ASIN
AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE
RÉPUBLIQUE DU BÉNIN

2026

Rapport annuel de vulnérabilités et d'incidents

Vulnérabilités, incidents et écart de conformité du cyberespace béninois.



Sommaire

Glossaire 4

Chiffres clés. 6

Message du Directeur Général de l'ASIN 9

À propos de l'ASIN 11

1. Introduction. 12

2. Objectifs du rapport 13

3. Cibles 14

4. Cadre Méthodologique 16

5. Périmètre du rapport 18

6.Restrictions et limites 19

7. Analyse des vulnérabilités 20

a. Analyse des vulnérabilités critiques 21

b. Répartition sectorielle des vulnérabilités critiques. 22

c. Évolution des vulnérabilités 26

d. Causes des vulnérabilités 27

8. Analyse des fuites de mots de passe 30

a. Répartition des cas de fuites de mots de passe par secteur. 30

b. Causes des fuites de mots de passe 31

c. Les failles qui rendent l'hameçonnage possible 32

d. Impact des identifiants exposés 33

9. Analyse des Incidents 34

a. Causes des incidents 34

b. Types des incidents répertoriés 35

c. Classification des types d'attaques par secteur. 37

d. Évolution des attaques 40

10. Les écarts de conformité à la PSSIE 42

a. Présentation de la démarche d'audit 42

b. Panorama des écarts de conformité. 44

c. Détail des écarts de conformité par domaine 45
d. Analyse des écarts de conformité relevés 48
e. Panorama des taux de conformité 49

11. Recommandations spécifiques 51

12. Recommandations globales 55

13. Conclusion 57

Annexe 58

I. Glossaire

Antivirus : Solution chargée de détecter, bloquer ou supprimer les logiciels malveillants présents sur un équipement.

ASIN : Agence des Systèmes d'Information et du Numérique.

Audit : Examen structuré d'un système, d'une application ou d'une organisation afin d'évaluer son niveau de sécurité, de conformité ou d'exposition.

Authentification : Processus permettant de confirmer l'identité d'un utilisateur, d'un service ou d'un équipement.

Backdoor (Porte dérobée) : Accès dissimulé dans un système permettant une prise de contrôle de ce dernier à distance.

bjCSIRT : Équipe nationale de réponse aux incidents de cybersécurité du Bénin.

Botnet : Réseau d'ordinateurs infectés et contrôlés à distance par un acteur malveillant pour mener des actions coordonnées, notamment des attaques DDoS.

Brute force : Technique consistant à tester massivement des combinaisons d'identifiants ou de mots de passe jusqu'à l'obtention d'un accès valide.

CMS (Content Management System) : Outil de création et de gestion de sites web.

Cross-Site Scripting (XSS) : Vulnérabilité permettant l'injection de scripts malveillants dans une application web, généralement exécutés dans le navigateur d'un utilisateur légitime compromettant ainsi la sécurité des données ou le fonctionnement de l'application.

CSRF (Cross-Site Request Forgery) : Attaque poussant un utilisateur authentifié à exécuter, à son insu, une action non désirée sur une application.

DDoS : Attaque par déni de service distribué visant à rendre un service indisponible en le saturant de requêtes provenant de multiples sources.

Défacement : Modification non autorisée du contenu ou de l'apparence d'un site web à la suite d'une compromission.

Hameçonnage : Technique de fraude visant à tromper une cible pour obtenir des identifiants, informations personnelles ou données sensibles.

Injection SQL : Faille permettant à un acteur malveillant d'accéder à une base de données, de la modifier ou d'en extraire des informations via des requêtes malveillantes.

Malware : Programme conçu pour nuire à un système, voler des données, perturber un service ou faciliter une compromission.

OIIC : Opérateurs d'Infrastructures d'Information Critiques.

PPIIC : Politique de Protection des Infrastructures d'Information Critiques.

PSSIE : Politique de Sécurité des Systèmes d'Information de l'Etat.

RCE (Remote Code Execution) : Vulnérabilité permettant l'exécution de commandes ou de code à distance sur un système ciblé.

RSSI : Responsable de la Sécurité des Systèmes d'Information.

