ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

Analyse exploratoire des vulnérabilités potentielles d'un système d'information municipal et stratégies de sécurisation : Cas de l'Hôtel de Ville de Kananga.

MPINDA MUTSHIPAYI Albert,
Chef de Travaux à l'Université Pédagogique de Kananga
TSHIBAKA KATUMONANGANI Emmanuel,
Professeur à l'Université Pédagogique Nationale

Résumé

La numérisation des services publics municipaux est un vecteur essentiel de la modernisation administrative et de l'amélioration de la gouvernance locale. Cependant, cette transition expose les systèmes d'information (SI) des collectivités territoriales à des cybermenaces croissantes. Cette étude exploratoire vise à identifier et analyser les vulnérabilités potentielles du système d'information de l'Hôtel de Ville de Kananga, en République Démocratique du Congo (RDC), et à proposer des stratégies de sécurisation des données adaptées au contexte local. En s'appuyant sur une revue de littérature documentaire et une analyse contextuelle de l'environnement numérique congolais, nous mettons en évidence une triade de vulnérabilités critiques : techniques (obsolescence des infrastructures), humaines (manque de sensibilisation et de formation) et organisationnelles (absence de politiques de sécurité formelles). Les résultats suggèrent que l'approche de sécurisation doit être holistique, intégrant des mesures techniques robustes, un renforcement des capacités humaines et l'adoption d'un cadre de gouvernance de la cybersécurité aligné sur les initiatives nationales de la RDC. Cette recherche contribue à la littérature en fournissant un cadre d'analyse de risques spécifique aux administrations locales des pays en développement et en proposant des recommandations pratiques pour la résilience numérique.

Mots-clés : *Analyse exploratoire, Vulnérabilité, Système d'Information, Stratégies de sécurisation.*

JEL CLASSIFICATION : H83, O33, M15, L86, D73

DOI : https://doi.org/10.66405/3136-2656.recodd.v1.4.5

Abstract

The digitalization of municipal public services is an essential driver of administrative modernization and improved local governance. However, this transition exposes the information systems (IS) of local government authorities to increasing cyber threats. This exploratory study aims to identify and analyze potential vulnerabilities in the information system of Kananga City Hall, in the Democratic Republic of the Congo (DRC), and to propose data security strategies tailored to the local context. Drawing on a documentary literature review and a contextual analysis of the Congolese digital environment, this study highlights three critical categories of vulnerabilities: technical

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

vulnerabilities (outdated infrastructure), human vulnerabilities (lack of awareness and training), and organizational vulnerabilities (absence of formal security policies). The findings suggest that a holistic approach to cybersecurity is required, integrating robust technical measures, human capacity building, and the adoption of a cybersecurity governance framework aligned with national initiatives in the DRC. This research contributes to the literature by providing a risk analysis framework specifically designed for local government administrations in developing countries and by proposing practical recommendations to strengthen digital resilience.

Keywords: Exploratory Analysis, Vulnerability, Information System, Security Strategies.

JEL CLASSIFICATION : H83, O33, M15, L86, D73

DOI : https://doi.org/10.66405/3136-2656.recodd.v1.4.5

1. Introduction

1.1. Contexte et Problématique

L'ère numérique a transformé la manière dont les administrations publiques interagissent avec les citoyens et gèrent leurs opérations internes. Les municipalités, en tant que premier niveau de contact entre l'État et la population, sont au cœur de cette transformation, utilisant des Systèmes d'Information (SI) pour gérer des données sensibles telles que l'état civil, les registres fonciers, la fiscalité locale et les services sociaux[1]. Cette numérisation, bien que prometteuse en termes d'efficacité et de transparence, introduit simultanément des risques majeurs, notamment en matière de cybersécurité.

Les collectivités territoriales sont devenues des cibles privilégiées pour les cybercriminels. Les attaques par rançongiciel (ransomware) contre les municipalités ont explosé ces dernières années, entraînant des interruptions de services critiques, des pertes financières considérables et la compromission de données personnelles[2]. Dans les pays en développement, et particulièrement en Afrique subsaharienne, ces vulnérabilités sont exacerbées par des facteurs structurels : infrastructures numériques limitées, budgets de sécurité restreints, pénurie d'experts qualifiés et cadres réglementaires émergents[3].

L'Hôtel de Ville de Kananga, capitale de la province du Kasaï Central en RDC, s'inscrit dans ce contexte de transition numérique. Bien que les informations spécifiques sur son SI soient rares, l'étude exploratoire de ce cas est cruciale. La RDC a

[1] ANSSI/AMF. (2020). *Guide de la cybersécurité pour les communes et intercommunalités*. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).
[2] CERT-FR. (2025). *Alerte sur les cybermenaces contre les collectivités territoriales*. Centre Gouvernemental de Veille, d'Alerte et de Réponse aux Attaques Informatiques.
[3] Gauthier, M. H. (2025). *De la différenciation à la coopération territoriale pour valoriser les données: légitimité, enjeux et implication des Régions*. Journées Doctorales de l'Association de Science Régionale de Langue Française.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

récemment adopté un Plan National du Numérique (PNN) et une Stratégie Nationale de Cybersécurité (SNC), reconnaissant l'importance de la protection de son cyberespace[4]. Cependant, la mise en œuvre de ces politiques au niveau local, notamment dans des villes comme Kananga, reste un défi majeur.

La problématique centrale de cette étude est la suivante : Quelles sont les vulnérabilités critiques du système d'information de l'Hôtel de Ville de Kananga, et quelles stratégies de sécurisation des données, alignées sur les standards académiques internationaux et adaptées au contexte congolais, peuvent être proposées pour renforcer sa résilience numérique ?

1.2. Objectifs de l'Étude

L'objectif général de cette recherche est de contribuer à la sécurisation des systèmes d'information des administrations locales en RDC. De manière spécifique, l'étude vise à :

- ✓ Identifier les principales catégories de vulnérabilités (techniques, humaines, organisationnelles) auxquelles un SI municipal dans un contexte comme Kananga est susceptible d'être exposé.
- ✓ Analyser l'impact potentiel de ces vulnérabilités sur la continuité des services publics et la confidentialité des données.
- ✓ Proposer un ensemble de stratégies de sécurisation des données et de gouvernance de la cybersécurité, fondées sur les meilleures pratiques internationales (ISO 27001, NIST) mais adaptées aux réalités socio-économiques et technologiques de Kananga.

