensibilisation à la sécurité et aux meilleures pratiques en matière de protection des données.

4) Formation continue et certifications

Dans un domaine aussi dynamique que les TIC, la formation continue est essentielle. Les employés doivent être encouragés à obtenir des certifications reconnues dans leurs domaines de spécialisation et à participer régulièrement à des sessions de mise à jour des compétences.

IX.1.3 Modalités de formation

La formation peut être dispensée sous diverses formes, en fonction des ressources disponibles et des besoins des participants.

1) Formations en présentiel

Les formations en présentiel offrent l'avantage d'une interaction directe avec les formateurs et les autres participants. Elles sont particulièrement efficaces pour les formations pratiques où les démonstrations et les exercices en temps réel sont nécessaires.

2) Formations en ligne

Les formations en ligne offrent plus de flexibilité et permettent aux employés de suivre les cours à leur propre rythme. Elles sont idéales pour les programmes de formation continue et pour couvrir des sujets théoriques ou des compétences qui ne nécessitent pas de pratique immédiate.

3) Ateliers et séminaires

Les ateliers et séminaires sont des formats de formation courts et intensifs souvent utilisés pour introduire de nouvelles technologies ou pour discuter de sujets spécifiques. Ils peuvent également servir de forums pour le partage des meilleures pratiques entre différents départements ou institutions.

4) Mentorat et coaching

Le mentorat est une méthode efficace pour le transfert de connaissances de manière personnalisée. Les employés plus expérimentés peuvent guider leurs collègues dans l'application des compétences apprises, aidant ainsi à renforcer la cohésion de l'équipe et à assurer une continuité des connaissances au sein de l'institution.

IX.1.4 Évaluation et suivi de la formation

Un plan de formation efficace ne se termine pas avec la délivrance des sessions de formation. Il est crucial de mettre en place un système d'évaluation pour mesurer l'impact des formations et ajuster les programmes en conséquence.

1) Évaluation des connaissances

Des tests ou des évaluations pratiques doivent être utilisés pour mesurer l'acquisition des compétences par les participants. Cela permet de s'assurer que les objectifs de formation sont atteints et que les employés sont prêts à appliquer ce qu'ils ont appris dans leur travail quotidien.

2) Suivi post-formation

Un suivi régulier après la formation est essentiel pour évaluer comment les nouvelles compétences sont appliquées dans l'environnement de travail. Cela doit inclure des sessions de restitution, des analyses de performance et des ajustements du programme de formation en fonction des retours des participants.

3) Amélioration continue

La formation ne doit pas être statique. Les programmes doivent être régulièrement mis à jour pour refléter les nouvelles technologies, les changements dans les politiques institutionnelles et les évolutions des menaces en matière de cyber sécurité. La collecte de feedback des participants et l'analyse des tendances permettent d'améliorer continuellement le plan de formation.

La formation et le renforcement des capacités sont des éléments fondamentaux pour la réussite des systèmes d'information des institutions publiques. En investissant dans le développement des compétences des employés, les institutions publiques peuvent non seulement améliorer l'efficacité et la sécurité de leurs opérations, mais aussi garantir une adaptation réussie aux évolutions technologiques. Un plan de formation bien conçu, axé sur l'évaluation des besoins, la conception de programmes adaptés, des modalités de formation variées et un suivi rigoureux, est la clé pour bâtir une force de travail compétente et résiliente dans un paysage numérique en constante évolution.

IX.2 Gestion des compétences

La gestion des compétences au sein des institutions publiques revêt une importance capitale, surtout dans le contexte actuel de transformation numérique. Avec l'évolution rapide des technologies et des méthodes de travail, il devient essentiel d'avoir une approche structurée pour identifier, développer et gérer les compétences des employés. Une gestion efficace des compétences assure non seulement que les employés possèdent les connaissances et les habiletés nécessaires pour accomplir leurs tâches, mais également qu'ils sont préparés à relever les défis futurs et à s'adapter à de nouvelles exigences.

IX.2.1 Identification et cartographie des compétences

L'identification des compétences existantes et requises est la première étape d'une gestion efficace des compétences.