SIEM : Solution centralisée qui collecte, corrèle et analyse en temps réel les journaux et événements de sécurité provenant de divers systèmes afin de détecter les incidents de sécurité.

SPF / DKIM / DMARC : Mécanismes de sécurité permettant de vérifier l'origine et l'intégrité des courriels afin de limiter l'usurpation de domaine.

SSRF : Vulnérabilité permettant à un attaquant d'exploiter un serveur pour accéder à des ressources internes, normalement inaccessibles.

Token CSRF : Jeton de protection utilisé par une application web pour vérifier qu'une requête provient bien d'une action légitime de l'utilisateur.

WAF (Web Application Firewall) : Dispositif de filtrage destiné à protéger les applications web contre des attaques applicatives courantes.

II. Chiffres clés

Le cyberespace béninois en 2025

L'essentiel de l'année en cinq indicateurs

456

Vulnérabilités identifiées

+22 % vs 2024

375 → 456

112

Vulnérabilités critiques

24 % du total

Broken Access Control = n°1

977

Fuites de mots de passe

Fuites de mots de passe

Threat intel externe

23

Incidents traités

–49 % vs 2024

45 → 23

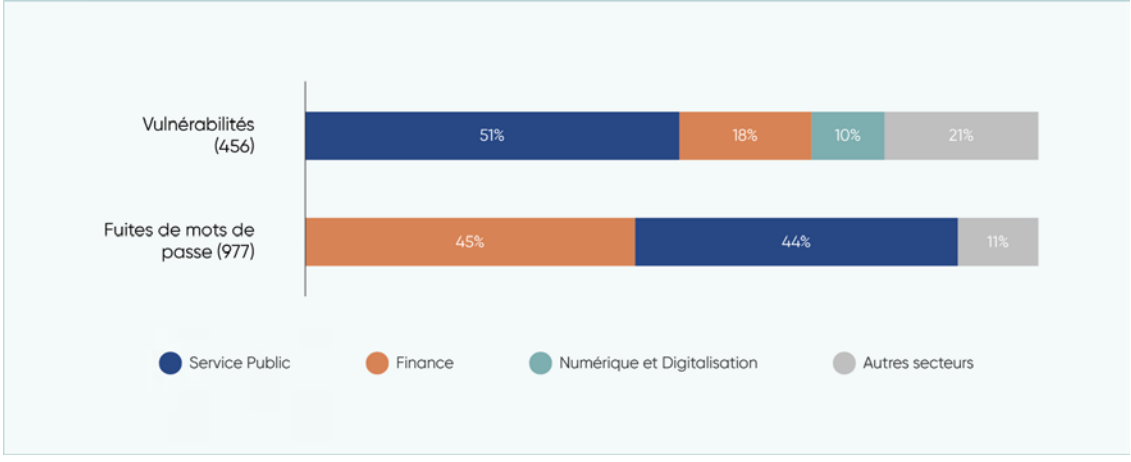
71

Écarts de conformité à la PSSIE

14.3 % de structures conformes

07 structures auditées

Les chiffres clés de l'année 2025 mettent en évidence les éléments suivants : les vulnérabilités identifiées révèlent les faiblesses des systèmes d'information, les identifiants exposés témoignent de la compromission des accès numériques, tandis que les incidents traités traduisent l'exploitation effective de ces faiblesses par des acteurs malveillants. Les écarts de conformité quant à eux révèlent une faible application des exigences des référentiels nationaux de sécurité des systèmes d'information. Ensemble, ces indicateurs dressent un état synthétique de la menace et des principaux enjeux de cybersécurité au Bénin.



La concentration sectorielle observée confirme que certains secteurs demeurent particulièrement exposés aux cybermenaces. Cette tendance appelle à une priorisation des efforts de prévention, de protection et de renforcement de leur résilience.

III. Message du Directeur Général de l'ASIN

L'année 2025 a confirmé l'accélération de la transformation numérique de notre pays, mettant en évidence la nécessité croissante de garantir la sécurité et la résilience des infrastructures qui soutiennent cette dynamique.

La multiplication des services numériques, l'interconnexion croissante des systèmes d'information et l'adoption de technologies innovantes constituent des leviers essentiels de développement et de compétitivité. Elles exposent cependant les organisations et les citoyens à des cybermenaces d'une sophistication et d'une intensité sans précédent.

