International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122

Importance de la Cybersécurité dans la Gestion des Données Administratives et Pédagogiques de l'Institut Supérieur Pédagogique de Mbandaka

[Importance of Cybersecurity in the Management of Administrative and Academic Data at the Higher Institute of Pedagogical of Mbandaka]

MPUTSHU BONYOMA Francis[1] ; MPAO IFUFA Junior[1] ; KASI OTAWA Ruphin[1] ; MATONDO FALANGA Junior[1,3] ; MAYALA LEMBA Francis[2,]

[1]Institut Supérieur Pédagogique de Mbandaka
[2]Université Pédagogique Nationale, Kinshasa
[3]Centre de Recherche en Eau et Environnement
République Démocratique du Congo

Résumé : La transformation numérique du secteur de l'enseignement supérieur en République Démocratique du Congo expose les institutions académiques à des risques accrus de cybersécurité. Cette étude menée à l'ISP Mbandaka a pour objectif d'évaluer la gestion des données administratives et pédagogiques, d'identifier les vulnérabilités critiques et de proposer des stratégies d'amélioration. À travers un dispositif méthodologique combinant enquête par questionnaire auprès de 25 agents, entretiens semi-directifs et audit technique, les résultats révèlent une forte exposition aux cybermenaces : absence de Politique de Sécurité du Système d'Information (PSSI), déficit de formation, infrastructures obsolètes et absence de mécanismes de contrôle d'accès. Les recommandations proposées s'alignent sur les normes internationales telles que le NIST et l'ISO 27001, afin de renforcer la gouvernance numérique et la résilience du système d'information de l'ISP Mbandaka.

Mots clés : cybersécurité, gestion, base de données, ISP

Abstrat : The digital transformation of the higher education sector in the Democratic Republic of the Congo exposes academic institutions to increased cybersecurity risks. This study conducted at ISP Mbandaka aims to assess the management of administrative and academic data, identify critical vulnerabilities, and propose improvement strategies. Using a methodological approach combining a questionnaire survey of 25 staff members, semi-structured interviews, and a technical audit, the results reveal a high exposure to cyber threats: the absence of an Information System Security Policy (ISSP), lack of training, obsolete infrastructure, and the absence of access control mechanisms. The proposed recommendations align with international standards such as NIST and ISO 27001, with the objective of strengthening digital governance and the resilience of the information system at ISP Mbandaka.

Keywords: Cybersecurity, Management, Database, ISP.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122

I. INTRODUCTION

La digitalisation des systèmes académiques et administratifs constitue aujourd'hui une nécessité pour les établissements d'enseignement supérieur en RDC. [1] À l'ISP Mbandaka, cette transition se manifeste par l'usage croissant des outils numériques pour la gestion des dossiers du personnel, des états de paie, des notes, des délibérations et de l'inscription en ligne. Toutefois, cette opportunité s'accompagne de défis importants liés à la cybersécurité.

La littérature congolaise et internationale signale plusieurs facteurs de vulnérabilité, notamment : l'insuffisance des moyens techniques, le manque de formation, l'utilisation d'équipements obsolètes et l'absence de cadres réglementaires opérationnels. Alors que [1] et [2] soulignent la fragilité du numérique dans les institutions provinciales, [3] évoque la faible culture de cybersécurité dans les milieux académiques.

Face à ces constats, la présente étude vise à répondre à la question suivante : Quelle est l'importance de la cybersécurité dans la gestion des données administratives et pédagogiques de l'ISP Mbandaka, et quelles mesures doivent être priorisées pour renforcer la sécurité de son système d'information ?

Plus spécifiquement, l'étude cherche à :

- Évaluer l'état actuel de gestion des données au sein de l'ISP ;
- Identifier les risques et vulnérabilités présents dans le système d'information ;
- Proposer des recommandations adaptées au contexte institutionnel.

II. MATERIEL ET METHODES

2.1. Milieu d'étude

L'Institut Supérieur Pédagogique est situé dans l'avenue IPEKO n°03, commune de Wangata/Mbandaka.

L'ISP/Mbandaka est la première institution de formation supérieure de la grande province de l'équateur. Il est démarré ses activités en 1968, le tout premier diplômé en 1970 du département de français à cette époque il n'eut qu'un seul cycle, graduat. Le premier diplômé en licence été de l'année 1976-1977 en sciences exactes au département de math-physique. La plupart des enseignants au début de sa création étaient des expatriés des différentes nationalités : belge, français…

En effet, le 09 Décembre 1963 le Gouverneur de province de la cuvette centrale exprima devant l'assemblée provinciale l'idée de la création d'une régence à Mbandaka, alors coquillâtes ville

La demande de ladite régence qui fut rapidement introduite par la Direction provinciale de l'Enseignement reçue l'accord de principe et même des encouragements du ministre de l'Education Nationale du gouvernement central par la lettre N°EDN/MS/137 du 1er Février 1964. Et le projet fut définitivement agrée par le gouvernement central lors de sa réunion du 20 juillet 1964.

