

SPECIFICATIONS IT MINIMALES AU SEIN DES ADMINISTRATIONS

MARS 2024

HISTORIQUE DES CHANGEMENTS

N°	Auteur	Version	Date de publication	Détails des modifications
1	ATD	1.0	Mars 2024	Première version

METADATA

N°	Élément	Valeurs
1	Titre	Spécifications TIC minimales au sein des administrations
4	Version, mois, année de publication du document	Version 1.0, Mars 2024
5	Auteur	Agence Togo Digital (ATD)
7	Niveau d'application	Obligatoire
8	Régulateur	ATD
9	Audience cible	Toutes les institutions publiques (y compris les autorités locales et nationales) ; les administrations et le grand public.
10	Droits	ATD
11	Format	PDF, Word
12	Sujet	TIC au sein des administrations

Sommaire

1.	Introduction.....	1
1.1.	Objectifs	1
1.2.	Avantages.....	1
2.	Accès à internet	3
2.1.	Togocom	3
2.2.	Moov-Africa	7
2.3.	Groupe Vivendi Africa (GVA).....	8
2.4.	Téolis.....	10
2.5.	Café Informatique.....	10
2.6.	Réseau gouvernemental E-gouv	11
a.	Définition du réseau E-gouv.....	11
b.	Objectif du réseau E-gouv	12
c.	Infrastructure Technique	13
3.	Le réseau local.....	14
3.1.	Conception du réseau	14
3.1.1.	Définition de la bande passante	14
3.1.2.	Choix des technologies à haut débit	17
3.1.3.	Conception de schéma de réseau physique	17
3.1.4.	Conception de schéma de réseau logique.....	17
3.1.5.	Gestion et surveillance du réseau.....	17
3.2.	Implémentation de réseaux.....	18
3.2.1.	Éléments du réseau	18
3.2.1.1.	Equipements du réseau	18
3.2.1.2.	Equipements des utilisateurs finaux	19
3.2.2.	Gestion de l'alimentation électrique.....	22
3.2.2.1.	Alimentation	22
3.2.2.2.	Groupes électrogènes.....	23
3.2.2.3.	Les kits solaires	23
3.2.3.	Salle de communication.....	24
3.2.4.	Installation et configuration du réseau	25
3.3.	Gestion de réseaux	25

3.3.1.	Performance du Réseau.....	25
3.3.2.	Maintenance du Réseau.....	26
3.3.3.	Référencement du câblage réseau.....	27
3.3.4.	Sécurité du réseau	27
3.4.	Réseau minimal des administrations.....	27
3.4.1.	Définition.....	27
3.4.2.	Objectif	28
3.4.3.	Existence sur le terrain.....	28
3.4.3.1.	Accès à électricité.....	28
3.4.3.2.	Accès à internet.....	30
3.4.3.3.	Les locaux.....	30
3.4.4.	Classification des administrations.....	31
3.4.5.	Architecture réseau minimal des administrations.....	33
3.5.	Sauvegarde du poste de travail.....	42
3.6.	Gestion des Équipements Informatiques.....	42
3.6.1.	Accès au Système (Connexion au Réseau Local - LAN)	42
3.6.2.	Gestion des Ordinateurs	42
3.6.3.	En cas de Vol ou la Perte	42
3.6.4.	Appareils des utilisateurs	43
3.6.5.	Règles d'entretien.....	43
3.6.6.	Responsabilités.....	43
3.7.	Maintenance du matériel	43
4.	Acquisition des matériels informatiques.....	45
4.1.	Contexte.....	45
4.2.	La marketplace	45
4.2.1.	Définition.....	45
4.2.2.	Objectifs	45
4.3.	Avantages.....	45
5.	Gestion des données	47
5.1.	Catégories de données à protéger.....	47
5.1.1.	Disponibilité des Données :.....	47
5.1.2.	Normalisation des Données Partagées :.....	47
5.1.3.	Identificateurs de Données :.....	47
5.1.4.	Sauvegarde et Récupération des Données :.....	47

5.1.5.	Catégories de Données à Protéger :	47
5.1.6.	Classification des Données :	47
5.1.7.	Politiques d'Accès aux Données :	48
5.1.8.	Chiffrement des Données :	48
5.1.9.	Gestion du Cycle de Vie des Données :	48
5.1.10.	Audit des Accès :	48
5.1.11.	Formation des Utilisateurs :	48
5.2.	Chiffrement	48
5.3.	Sauvegarde et restauration	49
5.4.	Journalisation et supervision de la sécurité	50
6.	Cybersécurité	51
6.1.	Minimiser l'exposition des systèmes aux réseaux externes	51
6.2.	Mettre en œuvre la segmentation du réseau	52
6.3.	Mise à jour des systèmes informatiques	52
6.4.	Téléchargement des programmes	53
6.5.	Antivirus	53
6.6.	Décommissionnement	54
6.7.	Comptes de messagerie et messagerie officielle	55
6.8.	Imprimantes et scanner	56
6.9.	Incident de sécurité	56
6.9.1.	Exemples d'incident de sécurité	56
6.9.2.	Gestion des incidents de sécurité	57
6.10.	Sensibilisation à la cybersécurité au niveau de l'institution	57
7.	Applications logicielles	59
7.1.	Modèle architectural	59
7.1.1.	Principes Fondamentaux de l'Architecture :	59
7.1.2.	Couches de l'Architecture :	59
7.1.3.	Technologies et Normes :	60
7.2.	L'usage de logiciels libres	60
8.	Développement logiciel	62
8.1.	Approche pour le développement d'applications	62
8.2.	Langages	62
8.3.	Plateformes	62
8.4.	Framework	62

8.5.	Développement mobile	62
8.6.	Conception Web adaptative	63
9.	Administration des systèmes d'information	64
9.1.	Protection des mots de passe.....	64
9.1.1.	Longueur des mots de passe	64
9.1.2.	Règles de complexité des mots de passe.....	64
9.1.3.	Délai d'expiration des mots de passe.....	65
8.1.3.	Contrôle de la robustesse des mots de passe	65
8.1.4.	Stockage des mots de passe.....	66
8.2.	Accès aux systèmes	66
8.2.1.	Identification.....	66
8.2.2.	Authentification.....	66
8.2.3.	Droits d'administration	66
8.2.4.	Comptes Utilisateurs	66
8.2.5.	Contrôles d'Accès	66
8.2.6.	Journaux d'Accès et Surveillance	67
8.2.7.	Accès à Distance	67
9.	Désactivation des Comptes	67
10.	Audit Régulier	67
	Revue et mise à jour du document	67
	Annexe 1 : Procédures E-Gouv	68
1.	Intégration et contrat.....	68
1.1.	Aperçu	68
1.2.	Informations sur le client	68
1.3.	Vérification des antécédents ou diligence raisonnable.....	68
1.4.	Négociation de contrats.....	68
1.5.	Signature du contrat	68
1.6.	Configuration du client sur la plateforme de gestion des commandes	69
2.	Étapes du processus de facturation	69

Liste des figures

Figure 1 : Couverture filaire de Togocom	4
Figure 2 : Couvertures 3G et 4G de Togocom	6
Figure 3 : Couvertures 3G et 4G de Moov	8
Figure 4 : Couverture GVA	9
Figure 5 : Accès à internet dans les administrations	29
Figure 6 : Sources d'alimentation électrique	29
Figure 7 : Accès internet dans les administrations.....	30
Figure 8 : Nombre de locaux des administrations.....	31
Figure 9 : Architecture physique minimale pour une administration de type "A"	33
Figure 10 : Architecture physique minimale pour une administration de type "C"	38
Figure 11 : Exemple de kit mobile.....	41

Liste des tableaux

Tableau 1 : Offres internet de Togocom.....	4
Tableau 2 : Produits de Togocom	6
Tableau 3 : Offres internet de Moov-Africa.....	7
Tableau 4 : Produits de Moov-Africa	8
Tableau 5 : Offres internet de GVA.....	9
Tableau 6 : Offres internet de Téoilis.....	10
Tableau 7 : Offres internet de Café.....	10
Tableau 8 : Autres types de modem 3-4G	11
Tableau 9 : Débit internet minimal par activité.....	15
Tableau 10 : Exemples de débit internet en fonction du type et de la taille des institutions.....	15
Tableau 11 : Exigences minimales de bande passante selon le nombre d'utilisateurs et de ressources.....	16
Tableau 12: Configurations matérielles en fonction de l'usage	21
Tableau 13 : Les types d'alimentation électrique	22
Tableau 14 : Recommandations pour la performance du réseau	26
Tableau 15 : Recommandations pour la maintenance du réseau.....	26
Tableau 16 : Dimensionnement du réseau des administrations de type "A"	34
Tableau 17 : Dimensionnement des équipements utilisateur final des administrations de type "A"	35
Tableau 18 : Dimensionnement du réseau des administrations de type "B"	36
Tableau 19 : Dimensionnement des équipements utilisateurs final des administrations de type « B »	37
Tableau 20 : Dimensionnement du réseau des administrations de type "C"	38
Tableau 21 : : Dimensionnement des équipements utilisateurs final des administrations de type "C"	39
Tableau 22 : Estimation de la consommation des équipements.....	39
Tableau 23 : Estimation de la puissance des groupes électrogènes	40
Tableau 24 : Liste des administrations n'ayant qu'un seul personnel	40
Tableau 25 : Maintenance du matériel.....	44
Tableau 26 : Recommandation pour minimiser l'exposition des systèmes aux réseaux externes	51
Tableau 27 : Principes pour l'architecture.....	59
Tableau 28 : Couches de l'architecture des logiciels.....	59
Tableau 29 : Avantages de l'utilisation des logiciels libres	60
Tableau 30 : Principes de développement.....	62
Tableau 31 : Paradigmes de conception web	63
Tableau 32 : Recommandation pour la longueur des mots de passe.....	64

1. Introduction

Ce document vise à établir un cadre uniforme et cohérent pour la mise en œuvre des technologies de l'information et de la communication (TIC) au sein des institutions gouvernementales du Togo. En reconnaissant l'importance cruciale des TIC pour le développement national, ce guide a pour objectif d'assurer une mise en œuvre efficace, sécurisée et durable des systèmes informatiques, favorisant ainsi une gouvernance améliorée et un service public plus accessible et réactif.

1.1. Objectifs

L'objectif principal de ce document est de fournir un cadre structuré et cohérent pour la mise en œuvre et la gestion des technologies numériques au service des objectifs institutionnels. Plus spécifiquement, ce document vise à :

- Standardiser l'infrastructure et les pratiques TIC : Établir des normes uniformes pour l'acquisition, l'utilisation et la maintenance des équipements et systèmes TIC, garantissant ainsi l'interopérabilité, la sécurité, et l'efficacité à travers toutes les branches et niveaux de l'administration.
- Orienter les investissements TIC : Fournir une direction claire pour les futurs investissements en technologies, assurant que les dépenses sont alignées avec les objectifs stratégiques de l'administration et qu'elles apportent une valeur ajoutée mesurable.
- Améliorer la gouvernance TIC : Définir les responsabilités, les processus de prise de décision, et les mécanismes de contrôle pour la gestion des ressources TIC, renforçant ainsi la gouvernance et la responsabilité organisationnelle.
- Assurer la sécurité et la conformité : Mettre en place des directives pour protéger les données et les systèmes contre les cybermenaces, tout en s'assurant que les pratiques TIC respectent les normes légales et réglementaires applicables.
- Faciliter la transformation numérique : Accélérer l'adoption des technologies numériques pour moderniser l'administration publique, améliorer la prestation des services aux citoyens, et favoriser une culture de l'innovation et de l'efficacité.
- Renforcer l'accès et l'inclusion numérique : Garantir que les initiatives TIC prennent en compte et adressent les besoins de toutes les administrations
- Optimiser la gestion des ressources TIC : Fournir des lignes directrices pour une allocation et une utilisation efficiente des ressources TIC, maximisant le retour sur investissement et minimisant le gaspillage.

1.2. Avantages

L'adoption de ce document offre plusieurs avantages significatifs. Premièrement, il permet d'harmoniser les efforts de digitalisation à travers toutes les institutions, garantissant ainsi une sécurité et une fiabilité optimales des systèmes TIC. Deuxièmement, il promeut l'efficacité et la réduction des coûts en évitant la duplication des efforts et en encourageant l'utilisation de

solutions partagées. Enfin, il facilite l'intégration et l'évolutivité des futures technologies, positionnant le Togo comme un acteur compétitif dans l'économie numérique mondiale.

2. Accès à internet

Dans un monde de plus en plus numérisé, la connectivité internet est devenue un pilier central du fonctionnement efficace des administrations publiques. Au Togo, comme dans de nombreux pays, l'accès à une connexion internet fiable et rapide est essentiel pour permettre aux administrations de remplir leurs missions de service public. Cette connectivité permet non seulement une communication fluide et rapide avec les citoyens, mais elle est également cruciale pour la modernisation des services administratifs, l'amélioration de la transparence et le renforcement de la gouvernance.

Dans ce contexte, le rôle des fournisseurs d'accès internet (FAI) au Togo est primordial. Ces acteurs du secteur des télécommunications fournissent l'infrastructure nécessaire pour assurer une connectivité de qualité aux administrations. Le paysage des FAI au Togo est marqué par une diversité d'offres, allant des connexions à large bande fixe aux solutions mobiles 4G, adaptées aux différents besoins des administrations.

Ce chapitre explorera donc les différentes facettes de l'accès internet pour les administrations togolaises, en analysant les offres des FAI présents sur le marché et en soulignant les enjeux liés à la digitalisation des services publics.

2.1. Togocom

Togocom offre une gamme étendue de services Internet, incluant des solutions haut débit via la fibre optique et des liaisons spécialisées. Ses offres sont adaptées à une variété d'usages professionnels, garantissant des débits élevés et une connectivité stable, essentielle pour les administrations publiques.

Pour ce faire, Togocom a déployé un backbone d'environ 1.500 km du nord au sud du pays sur les axes Lomé-Atakpamé-Cinkassé, Lomé-Kpalimé-Atakpamé ainsi que Lomé-Aného. Chaque liaison du réseau est constituée de 24 fibres optiques. Elle est dédoublée à Lomé (2 x 48 fibres) et sur les tronçons Atakpamé-Kara et Kara-Cinkasse.

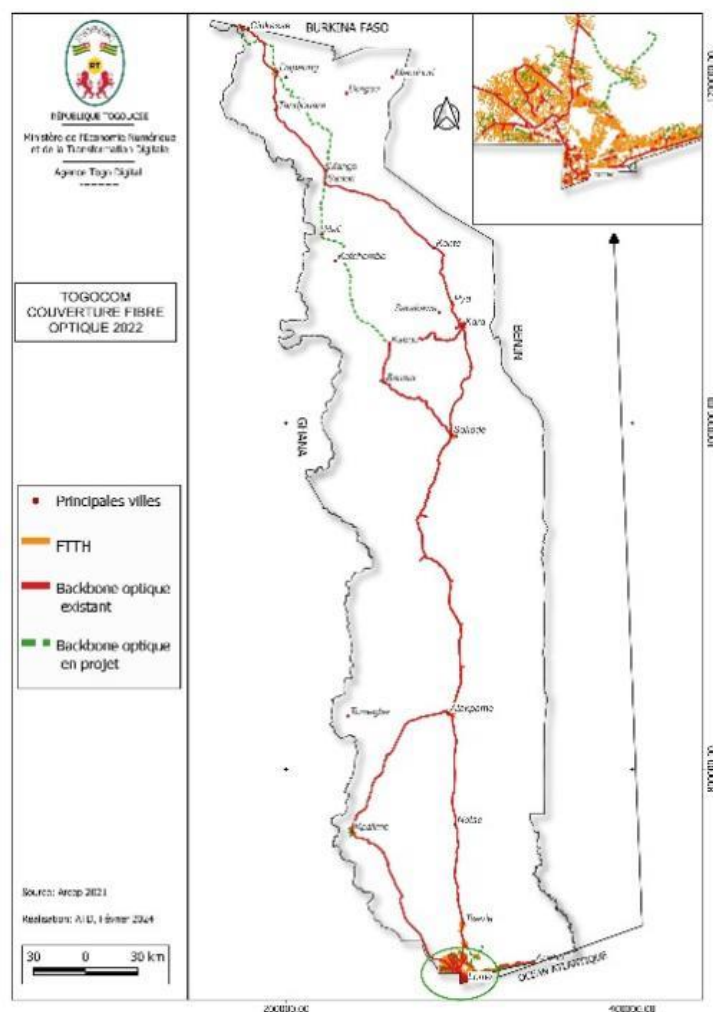


Figure 1 : Couverture filaire de Togocom

Ce réseau backbone de fibres a été conçu pour raccorder toutes les Préfectures et les importantes zones économiques du pays, soit une quarantaine de villes. Il propose trois (03) types d'offres, selon le tableau ci-dessous [1]:

Tableau 1 : Offres internet de Togocom

Type de clients	Type d'offre	Description	Prix
Résidentiel	Silver	Jusqu'à 50 Mbps +3 600 minutes d'appel vers fixe	15.000 F CFA
	Gold	Jusqu'à 100 Mbps + 3600 minutes d'appel vers fixe & 120 minutes d'appel vers mobile	25.000 F CFA
	Platinum	Jusqu'à 200 Mbps + 3600 minutes d'appel vers fixe &	30.000 F CFA

		120 minutes d'appel vers mobile	
Professionnel	Pro small	Jusqu'à 250 Mbps + 14400 minutes d'appel vers Fixe & 120 minutes d'appel vers mobile	55.000 F CFA
	Pro	Jusqu'à 300 Mbps + 14400 minutes d'appel vers Fixe & 120 minutes d'appel vers mobile	75.000 F CFA
Entreprise	Pro plus	Jusqu'à 350 Mbps + 14 400 minutes d'appel vers Fixe & 120 minutes d'appel vers mobile	125.000 F CFA
	Pro cyber	Jusqu'à 400 Mbps + 14 400 minutes d'appel vers Fixe & 120 minutes d'appel vers mobile	200.000 FCFA

Pour les administrations dans les zones rurales ne pouvant pas souscrire à l'offre de fibre, Togocom propose des produits basés sur les cartes SIM pour les connecter à internet.