1) Cartographie des compétences

Cette démarche implique la création d'une "carte" des compétences actuelles au sein de l'institution. Elle permet de visualiser les compétences disponibles dans chaque département ou

unité, d'identifier les domaines de force et de faiblesse, et de planifier les besoins futurs. Cette cartographie se base sur des évaluations régulières des employés, des entretiens, et des auto-évaluations.

2) Identification des compétences clés

Chaque institution doit définir quelles sont les compétences stratégiques nécessaires pour soutenir ses objectifs. Cela peut inclure des compétences techniques spécifiques (comme la gestion de réseaux ou le développement logiciel), des compétences en gestion (comme la gestion de projets ou la gouvernance informatique), ainsi que des compétences transversales (comme la communication ou la résolution de problèmes).

3) Analyse des lacunes

Une fois les compétences actuelles identifiées, il est important d'effectuer une analyse des lacunes. Cela permet de comprendre quelles compétences doivent être développées ou renforcées pour répondre aux objectifs de l'institution. Cette analyse doit être dynamique, en tenant compte des changements technologiques et des nouvelles missions confiées à l'institution.

IX.2.2 Développement des compétences

Une fois les compétences nécessaires identifiées, il est crucial de mettre en place des stratégies pour développer ces compétences au sein de l'institution.

1) Programmes de développement personnalisés

Le développement des compétences doit être personnalisé en fonction des besoins individuels des employés. Les institutions peuvent créer des parcours de formation spécifiques pour chaque employé, alignés avec leurs fonctions actuelles et leurs perspectives d'évolution. Cela permet de garantir une montée en compétences continue et adaptée aux besoins de l'institution.

2) Utilisation des outils technologiques

Avec l'avènement des plateformes d'apprentissage en ligne, les institutions publiques peuvent tirer parti des technologies pour offrir des formations plus flexibles et accessibles. Les outils d'e-learning, les webinaires, et les plateformes de gestion des compétences permettent de former un grand nombre d'employés de manière efficace, tout en facilitant le suivi des progrès et l'évaluation des compétences acquises.

3) Mentorat et coaching

Le mentorat est un outil puissant pour le développement des compétences, surtout dans les environnements complexes comme les institutions publiques. Les employés plus expérimentés peuvent jouer un rôle de guide pour leurs collègues moins expérimentés, en partageant leur savoir-

faire et en les aidant à naviguer dans les défis professionnels. Le coaching, de son côté, peut aider à développer des compétences spécifiques ou à surmonter des obstacles particuliers dans la carrière d'un employé.

4) Rotations et mobilité interne au sein des équipes IT

Encourager la mobilité interne et les rotations postes est une méthode efficace pour élargir les compétences des employés. Cela permet non seulement de développer des compétences techniques spécifiques à différents départements, mais aussi de renforcer la compréhension globale des processus institutionnels et d'améliorer la collaboration entre les équipes.

IX.2.3 Suivi et évaluation des compétences

Le suivi et l'évaluation des compétences sont des composantes essentielles de la gestion des compétences. Ils permettent de s'assurer que les efforts de développement des compétences portent leurs fruits et que les employés continuent de répondre aux besoins de l'institution.

1) Évaluations périodiques

Il est important de mettre en place un système d'évaluations régulières pour suivre l'évolution des compétences des employés. Ces évaluations peuvent prendre la forme d'examens, d'entretiens d'évaluation, ou d'auto-évaluations. Elles doivent permettre de mesurer non seulement les compétences techniques mais aussi les compétences transversales et comportementales.

2) Indicateurs de performance

Pour une gestion des compétences efficace, il est nécessaire de définir des indicateurs de performance clairs. Ces indicateurs peuvent inclure le taux de participation aux formations, les résultats des évaluations, le niveau de satisfaction des employés, et l'impact des compétences acquises sur la performance institutionnelle. L'analyse de ces indicateurs permet d'ajuster les programmes de formation et de développement en fonction des besoins réels.

3) Feedback continu

Le feedback est une composante cruciale de la gestion des compétences. Les employés doivent recevoir un retour d'information régulier sur leurs progrès, ainsi que des recommandations pour l'amélioration continue. Cela renforce la motivation, encourage l'apprentissage autonome et aide les employés à aligner leurs efforts de développement sur les objectifs institutionnels.