1.3. Méthodologie de Recherche

La recherche scientifique a toujours été sanctionnée par de méthodologies requises selon qu'il s'agit de tel ou tel autre domaine. Pour atteindre nos objectifs assignés à travers cette recherche et Compte tenu de la nature exploratoire du sujet et de l'accès limité aux données internes de l'Hôtel de Ville de Kananga, nous avons utilisé une ***approche mixte*** (quantitative et qualitative) appuyée par les techniques d'observation, d'interview directe et documentaire**.**

1.4. Structure de l'Article

Le présent article est structuré en six sections principales. Après cette introduction, la Section 2 présente la revue de littérature et le cadre théorique. La Section 3 détaille le contexte de l'étude (Kananga et la RDC). La Section 4 propose une analyse exploratoire des vulnérabilités potentielles. La Section 5 développe les stratégies de sécurisation recommandées. Enfin, la Section 6 présente la conclusion, les limites de l'étude et les perspectives de recherche futures.

[4] Présidence de la RDC. (2023).*Stratégie Nationale de Cybersécurité* 2022-2025.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

2. Revue de Littérature et Cadre Théorique

2.1. Définitions et Enjeux du Système d'Information Municipal

a) *Analyse exploratoire :*c'est une démarche qui consiste à examiner un ensemble de données afin de mieux les comprendre, de repérer des tendances, de détecter des anomalies et de formuler des analyses plus approfondies.

b) Vulnérabilité : c'est le fait d'être fragile, exposé à un danger ou susceptible d'être blessé, affecté ou exploité.

c) *Système d'Information Municipal* : Un Système d'Information Municipal (SIM) est l'ensemble des ressources (matérielles, logicielles, humaines et organisationnelles) qui permettent à une administration locale de collecter, traiter, stocker et diffuser l'information nécessaire à l'exercice de ses missions. Les fonctions clés d'un SIM incluent la gestion de l'état civil, la gestion financière et fiscale, l'urbanisme et la gestion des ressources humaines.

d) *Stratégies de sécurisation :* désignent l'ensemble des mesures, des méthodes et des actions mises en place pour protéger les personnes, les biens, les informations, les infrastructures ou les systèmes contre les risques, les menaces et les dangers.

L'enjeu principal du SIM réside dans la nature des données qu'il manipule :

- Données à caractère personnel (DCP) : Informations sur les citoyens (identité, adresse, situation familiale). Leur compromission peut entraîner des atteintes à la vie privée et des fraudes.
- Données stratégiques : Plans d'urbanisme, budgets, informations de sécurité publique. Leur altération ou divulgation peut nuire à la gouvernance et à la sécurité territoriale.

2.2. Cadre Conceptuel des Vulnérabilités et des Risques

La cybersécurité repose sur le triptyque Confidentialité, Intégrité, Disponibilité (CID). Une vulnérabilité est une faiblesse dans un système qui peut être exploitée par une menace (intentionnelle ou accidentelle) pour causer un dommage[5]. Le risque est la probabilité qu'une menace exploite une vulnérabilité, multipliée par l'impact potentiel.

Nous adoptons une typologie des vulnérabilités en trois dimensions, largement reconnue dans la littérature[6]:

2.2.1. Vulnérabilités Techniques

Elles sont liées aux faiblesses des infrastructures matérielles et logicielles.

[5] Marchand, J. (2024). Collectivités territoriales, données personnelles et cybersécurité. Lexbase Public.
[6] ISO/IEC 27001:2022.Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

- Obsolescence des équipements : Utilisation de serveurs, postes de travail ou systèmes d'exploitation non supportés par les éditeurs, ne recevant plus de correctifs de sécurité.
- Configuration par défaut ou faible : Mots de passe par défaut, services inutiles ouverts, absence de segmentation réseau.
- Absence de mécanismes de défense : Manque de pare-feu (firewall), de systèmes de détection d'intrusion (IDS) ou de solutions antivirus centralisées et à jour.

2.2.2. Vulnérabilités Humaines

L'utilisateur final est souvent le maillon faible de la chaîne de sécurité.

- Erreur humaine/Négligence : Perte de supports amovibles, utilisation de mots de passe faibles, non-respect des procédures.
- Ingénierie sociale : Succès des attaques de phishing (hameçonnage) ou de spear-phishing visant à obtenir des identifiants ou à installer des logiciels malveillants.
- Manque de formation : Absence de sensibilisation régulière aux menaces et aux bonnes pratiques de sécurité.

2.2.3. Vulnérabilités Organisationnelles et Processus

Elles concernent la gouvernance et la gestion de la sécurité.

- Absence de Politique de Sécurité des Systèmes d'Information (PSSI) : Manque de directives claires sur la gestion des accès, la sauvegarde, la réponse aux incidents.
- Gestion des accès défaillante : Droits d'accès trop larges (principe du moindre privilège non appliqué), non-révocation des accès des employés partants.
- Plan de Continuité d'Activité (PCA) et de Reprise d'Activité (PRA) inexistant : Incapacité à restaurer rapidement les services après un incident majeur (incendie, inondation, cyberattaque).

2.3. Cadres de Sécurisation des Données : Standards Internationaux

Pour proposer des stratégies robustes, il est impératif de se référer aux standards internationaux, qui servent de référence pour l'audit et l'amélioration continue de la sécurité.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

Tableau 1: Principales normes et cadres de référence en cybersécurité et leur pertinence pour l'administration de Kananga

Standard	Objectif Principal	Pertinence pour Kananga
ISO/IEC 27001	Établir, mettre en œuvre, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI).	Fournit un cadre de gouvernance complet, essentiel pour structurer les efforts organisationnels.
NIST Cybersecurity Framework (CSF)	Améliorer la gestion des risques de cybersécurité. Basé sur cinq fonctions : Identifier, Protéger, Détecter, Répondre, Rétablir.	Approche pratique et progressive, adaptable aux ressources limitées des administrations locales.
Règlement Général sur la Protection des Données (RGPD)	Protéger les données personnelles des citoyens de l'Union Européenne.	Bien que non directement applicable, ses principes (minimisation, droit d'accès, sécurité par conception) sont des références éthiques et légales pour la gestion des DCP.