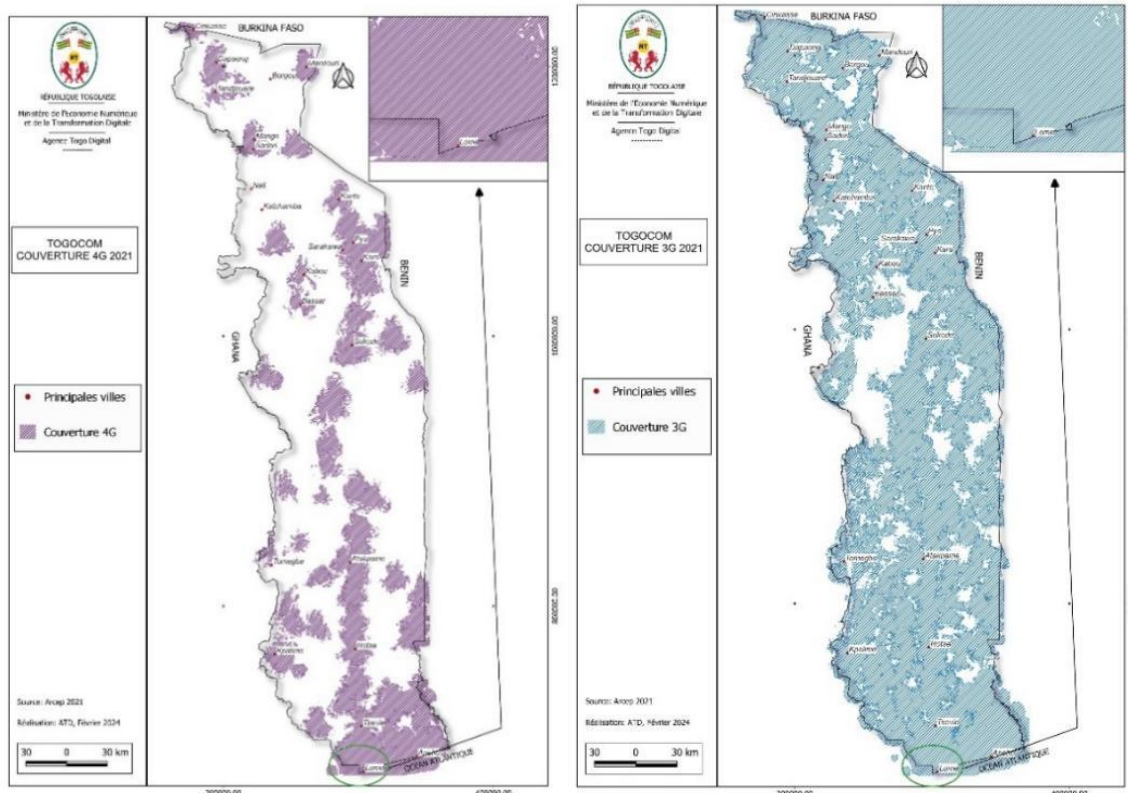






Figure 2 : Couvertures 3G et 4G de Togocom

Le tableau suivant en fait le résumé [2]:

Tableau 2 : Produits de Togocom

Image	Type de produit	Descriptions	Prix
	Box Harvilon 4G	Nano SIM double standby Connectivité trois ports LAN RJ45, RJ11 pour gigabit Ethernet pour la connexion par câbles d'appareils, PC, portables 32 appareils connectés en simultané WiFi 802.11 b/g/n 802a 3GPPP 4G/LTE, Cat4	49.900 F CFA
	Box Nokia 4G	Nano SIM double standby Connectivité trois ports LAN RJ45, RJ11 pour gigabit Ethernet pour la connexion par câbles d'appareils, PC, portables Utilisateurs en simultané WiFi 802.11 b/g/n 802a 3GPPP 4G/LTE, 3GPPP 5NR	49.900 F CFA

	RapidBox 5G	1 Box 5G 120Go de Data pendant 1 an Compatible 4G & 5G Sous condition d'être couvert par la zone 5G. Jusqu'à 15 appareils connectés.	295.000 F CFA
	MIFI ALCATEL 4G	Surfez et partagez Internet en toute mobilité 1 MiFi Alcatel 4G+ 1 kit 4G+ 60Go de DATA (valable 30 jours) Jusqu'à 15 appareils connectés.	39.900 F CFA

2.2. Moov-Africa

La société Moov Africa a déployé un backbone d'environ 800 km du nord au sud du pays sur l'axe Lomé-Atakpamé-Cinkassé. Le réseau est constitué de 96 fibres optiques. Ce réseau backbone, a été conçu pour raccorder toutes les préfectures et les importantes zones économiques sur l'axe routier, soit une trentaine de villes.

Contrairement à Togocom, l'offre internet de Moov-Africa se limite à l'internet mobile 4G. Voici les forfaits qu'il propose :



Tableau 3 : Offres internet de Moov-Africa

Nom	Description	Prix
iZi Small	6Go pour 30 jours	4500 F CFA
Medium	30Go pour 30 jours	9000 F CFA
iZi Large	75Go pour 30 jours	15000 F CFA
iZi Max	275Go pour 30 jours	50000 F CFA

Ces forfaits peuvent largement suffire pour les très petites ou petites administrations (au plus de 50 personnes) dont l'utilisation d'internet ne nécessite pas de grandes quantités de données mobiles

En complément de ces offres, Moov-Africa propose des « modems » pour un accès à plusieurs à internet. Les modèles sont :

Tableau 4 : Produits de Moov-Africa

Image	Nom	Description	Prix
	MoovPocket 4+	Permet de connecter 10 utilisateurs Autonomie de 8h 50Go à l'activation pendant 3 mois	49.900 F CFA
	MoovBox	50Go à l'activation pendant 3 mois Permet de connecter 32 utilisateurs Autonomie de 4h en utilisation intense	79.000 F CFA

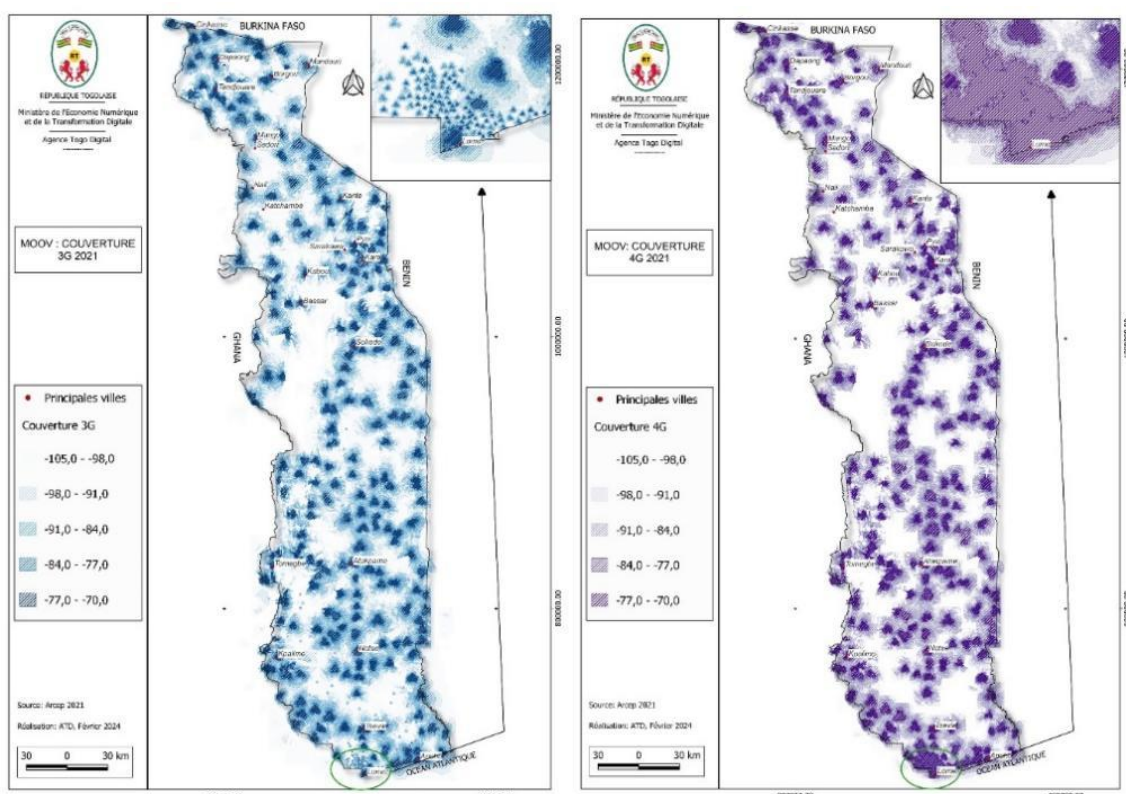


Figure 3 : Couvertures 3G et 4G de Moov

2.3. Groupe Vivendi Africa (GVA)

GVA (filiale du groupe Vivendi) se distingue par ses investissements dans les infrastructures de fibre optique, promettant des vitesses de connexion élevées et une fiabilité accrue.

Avec sa box « Canalbox » et revendiquant une couverture totale de la ville de Lomé tout en poursuivant l'élargissement de son réseau, elle peut s'avérer intéressante pour les administrations situées dans le grand Lomé

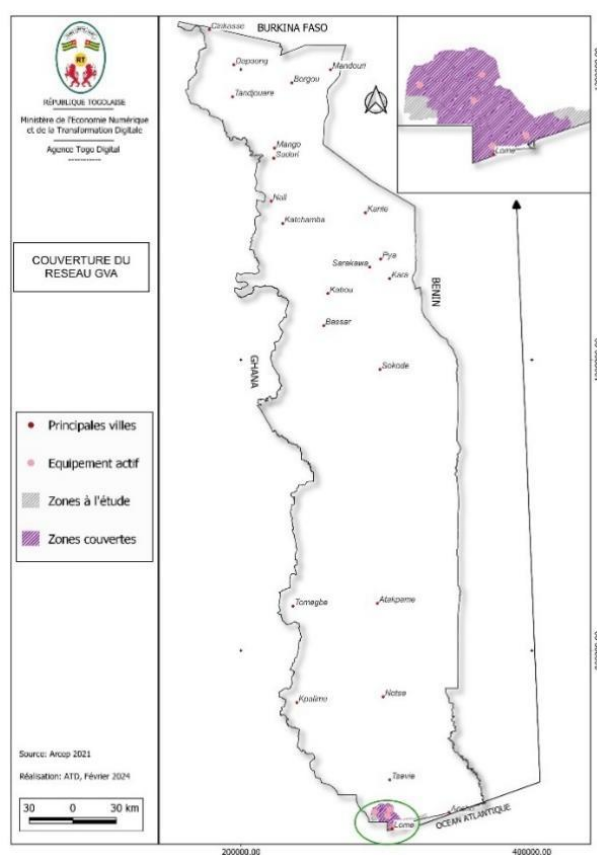


Figure 4 : Couverture GVA

Tableau 5 : Offres internet de GVA

Nom	Description	Prix
iZi Small	6Go pour 30 jours	4500 F CFA
Medium	30Go pour 30 jours	9000 F CFA
iZi Large	75Go pour 30 jours	15000 F CFA
iZi Max	275Go pour 30 jours	50000 F CFA

Les administrations intéressées pourraient donc se rapprocher de GVA afin d'obtenir plus d'informations sur leurs offres pour les professionnelles

2.4. Téolis

Offre des services couvrant le grand Lomé. Ils sont spécialisés dans les solutions orientées entreprises.

Tableau 6 : Offres internet de Téolis

Type d'offre	Description	Prix
Dream	Pour usage personnel Jusqu'à 10 Mbps	15.000 F CFA
Wifi Zone	Adaptée pour la commercialisation A partir de 50m/s	25.000 F CFA
Entreprise	Adapté pour les moyennes entreprises Jusqu'à 20m/s	30.000 F CFA
Business	Adapté pour les grandes entreprises 200m/s et plus	55.000 F CFA

2.5. Café Informatique

Les solutions Internet dédiées de CAFE offre aussi une connexion internet adaptée aux entreprises. Cette connectivité à est disponible en 2Mbps, 5Mbps, 10Mbps et plus si nécessaire.

Tableau 7 : Offres internet de Café




Type de clients	Description	Prix
Fibres pour les Particuliers et les PME	Jusqu'à 50 Mbps	15.000 F CFA
	Jusqu'à 100 Mbps	22.500 F CFA
	Jusqu'à 200 Mbps	30.000 F CFA
Fibres pour les entreprises	Bande passante jusqu'à 50 mbps IP publique Un compte Microsoft OneDrive de 1TO de sauvegarde	59.000 F CFA
	Jusqu'à 100 Mbps IP publique 1 compte Microsoft OneDrive de 1TO de sauvegarde	118.000 F CFA

Sans fil, liaisons dédiées	Jusqu'à 50 Mbps + 6 adresses IP publiques mobile	472.000 F CFA
	Jusqu'à 100 Mbps	944.000 FCFA

Note importante sur les prix : Les prix indiqués dans ce document sont valables à la date du 20 février 2023, et sont sujets à modification. Pour obtenir les informations les plus récentes et précises concernant nos prix, veuillez consulter les sites web des fournisseurs.

En plus des équipements cités plus haut proposés par Togocom et Moov, d'autres équipements basés sur la 4G peuvent également être utilisés. On a entre autres :

Tableau 8 : Autres types de modem 3-4G

Image	Type de produit	Descriptions	Prix
	Routeur Extérieur étanche 4G LTE avec Emplacement pour Carte SIM	Routeur extérieur 4G LTE CPE conçu pour que les utilisateurs WIFI accèdent à Internet via UMTS/HSPA/LTE Peut être connecté à 16 appareils en même temps	83278,9 F CFA
	KuWiFi Routeur de Carte SIM extérieur 4G LTE avec Emplacement pour Carte sim	Amplificateur 4g peut être connecté à 10 appareils en même temps 1 Port RJ45	31523,41 F CFA
	Cudy Routeur 4G LTE	Client VPN PPTP / L2TP préinstallé pour la sécurité 4 ports Ethernet Ports WAN / LAN flexibles pour une double connectivité	35906,79 F CFA

2.6. Réseau gouvernemental E-gouv

a. Définition du réseau E-gouv

Le réseau E-Gouv du Togo est bien plus qu'une infrastructure technologique ; il représente une vision pour l'avenir, un engagement envers l'amélioration continue des services publics et une

promesse d'inclusion numérique pour tous les citoyens. À travers cette initiative, le Togo démontre son engagement à utiliser la technologie pour catalyser le développement socio-économique, améliorer l'efficacité gouvernementale et renforcer la confiance des citoyens dans l'administration publique.

Le réseau E-Gouv dont l'objectif est de renforcer l'efficacité de l'administration et la rapprocher des citoyens a été inauguré le 24 Avril 2017. Ce réseau en fibre optique d'environ 300 km permet d'interconnecter les sites (plus de 600 bâtiments à ce jour) de l'administration publics (CHU, centres de santé, plus du tiers des lycées publics, universités, toutes les institutions de la Républiques et tous les ministères) dans la ville de Lomé. Chacun des sites raccordés au réseau dispose, outre de l'accès au réseau IP privé de l'administration public, d'un accès internet haut débit de 100 Mb par seconde et par bâtiment.

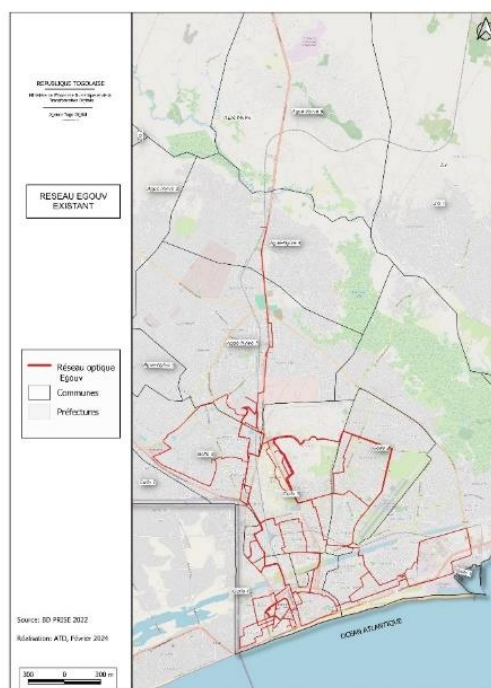


Figure 3 : Couverture du réseau E-gouv

b. Objectif du réseau E-gouv

Les objectifs du réseau E-Gouv sont de :

- Doter les services de l'administration publique, les universités, les écoles, les hôpitaux et les autres structures publiques, d'un accès Internet de grande capacité et d'une qualité de service irréprochable ;
- Améliorer la circulation sécurisée de l'information entre les services de l'administration mais également entre les usagers du service public (citoyens, investisseurs, etc.) ;
- Moderniser et rationaliser l'administration publique par l'optimisation des démarches et procédures administratives (il sera plus simple et plus rapide d'accéder aux informations de l'administration) ;
- Mettre à disposition des agents de l'Etat un environnement TIC moderne et des outils plus adaptés pour faciliter leurs missions.