Dans ce contexte, l'Agence des Systèmes d'Information et du Numérique, à travers son pôle sécurité numérique notamment les équipes de réponse aux incidents de sécurité informatique (bjCSIRT) et celles du département confiance et conformité, poursuit avec vigilance et détermination sa mission de protection du cyberespace béninois.

Au cours de l'année écoulée, nos équipes ont traité des campagnes d'hameçonnage ciblé, des compromissions de comptes, l'exploitation de vulnérabilités affectant des systèmes exposés, ainsi que des tentatives d'atteinte à la disponibilité et à l'intégrité de services numériques critiques sans oublier les risques de non-conformité majeurs relativement aux référentiels étatiques de sécurité des systèmes d'information.

Ces constats rappellent que les cybermenaces ne constituent plus un risque hypothétique. Elles représentent une réalité tangible qui concerne l'ensemble des acteurs de l'écosystème numérique, indépendamment de leur taille, de leur secteur d'activité ou de leur niveau de maturité technologique. Aussi, la démocratisation de l'usage des systèmes d'intelligence artificielle apporte une couche supplémentaire qui accroît l'exposition et l'exploitation des vulnérabilités sur les SI.

À travers cette édition du Rapport annuel de vulnérabilités et d'incidents, l'ASIN entend partager les principales tendances observées, sensibiliser les parties prenantes aux risques émergents et promouvoir les bonnes pratiques indispensables à notre résilience collective.

Ce document se veut avant tout être un outil d'information, de sensibilisation et d'aide à la décision. Il marque une étape importante dans le suivi de l'état de la cybersécurité au Bénin à l'ère de la transformation numérique des administrations publiques, des opérateurs économiques et des infrastructures numériques nationales.

Cette nouvelle publication offre une analyse plus détaillée des tendances observées, une caractérisation plus fine des risques par secteur d'activité ainsi qu'une meilleure compréhension des facteurs techniques, organisationnels et humains qui continuent d'affecter la sécurité des systèmes d'information. Sans aucun doute, ce Rapport contribuera à soutenir la professionnalisation progressive de la fonction RSSI, à encourager les audits de conformité et

améliorer les mécanismes de remontée et de gestion des incidents.

À l'échelle régionale et internationale, les analyses mettent en évidence une évolution rapide des modes opératoires des cybercriminels sous l'effet de l'intelligence artificielle, face auxquels des actions structurantes sont déployées, notamment la dotation d'outils et d'équipements spécialisés avec des solutions de nouvelle génération destinées à améliorer les capacités d'investigation numérique, d'analyse technique, de renseignement et de réponse.

D'emblée, l'intelligence artificielle doit être appréhendée à la fois comme un levier d'amélioration des capacités de cybersécurité et comme une source émergente de risques nécessitant un encadrement approprié.

L'enjeu pour l'Agence est de poursuivre la montée en maturité du dispositif national de cybersécurité afin que les ambitions de transformation numérique du Bénin s'accompagnent d'un niveau de confiance, de résilience et de sécurité conforme aux standards internationaux.

En ma qualité de Directeur Général, je réaffirme l'engagement de l'Agence à garantir la sécurité des infrastructures numériques nationales, à renforcer les capacités de prévention et de réponse aux incidents, et à instaurer un climat de confiance propice à l'essor de l'économie numérique.

Ensemble, œuvrons pour un Bénin numériquement sécurisé.