Source **:** *Nous-mêmes à partir des standards internationaux en cybersécurité (ISO/IEC 27001, NIST CSF, RGPD), 2025*.

Commentaire :

Ce tableau présente une comparaison synthétique de trois référentiels majeurs en matière de cybersécurité et démontre leur potentiel d'adaptation au contexte administratif de Kananga.

- *ISO/IEC 27001 offre un cadre méthodologique formel pour instaurer un système de management de la sécurité de l'information. Sa pertinence réside dans sa capacité à structurer de manière durable les processus, ce qui constitue un besoin essentiel dans un environnement où la gouvernance des données reste insuffisamment organisée.*
- *Le NIST Cybersecurity Framework (CSF), avec son approche pragmatique articulée autour des fonctions* Identifier, Protéger, Détecter, Répondre et Rétablir, *représente une alternative flexible. Son adaptabilité en fait un outil particulièrement pertinent pour les administrations disposant de ressources limitées, comme c'est le cas à Kananga.*
- ***Le RGPD**, bien qu'applicable juridiquement à l'Union européenne, apporte des principes fondamentaux sur la protection des données personnelles. Ses exigences – sécurité dès la conception, minimisation des données, droits des personnes – constituent des références universelles pouvant inspirer la mise en place de bonnes pratiques locales pour la gestion des données à caractère personnel (DCP).*

Dans l'ensemble, ces standards constituent une base stratégique pour renforcer la sécurité des systèmes d'information et améliorer la maturité numérique de l'administration étudiée.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

L'application de ces cadres à Kananga doit être progressive et pragmatique, en privilégiant les mesures à faible coût et à fort impact, comme la sensibilisation et la formalisation des procédures.

3. Contexte de l'Étude : L'Hôtel de Ville de Kananga

3.1. Présentation de la Ville de Kananga.

3.1.1. Aperçu historique de la Ville de Kananga.

a) Date de la création

Kananga a été érigé en Ville par l'Ordonnance n° 092/357 du 06/09/1958 du Gouverneur général de la Colonie belge.

b) Evolution dénominative.

1) 1958 à 1972 : Ville de Luluabourg.
2) 1972 à 1976 : Sous-Région urbaine de Kananga (Loi n° 77-028 du 19/02/1982).
3) 1998 à nos jours : Ville de Kananga (Décret-Loi n° 089 du 02/07/1998).

La Ville de Kananga est située dans la province du Kasaï-Central, en République Démocratique du Congo (RDC). Elle est non seulement un Centre administratif et économique important de la région, mais elle a également une histoire marquée par les bouleversements politiques et sociaux qui ont façonné la RDC au fil des années. La mairie de Kananga, en tant qu'entité administrative, a joué un rôle central dans la gestion locale, la gouvernance et l'organisation de la Ville.

c) Origines et fondation de Kananga.

Le nom "**Kananga**" a plusieurs origines possibles, mais l'histoire de la Ville remonte à la période précoloniale, où elle était un centre important du Royaume Kuba. Kananga était alors un point de convergence pour les différents clans de la région, notamment ceux du groupe ethnolinguistique Luba.

Cependant, c'est à l'époque coloniale, sous le régime belge, que Kananga a commencé à se développer comme une ville administrativement organisée. Elle a été fondée au début du 20ème siècle comme une petite localité de commerce et d'administration, avant de devenir un Centre plus vaste au fil des décennies.

L'explorateur allemand Hermann Wißmann fonda en 1884 la station de Luluabourg, située sur la rive droite de la rivière Lulua. Les Luba s'orientent en regardant en tête, en amont, c'est-à-dire la source d'une rivière. Le deuxième nom de ce poste aussi répandu que le premier était Malandji-a-Nshinga. Il est possible que ce nom de Malandji ait été suggéré par les 400 porteurs originaires de Malange en Angola. Mais il faudrait noter que cette hypothèse popularisée par les manuels scolaires n'explique rien, car le nom *Malandji*, singulier *Dilandji* "limace, limacon" et "réflexion, recherche" (provenant du verbe -*landa*), est Luba et que beaucoup de ces porteurs parlaient la langue Luba. En plus, on rencontre beaucoup de noms topographiques communs dans le Kasaï et en Angola. Après l'extension de Luluabourg de l'autre côté de la rive, donc sur la rive gauche de la Lulua, l'ancien emplacement continua à s'appeler Malandji-Makulu (ancienne Malandji), nom conservé jusqu'à nos jours. Toutefois le nom de Malandji-Makulu souligne que la

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

nouvelle extension de Luluabourg est Malandji-Mapya-mapya (Nouvel Malandji), appelé aussi Malandji-a-Nshinga (Malandji de lignes de communication).

Lors de la Table Ronde de Bruxelles où fut négociée l'indépendance du Congo, les différents représentants congolais s'étaient mis d'accord pour déplacer la capitale de Léopoldville à Luluabourg à cause de sa position centrale. Sous la conduite du sécessionniste Albert Kalonji, la province du Sud-Kasai déclara son indépendance en 1960. La capitale en était Bakwanga (aujourd'hui Mbuji-Mayi). 1962 vit le retour de la province sous le contrôle du gouvernement de Kinshasa. Luluabourg demeurera toujours la capitale du Kasaï-Occidental.