Le nouvel Institution s'installa provisoirement dans l'un de pavillon de l'ex-hôpital Léopold II occupé jadis par l'Ecole Technique Agricole et actuellement par la Sous-Division de l'enseignement primaire et secondaire de Mbandaka I et l'Institut Techniques Commerciale de Bakusu.

L'ouverture de la première année académique fut annoncée, par un communiqué de la Direction Provinciale de l'Enseignement du 20 Février 1964 à la rentrée scolaire de septembre 1964. Mais l'Institut Pédagogique national (IPN). S'empara cette année des candidats de l'Institut Supérieur de Mbandaka et ce dernier ne put fonctionner, faute d'étudiants. Il a fallu attendre quatre ans, soit 15 Janvier 1968 pour que l'ouverture de cet Institution Supérieur (Ecole Normale Moyenne à cette époque) devienne effective.

Et l'inauguration de ISP/Mbandaka, Ecole Normale Moyenne officielle à l'époque eut lieu non pas à l'ex-hôpital Léopold II mais plutôt à l'école Normal Primaire d'Etat, actuellement Institut MOTEYI, à Mbandaka II ou il fonctionna pendant 3 mois avant d'être transféré dans les installations de l'actuelles école d'application de l'ISP/ Mbandaka (EDAP-ISP) pour raison d'exiguïté des locaux.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122

Durant la première année, l'Ecole fonctionna sous la supervision de la Direction Provinciale de l'Enseignement de la province de la cuvette centrale.

Le 20 septembre 1968, Monsieur KATANGA TSHITENGE en fut désigné Directeur Général et trois jours plus tard, c'est-à-dire le 23 septembre de la même année, le nouveau Directeur Général ouvrit la 2ème Année académique.

Trois faits majeurs marquèrent les débuts de l'école Normale Moyenne :

- Le manque de fonds nécessaires pour le fonctionnement de l'établissement
- La brièveté de la première année académique
- Le non sélection des candidats admis.

En effet, le nouvel Institution qui fonctionnait sous la supervision de la Direction Provinciale de l'Enseignement ne disposait pas de budget propre et autonome lui permettant de faire face aux problèmes spécifiques. La première année académique ne durant que six mois.

A partir de l'année académique 1971-1972, à la faveur de la réforme universitaire promulguée par l'ordonnance n°71/075 du 06 Aout 1971, l'Ecole Normale Moyenne Officielle comme toutes les universités et tous les Institut Supérieurs du Zaïre, fut intégré dans la grande Institut d'Enseignement Supérieur dénommé UNIVERSITE NATIONALE DU ZAIRE (UNAZA). L'école Normale Moyenne Officielle devint alors Institut Supérieur Pédagogique de Mbandaka. Et c'est durant cette période de l'UNAZA que l'Institut connut une grande évolution et un grand rayonnement. Comme on pourra remarquer, c'est après son intégration au sein de l'UNAZA que les nombreux départements furent ouverts et fut aussi obtenu l'autorisation de délivrer des diplômes de licence en pédagogie appliquée.

2.2. Méthodologie

L'étude adopte une approche descriptive et analytique.

2.2.1. Population et échantillon

L'enquête a ciblé 25 agents de l'ISP Mbandaka, sélectionnés de manière raisonnée parmi les services sensibles : Secrétariat Académique, Direction Administrative, Comptabilité et Service Informatique.

2.2.2. Instruments de collecte des données

Trois outils principaux ont été utilisés :

- Questionnaire structuré administré aux 25 agents ;
- Entretiens semi-directifs menés auprès de responsables clés ;
- Audit technique rapide comprenant :
    - Inventaire des équipements,
    - État des mises à jour,
    - Vérification des antivirus,
    - Analyse préliminaire des vulnérabilités.

2.2.3. Traitement des données

Les réponses cochées sur les questionnaires d'enquêtes ont été dépouillées sous forme de tableaux, et des graphiques ont été générés afin de faciliter l'interprétation visuelle.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122

III. RESULTATS ET DISCUSSION

3.1. Résultats

3.1.1. Vulnérabilité des données pédagogiques

Les résultats montrent une forte exposition des données sensibles.

Tableau 1 : Où stockez-vous habituellement les données pédagogiques (notes, PV, listes) ?