IV. À propos de l'ASIN



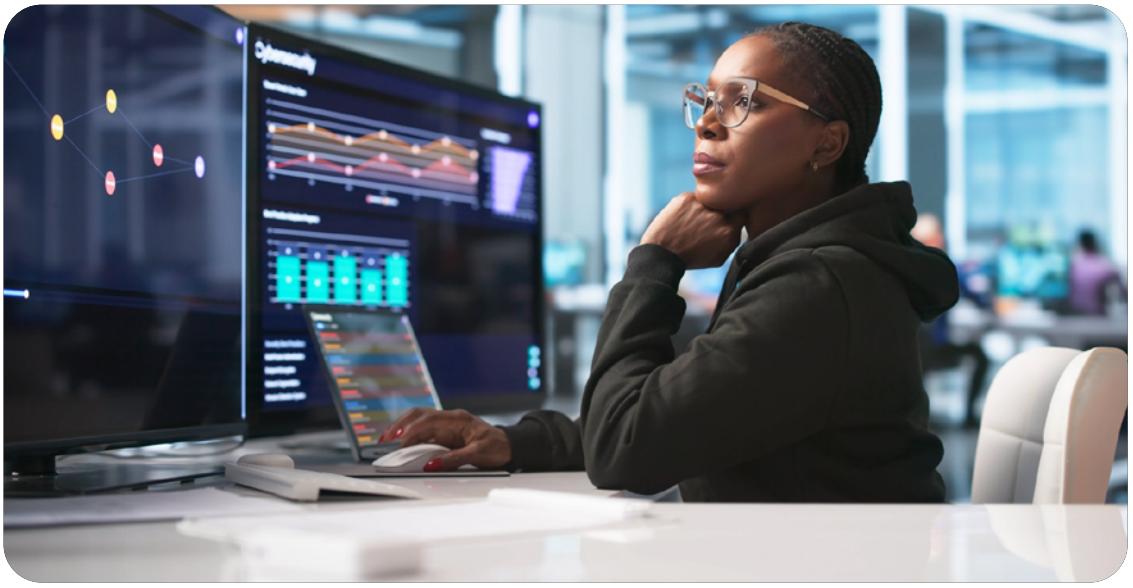
Créée par le décret N°2022-324 du 1er juin 2022, l'Agence des Systèmes d'Information et du Numérique (ASIN) est un établissement public à caractère social et scientifique, doté de la personnalité morale et de l'autonomie financière.

Placée sous la double tutelle du Ministère de l'Économie et des Finances et du Ministère de la Transformation Digitale et de l'Innovation, en charge de la stratégie nationale d'intelligence artificielle (anciennement Ministère du Numérique et de la Digitalisation), l'ASIN est née de la fusion des quatre (04) agences d'exécution qui composaient le cadre institutionnel pour l'opérationnalisation des projets du secteur du numérique depuis 2016 à savoir :

- Agence pour le Développement du Numérique (ADN)
- Agence des Services et Systèmes d'Information (ASSI)
- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
- Agence Béninoise du Service Universel des Communications Électroniques et de la Poste (ABSU-CEP).

L'ASIN assure la mise en œuvre opérationnelle des programmes et projets liés au développement des services numériques, des systèmes d'information et de leur sécurisation. Son positionnement permet de renforcer la cohérence de l'action publique numérique et d'articuler, dans une même dynamique, transformation digitale, gouvernance des systèmes d'information et cybersécurité.

1. Introduction



L'année 2025 confirme que la cybersécurité est désormais indissociable de la transformation numérique du Bénin. L'extension des services en ligne, l'interconnexion croissante des plateformes et la dépendance accrue aux systèmes d'information créent de nouvelles opportunités, mais exposent également les institutions à des risques plus nombreux, plus visibles et parfois plus rapides à exploiter.

La modernisation des services publics a profondément transformé les usages: démarches administratives, gestion de données, communication institutionnelle et services aux usagers reposent de plus en plus sur des environnements numériques. Cette évolution impose une vigilance renforcée sur la configuration des systèmes, la gestion des accès, la protection des données et la capacité à détecter rapidement les signaux d'attaque.

Dans cette perspective, le suivi annuel des vulnérabilités et des incidents devient un outil de pilotage. Il permet non seulement de mesurer l'exposition des entités concernées, mais aussi d'identifier les faiblesses récurrentes, de prioriser les actions correctives et de nourrir une culture de sécurité fondée sur les faits.

Le présent rapport analyse donc les vulnérabilités, incidents et écarts de conformité observés en 2025 sur les systèmes d'information des institutions de l'Etat et des OIIC. Il s'appuie sur les données collectées et validées par les services techniques compétents de l'ASIN, notamment le bjCSIRT ainsi que le Département Confiance et Conformité. Il permet également de situer l'année 2025 dans la trajectoire ouverte par les données consolidées de 2021 à 2024, afin de faire ressortir les continuités, les déplacements de risque et les priorités d'action.