MOBUTU SESE SEKO rebaptisa la Ville Kananga, appellation d'origine et ignorée par le pouvoir colonial. Et même, quand le capitaine Adolphe de Macar fit déplacer Malandji, la population, elle, appelait la Ville Kananga-Malandji wa Nshinga (wa Nshinga = des câbles électriques). Le successeur de Macar fut le capitaine Léon Braconnier qui fit prospérer grandement la région en intensifiant les cultures de riz, de maïs, de sorgho et en favorisant l'accroissement du gros et du petit bétail, faisant de cette ville le centre de distribution de toute la région voisine. Il œuvra à l'amélioration des conditions de vie des Blancs et des Noirs, notamment par la construction d'habitations en briques. Ce fut également lui qui eut l'idée d'établir les premiers impôts en nature.

d) Période coloniale.

Pendant la colonisation belge, Kananga était d'abord un poste administratif dans le secteur des mines et de l'exploitation des ressources naturelles, en particulier du cuivre et du cobalt. La ville est devenue un centre commercial et administratif important de la province du Kasaï, contribuant à l'essor économique de la région. La structure administrative mise en place par les autorités coloniales a favorisé l'émergence de Kananga en tant que point de ralliement politique et administratif.

C'est également à cette époque que la ville a été dotée d'une administration municipale, avec des structures locales représentant l'autorité coloniale belge. La mairie de Kananga était sous le contrôle direct de l'administration coloniale, et la population locale avait un rôle limité dans la gestion de la ville.

3.1.2. Aperçu géographique et administratif de la Ville de Kananga.

1°) Aperçu géographique.

La Ville de Kananga, notre cadre de recherche, est l'une de deux villes que compte la Province du Kasaï Central. Anciennement appelée Luluabourg, Kananga est une ville comptant plus de 2.000.000 d'habitants. Elle est la capitale de la Province du Kasaï-Central et le siège de l'Archidiocèse de Kananga. Elle est située à proximité de la rivière Lulua sur la route nationale n° 1 à 1093 km à l'Est de la Capitale Kinshasa.

La Ville de Kananga est située au cœur de la République Démocratique du Congo à 523km de latitude Sud et de 25° de longitude Est. Par sa position géographique, elle est bâtie au centre de la Province du Kasaï Central. Elle est enclavée et située à environ 800km de Kisangani, de Lubumbashi et environ 1000km de Kinshasa la Capitale.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

a) Limites

La Ville de Kananga est bornée de la manière ci-dessous :

- Au Nord par le Territoire de Demba ;
- Au Sud par le Territoire de Dibaya ;
- A l'Est par le Territoire de Dimbelenge ;
- A l'Ouest par le Territoire de Kazumba.

b) Climat.

La Ville de Kananga jouit d'un climat tropical chaud et humide caractérisé par deux saisons contrastées : la saison de pluie et la saison sèche. Sa pluviométrie est de 675mm.

c) Saisons

La Ville de Kananga a deux saisons : une sèche qui dure 3 mois allant du 15 mai au 15 août et une autre pluvieuse qui couvre 9 mois allant du 15 août au 15 mai.

d) Sol

Son sol est sablo-argileux avec une topographie très accidentée couverte de quelques érosions et ravins qui cernent dangereusement et menacent la Ville.

e) Superficie.

Chef-lieu de la Province du Kasaï Central comptant 348.399 électeurs recensés en 2023. Sa superficie totale est de **847Km²**.

f) Population et Densité.

La Ville de Kananga compte une population estimée à **2.011.557** en **2022**, cela donne une **densité** de l'ordre de **1.334,24 Hab/Km²** (TSHILEMBI, 2015 cité par NYOKA, 2020 et MUAMBA, 2022).

Evolution de la population de la Ville de Kananga au cours de trois dernières années :

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

Tableau 2 : Evolution de la population

Année / Population	2022	2023	2024	Population moyenne
Population congolaise				
Hommes	385.109	381.345	402.135	**389.529,67**
Femmes	445.255	445.500	435.250	**442.001,67**
Garçons	875.125	793.007	850.240	**839.457,33**
Filles	914.345	896.646	903.320	**904.770,33**
Total population	**2.619.834**	**2.516.498**	**2.590.945**	**2.575.759**
Population étrangère				
Hommes	267	235	341	**281,00**
Femmes	23	14	34	**23,67**
Garçons	5	7	12	**8,00**
Filles	4	5	14	**7,70**
Total pop. étrangère	**299**	**261**	**401**	**320,33**

Source : nous-mêmes

Commentaire :

A la lumière des données du tableau ci-dessus, la population de la Ville de Kananga a évolué de la manière suivante :

- En 2022, la Ville a regorgé une population totale de **2.619.834** constituée de 385.109 hommes, 445.255 femmes, 875.125 garçons et 914.345 filles plus une population étrangère totale de **299** constituée de 267 hommes, 23 femmes, 5 garçons et 4 filles ;
- En 2023, la Ville a regorgé une population totale de **2.516.498** constituée de 381.345 hommes, 445.500 femmes, 793.007 garçons et 896.646 filles plus une population étrangère totale de **261** constituée de 235 hommes, 14 femmes, 7 garçons et 5 filles ;
- En 2024, la Ville a regorgé une population totale de **2.590.945** constituée de 402.135 hommes, 435.250 femmes, 850.240 garçons et 903.320 filles plus une

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

population étrangère totale de **401** constituée de 341 hommes, 34 femmes, 12 garçons et 14 filles ;

- La population moyenne a évolué comme suit :
  - **2.575.759 p**our la population originaire dont **389.529,67** hommes, **442.001,67** femmes, **839.457,33** garçons, **904.770,33** filles ;
  - **320,33 p**our la population étrangère dont **281,00** hommes, **23,67** femmes, **8,00** garçons, **7,70** filles ;

g) Ethnographie.

Kananga comme ville héberge une population hétérogène à l'instar d'auto-ville du monde. Elle est habitée en grande partie par : les Lulua très majoritaires ainsi que les Luntu, les Bindji, les Otetela, les Songues, les Kuba, les Shilele, les Balubas, les Lubilanji, les Sala-Mpasu, et plusieurs autres groupes ethniques. Ce qui confère à cette dernière le caractère cosmopolite.

h) Relief et hydrographie

La Ville de Kananga se trouve sur le plateau du Kasaï et, est entrecoupée par des vallées humides. Elle dispose des cours d'eau suivants :

- ❖ Tshibashi : Qui est alimenté des eaux de Lungandu, Ndesha, Kamilabi et Malole ;
- ❖ Nganza : Qui est aussi alimenté par Katoka ;
- ❖ Le Sude-Est : est drainé par les rivières Lubi, Nkombua et Lulua coulant vers l'Ouest.

i) Végétation.