Réponse	N	F	%
Sur un ordinateur personnel non sécurisé	18	18	**72**
Sur un ordinateur de service	5	5	20
Sur un support externe (clé USB, disque dur)	2	2	8
Total	25	25	100

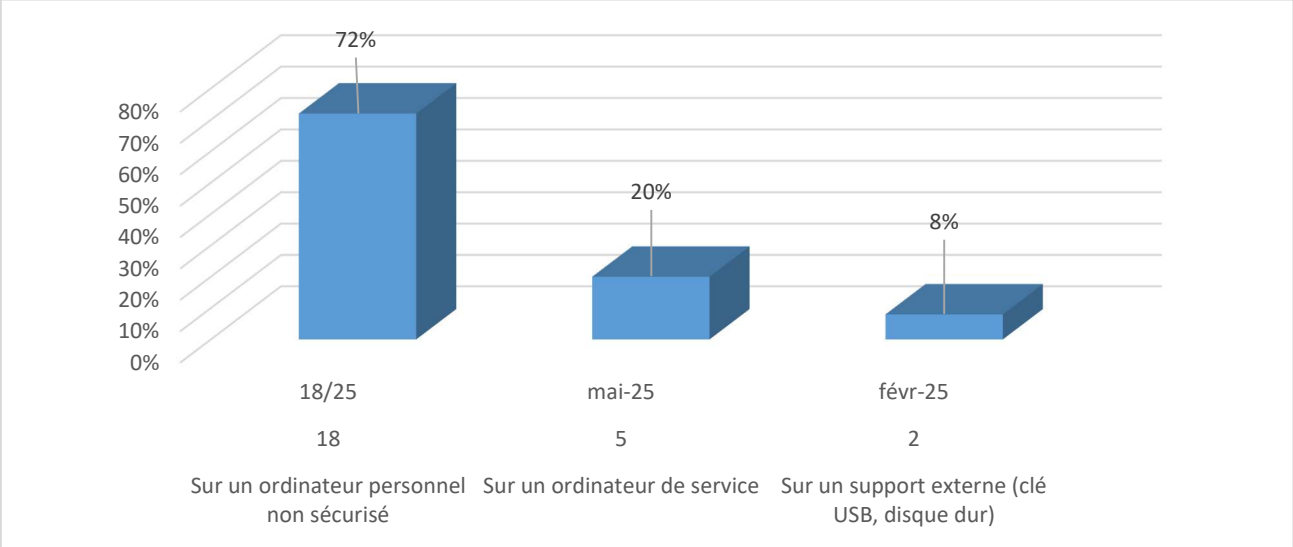


Figure 1 : Stockage habituellement des données pédagogiques

Les résultats montrent clairement que la majorité (72 %) stocke les données sensibles sur des appareils personnels, souvent non protégés. Cela constitue un risque majeur de fuite, perte ou manipulation de données pédagogiques.

Table 2 : Complexité des mots de passe utilisés

Réponse	N	F	%
Mots de passe simples (1234, nom, date de naissance)	19	19	**76**
Mots de passe moyens	4	4	16
Mots de passe complexes (longs + caractères spéciaux)	2	2	8
Total	25	25	100

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122

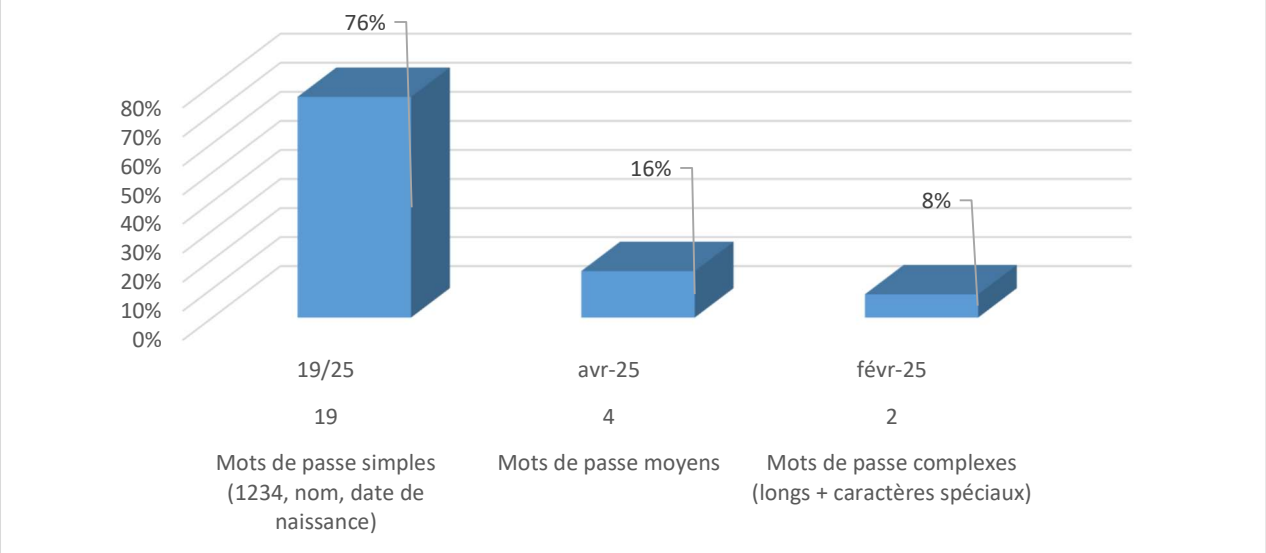


Figure 2 : Complexité des mots de passe utilisés

Environ 76 % des agents utilisent des mots de passe faibles, ce qui augmente considérablement les risques d'accès non autorisé aux systèmes internes.