2. Objectifs du rapport

Ce rapport vise à transformer les données collectées en 2025 en éléments d'aide à la décision. Il présente les vulnérabilités, incidents, écarts de conformité et tendances observées au sein du périmètre couvert par le pôle sécurité numérique de l'ASIN, tout en mettant en évidence les leviers de réduction du risque pour les entités concernées.

De manière spécifique, il s'agit de :

01

dresser un état consolidé des vulnérabilités documentées, en précisant leur criticité, leurs causes et leur répartition sectorielle ;

02

mettre en évidence les incidents les plus significatifs, notamment les fuites de mots de passe, les compromissions et les attaques observées ;

03

faire état des écarts de conformité relevés par rapport à la PSSIE ;

04

proposer des orientations concrètes pour renforcer la prévention, la détection, la réponse aux incidents de sécurité, la conformité et la maturité des SI aux référentiels nationaux de sécurité ainsi que la gouvernance cyber des institutions étatiques et des OIIC.

Ce rapport entend ainsi constituer un support de compréhension, de priorisation et de mobilisation au service d'une transformation numérique plus résiliente.

3. Cibles

Ce rapport est principalement destiné aux acteurs appelés à décider, piloter, sécuriser ou évaluer les systèmes d'information, notamment :

- décideurs des systèmes d'information des institutions étatiques et OIIC ;
- responsables de la sécurité des systèmes d'information ;
- fournisseurs de services de sécurité numérique qualifiés (FSSNQ) ;
- chercheurs ou étudiants en quête de données statistiques sur les vulnérabilités et écarts de conformité aux référentiels nationaux de cybersécurité ;
- consultants et cabinets dans le domaine de la cybersécurité.

Il peut également servir de référence **à toute personne intéressée par l'évolution des risques cyber dans l'écosystème public béninois**.

Par ailleurs, le périmètre sectoriel retenu s'aligne sur les domaines couverts par la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) et la Politique de Protection des Infrastructures d'Information Critiques (PPIIC).

Ces secteurs sont :





Dans le cadre de cette étude, le secteur Service Public regroupe les institutions étatiques et organismes publics impliqués dans la gestion des affaires publiques et l'exercice des missions de l'État.

4. Cadre Méthodologique

L'élaboration de ce rapport repose sur une démarche structurée combinant collecte d'informations, traitement analytique et validation par des experts techniques.

Étape 1

Collecte des données

Les données exploitées pour l'exercice 2025 proviennent de plusieurs sources opérationnelles et documentaires :

- rapports d'incidents et d'interventions du bjCSIRT ;
- rapports hebdomadaires de monitoring et annuels du bjCSIRT ;
- mémos de sécurité du bjCSIRT ;
- rapport d'audits de vulnérabilités du bjCSIRT ;
- bulletins d'alertes du bjCSIRT ;
- rapports d'audit organisationnel et de conformité à la PSSIE ;
- rapports des missions d'inspection annuelle du service conformité ;
- rapports d'incidents déclarés par le service juridique ;
- data breach ;

Étape 2

Validation des données collectées

Les données collectées ont ensuite fait l'objet d'une vérification afin d'en confirmer la cohérence, la traçabilité et l'alignement avec les sources exploitées.

Étape 3

Analyse des données collectées

Les informations validées ont été corrélées puis classées par nature, niveau de risque, secteur d'activité et période d'observation, afin de dégager les tendances principales.

Étape 4

Rédaction du rapport

Les résultats ont enfin été restitués sous forme d'analyses, de tableaux, de graphiques et de recommandations opérationnelles, structurés dans un rapport.

5. Périmètre du rapport

Le présent rapport couvre les vulnérabilités et incidents identifiés, conformément au RFC 2350 du bjCSIRT, ainsi que les écarts de conformité relevés par le Département confiance et conformité relatifs aux institutions étatiques à savoir :

les ministères du gouvernement ;	les agences gouvernementales ;	les institutions de la République établies par la constitution ;	les opérateurs d'Infrastructures d'Information Critiques (OIIC).