L'intégralité des bâtiments administratifs de la capitale est désormais connectée au réseau de fibre optique et les équipements nécessaires pour leur assurer un accès Internet haut-débit ont été installés.

c. Infrastructure Technique

Le réseau gouvernemental était basé sur les technologies Dense Wavelength Division Multiplexing (DWDM) et Multiprotocol Label Switching (MPLS) de l'équipementier Huawei. Le cœur du réseau MPLS, composé de deux boucles concentriques de 10 Gbps permet de connecter les nœuds primaires avec le centre de données « Lomé Datacenter ». Les nœuds de collectes sont quant à eux connectés chacun à deux nœuds du cœur de réseau pour des besoins de redondance. Autour de chaque nœud de collecte est créée une boucle de collecte permettant de relier les sites de l'administration publique dans la zone géographique desservie. Récemment la société CSquared Woezon a procédé à une contre mise à niveau du réseau central existant de la plate-forme Huawei vers la plate-forme Nokia en raison de la fin de la prise en charge des équipements Huawei. La nouvelle topologie en anneau pour le réseau Core IP/MPLS a actuellement une capacité totale de 100 Gbit/s par rapport au réseau existant de 10 Gbit/s. La configuration dispose également de la technologie GPON qui aidera à prendre en charge les utilisateurs à faible capacité et la possibilité de faire de la fibre optique jusqu'au domicile FTTH.

Le réseau est supervisé et géré à partir d'un Centre d'Opération du Réseau (NOC) colocalisé avec le centre de données national.

3. Le réseau local

Le réseau local (LAN) constitue la colonne vertébrale de l'infrastructure informatique des administrations. Il joue un rôle crucial dans la facilitation de la communication interne, le partage de ressources et l'accès sécurisé aux données. À une époque où la dépendance aux technologies de l'information ne cesse de croître, la conception, la mise en œuvre et la gestion d'un réseau local efficace et sécurisé deviennent primordiales pour les administrations. Ce chapitre s'attachera à explorer les spécifications techniques, les recommandations d'équipement et les exigences en termes de débit nécessaires pour optimiser les réseaux locaux administratifs, en tenant compte des défis et des besoins spécifiques à ce secteur.

La spécification d'un réseau local pour une administration implique une compréhension approfondie des besoins opérationnels et des objectifs de l'organisation. Cela inclut l'évaluation de la taille du réseau, le nombre d'utilisateurs, l'accès à internet ou à l'électricité... Tous ces éléments seront décrits pour fournir des propositions plus détaillées.

3.1. Conception du réseau

Lors de la phase de conception du réseau informatique au sein des administrations, certains prérequis sont nécessaires pour son dimensionnement.

3.1.1. Définition de la bande passante

L'évaluation des besoins minimums en bande passante pour une institution publique implique d'évaluer les besoins spécifiques et les habitudes d'utilisation de cette institution. Voici les critères à considérer pour pouvoir calculer le besoin minimum en bande passante :

- Nombre d'utilisateurs : Comptez le nombre d'utilisateurs qui se connecteront au réseau. Incluez à la fois le personnel et les visiteurs susceptibles d'utiliser le réseau de l'institution
- Nombre d'appareils : Déterminez le nombre d'appareils qui se connecteront au réseau, car chaque appareil consomme de la bande passante
- Habitudes d'utilisation :
 - Navigation Web : Estimez le comportement typique de navigation sur le Web des utilisateurs. La navigation Web de base consomme moins de bande passante que la diffusion en continu de médias ou le téléchargement de gros fichiers
 - Diffusion en continu : Si la diffusion en continu de vidéos est courante (par exemple, pour des cours en ligne ou la diffusion d'informations publiques), prenez en compte la bande passante requise par flux (par exemple, 720p, 1080p, 4K)
 - Téléchargements/Téléversements : Considérez la fréquence et la taille des téléchargements et des téléversements de fichiers. Les transferts de fichiers volumineux nécessitent plus de bande passante

Le tableau ci-dessous présente les débits Internet nécessaires pour les activités les plus courantes :

Tableau 9 : Débit internet minimal par activité

Type d'activité	Débit nécessaire (Mbps)
Appel audio	0,3
Envoyer un email ou naviguer sur internet	1
Surfer sur internet	1
Appel sur IP	Moins de 0.5
Télétravail	5 à 25
Téléchargement de fichiers	10
Réseaux sociaux	1
Streaming vidéo qualité standard	3-4
Streaming vidéo HD 1080p	5-8
Streaming vidéo HD 4K	25
Télécharger des fichiers volumineux	50 et plus
Appels vidéo qualité standard	1
Appels vidéo HD	1.5

Le tableau suivant liste des exemples de débit internet en fonction du type et de la taille des institutions :

Tableau 10 : Exemples de débit internet en fonction du type et de la taille des institutions

Bande passante globale nécessaire	Types d'activités
Débits : 4-10 Mbps	<ul style="list-style-type: none"> - Idéal pour les petites et moyennes entreprises avec un à cinq ordinateurs. - Permet de traiter son courrier électronique, de naviguer sur internet, de télécharger de petits fichiers ; - Non recommandé pour les entreprises qui ont une utilisation intensive d'Internet.
Débit : 25 Mbps	<ul style="list-style-type: none"> - Permet d'effectuer des téléchargements fréquents et le partage de fichiers ; - Bonne option pour les entreprises avec de nombreux utilisateurs.
	<ul style="list-style-type: none"> - Vitesse idéale pour les grandes entreprises qui dépendent fortement

Débit : 50 Mbps	des applications internet, du partage de fichiers, etc. - Prend en charge la vidéosurveillance HD, le streaming et la vidéoconférence
Débit : 110 Mbps	- Vitesse ultra-rapide et connexion transparente - Meilleure option pour les entreprises avec de nombreux utilisateurs travaillant sur le cloud ou à distance ; - Le débit de votre connexion permet la collecte de données en temps réel, le stockage, la vidéoconférence HD, etc.

- Croissance future : Prenez en compte la croissance future du nombre d'utilisateurs, d'appareils et de services. Les besoins en bande passante ont tendance à augmenter avec le temps
- Marge de sécurité : Il est recommandé d'ajouter une marge de sécurité (par exemple, 20 à 30 %) à votre calcul de la bande passante pour tenir compte des pics inattendus d'utilisation et garantir un réseau réactif

Vous pouvez utiliser la formule suivante pour estimer les besoins en bande passante :

$$[\text{Débit internet minimale requise} = (\text{Nombre d'utilisateurs}) \times (\text{Bande passante moyenne par utilisateur})]$$

Le tableau suivant énumère les exigences minimales en termes de débit internet selon le nombre d'utilisateurs et de ressources :

Tableau 11 : Exigences minimales de bande passante selon le nombre d'utilisateurs et de ressources

Exigences minimales de bande passante pour les institutions publiques et privées	
Nombre moyen d'utilisateur et de ressource par institution	Débit internet (Mbps)
1-10	2
11-20	4
21-30	6
31-40	8
41-50	10
51-60	12
61-70	14

71-80	16
81-90	18
91-100	20
101-120	24
121-140	28
141-160	32
161-180	36
181-200	40
201-240	48
241-280	56
281-320	64
321-360	72
361-400	80
+ 400	Dimensionnement spécifique

3.1.2. Choix des technologies à haut débit

- Choisissez une technologie haut débit appropriée en fonction de critères tels que la couverture, la vitesse et la scalabilité. Les options peuvent inclure le DSL, le câble, la fibre optique, le satellite ou les technologies sans fil
- Prenez en compte l'emplacement géographique de l'établissement et la disponibilité des différentes options haut débit

3.1.3. Conception de schéma de réseau physique

- Créez un schéma de réseau physique qui illustre la disposition du matériel de réseau, tels que les routeurs, les commutateurs, les points d'accès et les serveurs
- Dans cette topologie du réseau, incluez des informations sur les connexions physiques entre les appareils, l'infrastructure de câblage et l'emplacement de l'équipement

3.1.4. Conception de schéma de réseau logique

- Élaborez un schéma de réseau logique qui montre comment les données circulent à travers le réseau ainsi que les zones de segmentation logiques
- Dans cette topologie du réseau, incluez des détails sur l'adressage IP, les sous-réseaux, les VLAN (le cas échéant) et l'architecture générale du réseau

3.1.5. Gestion et surveillance du réseau

- Mettez en place des outils de gestion du réseau pour surveiller les performances du réseau, identifier les problèmes et optimiser les ressources

- Configurez des alertes et des notifications pour réagir rapidement à toute anomalie du réseau

3.2. Implémentation de réseaux

La partie suivante fournit des recommandations pour l'installation et la configuration du réseau. Ces recommandations sont conçues pour aider les organisations à mettre en place des réseaux sécurisés et fiables.

3.2.1. Éléments du réseau

L'architecture d'un réseau se compose de divers éléments interdépendants qui doivent être soigneusement sélectionnés et configurés pour répondre aux besoins spécifiques de l'administration.

3.2.1.1. Équipements du réseau

Les équipements du réseau, souvent appelés matériels réseau ou dispositifs réseau, sont les composants physiques utilisés pour interconnecter des ordinateurs, des serveurs, et d'autres dispositifs dans un réseau informatique. Ces équipements permettent la transmission des données entre les dispositifs sur le réseau, facilitent la gestion du trafic de données, et contribuent à la sécurité et à l'efficacité du réseau. Voici une liste des équipements de réseau les plus courants et leur fonction :

- Routeur (Router)

Fonction principale : Connecte plusieurs réseaux et dirige le trafic de données entre eux. Il opère principalement au niveau 3 (couche réseau) du modèle OSI.

- Commutateur (Switch)

Fonction principale : Connecte des dispositifs au sein d'un même réseau local (LAN) et dirige les données vers leur destination spécifique en utilisant l'adresse MAC. Il opère principalement au niveau 2 (couche de liaison de données) du modèle OSI.

- Point d'accès sans fil (Wireless Access Point, WAP)

Fonction principale : Permet aux dispositifs sans fil de se connecter à un réseau filaire, étendant le réseau à des dispositifs sans fil via des signaux radio.

- Modem

Fonction principale : Convertit les données entre les signaux numériques utilisés par les dispositifs informatiques et les signaux analogiques utilisés sur les lignes téléphoniques ou autres types de lignes de communication.

- Pare-feu (Firewall)

Fonction principale : Sécurise le réseau en contrôlant le trafic entrant et sortant selon des règles prédéfinies, bloquant ou autorisant les données en fonction de ces règles.

- Répéteur et Amplificateur

Fonction principale : Étend la portée des signaux réseau en les répétant ou en les amplifiant pour couvrir de plus grandes distances.

- Concentrateur (Hub)

Fonction principale : Un dispositif de réseau basique qui connecte plusieurs dispositifs dans un réseau local (LAN) en répétant les données reçues d'un port à tous les autres ports. Il opère de manière moins efficace qu'un commutateur.

- Pont (Bridge)

Fonction principale : Connecte deux segments de réseau pour fonctionner comme un seul réseau. Il filtre le trafic et peut réduire le volume de trafic sur un réseau en divisant celui-ci en deux segments.

- Passerelle (Gateway)

Fonction principale : Agit comme un point de jonction entre deux réseaux utilisant des protocoles de communication différents, facilitant la communication entre eux.

- Serveurs

Les serveurs constituent le cœur du réseau. Ils hébergent les applications, les bases de données et les services nécessaires au fonctionnement de l'administration. Ces serveurs peuvent inclure des serveurs de fichiers, des serveurs d'applications, des serveurs de bases de données, etc.

- Système de prévention/détection d'intrusion (IPS/IDS)

Fonction principale : Surveille le trafic réseau pour détecter et prévenir les activités suspectes, contribuant à la sécurité du réseau.

3.2.1.2. Équipements des utilisateurs finaux

Les équipements d'utilisateurs finaux incluent les ordinateurs de bureau, les ordinateurs portables, les tablettes, et les smartphones. Le choix de ces dispositifs dépend des tâches spécifiques à accomplir par les utilisateurs au sein de l'administration.

3.2.1.2.1. Caractéristiques minimal des équipements

- **Ordinateur de bureau**
 - Processeur (CPU) : Processeur dual-core ou quad-core, fréquence d'horloge d'au moins 2,0 GHz.
 - Mémoire vive (RAM) : 4 Go de RAM ou plus. Pour des performances plus fluides, 8 Go ou plus sont recommandés.

- Stockage : Disque dur de 500 Go ou plus. Un disque SSD (Solid-State Drive) est recommandé pour des performances plus rapides.
- Carte graphique : Une carte graphique intégrée est suffisante pour un usage bureautique standard. Pour les tâches graphiques ou les jeux, une carte graphique dédiée peut être nécessaire.
- Système d'exploitation : Windows 10, macOS ou une distribution Linux récente.
- Connectivité : Port Ethernet pour la connexion réseau filaire et au moins deux ports USB pour les périphériques.
- Affichage : Un écran d'au moins 19 pouces de diagonale et une résolution de 1366x768 pixels ou plus.
- Lecteur optique : Un lecteur/graveur de DVD est facultatif, car les supports physiques sont de moins en moins utilisés.
- **Ordinateur portable**
 - Processeur (CPU) : Processeur dual-core ou quad-core, fréquence d'horloge d'au moins 1,6 GHz.
 - Mémoire vive (RAM) : 4 Go de RAM ou plus. Pour de meilleures performances multitâches, 8 Go ou plus sont recommandés.
 - Stockage : Disque dur de 500 Go ou plus, ou un disque SSD d'au moins 128 Go.
 - Écran : Un écran de 13 pouces ou plus avec une résolution de 1366x768 pixels ou supérieure.
 - Batterie : Une batterie offrant une autonomie d'au moins 4 heures pour une utilisation mobile.
 - Connectivité : Wi-Fi intégré, au moins deux ports USB, un port HDMI ou DisplayPort pour connecter des écrans externes.
 - Poids : Selon l'utilisation prévue, un poids léger (ultrabook) ou un poids plus élevé pour des performances supérieures (ordinateur portable de jeu, station de travail).
 - Système d'exploitation : La plupart des ordinateurs portables sont livrés avec un système d'exploitation préinstallé, généralement Windows, macOS ou Chrome OS.
- **Photocopieur couleur**
 - Type : Laser multifonction A3, A4
 - Impression couleur : Oui
 - Système d'exploitation supportés : Windows, MacOS, Linux
 - Ecran : Ecran tactile couleur de 12.7 cm
 - Capacité de support standard : 1200 Feuilles
 - Type de support : Transparents, enveloppes, papier uni, étiquettes, papier recyclé, papier couché, papier, papier calque, papier lourd, papier fin, papier perforé, papier coloré
 - Fonctions : Numérisation vers e-mail, numérisation vers réseau, Data Security, numérisé vers le Cloud, numérisation vers FTP, numérisation vers SMB, Push Scan, Pull Scan, scan vers hôte USB, numérisation vers appareil mobile
- **Imprimante**
 - Type : Imprimante multifonction LaserJet color

- Mémoire : Mémoire DDR de 256Mo, mémoire flash de 256Mo
- Ecran : Ecran tactile couleur 2.7 pouce
- Fonctionnalité réseau : Oui, via Ethernet 10/100/1000
- **Tablette durcie**
 - Taille d'écran : LCD 10,1"
 - Résolution : 800 x 1280
 - Wi-Fi, Bluetooth
 - Emplacement pour la carte SIM
 - Mémoire RAM : 4 Go minimum
 - Mémoire ROM : 64 Go minimum
 - Système d'exploitation : Windows 11
- **Smart Feature phone**
 - Système d'exploitation : KaiOS
 - Ecran : 32 pouces
 - Carte Sim, réseau 2G,3G,4G
 - Wi-Fi, Bluetooth
 - Mémoire extensible par microSD

3.2.1.2.2. Recommandations pour les configurations matérielles en fonction de l'usage

Il est important de choisir la configuration matérielle appropriée en fonction de l'usage prévu. Le tableau ci-dessous présente des recommandations pour différentes catégories d'usage, allant des tâches de bureau basiques à des besoins plus exigeants tels que le développement logiciel et la création de contenu multimédia. Un choix judicieux du système d'exploitation, de processeur, de RAM, de GPU et de stockage est crucial pour garantir des performances optimales et une expérience utilisateur fluide.

Tableau 12: Configurations matérielles en fonction de l'usage

	Usage de Bureau Basique	Navigation Web et Messagerie Électronique	Multimédia	Travail Professionnel (Développement Logiciel)	Création de Contenu (Montage Vidéo 4K, Rendu 3D)
Système d'Exploitation	Windows 10 ou Windows 11 ou macOS	Windows 10 ou Windows 11, macOS ou une distribution Linux légère	Windows 10 ou Windows 11 ou macOS	Windows 10 Pro ou Windows 11 Pro, macOS ou un système d'exploitation préféré pour le développement	Windows 10 Pro ou Windows 11 Pro ou macOS

Processeur	Processeur double cœur (par exemple, Intel Core i3 ou équivalent)	Processeur double cœur (par exemple, Intel Celeron ou AMD A4)	Processeur quadricœur (par exemple, Intel Core i5 ou AMD Ryzen 5)	Processeur quadricœur ou supérieur (par exemple, Intel Core i7 ou AMD Ryzen 7)	Processeur multi-cœurs haute performance (par exemple, Intel Core i9 ou AMD Ryzen 9)
RAM	4 Go ou plus	4 Go ou plus	8 Go ou plus	16 Go ou plus	32 Go ou plus
GPU	-	-	Graphiques intégrés ou GPU dédié d'entrée de gamme	GPU dédié avec au moins 2 Go de VRAM	GPU dédié haut de gamme avec une VRAM significative
Stockage	SSD ou HDD de 128 Go	SSD ou HDD de 128 Go	SSD ou HDD de 256 Go	SSD de 512 Go ou plus	SSD de 1 To ou plus

3.2.2. Gestion de l'alimentation électrique

3.2.2.1. Alimentation

Une alimentation électrique fiable est nécessaire pour éviter les interruptions de service et les pertes de données causées par des pannes de courant. Ces recommandations sont conçues pour aider les organisations à se protéger contre les pannes de courant et à maintenir leurs opérations en cas de panne.