Table 3 : Existence d'un système de contrôle d'accès centralisé

Réponse	N	F	%
Oui	0	0	0
Non	25	25	**100**

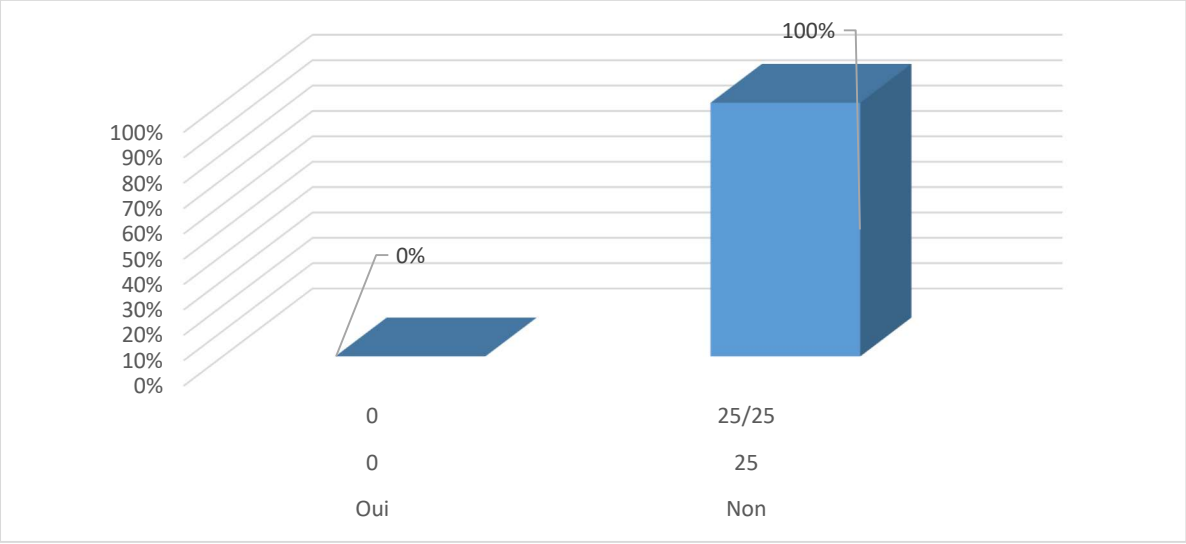


Figure 3 : Existence d'un système de contrôle d'accès centralisé

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122

Le résultat est alarmant : l'ISP Mbandaka ne dispose d'aucun système de contrôle d'accès centralisé. Chaque utilisateur gère son accès individuellement, créant un environnement très vulnérable.

Ces pratiques augmentent considérablement les risques d'altération ou d'accès non autorisé, comme l'ont déjà signalé Kapinga (2022) et Shabani (2018) pour d'autres institutions congolaises.

Table 4 : Avez-vous déjà reçu une formation en cybersécurité ?