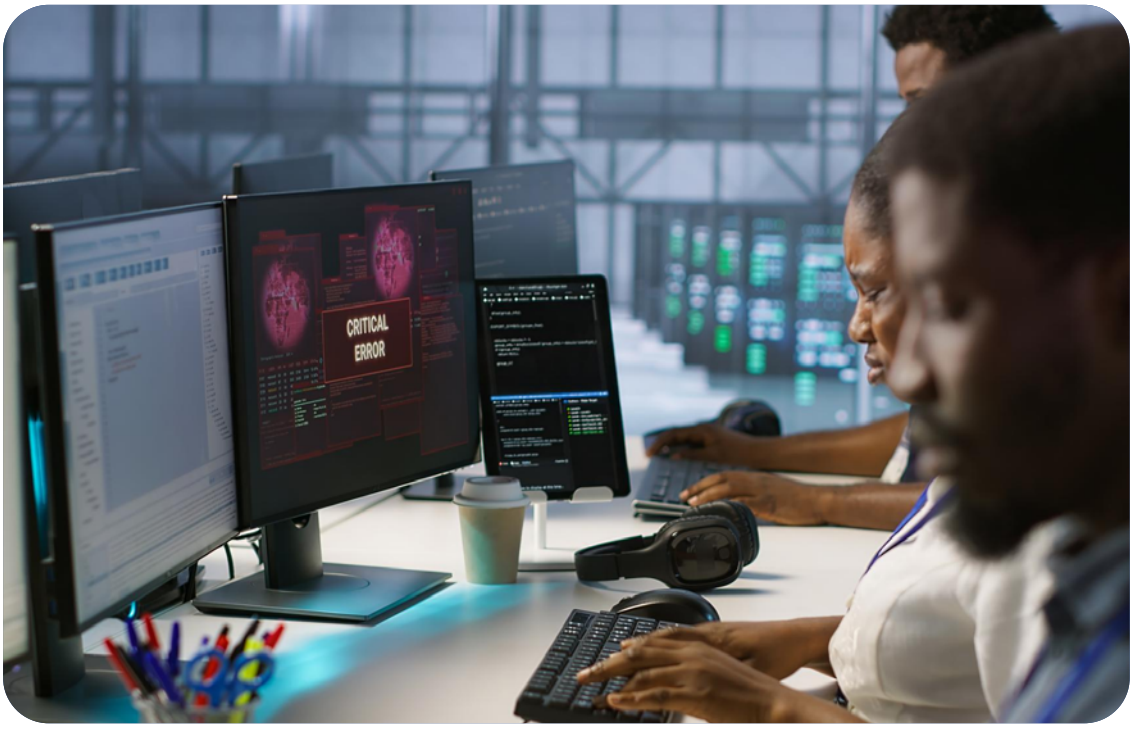
Dans le présent rapport, les ministères du Gouvernement, agences gouvernementales et institutions de la République établies par la constitution sont regroupés sous l'appellation **« institutions étatiques »**.



6. Restrictions et limites

Bien qu'une démarche méthodologique cohérente et rigoureuse ait été appliquée dans le cadre de la rédaction de ce rapport, il faut noter que, les résultats présentés doivent être interprétés à la lumière des limites suivantes :

- les analyses reposent sur les incidents, attaques et vulnérabilités déclarés au bjCSIRT ou identifiés par les équipes compétentes de l'ASIN ;
- les entités privées ne sont pas incluses, sauf lorsqu'elles relèvent du périmètre des opérateurs d'infrastructures d'information critiques.



Le cadre méthodologique, le périmètre et les limites de l'exercice ayant été précisés, le rapport présente les résultats de l'analyse des vulnérabilités identifiées au cours de l'année 2025.

7. Analyse des vulnérabilités

En 2025, quatre cent cinquante-six (456) vulnérabilités ont été identifiées sur les systèmes d'information des institutions officielles. La collecte annuelle confirme une exposition significative, avec une progression du volume par rapport aux trois cent soixante-quinze (375) vulnérabilités recensées en 2024. Elle met surtout en évidence une concentration plus marquée sur les niveaux modéré, élevé et critique, ce qui invite à renforcer la priorisation des remédiations. La répartition par niveau de risque est la suivante :

3% présentent un risque faible (12 cas) ;

40% présentent un risque modéré (181 cas) ;

33% présentent un risque élevé (151 cas) ;

24% présentent un risque critique (112 cas)

Comparativement aux années antérieures, la part des vulnérabilités faibles apparaît nettement plus réduite dans la collecte 2025, tandis que les niveaux modéré et élevé représentent désormais l'essentiel des constats. Cette évolution ne doit pas être interprétée uniquement comme une dégradation mécanique : elle peut aussi traduire un ciblage plus fin des contrôles, une meilleure qualification des failles et une remontée plus structurée des vulnérabilités réellement exploitables.