La végétation de la Ville de Kananga est appauvrie et menacée par les activités humaines dans sa périphérie (coupe de bois). Au départ la savane boisée qui cède à la savane herbeuse. Enfin, la galerie forestière le long des rivières (Lulua, Tshibashi, Muanza-Ngoma, …). Cette menace est permanente par le fait que la population coupe les bois pour fabriquer les braises, les briques cuites, les champs, etc. (Source : Service d'archives de la Commune de Kananga**)**.

j) Langues

Nous avons les langues suivantes :

- Français (langue officielle administrative) ;
- Tshiluba, Swahili, Lingala, Otetela, Anglais ;
- Une minorité des langues locales.

3.1.3. Structure organisationnelle de l'Hôtel de Ville de Kananga.

La structure organisationnelle est comprise en son organisation administrative telle que présentée dans les lignes qui suivent.

a) Conseil consultatif de la Ville

Les dispositions du Décret-loi n° 81 du 21 juillet 1998 de l'organisation des élections territoriales et administratives en RDC ont été respectées pour la première fois à l'issue des scrutins du 20 décembre 2023. Il reste que l'installation de son organe délibérant et l'élection de Maire et son Adjoint par le Conseil Urbain. La structure organisationnelle de la Ville de Kananga se présente de la manière suivante :

- Conseil Urbain (1),
- Mairie de la Ville (1),
- Communes (5)

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

- Quartiers (27),
- Avenues,
- Groupements incorporés (23),
- Villages (154).

3.1.4. Siège social Ville de Kananga.

Le siège social de l'Hôtel de Ville de Kananga est situé sur l'avenue de la Mission en pleine Ville de Kananga en allant vers la rivière Nganza.

3.1.5. Mission de l'Hôtel de Ville de Kananga.

L'Hôtel de Ville ou la Mairie est responsable de :

- La gestion des affaires municipales ;
- La planification urbaine ;
- La construction des infrastructures urbaines ;
- La santé ;
- L'éducation ;
- La sécurité ;
- Etc.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

3.2. Organigramme de la Mairie de Kananga

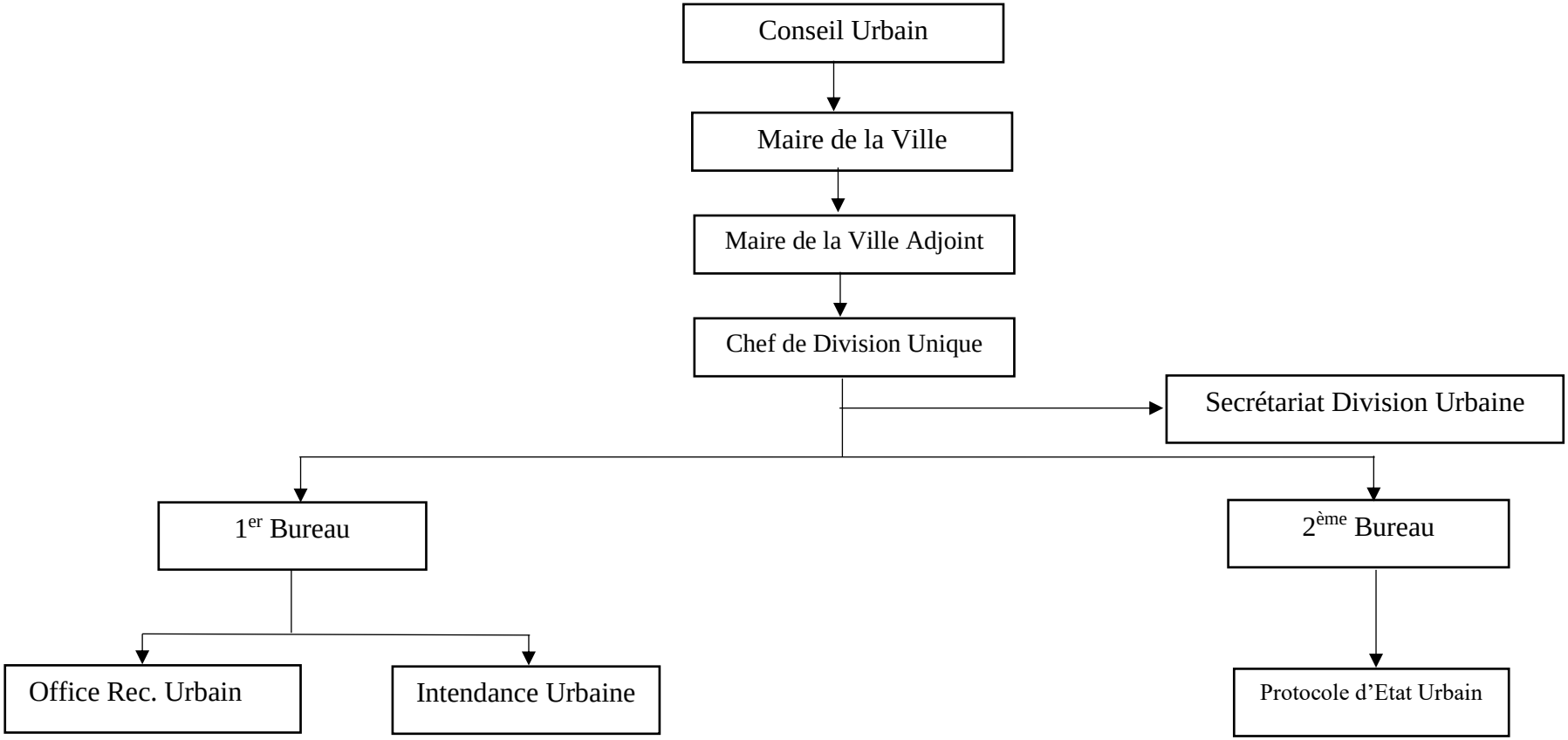


Figure 1 Organigramme générale de la Mairie de Kananga

Source : Rapport annuel de la Mairie de Kananga exercice 2023

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

3.2.1. L'Environnement Numérique en RDC

La RDC a pris des mesures significatives pour structurer son espace numérique, reconnaissant le rôle du secteur dans le développement économique et social.