Réponse	N	F	%
Oui	3	3	**12**
Non	22	22	88
Total	25	25	100

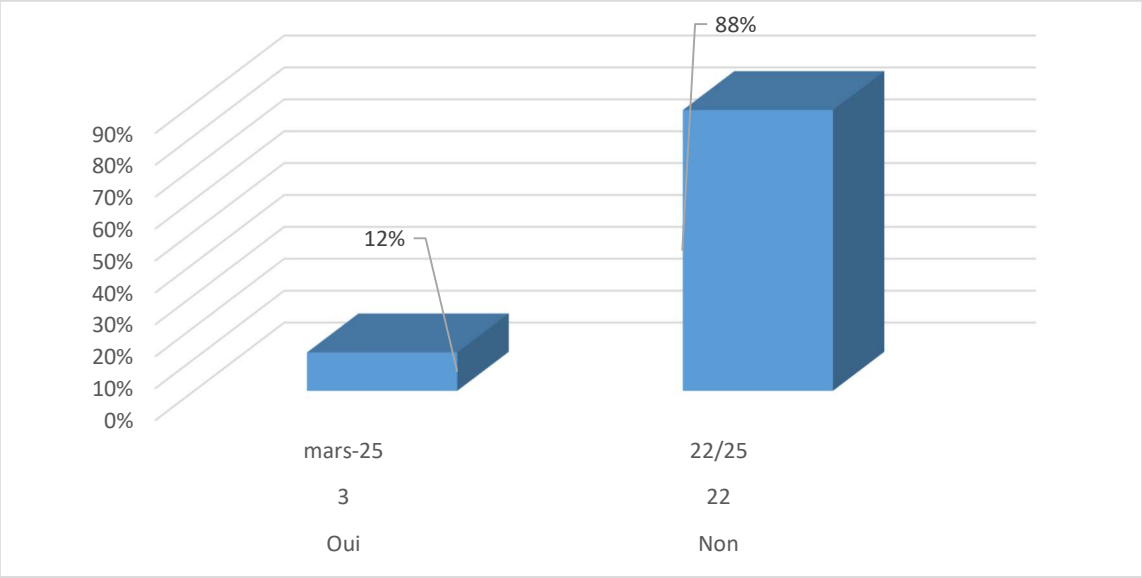


Figure : Avez-vous déjà reçu une formation en cybersécurité ?

La quasi-totalité du personnel (**88 %**) n'a reçu aucune formation sur les risques numériques, ce qui laisse un écosystème institutionnel très exposé.

Tableau 5 : Connaissez-vous les bonnes pratiques pour protéger les données ?

Réponse	N	F	%
Oui	6	6	24
Partiellement	11	11	44
Non	8	8	32
Total	25	25	100

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122

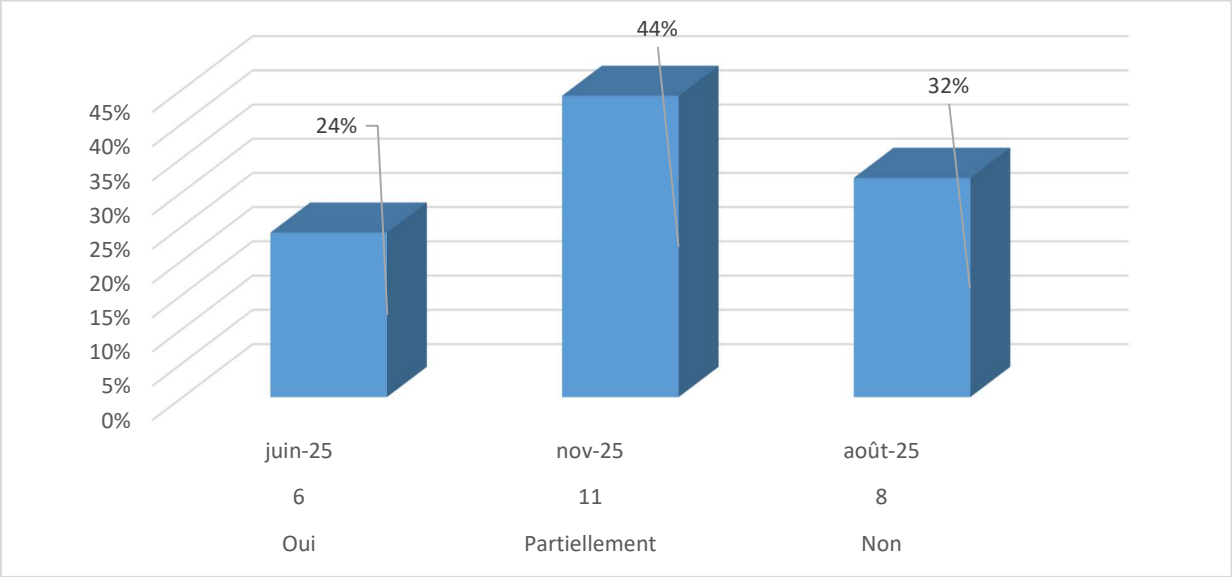


Figure 5 : Connaissez-vous les bonnes pratiques pour protéger les données ?

Seuls 24 % affirment connaître clairement les bonnes pratiques. Une majorité (76 %) ne maîtrise pas ou maîtrise peu les gestes de cybersécurité.

L'étude confirme les observations de Mbayo et Tshimanga (2019), qui soulignent l'importance du facteur humain dans les failles de sécurité en Afrique centrale.

L'usage fréquent de clés USB infectées demeure une source récurrente d'incidents.