IX.2.4 Alignement des compétences avec les objectifs institutionnels

Pour que la gestion des compétences soit efficace, elle doit être alignée avec les objectifs stratégiques de l'institution.

1) Planification stratégique des compétences

L'institution doit veiller à ce que les compétences développées soient en phase avec ses priorités stratégiques. Cela nécessite une planification à long terme qui anticipe les futurs besoins en compétences en fonction des évolutions technologiques, des changements réglementaires et des nouvelles missions.

2) Adaptation aux changements technologiques

Avec l'évolution rapide des technologies, il est crucial que la gestion des compétences soit suffisamment flexible pour s'adapter aux nouveaux outils et processus. Les employés doivent être formés aux dernières technologies et l'institution doit être prête à réagir rapidement aux changements pour rester compétitive et efficace.

3) Engagement des parties prenantes

La gestion des compétences ne doit pas être isolée des autres processus de l'institution. Elle doit impliquer toutes les parties prenantes y compris les dirigeants, les managers, et les employés eux-mêmes. Un engagement collectif garantit que les compétences développées répondent réellement aux besoins de l'institution et sont utilisées de manière optimale.

La gestion des compétences est un pilier central de la transformation numérique des institutions publiques. En adoptant une approche proactive pour identifier, développer, et gérer les compétences, les institutions peuvent non seulement améliorer leur efficacité opérationnelle, mais aussi se préparer à relever les défis futurs. Une gestion des compétences bien structurée garantit que les employés sont outillés pour contribuer activement à la réussite des systèmes d'information tout en soutenant la croissance et la résilience de l'institution dans un environnement en constante évolution.

X. SUIVI ET ÉVALUATION

Le suivi et l'évaluation sont des éléments clés pour assurer le succès de la mise en œuvre des systèmes d'information dans les institutions publiques. Ces processus permettent de mesurer l'efficacité des initiatives déployées, d'identifier les axes d'amélioration, et de garantir que les objectifs stratégiques sont atteints. Ils assurent également la transparence et la responsabilisation, en fournissant des données concrètes sur les performances des systèmes et des processus.

Une approche rigoureuse de suivi et d'évaluation contribue non seulement à optimiser l'utilisation des ressources, mais aussi à adapter les stratégies en fonction des retours d'expérience et des évolutions du contexte technologique et réglementaire.

X.1 Indicateurs de performance

Les indicateurs de performance, ou KPIs (Key Performance Indicators), sont des outils essentiels pour mesurer le succès des systèmes d'information. Ils permettent de quantifier les résultats atteints par rapport aux objectifs fixés et servent de base pour l'amélioration continue.

X.1.1 Définition des indicateurs

La définition des indicateurs de performance doit être alignée avec les objectifs stratégiques de l'institution. Chaque indicateur doit être :

- **Spécifique** : L'indicateur doit clairement décrire ce qu'il mesure. Par exemple, "le pourcentage de temps de disponibilité du réseau" est un indicateur spécifique.
- **Mesurable** : L'indicateur doit pouvoir être quantifié ou mesuré de manière précise. Par exemple, "la réduction des temps d'arrêt des systèmes" doit être exprimée en pourcentage ou en heures.
- **Atteignable** : Les objectifs fixés doivent être réalistes et basés sur les capacités de l'institution.
- **Pertinent** : L'indicateur doit être directement lié aux objectifs stratégiques. Par exemple, si l'objectif est de renforcer la sécurité des systèmes, un indicateur pertinent pourrait être "le nombre d'incidents de sécurité détectés et résolus".
- **Temporel** : Les indicateurs doivent être suivis sur une période définie pour permettre l'évaluation des tendances et des progrès.