Tableau 13 : Les types d'alimentation électrique

Recommandation	Description
Onduleurs (UPS)	Les onduleurs sont utilisés pour fournir une alimentation de secours en cas de coupure de courant. Ils permettent aux équipements de continuer à fonctionner pendant une durée déterminée, ce qui offre suffisamment de temps pour effectuer une sauvegarde des

	travaux en cours et éviter les pertes de données
Alimentation redondante	Pour les systèmes critiques, il est recommandé d'utiliser une alimentation redondante. Cela signifie que le serveur ou l'équipement dispose de deux alimentations physiques, pour éviter l'interruption de service dans le cas d'une panne
Gestion à distance de l'alimentation	Certains serveurs et équipements disposent de fonctionnalités de gestion à distance de l'alimentation qui permettent aux administrateurs de surveiller l'état des UPS et de recevoir des alertes en cas de problème.
Conformité aux Normes	S'assurer que toutes les installations électriques et les équipements respectent les normes de sécurité électrique en vigueur
Plan de continuité d'activité	Pour les institutions critiques, telles que les hôpitaux ou les centres de données, il est important d'avoir un plan de continuité d'activité en place en cas de panne électrique prolongée. Dans ce cas, ce PCA doit inclure des mesures pour maintenir les systèmes informatiques et de communication opérationnels

3.2.2.2. Groupes électrogènes

Les groupes électrogènes sont des dispositifs autonomes capables de produire de l'électricité. Ils sont utilisés pour pallier une éventuelle coupure d'alimentation électrique.

Ils sont habituellement installés à l'extérieur des locaux avec des couvertures antibruit ou dans des conteneurs.

3.2.2.3. Les kits solaires

Les kits solaires sont indiqués dans les zones rurales qui ne sont pas desservies par le réseau national de distribution de l'électricité.

Ils sont généralement constitués de :

- Panneaux solaires monocristallins
- Batteries pour le stockage de l'électricité
- Régulateur de tension

- Câbles régulateurs-batteries et panneaux solaires-régulateurs

La puissance des panneaux solaires et de la batterie dépendra du nombre d'équipement.

3.2.3. Salle de communication

Les institutions devraient disposer de salles de communication dans leurs locaux qui doit se conformer aux exigences minimales suivantes :

- **Exigences générales pour la conception d'une salle de communication :**

Les considérations générales suivantes pour la conception d'une salle de communication permettent une utilisation fonctionnelle de la salle, ainsi que la flexibilité dans le montage de l'équipement.

- Seuls les équipements pertinents pour la salle de communication doivent être présents dans la salle
- La hauteur du plafond doit être d'au moins 2 400 mm sans aucune obstruction. Par conséquent, un minimum de 3 000 mm est recommandé pour permettre le confinement thermique
- Le confinement thermique doit également avoir un dégagement minimum de 200 mm par rapport au plafond fini
- Le revêtement de sol (solide, carrelage) doit être conçu pour supporter les charges de sol actuelles et futures prévues
- Les portes d'accès doivent mesurer au minimum 900 mm de largeur et 2 000 mm de hauteur. De plus, la porte doit s'ouvrir vers l'extérieur. Si de gros équipements sont prévus, il est recommandé d'installer une double porte de 1 800 mm de large et 2 300 mm de haut
- Aucune fenêtre externe n'est recommandée
- Il est recommandé d'utiliser un revêtement de contreplaqué peint ignifuge de 19 mm pour couvrir au moins un mur de la salle de communication
- La protection incendie doit être conforme au plan du bâtiment principal
- **Exigences mécaniques et électriques :**
 - L'éclairage doit être d'au moins 500 lux horizontal et de 200 lux vertical
 - Un minimum de 2 prises de courant dédiées non commutées sur un circuit dédié. De plus, elles doivent être séparées des autres prises de courant du bâtiment
 - Une prise de courant dédiée pour les agents d'entretien doit être installée. Pour cette raison, évitez d'utiliser les prises de courant des armoires
 - La température doit être comprise entre 18 et 27 degrés Celsius (64-81°F)
 - Le point de rosée minimum doit être de 5,5 degrés Celsius (42°F)
 - Le point de rosée maximum doit être de 15 degrés Celsius (59°F).
 - L'humidité relative maximale doit être de 60 %.
 - La température et l'humidité doivent être conformes aux normes de classe B de l'ASHRAE
- **Considérations générales pour la conception d'une salle de communication :**

- La salle de communication doit être uniquement dédiée aux équipements pour le réseau
- La salle de communication doit être une zone d'accès restreinte par code/clé ou contrôle d'accès
- Le système de contrôle d'accès doit permettre d'enregistrer tous les accès à la salle de communication
- Lorsque vous travaillez dans la pièce, la porte doit être laissée ouverte en raison de la présence d'air refroidi recirculé.

3.2.4. Installation et configuration du réseau

Ce paragraphe va aborder les procédures d'installation et de configuration du réseau :

- **Équipement réseau :**
 - Installez les routeurs, les commutateurs, les points d'accès Wi-Fi et autres équipements nécessaires selon le schéma physique de votre réseau
 - Assurez-vous que les équipements sont installés dans des endroits accessibles pour la gestion et la maintenance
 - Configurez les équipements en suivant les meilleures pratiques et les spécifications de sécurité
- **Câblage réseau**
 - Installez le câblage réseau, qu'il s'agisse de câbles Ethernet, de fibres optiques ou de câbles coaxiaux, en suivant les normes appropriées
 - Utilisez des chemins de câbles et des conduits pour maintenir le câblage organisé et protégé contre les dommages
 - Évitez les interférences électromagnétiques en séparant les câbles de données des câbles d'alimentation
- **Sécurité physique**
 - Installez des systèmes de sécurité physique pour protéger les équipements dans la salle de communication, comme des caméras de sécurité et des systèmes de contrôle d'accès
 - Configurez les équipements réseau avec des paramètres de sécurité appropriés, tels que des pare-feux et des protocoles d'authentification

3.3. Gestion de réseaux

La gestion de réseau est un aspect essentiel de la maintenance d'une infrastructure réseau sécurisée et efficace

3.3.1. Performance du Réseau

Les recommandations suivantes permettront d'améliorer la disponibilité et les performances du réseau pour garantir une disponibilité accrue du réseau de communication :

Tableau 14 : Recommandations pour la performance du réseau

Concept	Description
Redondance	Mise en place de la redondance dans la conception du réseau pour garantir qu'en cas de défaillance d'un composant, il existe une solution de secours en place.
Équilibrage de Charge	Répartition du trafic réseau sur plusieurs serveurs ou trajets pour optimiser l'utilisation des ressources et éviter la surcharge d'un composant unique.
Temps de Réponse des Applications	Surveillance et optimisation des performances des applications pour garantir qu'elles réagissent rapidement aux demandes des utilisateurs.
Qualité de Service (QoS)	Priorisation et gestion du trafic réseau pour répondre aux exigences spécifiques de performance et de latence pour les applications critiques.

3.3.2. Maintenance du Réseau

Ces recommandations sont conçues pour aider les organisations à protéger leur réseau et à garantir qu'il puisse continuer à fonctionner en cas de problème.

Tableau 15 : Recommandations pour la maintenance du réseau

Recommandation	Description
Plan de Maintenance du Réseau	Élaboration d'un plan complet de maintenance continue du réseau.
Plan de Reprise d'Urgence	Préparation aux événements imprévus ou aux catastrophes susceptibles de perturber les opérations du réseau
Plan de Continuité d'Activité	Garantie que le réseau peut continuer à prendre en charge les fonctions essentielles pendant et après une catastrophe. Cela inclut les systèmes de sauvegarde, le stockage de données hors site et les capacités de basculement.

3.3.3. Référencement du câblage réseau

Ces recommandations sont conçues pour aider les organisations à identifier et à organiser correctement leurs câbles :

- Étiquetez chaque câble et chaque port sur les équipements réseau pour une identification facile.
- Utilisez des étiquettes claires et durables pour éviter les erreurs de connexion et faciliter la maintenance future.
- Organisez les câbles de manière soignée pour éviter les enchevêtrements et faciliter le dépannage.
- Testez tous les câbles pour vérifier la connectivité et la qualité du signal.
- Vérifiez les configurations des équipements réseau pour vous assurer qu'ils fonctionnent conformément aux spécifications.
- Toute structure de réseau devrait tenir compte des dernières normes de câblage.

3.3.4. Sécurité du réseau

Ces recommandations sont conçues pour aider les organisations à se protéger contre les menaces et les attaques :

- Mettez en place des mesures de sécurité robustes pour protéger le réseau et les données des utilisateurs :
- Utilisez des pare-feux pour contrôler le trafic entrant et sortant.
- Utilisez des systèmes de détection et de prévention des intrusions (IDPS) pour identifier et répondre aux menaces potentielles.
- Configurez des réseaux privés virtuels (VPN) pour un accès distant sécurisé.
- Mettez en place des mécanismes d'authentification solides, tels que l'authentification multi-facteurs (AMF).
- Mettez en place des réseaux « invité », uniquement pour les invités ou les personnes n'appartenant pas à votre administration
- Mettez régulièrement à jour et corrigez les dispositifs réseau pour résoudre les vulnérabilités de sécurité.
- Sensibilisez les utilisateurs aux meilleures pratiques de sécurité

3.4. Réseau minimal des administrations

3.4.1. Définition

Un réseau minimal pour une administration désigne une infrastructure informatique essentielle permettant la connectivité de base adaptée aux besoins spécifiques de chaque administration. Cela englobe plusieurs composants et services qui permettent aux membres de l'administration de communiquer, de partager des informations et d'accéder aux ressources numériques facilement. Il englobe également les équipements utilisateurs finaux leur permettant de fournir des services au public.

3.4.2. Objectif

L'objectif principal d'un réseau minimal pour une administration est de fournir une infrastructure informatique essentielle qui répond aux besoins spécifiques de l'administration en termes de connectivité. Cela vise à faciliter la communication entre les membres de l'administration, à permettre le partage d'informations et à assurer un accès facile aux ressources numériques. Dans un contexte de dépendance croissante aux technologies de l'information, la mise en place d'une infrastructure réseau solide est cruciale pour garantir le bon fonctionnement de l'administration. En optimisant la gestion des données et en rationalisant les opérations, la transition vers un réseau informatique efficace contribue à améliorer la communication interne, à renforcer la collaboration et à soutenir les activités administratives de manière plus efficace.

3.4.3. Existence sur le terrain

Une étude a d'abord été faite pour avoir une idée des réalités sur le terrain. Ces études ont été réalisées suivant les critères suivants :

- L'accès à l'électricité : il s'est agi d'analyser l'accès à l'électricité des administrations et de déterminer leurs moyens d'accès
- L'accès à internet : Il s'est agi de déterminer l'accès à internet des administrations avec les différents FAI utilisés
- Le nombre de locaux : Voir, sur le terrain de combien de locaux disposent les administrations.

3.4.3.1. Accès à électricité

La figure suivante montre l'accès à électricité dans les administrations. On remarque entre-autre que :

- Une majorité d'administration a accès à une source d'électricité (1997 contre 415)
- La position géographique de l'administration ne semble pas avoir d'incidence sur l'accès à l'électricité.

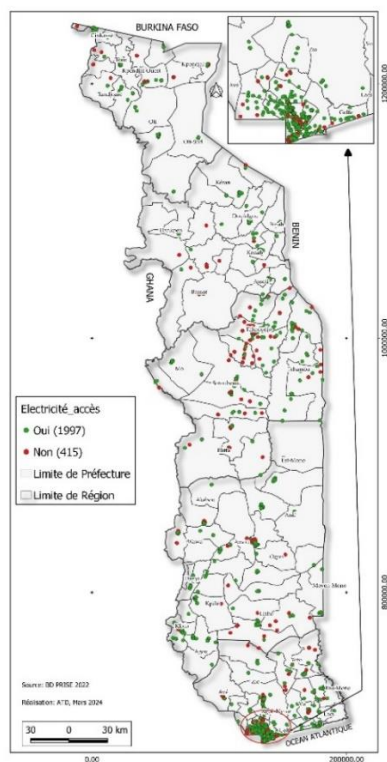


Figure 5 : Accès à internet dans les administrations

Les administrations ayant accès à l'électricité utilisent plusieurs sources pour s'alimenter, comme le montre la figure suivante :

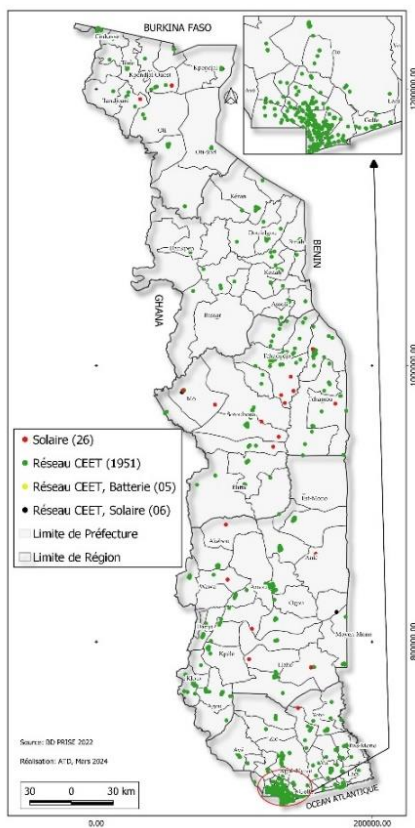


Figure 6 : Sources d'alimentation électrique

On remarque toutefois que :

- La CEET reste le fournisseur d'énergie le plus répandu pour les administrations
- En complément de la CEET, un petit nombre d'administrations utilisent des batteries ou l'énergie solaire pour assurer leur alimentation en énergie
- Quelques administrations (26) utilisent uniquement l'énergie solaire pour s'alimenter en énergie.

3.4.3.2. Accès à internet

La figure qui suit montre l'accès internet des administrations

On remarque que :

- Assez peu d'administrations ont accès à internet (31%)
- L'accès à internet n'est généralement pas fonction de la localité dans laquelle se situe l'administration

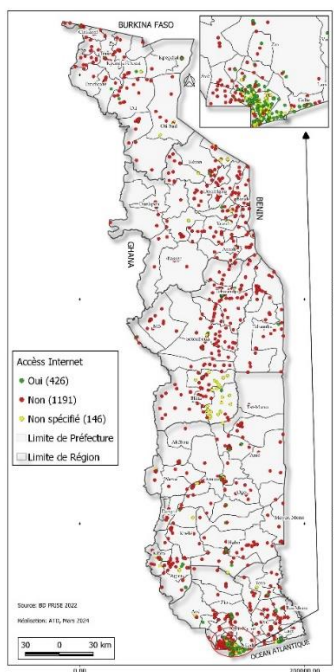


Figure 7 : Accès internet dans les administrations

3.4.3.3. Les locaux

La figure suivante montre une classification des administrations en fonction du nombre de local dont ils disposent.

On remarque ainsi que :

- Plusieurs administrations déclarent ne pas avoir de locaux
- La plupart des administrations ont entre 0 et 5 locaux (2122)

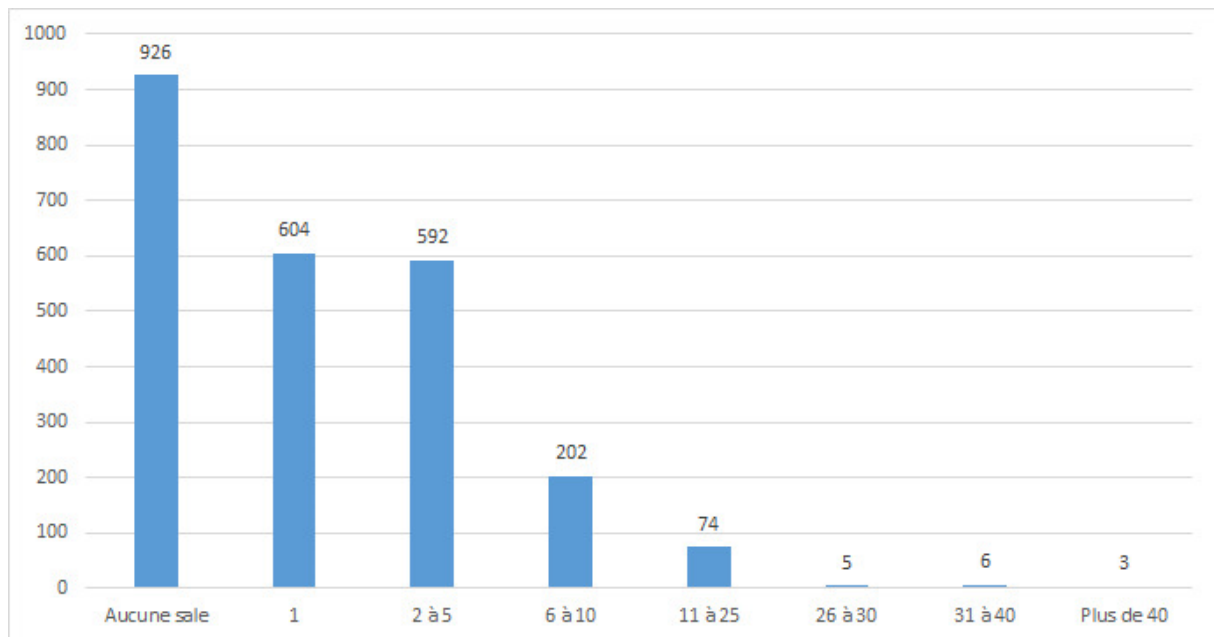


Figure 8 : Nombre de locaux des administrations

3.4.4. Classification des administrations

Plusieurs critères ont été établis pour la classification des administrations, dans l'objectif d'évaluer de manière précise leurs besoins. Cette démarche permet d'assurer que les éléments proposés sont parfaitement alignés avec les exigences et les réalités spécifiques de chaque administration.