Tableau 6 : Version des systèmes d'exploitation utilisés au service

Réponse	**N**	**F**	**%**
Windows 7 ou 8	20	20	80
Windows 10	4	4	16
Linux / autres	1	1	4
Total	25	25	100

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122

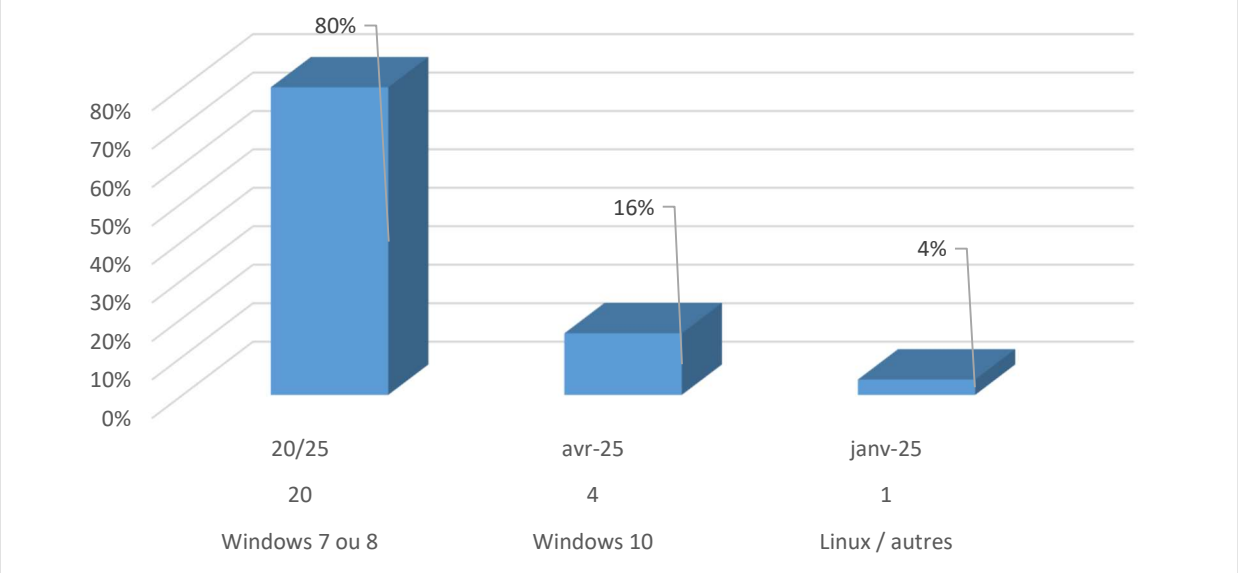


Figure 6 : Version des systèmes d'exploitation utilisés au service

La majorité (80 %) utilise encore Windows 7/8, systèmes obsolètes, non mis à jour et très vulnérables aux attaques modernes.

Ces faiblesses techniques favorisent la propagation de logiciels malveillants et augmentent le risque de perte totale des données.

Tableau 7 : Vos ordinateurs disposent-ils d'un antivirus fonctionnel et régulièrement mis à jour ?

Réponse	N	F	%
Antivirus non mis à jour	17	17	**68**
Antivirus installé et mis à jour	5	5	20
Aucun antivirus	3	3	12
Total	25	25	100

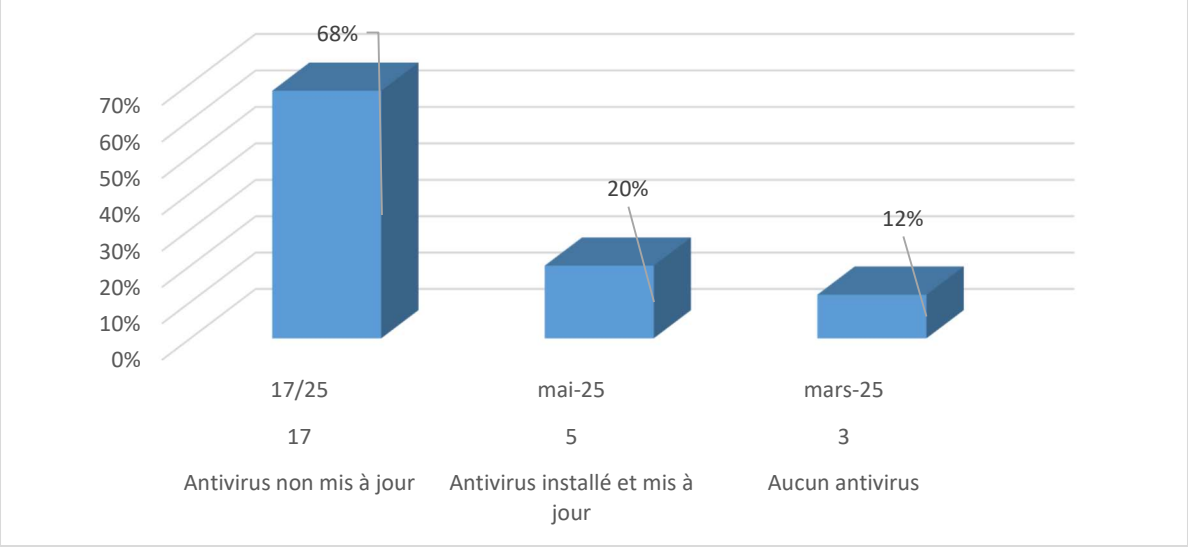


Figure 7 : Vos ordinateurs disposent-ils d'un antivirus fonctionnel et régulièrement mis à jour ?