3.2.2. Cadre Légal et Stratégique

- Plan National du Numérique (PNN) – Horizon 2025 : Vise à faire du numérique un levier de croissance. Il met l'accent sur l'infrastructure, la gouvernance et le contenu.
- Stratégie Nationale de Cybersécurité (SNC) 2022-2025 : Ce document reconnaît explicitement la vulnérabilité du cyberespace congolais et propose des axes stratégiques, notamment la création d'un cadre légal et institutionnel, et le renforcement des capacités[7].
- Code du Numérique : Ce cadre légal régit les activités numériques, y compris la protection des données personnelles et la lutte contre la cybercriminalité.

3.2.3. Défis de l'Infrastructure

Malgré ces avancées, l'infrastructure numérique en RDC, particulièrement en dehors de Kinshasa, reste limitée [9].

- Connectivité : L'accès à l'Internet est en augmentation, notamment via le mobile, mais la qualité et la stabilité de la connexion dans les administrations publiques peuvent être erratiques.
- Énergie : Les coupures de courant fréquentes et l'instabilité du réseau électrique constituent une menace majeure pour la disponibilité des SI, nécessitant des investissements coûteux en onduleurs et générateurs.
- Expertise : Il existe une pénurie d'experts en cybersécurité qualifiés, ce qui rend la maintenance et la sécurisation des systèmes souvent externalisées ou gérées par du personnel non spécialisé.

3.3. Synthèse Contextuelle pour l'Analyse

Le contexte de Kananga se caractérise par une volonté politique de numérisation (alignée sur le PNN) confrontée à une réalité opérationnelle de contraintes fortes (infrastructure, énergie, ressources humaines). L'étude exploratoire doit donc se concentrer sur les vulnérabilités typiques des SI en phase d'informatisation générale ou partielle dans un environnement à ressources limitées.

[7] Organisation internationale de normalisation.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

4. Analyse Exploratoire des Vulnérabilités Potentielles à l'Hôtel de Ville de Kananga

L'analyse suivante est une extrapolation basée sur les vulnérabilités génériques des SI municipaux (Section 2) appliquées aux contraintes contextuelles de Kananga (Section 3).

4.1. Vulnérabilités Techniques Critiques

Les vulnérabilités techniques sont les plus tangibles et souvent les plus coûteuses à corriger.

4.1.1. Obsolescence et Hétérogénéité du Parc Informatique

Nos investigations ont révélé que, l'Hôtel de Ville de Kananga utilise un parc informatique hétérogène, souvent composé des matériels provenant de dons ou d'achats ponctuels. La plupart de ces matériels sont caractérisés par :

- Systèmes d'exploitation non patchés : Utilisation de versions de Windows ou de logiciels qui ne reçoivent plus de mises à jour de sécurité (End-of-Life). Ces systèmes contiennent des failles connues et facilement exploitables par des outils automatisés.
- Absence de licences logicielles : L'utilisation de logiciels piratés ou sans licence expose non seulement à des risques légaux, mais aussi à l'installation de versions modifiées ou infectées par des malwares.
- Infrastructure réseau non sécurisée : Utilisation de routeurs/commutateurs de base, sans gestion centralisée, ni segmentation (VLAN) entre les différents services (état civil, finances, etc.). Un seul point de compromission peut mener à l'accès à l'ensemble du réseau.

4.1.2. Défauts de Sauvegarde et de Continuité

La menace la plus critique pour un SI municipal est la perte de données ou d'informations (registres d'état civil, cadastre).

- Sauvegardes non testées ou inexistantes : Les données sont souvent sauvegardées sur des disques durs externes moins sécurisés ou pas du tout. En cas de sinistre (incendie, panne matérielle, ransomware), la reprise d'activité est impossible.
- Absence de protection contre les surtensions : L'instabilité électrique, fréquente à Kananga, peut causer des dommages matériels irréversibles aux serveurs et aux postes de travail, menaçant la disponibilité des services.

4.2. Vulnérabilités Humaines et Culturelles

Dans un contexte où la culture numérique est en émergence, les vulnérabilités humaines sont amplifiées.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

4.2.1. Faible Sensibilisation à la Cybersécurité

Le personnel administratif, souvent formé aux méthodes traditionnelles, peut ne pas percevoir la gravité des menaces numériques.

- Utilisation de mots de passe faibles : Mots de passe simples, réutilisation du même mot de passe pour des applications professionnelles et personnelles.
- Comportement à risque : Ouverture de pièces jointes suspectes, navigation sur des sites non professionnels, connexion d'appareils personnels non sécurisés au réseau de la mairie.
- Ingénierie sociale : Le personnel est une cible facile pour les tentatives d'hameçonnage, car il manque de formation pour identifier les courriels frauduleux ou les appels d'usurpation d'identité.

4.2.2. Problèmes de Gestion des Privilèges

- Partage de comptes : L'utilisation de comptes génériques ou le partage de mots de passe entre collègues rend l'audit et la traçabilité des actions impossibles.
- Privilèges excessifs : Les utilisateurs ont souvent des droits d'accès bien supérieurs à ce qui est nécessaire pour leurs fonctions (principe du moindre privilège non appliqué), augmentant l'étendue des dommages en cas de compromission de leur compte.

4.3. Vulnérabilités Organisationnelles et de Gouvernance

Ces faiblesses sont souvent les plus profondes car elles nécessitent un engagement de la haute direction.

4.3.1. Absence de Politique de Sécurité Formelle

Sans une Politique de Sécurité des Systèmes d'Information (PSSI) officielle, les actions de sécurisation sont sporadiques et incohérentes.