Les critères de classification sont les suivants :

- Couverture électrique
- Couverture internet
- Taille des locaux

Ces critères ont donné le regroupement suivant :

- **Catégorie A : Administrations à haute capacité**
 - Électricité : Accès fiable à l'électricité avec peu ou pas de coupures.
 - Couverture réseau : Accès à la fibre optique ou à des connexions haut débit stables (4G au minimum).
 - Local : Locaux spacieux pouvant accueillir des équipements informatiques conséquents et des espaces de travail pour tous les employés.
- **Catégorie B : Administrations à capacité moyenne**
 - Électricité : Accès relativement fiable à l'électricité avec des coupures occasionnelles.
 - Couverture réseau : Couverture réseau principalement 3G ou 4G avec une bonne fiabilité.
 - Local : Locaux de taille moyenne capables d'accueillir une infrastructure informatique adaptée et des espaces de travail suffisants pour le personnel.
- **Catégorie C : Administrations à Faible Capacité**

- Électricité : Accès limité à l'électricité avec des coupures fréquentes.
- Couverture réseau : Couverture réseau faible, principalement 3G ou moins, avec une connectivité inégale.
- Local : Locaux petits à modérés, avec des limitations d'espace pour l'équipement et le personnel.
- **Catégorie D : Administrations en Milieu Extrêmement Contraint**
 - Électricité : Accès très limité ou inexistant à l'électricité, dépendance à des solutions alternatives comme les générateurs ou les panneaux solaires.
 - Couverture réseau : Faible couverture réseau
 - Local : Locaux inexistant ou souvent très restreints, nécessitant une optimisation de l'espace pour l'équipement et le personnel.

Les deux premières classifications sont celles qu'on pourrait retrouver dans les zones urbaines ou semi-urbaines alors que les deux dernières pourraient être retrouver dans les zones rurales. Cette classification n'est pas statique. Les efforts d'amélioration des infrastructures et des services peuvent permettre à une administration de passer d'une catégorie à une autre au fil du temps.

A l'intérieur de ces catégories, un autre dimensionnement est fait en fonction du nombre de personnel pour estimer la quantité des équipements utilisateurs finaux. Ce dimensionnement donne les résultats suivants :

- **Catégorie A**

Les administrations de catégorie A sont les mieux lotis. Elles disposent de locaux spacieux pour accueillir le personnel. On a donc :

- Les administrations ayant entre 0-10 personnes ;
- Les administrations ayant entre 11-50 personnes ;
- Les administrations ayant entre 51-90 personnes et
- Les administrations ayant plus de 90 personnes

- **Catégorie B**

La taille des locaux des administrations de catégorie B est moyenne. En termes de personnel, on a ainsi :

- Les administrations ayant entre 0-10 personnes ;
- Les administrations ayant entre 11-50 personnes ;
- Les administrations ayant entre 51-90 personnes

- **Catégorie C**

Les locaux des administrations de type C sont petites, avec des limitations d'espace pour le personnel et les équipements. Le dimensionnement en fonction du nombre d'utilisateur est le suivant :

- Les administrations ayant entre 0-10 personnes ;
- Les administrations ayant entre 11-50 personnes ;

- Catégorie D

Les administrations de type D ont de réels problèmes de locaux. Le dimensionnement en fonction du nombre d'utilisateurs se fera donc en considérant un nombre de personnel compris entre 0 et 10.

3.4.5. Architecture réseau minimal des administrations

L'architecture minimal du réseau des administrations dépend selon le type d'administration. Tandis que les différences sont peu marquées entre les catégories A et B, principalement en termes d'accès à Internet, les administrations de type C ou D pourraient présenter une organisation distincte de leurs composants physiques. Cette configuration est occasionnée par leurs couverture en électricité et internet difficile ou inexistante ainsi que par le manque de local.

3.4.5.1.1. Administration de type A (administrations à haute capacité)

Voici ci-dessous le schéma de l'architecture réseau physique minimal des administrations de Type A :

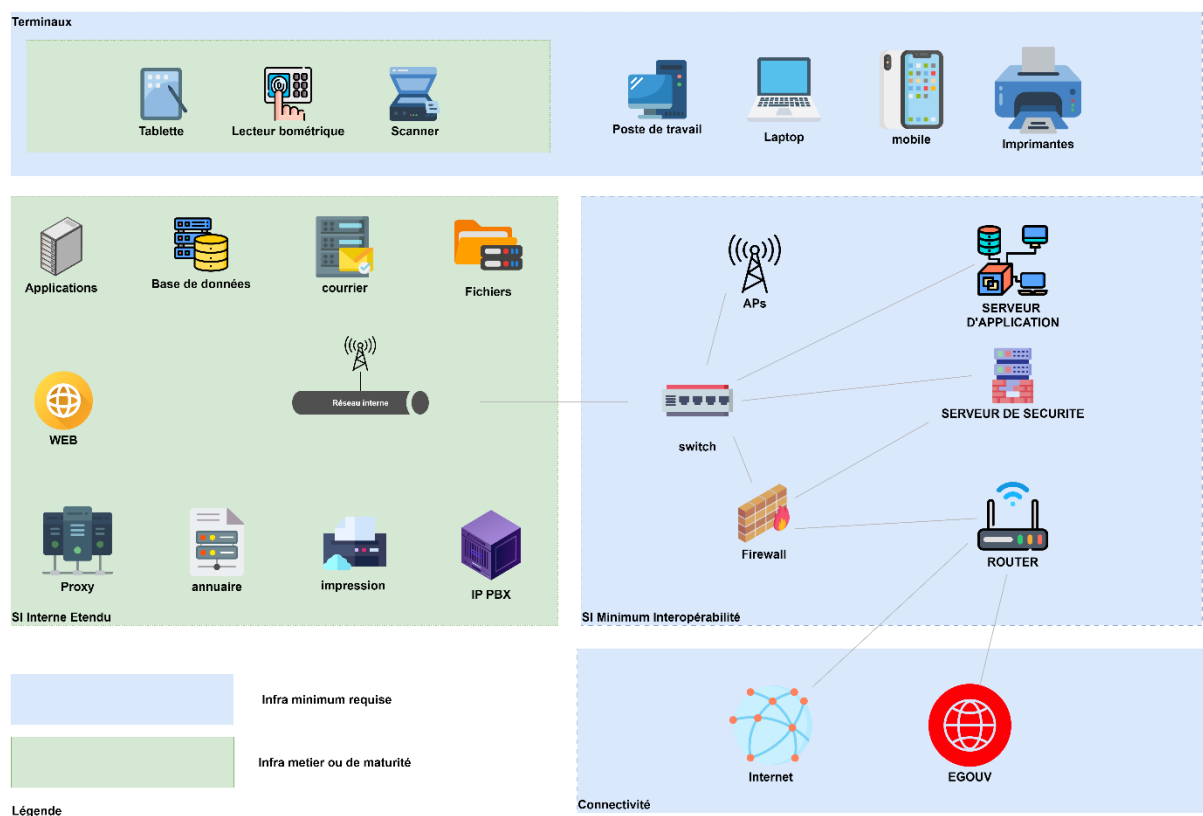


Figure 9 : Architecture physique minimale pour une administration de type "A"

Cette structure repose sur l'accès au réseau E-Gouv ou sur une vaste couverture en fibre optique fournie par l'un des opérateurs mentionnés précédemment (Togocom, GVA), permettant ainsi aux administrations d'obtenir la connectivité requise.

3.4.5.1.1.1. Dimensionnement du réseau en fonction des utilisateurs

Il est important de prévoir un nombre suffisant de composants réseaux en fonction du nombre d'utilisateurs sur le site, ceci pour s'assurer que tous les utilisateurs aient un accès internet adéquat pour leur activité.

Ce tableau propose ce dimensionnement en fonction de la taille des administrations :

Tableau 16 : Dimensionnement du réseau des administrations de type "A"

Nombre d'employés	Types d'activités	Besoins en fonction du nombre d'utilisateur
1-10 personnes	Idéal pour les petites administrations	1 Routeur pour la connectivité Internet sécurisée. 1 Firewall pour assurer la sécurité 1 Serveur de sécurité 1 Serveur d'application 1 Switch Réseau pour connecter tous les équipements au rése au local. 1 ou 2 Points d'Accès Wi-Fi pour couvrir l'ensemble des espaces de travail avec un signal Wi-Fi de qualité. 1 Rack serveur 24U
11-50 personnes	Idéal pour les moyennes administrations	1 à 2 Routeurs pour la connectivité Internet sécurisée. 1 Firewall pour assurer la sécurité 1 Serveur de sécurité 1 Serveur d'application 2 à 4 Switch Réseau pour connecter tous les équipements au réseau local. 3 à 5 Points d'Accès Wi-Fi pour couvrir l'ensemble des espaces de travail avec un signal Wi-Fi de qualité. 1 Rack serveur 24U
50-90 personnes	Idéal pour les grandes administrations	2-3 Routeurs pour la connectivité Internet sécurisée. 1 Firewall pour assurer la sécurité 1 Serveur de sécurité 1 Serveur d'application 4 à 6 Switch Réseau pour connecter tous les équipements au réseau local. 5 à 10 Points d'Accès Wi-Fi pour couvrir l'ensemble des espaces de travail avec un signal Wi-Fi de qualité. 1 Rack serveur 24U

90+ personnes	Idéal pour les très grandes administrations	+ de 3 Routeurs pour la connectivité Internet sécurisée. 1 Firewall pour assurer la sécurité 1 Serveur de sécurité 1 Serveur d'application 4 à 8 Switch Réseau pour connecter tous les équipements au réseau local. 10 à 12 Points d'Accès Wi-Fi pour couvrir l'ensemble des espaces de travail avec un signal Wi-Fi de qualité. 1 Rack serveur 24U
----------------------	---	---

3.4.5.1.2. Equipements des utilisateurs finaux

Les équipements utilisateurs finaux prévus pour les administrations de catégories A sont les suivantes :

- Des ordinateurs portables personnels (PC)
- Des ordinateurs desktop
- Des imprimantes
- Des copieurs et
- Des onduleurs

Le tableau suivant présente la quantité minimale de ces équipements en fonction de la taille de l'administration.

Tableau 17 : Dimensionnement des équipements utilisateur final des administrations de type "A"

Taille	PC	Ordinateur desktop	Imprimante	Copieur	Onduleur
0-10	2	2	1	1	1
11-50	10	10	2	1	2
51-90	20	40	5	2	4
+90	50	30	10	4	7

3.4.5.1.2. Administration de type B

Comme dit précédemment, il n'y a pas une grande différence entre l'architecture physique d'une administration de type B et celle d'une administration de type A.

L'une des grandes différences réside dans l'accès à internet. En effet, alors que l'administration de type A se trouve dans une zone disposant d'une bonne couverture filaire, l'administration de

type B se trouve dans une zone n'ayant accès qu'à de la couverture 4G ou 3G. Les offres de connexion filaires sont donc à exclure.

Toutefois, les offres d'internet par ondes hertziennes de TéoIs ou Café peuvent être étudiées. De plus, des outils comme *la Box Harvilon 4G* ou la *Box Nokia 4G* de togo.com - permettant d'avoir internet avec une carte SIM - disposant de port RJ45 peuvent également être indiqués.

3.4.5.1.2.1. Dimensionnement du réseau en fonction des utilisateurs

Ce dimensionnement en fonction du nombre d'utilisateurs donne les résultats suivants :

Tableau 18 : Dimensionnement du réseau des administrations de type "B"

Nombre d'employés	Types d'activités	Besoins en fonction du nombre d'utilisateur
1-10 personnes	Idéal pour les petites administrations	1 modem pour la connectivité Internet sécurisée. 1 Firewall pour assurer la sécurité 1 Serveur de sécurité 1 Serveur d'application 1 Switch Réseau pour connecter tous les équipements au réseau local. 1 ou 2 Points d'Accès Wi-Fi pour couvrir l'ensemble des espaces de travail avec un signal Wi-Fi de qualité. 1 Rack serveur 24U
11-50 personnes	Idéal pour les moyennes administrations	1 à 3 modems pour la connectivité Internet sécurisée. 1 Firewall pour assurer la sécurité 1 Serveur de sécurité 1 Serveur d'application 2 à 4 Switch Réseau pour connecter tous les équipements au réseau local. 3 ou 5 Points d'Accès Wi-Fi pour couvrir l'ensemble des espaces de travail avec un signal Wi-Fi de qualité. 1 Rack serveur 24U
50-90 personnes	Idéal pour les grandes administrations	4 à 8 modems pour la connectivité Internet sécurisée. 1 Firewall pour assurer la sécurité 1 Serveur de sécurité 1 Serveur d'application 4 à 8 Switch Réseau pour connecter tous les équipements au réseau local.

		5 ou 10 Points d'Accès Wi-Fi : pour couvrir l'ensemble des espaces de travail avec un signal Wi-Fi de qualité. 1 Rack serveur 24U
--	--	--

3.4.5.1.2.2. Equipement des utilisateurs finaux

Les équipements utilisateurs finaux prévus pour les administrations de catégories B sont les suivantes :

- Des ordinateurs portables personnels (PC)
- Des ordinateurs desktop
- Des imprimantes
- Des copieurs et
- Des onduleurs

Le tableau suivant présente la quantité minimale de ces équipements en fonction de la taille de l'administration.

Tableau 19 : Dimensionnement des équipements utilisateurs final des administrations de type « B »

Taille	PC	Ordinateur desktop	Imprimante	Copieur	Onduleur
0-10	2	1	1	1	1
11-50	6	8	2	1	2
51-90	30	20	3	2	4

3.4.5.1.3. Administration de type C

Les administrations de catégorie C se caractérisent par des capacités limitées, notamment l'absence de locaux adaptés pour accueillir une salle serveur. Face à cette contrainte, la solution serait un hébergement des équipements serveurs sur d'autres sites (Préfecture/Mairie...) situés à proximité, disposant de plus d'espace. Cette approche permettrait non seulement de pallier le manque d'infrastructure adéquate au sein des administrations de type C, mais également de garantir un accès sécurisé et efficace aux ressources informatiques nécessaires via un réseau privé virtuel (VPN).

En interne, la connexion internet peut être assurée par des périphériques basés sur la 4G ou la 3G proposés par Togocom et Moov. Un modem et/ou des points d'accès assurent la diffusion de la connexion internet à tout le personnel de l'administration.

L'architecture physique minimale est la suivante :

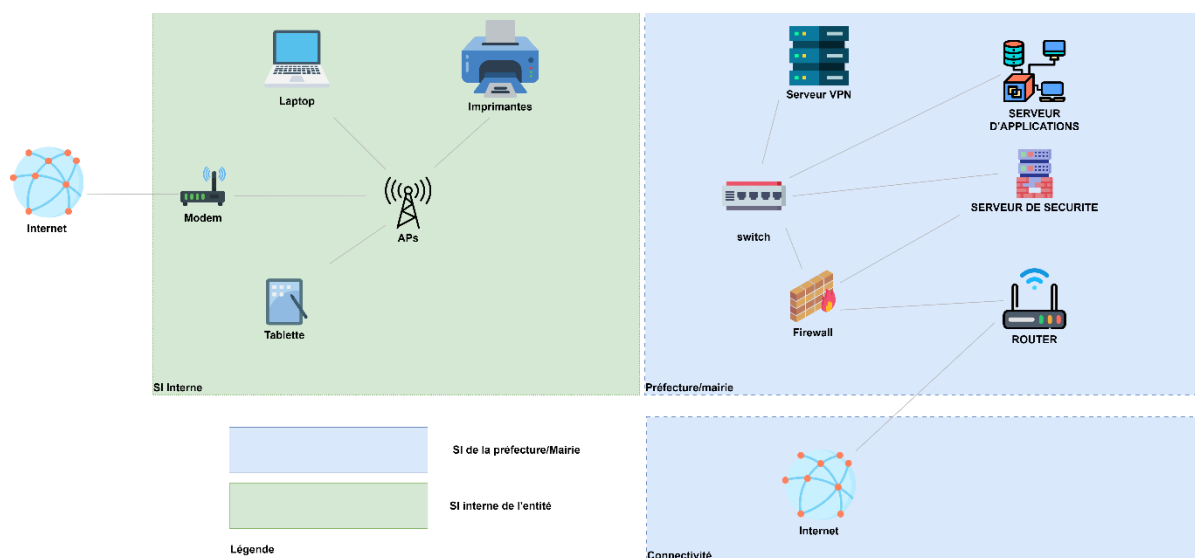


Figure 10 : Architecture physique minimale pour une administration de type "C"

3.4.5.1.3.1. Dimensionnement du réseau en fonction des utilisateurs

Comme dit plus haut, le réseau d'une administration de type C sera décomposé en deux parties :

- Une première partie dans un local administratif proche
- Une seconde partie dans les locaux de l'administration

La première partie reste la même pour les administrations de type A ou B en ce qui concerne les serveurs et équipements réseaux auxquels on ajoute un serveur VPN pour permettre une communication entre les deux parties du réseau.

Le dimensionnement de la seconde partie est la suivante :

Tableau 20 : Dimensionnement du réseau des administrations de type "C"

Nombre d'employés	Types d'activités	Besoins en fonction du nombre d'utilisateur
1-10 personnes	Idéal pour les petites administrations	1 modem pour la connectivité Internet sécurisée. 1 ou 2 Points d'Accès Wi-Fi pour couvrir l'ensemble des espaces de travail avec un signal Wi-Fi de qualité.
11-50 personnes	Idéal pour les moyennes administrations	1 à 2 modems pour la connectivité Internet sécurisée. 3 ou 5 Points d'Accès Wi-Fi pour couvrir l'ensemble des espaces de travail avec un signal Wi-Fi de qualité.

3.4.5.1.3.2. Equipement des utilisateurs finaux

Les équipements utilisateurs finaux prévus pour les administrations de catégories C sont les suivantes :

- Des ordinateurs portables personnels (PC)
- Des tablettes renforcées
- Des copieurs et
- Des onduleurs

Ces équipements doivent avoir un indice de protection de 58 (IP 58) pour être protégés contre les infiltrations de poussière limitée et l'immersion à long terme.