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122

Cette figure montre que 68 % utilisent un antivirus non à jour, rendant les machines vulnérables aux malwares modernes.

Ces faiblesses techniques favorisent la propagation de logiciels malveillants et augmentent le risque de perte totale des données.

Tableau 8 : Système de sauvegarde des données

Réponse	N	F	%
Sauvegarde automatisée	0	0	0
Sauvegarde manuelle	9	9	36
Pas de sauvegarde	16	16	64
Total	25	25	**100**

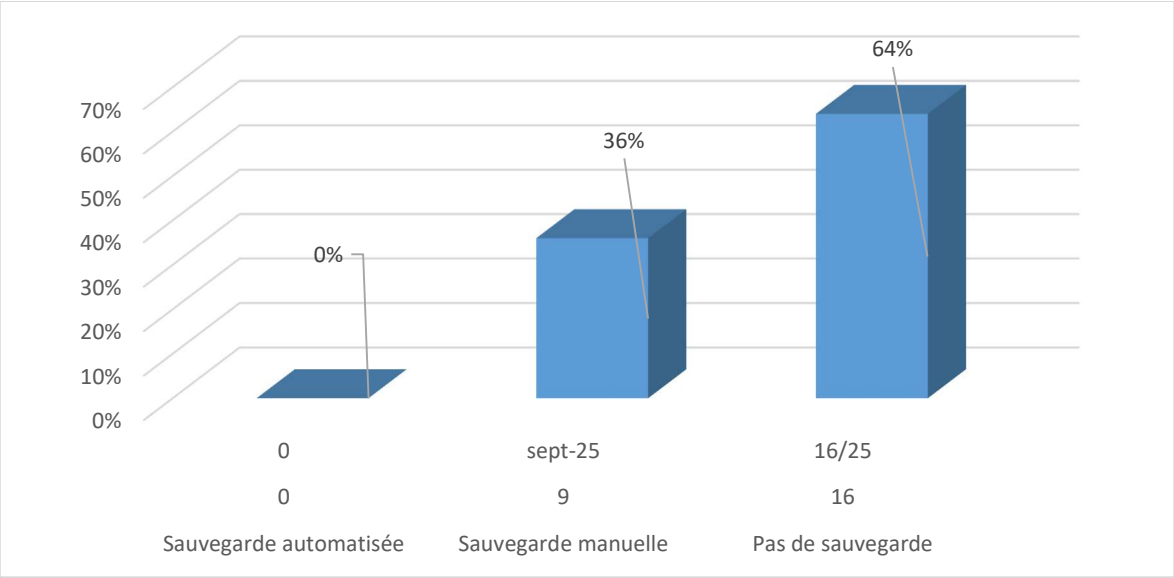


Figure 8 : Système de sauvegarde des données

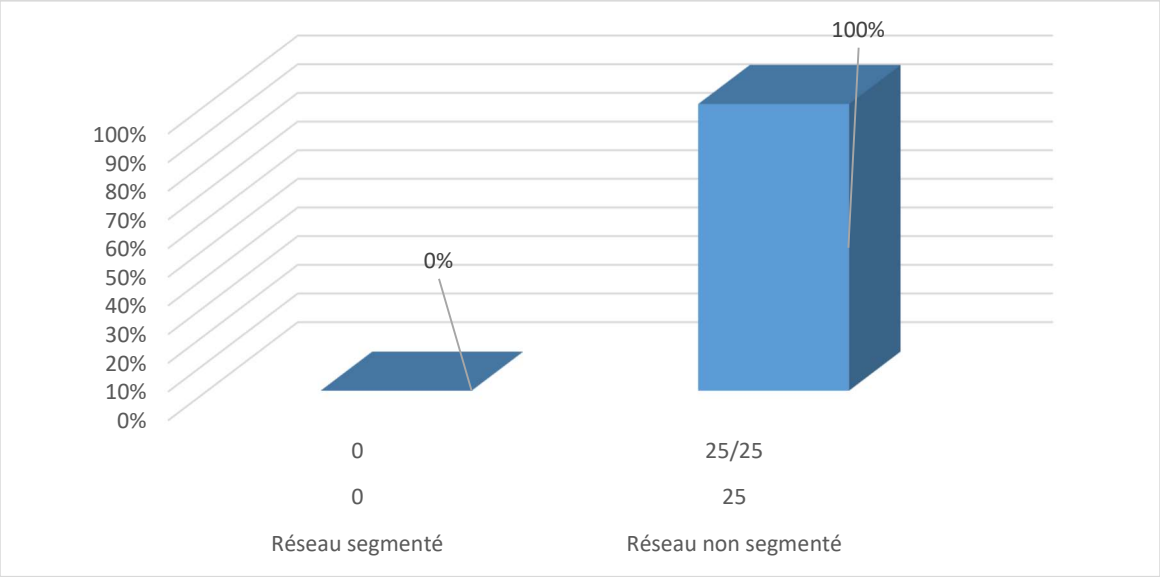
L'absence d'un système de sauvegarde automatisé expose l'ISP Mbandaka à la perte irrémédiable des données.