- Manque de procédures claires : Absence de protocoles pour l'installation de nouveaux logiciels, la gestion des incidents, ou la mise à jour des systèmes.
- Rôle de RSSI non défini : L'absence d'un Responsable de la Sécurité des Systèmes d'Information (RSSI) ou d'une cellule dédiée signifie que la sécurité n'est pas une responsabilité centrale et continue.

4.3.2. Dépendance Externe et Manque de Maîtrise

Dans un contexte de pénurie d'experts, la maintenance et le développement sont souvent confiés à des prestataires externes.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

- Dépendance non maîtrisée : L'Hôtel de Ville peut dépendre entièrement d'un prestataire sans disposer des compétences internes pour auditer ou vérifier la sécurité des solutions fournies.
- Documentation insuffisante : Les configurations et les architectures sont rarement documentées, rendant la reprise en main ou la résolution de problèmes complexes et coûteuse.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

4.4. Synthèse des Risques et Impacts Potentiels

Le tableau 3 synthétise les risques majeurs découlant de ces vulnérabilités pour l'Hôtel de Ville de Kananga.

Tableau 3 : Synthèse des Vulnérabilités, Menaces et Impacts Potentiels à Kananga

Vulnérabilité Critique	Menace Associée	Impact Potentiel	Niveau de Risque Estimé
Obsolescence technique	Attaque par rançongiciel (Ransomware)	Interruption totale des services (état civil, fiscalité), perte de données critiques.	Élevé
Faible sensibilisation	Hameçonnage (Phishing)	Vol d'identifiants, accès non autorisé aux bases de données, fraude financière.	Élevé
Instabilité électrique	Panne matérielle/Corruption de données	Perte irréversible des registres d'état civil non sauvegardés, indisponibilité prolongée.	Très Élevé
Absence de PSSI	Erreurs internes, fuite de données	Non-conformité légale (Code du Numérique RDC), atteinte à la réputation, sanctions.	Modéré à Élevé
Partage de comptes	Malveillance interne ou externe	Difficulté à identifier l'auteur d'une modification ou d'une suppression de données.	Modéré

Source : *Nous-mêmes à partir des données collectées auprès des services administratifs de Kananga et des référentiels internationaux d'analyse de risques (ISO 27005, NIST SP 800-30), 2025.*

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

Commentaire :

Ce tableau met en évidence les principales failles de sécurité rencontrées dans les services publics de Kananga et montre comment celles-ci se traduisent en menaces concrètes et en impacts potentiellement graves pour le fonctionnement administratif.

- *L'obsolescence technique constitue une vulnérabilité critique qui expose les systèmes à des attaques par rançongiciel. Les conséquences identifiées — interruption des services essentiels et perte de données — démontrent une dépendance élevée à des équipements non mis à jour, ce qui accroît le niveau de risque.*
- *La faible sensibilisation du personnel favorise les attaques d'ingénierie sociale, particulièrement le hameçonnage. Les risques associés incluent la compromission des bases de données et des systèmes de gestion financière, ce qui justifie un niveau de risque élevé.*
- *L'instabilité électrique, très fréquente dans la région, entraîne des pannes matérielles et des corruptions de données, notamment sur les registres d'état civil. L'absence de solutions de sauvegarde fiables rend l'impact potentiellement catastrophique, d'où un niveau de risque très élevé.*
- *L'absence d'une Politique de Sécurité des Systèmes d'Information (PSSI) expose l'administration à des erreurs humaines, à des fuites d'informations et à la non-conformité au Code du Numérique en RDC. Le risque est qualifié de modéré à élevé, car il affecte la gouvernance globale de la sécurité.*
- *Le partage de comptes utilisateurs accroît la vulnérabilité aux actes de malveillance interne ou externe. Cette pratique compromet la traçabilité des actions, rendant difficile l'identification des auteurs d'incidents, ce qui maintient un niveau de risque modéré.*

Dans l'ensemble, le tableau souligne la nécessité urgente d'une modernisation technologique, d'une politique de sécurité formalisée et d'un programme systématique de renforcement des capacités humaines pour réduire la surface d'exposition aux risques.

5. Stratégies de Sécurisation des Données : Propositions pour Kananga

Les stratégies proposées doivent être réalistes, progressives et alignées sur les capacités budgétaires et humaines de l'administration de Kananga, tout en s'inspirant des principes des cadres ISO 27001 et NIST.

5.1. Axe 1 : Renforcement Technique et Infrastructurel

L'objectif est de garantir la disponibilité et l'intégrité des données essentielles.

5.1.1. Priorité à la Sauvegarde (Le "3-2-1" Adapté)

La mesure la plus critique est la mise en place d'une politique de sauvegarde fiable et testée.

- **Règle 3-2-1 simplifiée :** Avoir au moins trois copies des données (l'originale et deux sauvegardes), sur au moins deux types de supports différents, dont au moins une copie hors site (ou déconnectée/hors ligne).

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

- **Protection contre l'instabilité électrique :** Investissement dans des onduleurs (UPS) de qualité pour tous les équipements critiques (serveurs, routeurs) et mise en place de procédures d'arrêt d'urgence en cas de coupure prolongée.

5.1.2. Gestion des Correctifs et des Logiciels

- **Inventaire et Standardisation :** Réaliser un inventaire précis du parc informatique. Standardiser les systèmes d'exploitation sur une version supportée (même si c'est une distribution Linux gratuite et sécurisée pour les postes de travail non critiques).
- **Mise à jour :** Mettre en place une procédure simple de mise à jour régulière des systèmes d'exploitation et des applications critiques (patch management).

5.1.3. Sécurité Périmétrique de Base

- **Pare-feu :** Déployer un pare-feu de base pour filtrer le trafic entrant et sortant, n'autorisant que les services strictement nécessaires.
- Antivirus Centralisé : Déployer une solution antivirus/anti-malware sur tous les postes de travail et serveurs, avec des mises à jour automatiques.

5.2. Axe 2 : Capital Humain et Sensibilisation

L'investissement dans le facteur humain est le plus rentable à court terme.