Le tableau suivant présente la quantité minimale de ces équipements en fonction de la taille de l'administration.

Tableau 21 : : Dimensionnement des équipements utilisateurs final des administrations de type "C"

Taille	PC	Tablette renforcée	Imprimante	Onduleur
0-10	2	1	1	1
11-50	6	8	2	2

3.4.5.1.3.3. Gestion de l'électricité

Étant donné que les administrations de catégorie C sont fréquemment confrontées à des fluctuations et des coupures d'électricité, il est primordial de prévoir l'installation d'un groupe électrogène. Cette mesure préventive vise à pallier les insuffisances du réseau électrique et à garantir une alimentation continue et stable, essentielle au bon fonctionnement des équipements informatiques et à la continuité des activités administratives.

Pour estimer la puissance de ce groupe électrogène, il faut pouvoir estimer la consommation en énergie des différents équipements. Les estimations sont les suivantes :

Tableau 22 : Estimation de la consommation des équipements

Matériel	Consommation
Tablette renforcée	30 W
PC	200 W
Copieur	1500 W
Imprimante	600 W

Ces estimations nous donnent la puissance suivante des groupes électrogènes à prévoir (avec une marge de 20%)

Tableau 23 : Estimation de la puissance des groupes électrogènes

Taille	Puissance
0-10 personnes	2 kVA
11-50 personnes	5 kVA

3.4.5.1.4. Administration de type D

Les administrations de type D sont généralement des annexes situées dans des zones reculées pour desservir les populations. Elles n'ont généralement qu'un seul local. Il peut s'agir d'annexe de centre d'état civil, d'agences togolaises de presse... avec un nombre de personnel réduit (Voir le tableau suivant).

Tableau 24 : Liste des administrations n'ayant qu'un seul personnel

ENTITE	NOMBRE	PERSONNEL
CENTRE D ETAT CIVIL	563	1
IPSL	15	1
ATOP	12	1
ACTION SOCIALE	11	1
TRESORERIE	8	1
ANADEB	3	1
ANVT	2	1
MAIRIE ANNEXE	2	1
TRAVAUX PUBLICS	2	1
ANPGF	1	1
BUREAU DE TOPOGRAPHIE	1	1
CAGIA	1	1
CONTROLE VETERINAIRE	1	1
CULTURE ET TOURISME	1	1
DIRECTION SECTEUR POLICE	1	1
DPERF	1	1
HYDRAULIQUE VILLAGEOISE	1	1
IGSS	1	1

ITRA	1	1
NUNYA LAB	1	1
POSTE VETERINAIRE	1	1
TDE	1	1

Elles dépendent généralement d'une agence principale en catégorie C ou B, et aident généralement à la délivrance de pièces administratifs ou à l'enregistrement d'informations. Elles n'ont donc pas besoin d'avoir des équipements logés dans une préfecture ou une mairie.

3.4.5.1.4.1. Accès à internet

En ce qui concerne l'accès à internet des administrations de Type D, un modem (type *MIFI ALCATEL 4G de Togocom* ou *MoovPocket4+*) peut être indiqué.

3.4.5.1.4.2. Equipement des utilisateurs finaux

Les équipements utilisateurs finaux pour les administrations de catégories D sont les suivantes :

- Un kit solaire
- Une imprimante
- Deux smart feature phone ou bien
- Une tablette renforcée ou bien
- Un kit mobile : Il s'apparente aux solutions d'enregistrement biométrique utilisées dans les campagnes de recensement. Il s'agit d'un « bureau portable » composé d'un ordinateur portable, d'un système d'alimentation avancée pouvant fonctionner toute une journée, d'un modem, de panneaux solaires ; le tout dans une valise résistante à la chaleur et à la poussière.



Figure 11 : Exemple de kit mobile

3.5. Sauvegarde du poste de travail

La sauvegarde des données est une mesure cruciale pour protéger les informations importantes contre la perte due à des pannes matérielles, des erreurs humaines, des logiciels malveillants, des catastrophes naturelles ou tout autre événement imprévu.

Il est essentiel d'établir un plan de sauvegarde régulier qui inclut la fréquence des sauvegardes, les données à sauvegarder et les méthodes de sauvegarde à utiliser (par exemple, sauvegardes sur site, sauvegardes hors site, sauvegardes dans le cloud).

Il est important de tester régulièrement le processus de récupération pour s'assurer que les données peuvent être restaurées avec succès en cas de besoin.

Les sauvegardes doivent être stockées de manière sécurisée pour éviter tout accès non autorisé. Les sauvegardes contenant des données sensibles doivent être chiffrées pour protéger leur confidentialité.

Automatisez le processus de sauvegarde pour éviter les oublis humains et garantir la cohérence des sauvegardes.

3.6. Gestion des Équipements Informatiques

Dans cette section, nous présenterons un ensemble de pratiques de sécurité informatique visant à garantir la protection de des actifs numériques.

3.6.1. Accès au Système (Connexion au Réseau Local - LAN)

- Établir une connexion réseau entre les appareils et l'infrastructure du réseau local (LAN).
- Utiliser des connexions filaires (Ethernet) ou sans fil (Wi-Fi) selon les besoins.
- Appliquer des protocoles de sécurité, tels que l'authentification et l'autorisation, pour gérer l'accès aux ressources réseau.

3.6.2. Gestion des Ordinateurs

- Encourager les utilisateurs à mettre fin à leurs sessions ou à se déconnecter de leurs ordinateurs lorsqu'ils s'éloignent.
- Si l'ordinateur est verrouillé, exiger un mot de passe pour le déverrouiller.
- Verrouiller les bureaux, les salles informatiques et les espaces de stockage en l'absence des utilisateurs.

3.6.3. En cas de Vol ou la Perte

- Signalez immédiatement le vol ou la perte de l'appareil à l'équipe de sécurité informatique et à la direction concernée de votre organisation.
- Effacer les Données à Distance si l'appareil contient des données sensibles, envisagez de l'effacer à distance pour éviter tout accès non autorisé. Certaines solutions de gestion à distance permettent cette fonctionnalité.

- Notifier les Autorités si le vol a été signalé aux autorités locales, coopérez avec elles et fournissez les informations nécessaires.

3.6.4. Appareils des utilisateurs

- Tous les appareils institutionnels utilisés par les employés doivent être étiquetés de manière distincte et enregistrés dans un système de gestion des actifs.
- L'étiquetage facilite l'identification, le suivi et la gestion des appareils au sein de l'organisation.
- Développez des procédures pour la retraite et la désactivation appropriées des appareils institutionnels en fin de vie.
- Assurez-vous que les données sont effacées de manière sécurisée avant de recycler ou de réaffecter les appareils
- Pour le transfert de données, utilisez uniquement des périphériques de stockage cryptés tels que des clés USB ou des disques durs externes approuvés par le département IT. Assurez-vous que les données sur ces appareils sont uniquement destinées à un stockage temporaire.
- Ne notez jamais aucun mot de passe sur un quelconque support

3.6.5. Règles d'entretien

- Évitez de placer les équipements informatiques à côté des climatiseurs ou de sources de chaleur excessive. L'humidité et la chaleur peuvent endommager les composants internes
- Choisissez des emplacements bien ventilés pour prolonger la durée de vie des équipements.
- Les utilisateurs ne doivent pas manger, boire ou fumer à proximité des équipements TIC. Les débris ou les liquides peuvent causer des défaillances
- Les bureaux équipés d'équipements informatique doivent être verrouillés lorsque les utilisateurs ne sont pas présents pour éviter le vol et les accès non autorisés.

3.6.6. Responsabilités

- Les utilisateurs sont responsables de la sécurité de leurs appareils et des données qu'ils contiennent. Cela inclut la création et la gestion de mots de passe forts, le respect des politiques de sécurité et la sensibilisation aux menaces de sécurité
- Le service informatique est responsable de la configuration, de la maintenance et de la gestion des appareils des utilisateurs. Cela inclut l'installation de logiciels, la résolution des problèmes techniques et la gestion des mises à jour de sécurité.

3.7. Maintenance du matériel

Ces recommandations sont conçues pour aider les organisations à mettre en place un programme de maintenance efficace :

Tableau 25 : Maintenance du matériel

Concept	Description
Plan de maintenance	Le plan de maintenance doit définir les tâches de maintenance qui doivent être effectuées, la fréquence à laquelle elles doivent être effectuées et les personnes responsables de leur exécution.
Documenter les activités de maintenance	Les activités de maintenance doivent être documentées pour faciliter le suivi et l'analyse
Gestion des actifs	La gestion des actifs est un processus qui consiste à suivre et à gérer les actifs d'une organisation. La maintenance matérielle doit être intégrée à la gestion des actifs pour garantir que les actifs sont correctement entretenus et que les coûts de maintenance sont optimisés.

4. Acquisition des matériels informatiques

4.1. Contexte

Les administrations publiques togolaises sont confrontées à des défis croissants en matière d'acquisition de matériels informatiques. Actuellement, chaque administration lance des appels d'offres de manière indépendante, entraînant une fragmentation des achats, des coûts élevés et une inefficacité globale dans le processus d'acquisition. Il serait bien d'avoir une plateforme permettant de centraliser et de suivre les achats

4.2. La marketplace

4.2.1. Définition

La proposition consiste à développer une Marketplace dédiée à l'acquisition des matériels informatiques pour les administrations publiques togolaises. Cette plateforme agira comme un espace centralisé où les fournisseurs agréés pourront proposer leurs produits, et les différentes entités gouvernementales pourront effectuer leurs achats de manière transparente et efficace

4.2.2. Objectifs

- Centralisation des Achats : La plateforme agira comme un point central pour la collecte des besoins en matériels informatiques de toutes les administrations, permettant une agrégation efficace des demandes ; mais aussi pour le suivi des différents appels d'offres.
- Transparence et Suivi : La plateforme offrira une visibilité complète sur les processus d'achat, depuis la soumission des offres jusqu'à la livraison, garantissant la transparence et facilitant le suivi des transactions.
- Évaluation des Fournisseurs : Intégration de mécanismes d'évaluation des fournisseurs par les utilisateurs finaux, permettant une sélection plus informée et la promotion de la qualité des services.
- Réduction des Coûts : La centralisation des achats permettra de négocier des tarifs préférentiels avec les fournisseurs, réduisant ainsi les coûts d'acquisition.

4.3. Avantages

- Efficacité dans la gestion des besoins : En centralisant les besoins, la plateforme permettra une gestion plus efficace des demandes, évitant les redondances, clarifiant les spécifications et améliorant la qualité des appels d'offres.
- Standardisation des processus : La transformation des besoins en appels d'offres standardisés facilitera la comparaison des offres, simplifiant ainsi le processus de sélection et garantissant une équité accrue.

- Optimisation des ressources : Les administrations pourront optimiser l'allocation de leurs ressources en collaborant sur des besoins similaires, évitant ainsi la duplication des efforts et maximisant l'efficacité des achats.
- Transparence et conformité : La plateforme favorisera la transparence tout au long du processus, assurant la conformité aux normes réglementaires et renforçant la confiance dans l'utilisation des fonds publics.

5. Gestion des données

La gestion des données est un processus complexe qui comprend un ensemble de tâches et de responsabilités visant à garantir la sécurité, l'intégrité et la disponibilité des données. Ces tâches et responsabilités comprennent la classification des données, le contrôle d'accès, le chiffrement, la sauvegarde et la restauration, la journalisation et la surveillance.

5.1. Catégories de données à protéger

Ces recommandations sont conçues pour aider les organisations à protéger leurs données sensibles et confidentielles, à garantir l'intégrité et la disponibilité des informations, tout en respectant les réglementations et en minimisant les risques :

5.1.1. Disponibilité des Données :

Les données doivent être accessibles lorsque nécessaire. Assurez-vous que les systèmes de stockage et les serveurs sont fiables et bien configurés pour garantir une disponibilité maximale.

5.1.2. Normalisation des Données Partagées :

Lorsque des données sont partagées entre plusieurs utilisateurs ou départements, assurez-vous qu'elles sont normalisées et structurées de manière cohérente pour éviter les confusions.

5.1.3. Identificateurs de Données :

Utilisez des identificateurs uniques pour les données afin de faciliter leur recherche, leur suivi et leur gestion.

5.1.4. Sauvegarde et Récupération des Données :

Mettez en place des procédures de sauvegarde régulières pour prévenir la perte de données en cas de défaillance matérielle.

Testez régulièrement les procédures de récupération pour vous assurer qu'elles fonctionnent correctement en cas de besoin.

5.1.5. Catégories de Données à Protéger :

Identifiez les catégories de données sensibles ou confidentielles qui nécessitent une protection particulière. Cela peut inclure des données personnelles, financières, médicales, etc.

5.1.6. Classification des Données :

Classez les données en fonction de leur sensibilité et de leur importance. Cela peut aider à déterminer les niveaux d'accès et de protection appropriés.

5.1.7. Politiques d'Accès aux Données :

Établissez des politiques de contrôle d'accès pour déterminer qui peut accéder à quelles données et à quelles fins. Suivez le principe du moindre privilège.

5.1.8. Chiffrement des Données :

Utilisez le chiffrement pour protéger les données sensibles lorsqu'elles sont stockées ou transitent sur le réseau.

5.1.9. Gestion du Cycle de Vie des Données :

Définissez des politiques pour la durée de conservation des données. Certaines données peuvent devoir être archivées ou supprimées après un certain temps.

5.1.10. Audit des Accès :

Surveillez les accès aux données sensibles en enregistrant les activités d'accès et en effectuant des audits réguliers.

5.1.11. Formation des Utilisateurs :

Sensibilisez les utilisateurs à l'importance de la protection des données, aux politiques de sécurité et aux meilleures pratiques en matière de manipulation des données.

5.2. Chiffrement

Le chiffrement des données est une technique de cryptographie qui consiste à transformer des données en un format illisible. Le texte chiffré ne peut être lu qu'en utilisant une clé de déchiffrement.

Le chiffrement des données est utilisé pour protéger la confidentialité des données, c'est-à-dire pour empêcher qu'elles ne soient lues par des personnes non autorisées. Il est utilisé dans de nombreux contextes, notamment :

- La protection des données personnelles et sensibles, telles que les numéros de cartes de crédit, les informations médicales et les données confidentielles.
- La protection des données transmises sur Internet, telles que les données bancaires, les données de connexion et les données de transactions en ligne.
- La protection des données stockées sur des supports physiques, tels que des disques durs, des clés USB et des cartes SD.

- **Chiffrer l'ensemble des périphériques de stockage utilisés pour l'administration** : Il est recommandé de procéder au chiffrement complet de l'ensemble des périphériques de stockage (disques durs, périphériques de stockage amovibles, etc.) utilisés pour les actions d'administration.

5.3. Sauvegarde et restauration

La sauvegarde et la restauration font référence aux technologies et aux pratiques permettant d'effectuer des copies périodiques de données et d'applications sur un périphérique secondaire distinct, puis d'utiliser ces copies pour récupérer les données et les applications, au cas où les données de départ et les applications sont perdues ou endommagées en raison d'une panne de courant, d'une cyberattaque, d'une erreur humaine, d'un sinistre ou de tout autre événement imprévu.

Il existe plusieurs méthodes de sauvegarde et de restauration. La méthode la plus courante consiste à utiliser un logiciel de sauvegarde. Le logiciel de sauvegarde peut être utilisé pour créer des copies de sauvegarde des données sur un disque dur externe, un serveur de stockage ou un service de sauvegarde en ligne.

- Des copies de sauvegarde des informations, des logiciels et des systèmes doivent être prises et testées régulièrement conformément à une politique de sauvegarde convenue.
- Veillez à la confidentialité des données en rendant leur lecture impossible à des personnes non autorisées en les chiffrant à l'aide d'un logiciel de chiffrement avant de les copier dans le « cloud ».
- Les sauvegardes des informations et des logiciels doivent être effectuées sur la base d'une politique de sauvegarde formelle pour garantir la continuité du service et la disponibilité des systèmes et des informations.
- Les sauvegardes des systèmes traitant des informations confidentielles doivent être cryptées en fonction des exigences de classification des informations. La fréquence et l'étendue des sauvegardes doivent être mutuellement convenues entre le personnel impliqué dans la gestion des services d'information et l'information/le système
- La capacité à restaurer les informations et les logiciels doit être testée périodiquement conformément à la politique de sauvegarde pour garantir que les informations peuvent être récupérées avec succès à partir du support de sauvegarde.
- Il est primordial de définir une politique de sauvegarde du SI d'administration, ceci afin de pouvoir rétablir le service à la suite d'un incident. Pour cela, les éléments à sauvegarder, le lieu de sauvegarde et les droits d'accès qui y sont associés doivent être clairement identifiés. Les sauvegardes doivent être réalisées régulièrement. Enfin, les procédures de restauration doivent être documentées et testées.
- Définir une politique de sauvegarde du SI d'administration Pour permettre de pallier la corruption ou l'indisponibilité de données dues à un incident ou une compromission, une politique de sauvegarde doit être définie et appliquée pour le SI d'administration. Pour les éléments les plus critiques, une sauvegarde hors ligne doit être prévue.

5.4. Journalisation et supervision de la sécurité

Les besoins de journalisation SI d'administration doivent donc être pris en compte dans l'étude de conception du SI d'administration. Une zone d'administration doit être dédiée aux services de journalisation. En effet, pour assurer une analyse pertinente des journaux d'événements, leur intégrité doit être garantie depuis leur génération jusqu'à leur lieu de stockage. En cas d'intrusion, les attaquants voudront effacer ou modifier les traces générées pour que leur présence ne soit pas détectée. Afin de couvrir ce risque, il est nécessaire de restreindre les accès à ces informations aux seules personnes ayant le besoin d'en connaître.