X.1.2 Types d'indicateurs de performance

Les indicateurs de performance peuvent être classés en plusieurs catégories, selon les domaines qu'ils mesurent :

- **Indicateurs d'efficacité** : Mesurent la capacité des systèmes d'information à atteindre les objectifs fixés, comme le taux de réussite des projets TIC ou la satisfaction des utilisateurs.
- **Indicateurs d'efficience** : Mesurent la capacité à utiliser les ressources de manière optimale, comme le coût par utilisateur d'un service ou la consommation de ressources matérielles et logicielles.
- **Indicateurs de qualité** : Évaluent la qualité des services fournis par les systèmes d'information, comme le taux d'erreurs dans les transactions ou le temps de réponse des applications.

- **Indicateurs de sécurité** : Mesurent la sécurité des systèmes, comme le nombre d'incidents de sécurité, le temps de réponse aux incidents, ou le taux de conformité aux normes de sécurité.

X.1.3 Suivi des indicateurs

Le suivi des indicateurs de performance doit être un processus continu. Les institutions doivent mettre en place des outils et des systèmes de reporting pour collecter, analyser, et diffuser les données de manière régulière. Les tableaux de bord interactifs, les rapports mensuels ou trimestriels et les revues de performance sont des exemples d'outils qui peuvent être utilisés pour ce suivi.

Les résultats obtenus doivent être comparés aux objectifs fixés pour identifier les écarts. Ces écarts doivent ensuite être analysés pour comprendre leurs causes et des actions correctives doivent être mises en place pour améliorer la performance.

X.2 Audit et contrôle

L'audit et le contrôle sont des mécanismes essentiels pour garantir la conformité, l'intégrité et la fiabilité des systèmes d'information dans les institutions publiques. Ils permettent de vérifier que les systèmes sont bien gérés, que les risques sont maîtrisés, et que les ressources sont utilisées de manière efficiente et efficace.

X.2.1 Types d'audits

Les audits des systèmes d'information peuvent être de plusieurs types, en fonction des objectifs visés :

- **Audit de conformité** : Cet audit vérifie que les systèmes d'information sont conformes aux lois, règlements, et standards en vigueur. Par exemple, il peut s'agir de vérifier la conformité aux réglementations sur la protection des données personnelles (comme le RGPD) ou aux normes de sécurité (comme l'ISO 27001).
- **Audit de sécurité** : Cet audit évalue les dispositifs de sécurité mis en place pour protéger les systèmes d'information contre les menaces internes et externes. Il examine les politiques de sécurité, les mesures de protection des réseaux, la gestion des accès, et les procédures de réponse aux incidents.
- **Audit de performance** : Cet audit analyse l'efficacité et l'efficience des systèmes d'information. Il évalue si les ressources sont utilisées de manière optimale et si les objectifs de performance sont atteints.

- **Audit des processus** : Cet audit examine les processus opérationnels liés aux systèmes d'information. Il s'agit de vérifier si les processus sont bien documentés, suivis, et améliorés en continu.

X.2.2 Processus d'audit

Le processus d'audit des systèmes d'information suit généralement plusieurs étapes clés :

- **Planification de l'audit** : Cette phase implique la définition des objectifs de l'audit, la sélection des domaines à auditer, et l'élaboration d'un plan d'audit détaillé. Il est essentiel d'impliquer toutes les parties prenantes et de s'assurer que l'audit est bien coordonné avec les autres activités de l'institution.
- **Collecte des informations** : Les auditeurs collectent les informations nécessaires pour évaluer les systèmes d'information. Cela peut inclure l'examen de documents, l'interview du personnel, l'observation des processus en action et l'analyse des logs et des rapports de systèmes.
- **Analyse et évaluation** : Les informations collectées sont analysées pour évaluer la conformité, la sécurité, et la performance des systèmes. Les auditeurs utilisent des outils d'analyse et des méthodes de benchmarking pour comparer les résultats obtenus avec les standards et les bonnes pratiques.
- **Rédaction du rapport d'audit** : Un rapport d'audit est rédigé pour présenter les résultats de l'audit, identifier les points forts et les points faiblesses, et formuler des recommandations d'amélioration. Le rapport doit être clair, concis, et structuré pour permettre une prise de décision rapide.
- **Suivi de l'audit** : Après la diffusion du rapport, il est crucial de mettre en place un plan de suivi pour s'assurer que les recommandations sont bien mises en œuvre. Les actions correctives doivent être suivies de près et des audits de suivi peuvent être réalisés pour vérifier leur efficacité.