5.2.1. Programme de Sensibilisation Continu

- **Formation Initiale et Annuelle :** Organiser des sessions de formation obligatoires pour tout le personnel sur les fondamentaux de la cybersécurité : gestion des mots de passe, identification du phishing, protection des données personnelles.
- **Affichage et Rappels :** Utiliser des affiches et des courriels de rappel réguliers sur les bonnes pratiques (ex. : "Ne jamais ouvrir une pièce jointe d'un expéditeur inconnu").

5.2.2. Renforcement des Politiques de Mots de Passe et d'Accès

- Mots de passe forts : Imposer l'utilisation de mots de passe complexes (longueur minimale, mélange de caractères) et leur renouvellement régulier.
- Principe du Moindre Privilège : Réviser les droits d'accès de chaque utilisateur pour s'assurer qu'ils n'ont accès qu'aux données et aux applications strictement nécessaires à l'exécution de leurs tâches.

5.3. Axe 3 : Gouvernance et Alignement Stratégique

Ces mesures assurent la pérennité des efforts de sécurisation.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

5.3.1. Adoption d'une Politique de Sécurité (PSSI Simplifiée)

L'Hôtel de Ville doit formaliser une PSSI, même si elle est initialement succincte.

- **Nomination d'un Référent Sécurité :** Désigner un agent (même à temps partiel) comme Référent Sécurité des Systèmes d'Information (RSSI), chargé de la mise en œuvre et du suivi des politiques de sécurité.
- **Procédures d'Incident :** Établir une procédure simple pour signaler et gérer les incidents de sécurité (qui contacter, quelles actions immédiates prendre).

5.3.2. Alignement avec le Cadre National

- **Conformité au Code du Numérique :** S'assurer que la collecte et le traitement des données personnelles respectent les dispositions du Code du Numérique de la RDC, notamment en matière de consentement et de sécurité.
- **Collaboration :** Établir des canaux de communication avec les autorités nationales de cybersécurité (si elles existent ou sont en cours de création dans le cadre de la SNC) pour partager les informations sur les menaces et bénéficier de l'expertise centrale.

6. Conclusion, Limites et Perspectives

6.1. Conclusion

Cette étude exploratoire a permis d'analyser les vulnérabilités potentielles du système d'information de l'Hôtel de Ville de Kananga, en les contextualisant dans l'environnement numérique de la RDC. Les résultats confirment que les risques majeurs ne sont pas seulement techniques, mais résident également dans les dimensions humaines et organisationnelles. L'obsolescence des infrastructures, le manque de sensibilisation du personnel et l'absence de politiques de sécurité formelles constituent une menace sérieuse pour la confidentialité, l'intégrité et la disponibilité des données municipales critiques.

Les stratégies de sécurisation proposées insistent sur une approche progressive et pragmatique :

- ✓ **Priorité à la résilience :** Mise en place immédiate de solutions de sauvegarde fiables et de protection contre les aléas électriques.
- ✓ **Investissement humain :** Formation et sensibilisation continues du personnel.
- ✓ **Gouvernance :** Formalisation d'une PSSI simplifiée et alignement sur le Code du Numérique de la RDC.

En adoptant ces mesures, l'Hôtel de Ville de Kananga peut non seulement se protéger contre les cybermenaces courantes, mais aussi renforcer la confiance des

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

citoyens dans la numérisation des services publics, contribuant ainsi à la modernisation de la gouvernance locale.

6.2. Limites de l'Étude

La principale limite de cette étude est son caractère exploratoire et non empirique. L'analyse des vulnérabilités est basée les défis généraux des administrations locales en RDC et des meilleures pratiques à adopter, et sur un audit technique direct du SI de l'Hôtel de Ville de Kananga.

La difficulté que nous pouvons signaler en passant est telle que, autres données essentielles et précises sur l'architecture réseau, les logiciels utilisés et les incidents passés n'étaient pas accessibles.

6.3. Perspectives de Recherche

Pour approfondir cette thématique, plusieurs pistes de recherche futures sont recommandées :

- ✓ Audit Empirique : Mener un audit de sécurité technique et organisationnel sur site à l'Hôtel de Ville de Kananga pour valider les vulnérabilités identifiées et quantifier les risques.
- ✓ Étude Comparative : Comparer les stratégies de sécurisation et les niveaux de maturité en cybersécurité entre plusieurs administrations locales en RDC (ex. : Kananga, Mbuji-Mayi, Kisangani) pour identifier les facteurs de succès et d'échec.
- ✓ Développement d'un Cadre de Maturité : Élaborer un modèle de maturité en cybersécurité spécifiquement adapté aux collectivités territoriales africaines à faibles ressources, permettant une évaluation et une amélioration continues.

BIBLIOGRAPHIE

1. ANSSI/AMF. (2020). Guide de la cybersécurité pour les communes et intercommunalités. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).
2. CERT-FR. (2025). Alerte sur les cybermenaces contre les collectivités territoriales. Centre Gouvernemental de Veille, d'Alerte et de Réponse aux Attaques Informatiques.
3. Gauthier, M. H. (2025). De la différenciation à la coopération territoriale pour valoriser les données: légitimité, enjeux et implication des Régions. Journées Doctorales de l'Association de Science Régionale de Langue Française.
4. Présidence de la RDC. (2023).Stratégie Nationale de Cybersécurité 2022-2025.
5. Marchand, J. (2024). Collectivités territoriales, données personnelles et cybersécurité. Lexbase Public.

ISSN: 3136-2648 (Version imprimée)
ISSN: 3136-2656 (Version digitale) | Volume 1, n°4 - Août 2026
DOI : 10.66405/3136-2656.recodd.v1.4.5

6. ISO/IEC 27001:2022.Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences. Organisation internationale de normalisation.
7. NIST. (2018).Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.
8. Mémoire Online. (2018).Conception et réalisation d'une base de données pour la gestion des équipements informatiques à la Mairie de Kananga.
9. Présidence de la RDC. (2019). Plan National du Numérique – Horizon 2025.
10. Verdi, U. (2023). L'éthique des données dans les chartes éthiques des collectivités territoriales. Communication & Organisation, (2), 51-68.