Tableau 9 : Segmentations du réseau interne

Réponse	N	F	%
Réseau segmenté	0	0	0
Réseau non segmenté	25	25	**100**

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 55 No. 2 February 2026, pp. 113-122



L'absence totale de segmentation réseau signifie que l'attaque d'un poste peut compromettre tout le système institutionnel.

3.2. Discussion

Les résultats indiquent que la cybersécurité demeure un grand défi à l'ISP Mbandaka. Les données sensibles ne sont pas protégées conformément aux normes, ce qui expose l'institution à des risques de fraude académique, de perte de données et d'usurpation d'identité.

Les observations recoupent les conclusions de Mutombo (2020), Kayembe (2021) et Shabani (2018), qui montrent que les institutions académiques congolaises manquent de politiques de gouvernance numérique robustes et d'un cadre de sécurité approprié.

Un risque pour l'intégrité académique

L'altération des notes, la disparition de relevés ou la falsification des documents académiques entament directement la crédibilité de l'institution. Comme l'explique Mutombo (2020), la fiabilité du système d'information est indispensable pour garantir des délibérations équitables et la reconnaissance des diplômes.

Un déficit de gouvernance de l'information

L'absence de PSSI, de plan de reprise d'activité ou même de directives de base (mots de passe, gestion des accès, politique d'usage des outils numériques) montre que l'ISP n'a pas encore intégré la cybersécurité dans sa stratégie institutionnelle.

Une problématique structurelle dans les institutions provinciales

Les établissements situés en province, loin des pôles technologiques, rencontrent des difficultés similaires telles que le manque de ressources, infrastructures vieillissantes, faible accompagnement technique (Kayembe, 2021). L'ISP-Mbandaka apparaît ainsi comme un cas représentatif du défi national.

Nécessité d'un changement de culture numérique

La cybersécurité ne peut être efficace que si elle devient une préoccupation partagée par tous : administratifs, enseignants, étudiants, direction. Schneier (2015) insiste sur ce point : la sécurité informatique est d'abord un comportement, avant d'être un logiciel.

CONCLUSION

Cette étude démontre que la cybersécurité est essentielle pour garantir la fiabilité des données administratives et pédagogiques de l'ISP de Mbandaka.

Les vulnérabilités identifiées sont les suivantes : absence de PSSI, faiblesse des infrastructures, manque de formation, exposent l'institution à des risques majeurs : altération des notes, perte de données, fraude académique, usurpation d'identité, et perte de crédibilité.

Pour se prémunir contre ces risques, l'ISP doit :

1. Élaborer une Politique de Sécurité du Système d'Information (PSSI).
2. Renforcer son infrastructure technique (pare-feu professionnels, machines à jour, segmentation réseau).
3. Mettre en place un système de sauvegarde automatisé et externalisé.
4. Former régulièrement le personnel à l'hygiène numérique.
5. Créer un comité interne de cybersécurité chargé de superviser et d'auditer les pratiques.

L'intégration de la cybersécurité dans la stratégie institutionnelle de l'ISP est une condition essentielle pour assurer la continuité pédagogique, la crédibilité académique et la protection du patrimoine informationnel.

REFERENCES

[1] Kayembe, L. (2021). Gouvernance Numérique et Sécurité des Données dans les Universités Congolaises. Lubumbashi : Presses Universitaires du Katanga.

[2] Mutombo, J.-P. (2020). "Vulnérabilité des Systèmes d'Information des Universités Congolaises". Revue Congolaise des Sciences et Techniques Appliquées, 5(1), 45–60.

[3] Mbayo, E. & Tshimanga, P. (2019). Évaluation de la maturité numérique dans les institutions publiques de RDC. Rapport académique, Université de Kinshasa (UNIKIN).

[4] Anderson, R. (2020). Security Engineering. John Wiley & Sons.

[5] Kapinga, B. (2022). Cybercriminalité et enjeux éthiques dans l'administration publique congolaise. Éditions Universitaires Africaines.

[6] Schneier, B. (2015). Data and Goliath. W.W. Norton.

[7] Shabani, M. (2018). Sécurité des réseaux informatiques : Analyse et perspectives pour les établissements d'enseignement supérieur en RDC. Mémoire de Master, Université de Kinshasa.

[8] NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity.

[9] UNESCO. (2019). Data Security and Higher Education.