X.2.3 Contrôle continu

En plus des audits périodiques, les institutions publiques doivent mettre en place des mécanismes de contrôle continu pour surveiller en temps réel les systèmes d'information. Ces contrôles peuvent inclure :

- **Surveillance des journaux d'activité** : La surveillance des logs système permet de détecter rapidement les anomalies, les incidents de sécurité ou les erreurs opérationnelles.

- **Contrôles automatisés** : Les institutions peuvent déployer des outils de contrôle automatisés pour vérifier en continu la conformité des systèmes avec les politiques internes et les régulations externes.
- **Revues de performance régulières** : Des revues régulières de performance, basées sur les indicateurs de performance définis, permettent d'identifier les problèmes avant qu'ils ne deviennent critiques.
- **Gestion des risques** : Un processus de gestion des risques doit être intégré au contrôle continu, afin de détecter et de mitiger les risques émergents liés aux systèmes d'information.

Le suivi et l'évaluation sont cruciaux pour la réussite de la transformation numérique dans les institutions publiques. Les indicateurs de performance, audits et contrôles permettent de mesurer les progrès, d'assurer la conformité et l'efficience des systèmes. Ces mécanismes aident les institutions à atteindre leurs objectifs et à se préparer aux défis futurs.

XI.GESTION DE PROJETS TIC

XI.1. Lancement de projet TIC

Tous les projets TIC doivent être issus de l'évaluation de la planification stratégique TIC. Il est conseillé à toutes les institutions publiques d'associer le SETIC au démarrage du projet, dès l'élaboration du concept du projet.

XI.2. Documentation de projet TIC

La documentation appropriée de tous les projets TIC dans l'ensemble du gouvernement doit inclure le contexte et la justification du projet, les résultats et les résultats prévus, les principaux éléments du projet, le plan de mise en œuvre, l'analyse et l'atténuation des risques liés à la mise en œuvre du projet, les ressources proposées (humaines et financières) et le cadre de suivi et d'évaluation proposé.

XI.3. Mise en œuvre du projet TIC

Le mode de mise en œuvre agile qui permet une visibilité des détails du projet et la capacité de gérer les changements est conseillé pour la mise en œuvre du projet TIC dans les institutions publiques.

XII. FONCTION TIC, PERSONNEL ET FORMATION

XII.1. Comité TIC

1) Comité TIC

Il est impératif que toutes les institutions publiques établissent un comité TIC.

2) Rôle du comité TIC

Le rôle principal du comité TIC est de définir la stratégie TIC de l'institution et de s'assurer que tous les projets TIC au sein des départements et agences respectifs sont bien coordonnés et alignés sur les objectifs stratégiques globaux de l'institution.

3) Membres du comité TIC

Ils peuvent varier d'une entité à l'autre, mais tous les comités TIC doivent au moins être composés de : responsable TIC, responsable de la planification et responsable des finances.

4) Fonctionnement du comité TIC

Ce comité doit se réunir au moins une fois par trimestre ; le comité TIC de l'institution est censé s'assurer que les TIC sont exploitées pour améliorer les processus opérationnels au sein des institutions et de meilleurs services aux utilisateurs. Ce comité doit collaborer étroitement avec l'équipe technique TIC du secteur.

XII.2. Unité TIC

La structure TIC des entités publiques est établie par consultation entre l'entité concernée et le SETIC via le Ministère en charge des TIC. Idéalement, la ligne hiérarchique de la fonction TIC devrait être directement rattachée au responsable de l'institution. Dans le cas contraire, il est conseillé à l'unité TIC de tenir le responsable de l'institution au courant des opérations et des plans TIC de l'institution. Les responsabilités et les exigences du poste doivent être alignées sur les exigences et responsabilités standards des postes TIC.

XIII.CONSÉQUENCES DE NON-CONFORMITÉ

Le non-respect de ces directives peut entraîner des mesures disciplinaires, dans lesquelles l'individu assumera tous les risques et dommages causés par la non application de ces directives. Les exceptions à ces directives ne seront autorisées que si elles sont approuvées par le SETIC.