- La journalisation doit être activée sur tous les systèmes à haut risque, y compris les systèmes de sécurité et systèmes traitant des informations sensibles, ou pour capturer, maintenir et surveiller les activités des journaux
- Ces journaux doivent être conservés (et disponibles) pendant 180 jours, ou plus si nécessaire.
- Les problèmes techniques doivent être enregistrés, surveillés et signalés au responsable approprié.

6. Cybersécurité

La sécurité informatique constitue un défi majeur pour des organisations de toutes tailles, car les incidents de sécurité deviennent de plus en plus fréquents et peuvent avoir des conséquences dévastatrices, notamment la perte de données sensibles, l'interruption des activités et le vol d'identité. Pour se protéger contre les cyberattaques, les organisations doivent mettre en place un plan de sécurité informatique complet. Ce plan doit inclure une variété de mesures de sécurité, telles que :

- Des mises à jour régulières des systèmes et logiciels
- L'utilisation d'un antivirus et d'un pare-feu
- Le décommissionnement (abandon) correct des systèmes et équipements obsolètes ou non sécurisés
- La limitation de l'exposition des systèmes aux réseaux externes
- La mise en œuvre de la segmentation du réseau
- La sensibilisation à la cybersécurité au niveau de l'institution

Chacune de ces mesures de sécurité joue un rôle important dans la protection des systèmes informatiques contre les cyberattaques. L'application d'un plan de sécurité informatique complet peut aider les organisations à réduire le risque d'attaques et à protéger leurs données et leurs systèmes.

6.1. Minimiser l'exposition des systèmes aux réseaux externes

Pour minimiser l'exposition des systèmes aux réseaux externes et renforcer la sécurité informatique, il est essentiel de mettre en œuvre plusieurs pratiques et mesures de sécurité. Voici quelques recommandations :

Tableau 26 : Recommandation pour minimiser l'exposition des systèmes aux réseaux externes

Recommandation	Description
Pare-feu	Utilisez des pare-feux pour contrôler le trafic réseau entrant et sortant. Configurez-les pour permettre uniquement les connexions nécessaires et bloquer tout le reste.
Segmentation réseau	Divisez votre réseau en segments ou zones, en fonction de la sensibilité des données et des besoins d'accès. Limitez l'accès aux segments internes aux seuls utilisateurs et systèmes autorisés.
	Si vous avez besoin d'accès à distance aux systèmes internes, utilisez des méthodes

Accès à distance sécurisé	sécurisées telles que les réseaux privés virtuels (VPN) ou des solutions d'accès à distance sécurisé. Limitez strictement ces accès.
Limitier l'accès aux systèmes	Seuls les utilisateurs autorisés doivent avoir accès aux systèmes. Cela peut être fait en utilisant des groupes et des rôles d'utilisateurs.

6.2. Mettre en œuvre la segmentation du réseau

La segmentation du réseau est une pratique de sécurité qui divise un réseau en sous-réseaux plus petits. Cela peut aider à limiter la propagation des attaques de pirates et à améliorer la sécurité globale du réseau. Il existe plusieurs façons de mettre en œuvre la segmentation du réseau tel que :

- Mettez en place des réseaux locaux virtuels (VLAN) pour restreindre l'accès. Les VLANs isolent logiquement les segments réseau, vous permettant de contrôler le flux de trafic entre différents groupes. Vous pouvez configurer des règles de pare-feu, des routages et des listes de contrôle d'accès (ACL) pour restreindre la communication entre les VLANs.
- Sécurisez tout accès distant au réseau ou aux systèmes de l'organisation en utilisant des réseaux privés virtuels (VPN). Les VPN chiffrent la communication entre l'utilisateur distant et le réseau, rendant beaucoup plus difficile l'interception d'informations sensibles par des utilisateurs non autorisés.
- ACL sont des ensembles de règles qui définissent le trafic réseau autorisé ou refusé en fonction de divers critères, tels que les adresses IP source et de destination ou les protocoles. Vous pouvez contrôler la communication entre différents segments et restreindre l'accès à des ressources spécifiques en configurant ACL.
- Renforcez encore la sécurité en limitant le nombre d'adresses IP autorisées à se connecter à distance. Cette restriction garantit que seuls les dispositifs autorisés peuvent établir des connexions à distance, réduisant ainsi la surface d'attaque.

6.3. Mise à jour des systèmes informatiques

Les mises à jour sont importantes pour la sécurité et la fiabilité des systèmes informatiques. Les mises à jour peuvent inclure des correctifs des bugs, des améliorations de performances, de nouvelles fonctionnalités et des mises à jour de sécurité.

Il est important d'installer les mises à jour dès qu'elles sont disponibles. Les mises à jour de sécurité peuvent aider à protéger les systèmes contre les menaces de sécurité, telles que les virus, les logiciels malveillants et les attaques de piratage.

- Utiliser des solutions matérielles et logicielles maintenues

Par habitude, par négligence ou par souci d'économies, il peut arriver que l'on conserve du matériel ou des logiciels au-delà de leur "cycle de vie", c'est-à-dire après la période pendant laquelle leur fabricant ou éditeur garantit leur maintien en conditions de sécurité. Tout matériel ou logiciel qui ne peut plus être mis à jour doit être retiré ou désinstallé.

- Activer la mise à jour automatique des logiciels et des matériels

Les mises à jour du système d'exploitation et de tous les logiciels utilisés doivent être effectuées dès que possible, à chaque mise à disposition d'un correctif par leurs éditeurs. Cela est d'autant plus important pour tous les matériels exposés à Internet. Il est recommandé d'activer les fonctions de mise à jour automatique proposées par les éditeurs. En complément, des mises à jour hors calendrier peuvent survenir en cas de détection d'une vulnérabilité, et devront être appliquées dès que possible

6.4. Téléchargement des programmes

Dans le contexte de téléchargement de ressources sur internet et afin de veiller à la sécurité de vos systèmes d'information et de vos données, il est important de considérer les points suivants :

- Téléchargez vos programmes sur les sites de leurs éditeurs ou d'autres sites de confiance ;
- Pensez à décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires ;
- Restez vigilants concernant les liens sponsorisés et réfléchir avant de cliquer sur des liens ;
- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue

6.5. Antivirus

Les antivirus permettent d'accroître la sécurité des serveurs et des postes de travail de plusieurs types d'attaques, comme les virus informatiques ou les ransomware et permettent de réduire le risque de compromettre les systèmes d'information.

- Un antivirus doit être déployé sur tous les équipements, en priorité ceux connectés à Internet (postes de travail, serveurs de fichier, etc.). Un antivirus protège des menaces connues, qui évoluent très rapidement : des centaines de milliers de codes malveillants apparaissent chaque jour. Ainsi, il faut tenir à jour le logiciel en lui-même et sa base de données de signatures. Cette base de données est l'élément qui permet l'identification de programmes et fichiers malveillants, sans mise à jour fréquente, la protection offerte par l'antivirus s'en trouve très rapidement amoindrie.
- Les antivirus commerciaux proposent une mise à jour automatique, et un scan automatique des espaces de stockage : il est indispensable de procéder à l'activation de ces mécanismes dans les paramètres. Par ailleurs, il peut être préconisé, en fonction de

vos usages, de souscrire aux fonctionnalités complémentaires proposées par de nombreux éditeurs logiciels tels qu'un pare-feu, un filtrage Web, un VPN, des outils anti-hameçonnage.

- Il est recommandé de mettre en œuvre une gestion centralisée des antivirus afin de pouvoir assurer un suivi et un contrôle du bon déploiement de ceux-ci sur l'ensemble des équipements à disposition et utilisés.

6.6. Décommissionnement

Le décommissionnement est le retrait d'un système ou d'un équipement et fait référence au processus de mise hors service planifiée de ces ressources informatiques.

Le décommissionnement poursuit généralement un ou plusieurs des objectifs suivants :

- **Obsolescence Technologique** : Identifiez les systèmes ou les équipements TIC qui ont atteint la fin de leur cycle de vie technologique.
- **Non-Conformité et Sécurité** /Évaluez les systèmes qui ne sont plus conformes aux normes de sécurité actuelles.
- **Coût Élevé d'Entretien** : Analysez les coûts associés à la maintenance continue des systèmes vieillissants par rapport à leur utilité.

Processus de Décommissionnement

- Identifiez les applications logicielles à décommissionner en effectuant une évaluation approfondie de leur utilité, de leur coût d'exploitation, de leur sécurité et de leur pertinence pour l'organisation.
- Établissez un plan détaillé pour le processus de décommissionnement, la manière dont les données seront migrées ou archivées, comment les utilisateurs seront formés pour utiliser de nouvelles solutions, et comment l'application sera supprimée.
- **Migration ou archivage des données** : Si des données sont associées à l'application, assurez-vous de les migrer vers un emplacement approprié ou de les archiver conformément aux exigences légales et réglementaires.

Voici quelques conseils pour décommissionner vos systèmes informatiques ou réseaux informatiques en toute sécurité :

- Planifiez le décommissionnement et assurez-vous d'avoir les ressources nécessaires pour l'effectuer.
- Sauvegardez toutes les données importantes avant de retirer les systèmes ou réseaux de la production.
- Désactivez tous les comptes utilisateurs et retirez les accès aux systèmes ou réseaux.
- Supprimez toutes les données sensibles, telles que les informations personnelles ou les données confidentielles.
- Mettez à jour la documentation pour refléter le décommissionnement des systèmes ou réseaux.

- Effectuez un audit du décommissionnement pour vous assurer qu'il a été effectué correctement.

6.7. Comptes de messagerie et messagerie officielle

La messagerie est le principal vecteur d'infection du poste de travail. En un clic, vous pouvez être victime d'hameçonnage (ou phishing en anglais), pour s'en prémunir, quelques reflexes à adopter

- Les outils de collaboration, de conférence et de communication approuvés (par exemple, WebEx, Microsoft Teams) doivent être utilisés uniquement d'une manière conforme aux politiques de l'organisation en matière de confidentialité, y compris le manuel mondial de gestion de la qualité et des risques
- Vérifier les identités des destinataires (émetteurs), lire son adresse mail en détail, ne pas se fier à ce que l'outil de messagerie vous facilite la reconnaissance de vos interlocuteurs. Et si quelque chose vous paraît anormal, il ne faut pas hésiter à contacter directement l'émetteur du mail.
- Faire attention aux pièces jointes qui sont dans le corps du message, et à ne pas cliquer sur les liens URL, ce qui peut être très dangereux.
- Assurez-vous que votre application de messagerie est toujours à jour avec les derniers correctifs de sécurité.
- Prenez votre temps avant de répondre aux demandes inhabituelles, demandez des éclaircissements, appelez la personne concernée pour vérifier l'authenticité de l'e-mail.
- Désactiver l'ouverture automatique des documents en pièce jointe
- Ne répondez jamais à une demande de codes confidentiels
- Évitez d'accéder à votre messagerie depuis des réseaux Wi-Fi publics non sécurisés. Si vous devez le faire, utilisez un réseau privé virtuel (VPN) pour sécuriser votre connexion.
- Choisissez une plateforme de messagerie réputée qui offre des fonctionnalités de sécurité robustes. Des services de messagerie tels que Gmail, Outlook intègrent des mesures de sécurité avancées.
- Si l'on sait que des informations ont été envoyées à un destinataire involontaire, cela doit être immédiatement signalé conformément aux procédures locales, par exemple en le responsable de la protection de la vie privée (le cas échéant) afin que les mesures nécessaires puissent être prises.
- Si nécessaire, les pièces jointes des e-mails doivent être cryptées séparément. Dans ces cas, les pièces jointes doivent d'abord être cryptées à l'aide d'un produit approuvé (par exemple WinZip) et le fichier crypté/zippé est ensuite joint au message électronique. Lors de l'envoi des pièces jointes cryptées, l'expéditeur doit également fournir le mot de passe. Pour garantir la sécurité des données, le mot de passe doit être fourni par une autre méthode de communication, par exemple en appelant directement le destinataire ou en utilisant un SMS

6.8. Imprimantes et scanner

Les imprimantes et les scanners sont des périphériques qui peuvent également être utilisés pour compromettre la sécurité des données. Pour protéger les imprimantes et les scanners contre les cybermenaces, il est important de mettre en œuvre des mesures de sécurité appropriées. Ces mesures comprennent :

- Imposer des mots de passe pour l'accès aux interfaces de gestion des imprimantes, évitant ainsi toute utilisation ou configuration non autorisée
- Assurez-vous que les imprimantes sont sécurisées pour empêcher l'accès non autorisé aux données stockées
- Certaines imprimantes offrent la possibilité de chiffrer les données avant l'impression pour une protection accrue
- Les interfaces de gestion des imprimantes doivent être protégées par un mot de passe pour empêcher les utilisations ou configurations non autorisées
- Instaurer une politique stricte exigeant que les documents imprimés sensibles soient retirés immédiatement de l'imprimante pour éviter toute divulgation non autorisée
- Seul le personnel de maintenance autorisé doit effectuer des réparations d'imprimantes
- Les utilisateurs doivent gérer efficacement les ressources d'impression en n'imprimant que lorsque cela est nécessaire.

6.9. Incident de sécurité

6.9.1. Exemples d'incident de sécurité

Les incidents de sécurité doivent être immédiatement signalés conformément aux procédures locales établies, afin que les actions correctives appropriées puissent être mises en œuvre le plus rapidement possible.

Voici des exemples d'incidents qui doivent être signalés :

- Toute violation de données, y compris la mauvaise direction d'e-mails, la perte de données/informations, de capital intellectuel, de logiciels ou d'actifs physiques (ou d'informations client/tiers), le transfert à un destinataire non autorisé, y compris, par exemple, des informations sur des ordinateurs portables, des téléphones intelligents, des périphériques USB, des documents et des documents de travail
- Si un membre du personnel estime que ses informations d'identification peuvent avoir été compromises ou perdu, ou en cas de perte ou de vol d'un jeton ou d'un autre dispositif d'accès
- Toute infection par un logiciel malveillant, réelle ou suspectée, entraînant une divulgation potentielle d'informations ou perte de contrôle de l'appareil
- Si un membre du personnel prend connaissance d'une faille de sécurité ou d'une vulnérabilité
- Toute violation de la Politique

- Une menace ou un incident relatif à la sécurité de l'information est défini comme toute situation ou événement dans lequel la confidentialité, l'intégrité, la disponibilité ou la conformité des informations à toute loi, réglementation ou politique pertinente peut être (dans le cas d'une menace) ou a été (dans le cas d'un incident) compromis.
- Une chaîne d'e-mails a été reçue de quelque source que ce soit

6.9.2. Gestion des incidents de sécurité

La gestion des incidents de sécurité est le processus de détection, d'analyse, de réponse et de récupération d'un incident de sécurité. Il s'agit d'une étape essentielle de la sécurité de l'information, car elle permet aux organisations de minimiser les impacts d'un incident et de protéger leurs données et leurs systèmes.

Le processus de gestion des incidents de sécurité comprend généralement les étapes suivantes :

1. Détection : l'identification d'un incident de sécurité. Cela peut être fait en surveillant les systèmes et les réseaux pour détecter des activités suspectes, ou en réponse à un rapport d'incident d'un utilisateur.
2. Analyse : la compréhension de la nature et de l'étendue de l'incident. Cela implique l'analyse des données collectées lors de la phase de détection, ainsi que la collaboration avec les parties prenantes concernées.
3. Réponse : la prise de mesures pour limiter les impacts de l'incident. Cela peut inclure l'isolement de l'incident, la restauration des systèmes et des données, et la notification des parties prenantes concernées.
4. Récupération : la restauration des opérations normales après l'incident. Cela implique la mise en œuvre de mesures correctives pour éviter que l'incident ne se reproduise.

6.10. Sensibilisation à la cybersécurité au niveau de l'institution

Tous les employés de l'organisation doivent recevoir une sensibilisation et une formation appropriées ainsi que des mises à jour régulières des politiques et procédures de l'organisation, en fonction de leur fonction

- Organisez des sessions de formation régulières pour les employés sur les sujets liés à la sécurité en ligne, tels que les meilleures pratiques de gestion des mots de passe, la reconnaissance des attaques de phishing, etc.
- Proposez des formats variés, tels que des ateliers en personne, des webinaires en ligne et des modules de formation interactifs.
- Tenez les parties prenantes informées des dernières menaces en ligne et des tactiques d'attaques par le biais de newsletters, de courriers électroniques ou de notifications push.
- Partagez des études de cas réels pour illustrer les risques potentiels et les mesures de prévention.

- Fournissez des ressources de référence, comme des guides pratiques, des manuels de sécurité en ligne et des vidéos tutoriels, que les utilisateurs peuvent consulter à tout moment.
- Intégrez la sécurité dans la culture de l'organisation en encourageant les discussions régulières sur les meilleures pratiques et les préoccupations en matière de sécurité.

7. Applications logicielles

7.1. Modèle architectural

7.1.1. Principes Fondamentaux de l'Architecture :

L'architecture des applications logicielles joue un rôle central dans la gestion et l'efficacité des systèmes informatiques au sein des ministères. Dans cette section, nous décrirons le modèle d'architecture des applications logicielles, qui sert de base à la conception, au développement, à la mise en œuvre et à la gestion de nos solutions logicielles.