XIV.CYCLE DE RÉVISION DES DOCUMENTS

Le SETIC révisera ces lignes directrices chaque année ou lorsque cela sera jugé nécessaire pour résoudre les nouveaux problèmes découlant de l'utilisation des systèmes d'information et des tendances technologiques émergentes dans l'industrie. Le service informatique de chaque institution publique doit enquêter et assurer le suivi des non conformités signalées et suspectées et prendre les mesures correctives nécessaires.

CONCLUSION GÉNÉRALE

Le Concept Type des Systèmes d'Information des Institutions Publiques (CTSIIP), tel qu'il a été élaboré à travers ce document, constitue une feuille de route stratégique essentielle pour la transformation numérique du secteur public. Dans un contexte où les services publics commencent à se digitaliser sans cadre normatif clair, ce CTSIIP offre une vision structurée et cohérente pour uniformiser et optimiser l'utilisation des TIC au sein de toutes les institutions publiques.

La vision stratégique définie dans ce document établit une direction à long terme pour l'évolution des systèmes d'information publics, en s'appuyant sur des principes directeurs solides en s'alignant sur les objectifs de la « **Vision Burundi pays émergent en 2040 et pays développé en 2060 »**. Ceux-ci visent à garantir que les systèmes mis en place soient non seulement efficaces et innovants, mais également sécurisés et résilients face aux défis technologiques et aux menaces émergentes.

L'infrastructure réseau et système, détaillée dans les sections consacrées, est le pilier de cette transformation, assurant la connectivité, la communication, la gestion de données et la sécurité nécessaires pour un environnement numérique robuste. La sécurité des systèmes informatiques et des données a été abordée de manière exhaustive, soulignant l'importance de protéger les actifs numériques critiques, de gérer efficacement les accès et identités et d'assurer la continuité des services dans toutes les situations.

En parallèle, la gestion des applications logicielles a été développée pour s'assurer que les solutions logicielles sont adaptées, sécurisées, et bien intégrées aux besoins des institutions. Le plan de déploiement proposé offre une feuille de route claire et des stratégies pour la gestion du changement, en identifiant les ressources nécessaires pour atteindre les objectifs fixés.

Enfin, la communication interne et externe et le renforcement des capacités des ressources humaines sont présentés comme des éléments clés pour garantir l'adhésion de tous les acteurs concernés et pour développer les compétences nécessaires à la gestion des nouveaux systèmes. Le

suivi et l'évaluation viennent couronner ce processus, avec des indicateurs de performance et des mécanismes d'audit conçus pour maintenir le cap sur les objectifs à long terme.

En somme, ce CTSIIP est conçu pour guider les institutions publiques vers une transformation numérique réussie, en alignant les technologies de l'information sur les besoins stratégiques du pays, en renforçant la sécurité et l'efficacité des systèmes, et en assurant une gestion proactive et continue des défis technologiques à venir. Il jette les bases d'un environnement numérique intégré, sécurisé, et durable, capable de soutenir le développement socio-économique du pays dans les années à venir.

ANNEXES

1. Références et Bibliographie

[1] Jeffrey S. Beasley, Piyasat N. (2012) *Networking essentials* (3rd Edition). Pearson Education, Inc.

[2] SMB University. (2006). *Networking Fundamentals* (SMBUF-1). Cisco Systems, Inc.

[3] RISA. (2019). *Ict implementation guidelines in government institutions* (1st Edition). Technical directives.

[4] ICT Authority. (2019). *Government Systems and Applications Standard* (2nd Edition). ICTA.6.002:2019.

[5] Lecture, N. (2019-20). *Computer Networks* (R15A0513). B. TECH III YEAR – II SEM (R15).

[6] ASHRAE. (2016). *Data Center Power Equipment Thermal Guidelines and Best Practices* (TC9.9).

[7] Cisco. "What is a Lan? "Cisco, n.d., https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html. Consulté le 17 Juillet 2024.

[8] Steve P. *11 Types of Networks: Understanding the Differences*." Auvik, n.d., https://www.auvik.com/franklyit/blog/types-of-networks/. Consulté le 10 Août 2024.