Le modèle d'architecture des applications logicielles repose sur les principes suivants :

Tableau 27 : Principes pour l'architecture

Principes Fondamentaux de l'Architecture	Description
Modularité et Composabilité	Les applications sont découpées en modules indépendants, ce qui facilite la réutilisation, la maintenance, et l'évolutivité. Les modules peuvent être assemblés pour créer des solutions spécifiques
Compatibilité	Les applications sont conçues pour interagir efficacement avec d'autres systèmes, tant internes qu'externes, en utilisant des normes ouvertes et des protocoles standard
Sécurité	La sécurité est une composante intégrale de chaque application, avec des mécanismes de gestion des identités, de l'authentification et de l'autorisation, ainsi que la protection des données
Extensibilité	Les applications sont conçues pour être évolutives, ce qui permet d'ajouter de nouvelles fonctionnalités ou d'adapter les systèmes aux besoins changeants sans réinventer la roue

7.1.2. Couches de l'Architecture :

Le modèle d'architecture logicielle se compose de trois couches principales :

Tableau 28 : Couches de l'architecture des logiciels

Couche de l'architecture	Description
Couche de Présentation	Cette couche est responsable de l'interface utilisateur, qu'il s'agisse d'applications Web, d'applications mobiles ou d'interfaces

	utilisateur graphiques (GUI). Elle offre une expérience utilisateur intuitive et responsive
Couche Applicative	Au cœur de cette couche se trouvent les composants et les services métier qui gèrent la logique fonctionnelle des applications. Elle traite les requêtes de l'interface utilisateur, interagit avec les bases de données et les systèmes externes, et assure la gestion des workflows
Couche de Données	Cette couche gère la persistance des données. Elle comprend les bases de données, les systèmes de stockage, et les mécanismes de sauvegarde pour garantir l'intégrité et la disponibilité des données

7.1.3. Technologies et Normes :

Nous encourageons l'utilisation de technologies et de standards pour mettre en œuvre notre modèle d'architecture des applications/logicielles. Cela inclut l'utilisation de langages de programmation appropriés, de frameworks de développement, de protocoles d'API ouverts, et de bases de données adaptées aux besoins spécifiques de chaque application.

7.2. L'usage de logiciels libres

L'adoption du logiciel libre se présente comme une décision stratégique d'une importance capitale pour le déploiement des systèmes d'informations à travers les ministères et les structures publique.

Dans ce tableau, nous allons décrire les avantages de l'utilisation de logiciels libres.

Tableau 29 : Avantages de l'utilisation des logiciels libres

Avantages	Description
Liberté et Contrôle	L'utilisation de logiciels libres accorde un degré de liberté et de contrôle important sur nos systèmes informatiques. Ils permettent une indépendance d'un éditeur de logiciel unique, et permettent de faire évoluer ces derniers en fonction de nos besoins en évitant les contraintes imposées par des logiciels propriétaires
Économie de Coûts	L'utilisation de logiciels libres représente souvent une économie significative par rapport aux solutions propriétaires

Sécurité et Transparence	Les logiciels libres offrent une transparence totale sur leur fonctionnement interne, ce qui signifie que nos ministères peuvent auditer, inspecter et vérifier le code
Pérennité	En adoptant des logiciels libres, nous garantissons la pérennité de nos solutions. Notre ministère n'est pas soumis aux fluctuations commerciales ou aux décisions d'abandon de produits par des éditeurs tiers
Collaboration et Communauté	L'utilisation de logiciels libres s'accompagne d'une participation active à des communautés de développement. Cela favorise la collaboration avec d'autres organisations gouvernementales et non gouvernementales, permettant ainsi de partager des solutions, des connaissances et des bonnes pratiques pour le bénéfice commun

8. Développement logiciel

8.1. Approche pour le développement d'applications

Pour un développement réussi d'applications au sein des ministères, nous préconisons les principes suivants :

Tableau 30 : Principes de développement

Principes	Description
Méthodologie Agile	Adoption des méthodologies agiles telles que Scrum ou Kanban pour favoriser la collaboration, la flexibilité et la réactivité aux besoins changeants
Engagement des Utilisateurs	L'implication des utilisateurs finaux dans le processus de développement pour garantir que les applications répondent à leurs besoins
Test Continu	La mise en place des pratiques de test automatisé et de test continu pour identifier et corriger les problèmes plus tôt dans le cycle de développement

8.2. Langages

Pour le choix des langages de programmation privilégiez des langages polyvalents tels que Python, Java, ou JavaScript, qui conviennent à une variété de tâches de développement

8.3. Plateformes

Le choix de la plateforme de déploiement dépendra des besoins spécifiques de chaque projet, mais généralement on privilégiera un hébergement sur un serveur d'application tel qu'Apache Tomcat, NodeJS, pour des applications Web complexes ou l'exploitation des services cloud sécurisés et évolutifs telles que AWS, ou Google Cloud.

8.4. Framework

Privilégiez l'utilisation des Framework pour accélérer le développement et renforcer la sécurité de vos solutions.

L'utilisation des Framework Web tels Python Django, Ruby on Rails, ou Spring Boot vont accélérer et faciliter le développement et des Framework Front-end basé sur Javascript comme React, Angular ou Vue.js vont permettre de créer des interfaces utilisateur modernes et réactives.

8.5. Développement mobile

Pour le développement d'applications mobile Privilégiez des solutions multiplateformes comme React Native ou Flutter pour réduire les coûts et accélérer le développement

8.6. Conception Web adaptative

La conception web adaptative est essentielle pour garantir l'accessibilité et l'expérience utilisateur. Les paradigmes suivants vous permettront de garantir un rendu universel à vos différentes plateformes

Tableau 31 : Paradigmes de conception web

Paradigme	Description
Responsive Design	Assurer que les applications web et mobile sont conçues pour s'adapter aux différents appareils, des ordinateurs de bureau aux smartphones
Accessibilité	Respecter les normes d'accessibilité (comme les WCAG) pour garantir que les applications sont utilisables par tous, y compris les personnes handicapées

9. Administration des systèmes d'information

9.1. Protection des mots de passe

Une politique de sécurité de mots de passe est caractérisée par la définition de certains éléments associés à la gestion des mots de passe :

9.1.1. Longueur des mots de passe

La longueur est une composante importante de la sécurité d'une authentification par mots de passe. Il est souvent plus efficace d'allonger un mot de passe que de chercher à le rendre plus complexe pour en augmenter l'entropie. Définir une longueur minimale permet d'avoir un certain contrôle sur le niveau de sécurité apporté par les mots de passe lors de leur création par les utilisateurs.

- **Imposer une longueur minimale pour les mots de passe** : Il est recommandé de définir une longueur minimale pour les mots de passe lors de leur création en fonction du niveau de sécurité visé par le système d'information

Les recommandations de longueurs minimales en fonction du niveau de sensibilité sont résumées dans ce tableau :

Tableau 32 : Recommandation pour la longueur des mots de passe

Niveau de sensibilité	Longueur minimale en nombre de caractère	Taille de clé équivalente en bits
Faible à moyen	Entre 9 et 11	≈ 65
Moyen à fort	Entre 12 et 14	≈ 85
Fort à très fort	Au moins 15	≥ 100

Dans des contextes de sensibilité forte à très forte, il est recommandé d'utiliser l'authentification multifacteur

- **Ne pas imposer de longueur maximale pour les mots de passe** : Selon les systèmes, il est recommandé de ne pas fixer de limite à la longueur maximale d'un mot de passe afin de permettre aux utilisateurs d'avoir recours à des phrases de passe ou longs mots de passe.

9.1.2. Règles de complexité des mots de passe

La notion de complexité d'un mot de passe désigne usuellement le choix du jeu de caractères dans lequel les caractères composant un mot de passe sont choisis.

Au moment de la création ou du renouvellement d'un mot de passe par un utilisateur, il est recommandé de mettre en œuvre des règles de complexité tout en proposant un jeu de

caractères le plus large possible, nous recommandons des mots de passe d'au moins 9 caractères alphanumériques en alternant des majuscules et des caractères spéciaux.

9.1.3. Délai d'expiration des mots de passe

- **Ne pas imposer par défaut des délais d'expiration sur les mots de passe des comptes non sensibles :** Si la politique de mots de passe exige des mots de passe robustes et que les systèmes permettent son implémentation, alors il est recommandé de ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles comme les comptes utilisateur.
- **Imposer un délai d'expiration sur les mots de passe des comptes à privilèges :**
Il est recommandé d'imposer un délai d'expiration sur les mots de passe des comptes très sensibles comme les comptes administrateurs. Ce délai d'expiration peut par exemple être fixé à une durée comprise entre 1 et 3 ans. En cas d'incidents de sécurité (comme une suspicion de compromission de la base de données contenant des mots de passe), une expiration immédiate des mots de passe des comptes concernés doit être imposée.
- **Révoquer immédiatement les mots de passe en cas de compromission suspectée ou avérée :** En cas de compromission suspectée ou avérée d'un système d'authentification, tous les mots de passe concernés par ce système doivent être renouvelés immédiatement (de l'ordre de la journée). Au-delà de ce délai, les comptes concernés doivent être désactivés et une procédure de réactivation pour les utilisateurs doit être mise en œuvre.

8.1.3. Contrôle de la robustesse des mots de passe

De nombreux contrôles permettent de s'assurer que les mots de passe créés offrent une robustesse en accord avec le niveau de sécurité souhaité, par exemple :

- Mettre en place des mécanismes automatiques et systématiques permettant de vérifier que les mots de passe respectent bien les règles définies dans la politique de sécurité
- Comparer les mots de passe lors de leur création ou de leur renouvellement à une base de données répertoriant les mots de passe les plus utilisés ou bien ceux qui ont été compromis
- Repérer les mots de passe contenant des motifs (ou des répétitions de motifs) spécifiques (comme une suite de chiffre telle que « 12345 », la suite des premières lettre des claviers comme « azerty »,etc);
- Repérer les mots de passe contenant des informations personnelles saisies lors de la création du compte, comme les noms et prénoms ou encore les dates de naissance

8.1.4. Stockage des mots de passe

Le stockage sécurisé des mots de passe repose par l'application d'algorithmes de hachage tels que SHA-3, garantissant ainsi que les informations d'identification demeurent confidentielles et inviolables.

8.2. Accès aux systèmes

Les recommandations suivantes sont conçues pour aider les organisations à réduire les risques d'accès non autorisé et à protéger leurs informations sensibles.

8.2.1. Identification

Il est indispensable de dissocier les rôles sur le système d'information, en particulier le rôle d'administration ayant des droits privilégiés.

- **Des comptes d'administration dédiés** : L'administrateur doit disposer d'un ou plusieurs comptes d'administration dédiés, distincts de son compte utilisateur. Les mots de passe d'authentification doivent être différents suivant le compte utilisé.

8.2.2. Authentification

- Exigez des mots de passe solides qui incluent une combinaison de lettres, de chiffres et de caractères spéciaux.
- Mettez en place une authentification à facteurs multiples (MFA) pour renforcer la sécurité en demandant aux utilisateurs de fournir plusieurs formes de vérification.

8.2.3. Droits d'administration

Il est recommandé de déployer des politiques de sécurité dans le but pour définir les privilèges de chaque compte d'administration, de contrôler l'accès aux outils d'administration en fonction du juste besoin opérationnel et de renforcer l'authentications

8.2.4. Comptes Utilisateurs

- Créez des comptes d'utilisateurs avec le niveau d'accès approprié en fonction des rôles et des responsabilités.
- Passez régulièrement en revue et mettez à jour les permissions des comptes d'utilisateurs à mesure que les rôles changent ou lorsque les employés quittent l'organisation.

8.2.5. Contrôles d'Accès

- Utilisez des mécanismes de contrôle d'accès pour restreindre l'accès non autorisé aux données sensibles et aux ressources du système.

- Mettez en œuvre un Contrôle d'Accès Basé sur les Rôles (RBAC) pour attribuer des permissions en fonction des rôles prédéfinis dans l'organisation.

8.2.6. Journaux d'Accès et Surveillance

- Surveillez les journaux d'accès pour identifier les utilisateurs qui accèdent aux systèmes et déterminer les actions qu'ils ont effectuées
- Configurez des alertes pour les activités suspectes ou non autorisées.

8.2.7. Accès à Distance

- Si l'accès à distance est nécessaire, utilisez des méthodes sécurisées telles que les réseaux privés virtuels (VPN) et les connexions chiffrées.
- Mettez en place des restrictions sur l'accès à distance, en n'autorisant par exemple l'accès que depuis des adresses IP spécifiques.

9. Désactivation des Comptes

- Désactivez rapidement les comptes d'utilisateurs lorsque les employés quittent l'organisation ou n'ont plus besoin d'accès.
- Assurez-vous que l'accès des employés résiliés est révoqué immédiatement pour éviter tout accès non autorisé.

10. Audit Régulier

- Effectuez régulièrement des audits des comptes d'utilisateurs et des permissions d'accès pour identifier les éventuelles incohérences ou risques potentiels pour la sécurité.

Revue et mise à jour du document

Ce document sera révisé annuellement afin de prendre en compte de nouvelles problématiques résultant de l'utilisation des systèmes informatiques et des tendances technologiques émergentes dans l'industrie

Annexe 1 : Procédures E-Gouv

1. Intégration et contrat

1.1. Aperçu

Le processus d'intégration du client est initié lorsqu'un client potentiel a été identifié et contacté par l'équipe commerciale de CSquared Woezon. Avant de lancer le processus d'intégration du client, l'équipe de vente est chargée de s'assurer que le client signe un accord de non-divulgaration et fournit une copie de la licence de l'organisme de réglementation.

1.2. Informations sur le client

L'équipe de vente envoie un e-mail au client pour lui demander des informations précontractuelles, y compris les documents suivants requis pour le processus de vérification de crédit :

- Licence d'utilisation
- Certificat de constitution
- Détails de l'enregistrement fiscal

Le client fournit les informations et la documentation demandées à l'équipe de vente par e-mail. L'équipe de vente partage tous les documents justificatifs avec l'équipe de facturation qui, en retour, envoie ces documents à l'OTC pour vérification de crédit.

1.3. Vérification des antécédents ou diligence raisonnable

L'équipe de facturation demande une vérification de la solvabilité, le contrôle de la lutte contre le blanchiment d'argent.

OTC effectue la vérification de la solvabilité (sur la base des seuils de conditions de paiement convenus à l'avance avec CSquared) et met à jour l'e-mail avec les résultats et la recommandation, en ajoutant l'équipe financière à l'e-mail pour approbation. Les détails de la vérification de crédit sont partagés avec l'équipe de vente pour être inclus dans les négociations contractuelles.

1.4. Négociation de contrats

Une fois les conditions de paiement approuvées, l'équipe de vente engage le directeur national et le support juridique de CSquared pour examiner les détails du contrat avant de finaliser les négociations avec le client.

1.5. Signature du contrat

L'équipe de CSquared Woezon est chargée de s'assurer que le contrat est signé par les signataires concernés conformément à la politique. La signature finale de CSquared est fournie par le Country Manager, le Directeur Financier et le CEO.

CSquared Woezon est responsable de :

- S'assurer qu'une copie papier du contrat signé est déposée au bureau CSquared local
- S'assurer qu'une copie numérisée du contrat signé est stockée sur le Drive partagé Sales

- Informer l'équipe de facturation que le contrat a été entièrement signé et enregistré sur le Drive partagé

L'équipe de facturation envoie par e-mail le contrat signé à l'équipe financière et à l'OTC et met à jour le dossier de l'accord-cadre de service avec les détails du contrat convenu.

1.6. Configuration du client sur la plateforme de gestion des commandes

L'équipe de facturation demande au client de lui fournir trois contacts pour la configuration de la plateforme de gestion des commandes. La plateforme de gestion des commandes permet au client de commander directement via le portail.

Le client fournit ces informations à l'équipe de facturation du CSquared Woezon pour l'enregistrement et la configuration de la plateforme de gestion des commandes.

L'équipe de facturation entame une session d'accueil du client pour présenter la plateforme de gestion des commandes, la topologie technique, les finances et la facturation, ainsi que le respect du contrat.

L'équipe de vente assure le suivi avec le client pour garantir la soumission des formulaires de commande et le traitement de la commande.

2. Étapes du processus de facturation

Les différentes étapes du processus de facturation CSquared Woezon :

- i. Analysez les conditions contractuelles, les différents modèles de crédit et les conditions facturables.
- ii. Générez la facture, téléchargez le modèle à partir du créateur de fichier de facturation CSquared Woezon.
- iii. Analysez le modèle de calcul des crédits de service et de suivi des irrégularités.
- iv. Examinez le modèle de facturation en détail, c'est-à-dire les crédits, les frais d'installation et le MRC en fonction du type de contrat.
- v. Envoyez le modèle de téléchargement de facturation à l'équipe de surveillance mensuelle (MOT) pour examen et approbation.
 - a. Si le montant facturé est correct, le modèle de facturation est approuvé et PGM Finance en est informé.
 - b. Si le montant facturé n'est pas correct, les erreurs sont notées dans le journal et le PGM Finance est notifié, puis le rapprochement est effectué avant que le modèle de facture ne soit approuvé et que le PGM Finance ne soit notifié.
- vi. L'équipe DDT évalue et vérifie le fichier, les décimales, le nom du client.
 - a. Si le fichier est correct, la facture finale est générée.
 - b. Si le fichier n'est pas correct, nous procédons à la correction et nous la revoyons à l'équipe de facturation de la TNT, une fois les corrections effectuées nous générons la facture finale.
- vii. Vérification de la facture finale sur les points suivants :
 - a. Le nom du client
 - b. Le numéro de TVA
 - c. Période de facturation

- viii. Envoi des factures.
 - a. Si la facture finale est correcte, nous créons un addendum à la facture, le tamponnons avec le cachet de CSquared, et procédons à la livraison de la facture en version pdf.
 - b. Si la facture finale n'est pas correcte, nous la corrigeons, nous générons une nouvelle facture corrigée, nous vérifions à nouveau la facture finale sur les points suivants :
 - i. Le nom du client
 - ii. Le numéro de TVA
 - iii. Période de facturation
- ix. Si la facture finale est correcte, un addendum à la facture est créé et tamponné avec le cachet de CSquared Woezon, et procéder à la livraison de la facture en version pdf.
- x. Une fois la facture reçue au bureau du client, nous en accusons réception en estampillant une copie de la facture avec le cachet du client, dont une copie sera ensuite envoyée à PGM Finances.
- xi. Une fois cette étape franchie, nous procéderons au processus de collecte selon le délai stipulé dans le contrat.

En cas de rejet ou d'annulation de la facture, nous suivons la procédure appropriée.