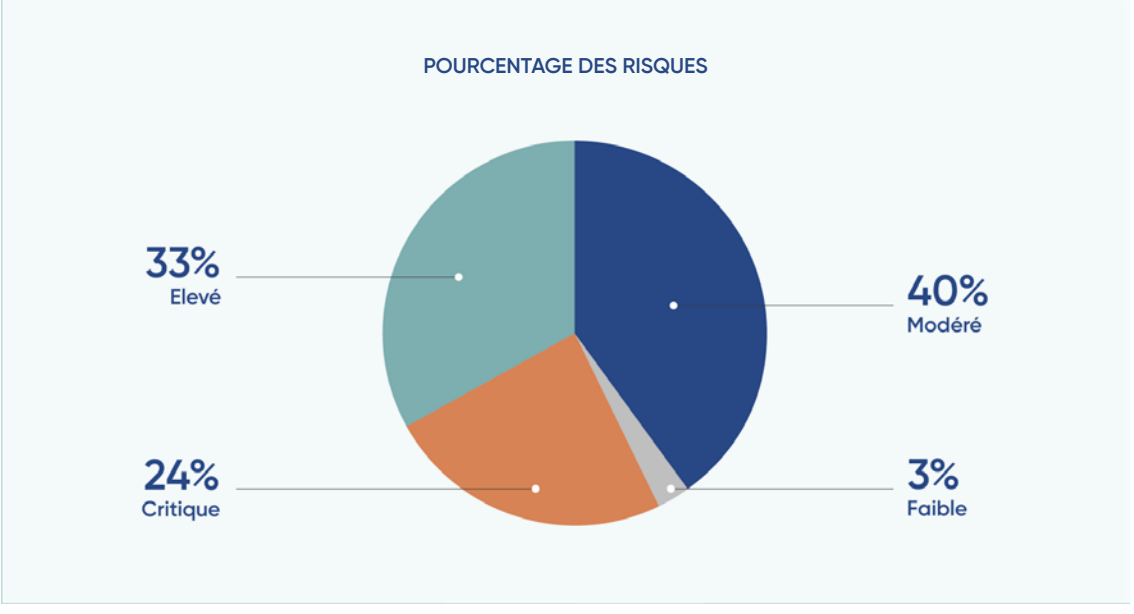


Figure 1 : Répartition des vulnérabilités selon le niveau de risque

a. Analyse des vulnérabilités critiques

Une étude spécifique a été menée sur les vulnérabilités classées comme critiques selon la grille d'évaluation du bjCSIRT disponible en annexe. Ces failles présentent une probabilité d'exploitation élevée et des impacts élevés sur la confidentialité, l'intégrité ou la disponibilité des systèmes.

Les principales vulnérabilités critiques observées sont les suivantes :

- **Broken Acces Control (53 cas) :** mauvaise gestion des droits d'accès, permettant à un utilisateur non autorisé d'atteindre des fonctions ou ressources critiques ;
- **Remote Code Execution (29 cas) :** vulnérabilité permettant à un acteur malveillant d'exécuter à distance des commandes ou du code sur le système ciblé ;
- **Broken Authentication (11 cas) :** faiblesse des mécanismes d'authentification pouvant faciliter le contournement d'accès, la prise de contrôle de compte ou l'usurpation d'identité ;
- **Unrestricted File Upload (8 cas) :** absence de contrôle suffisant sur les fichiers téléversés, pouvant conduire à l'exécution de code arbitraire, la compromission du système ou l'hébergement de contenus non autorisés ;
- **SQL Injection (5 cas) :** manipulation des entrées utilisateur afin d'injecter des requêtes malveillantes vers une base de données et d'accéder, modifier ou supprimer des informations.

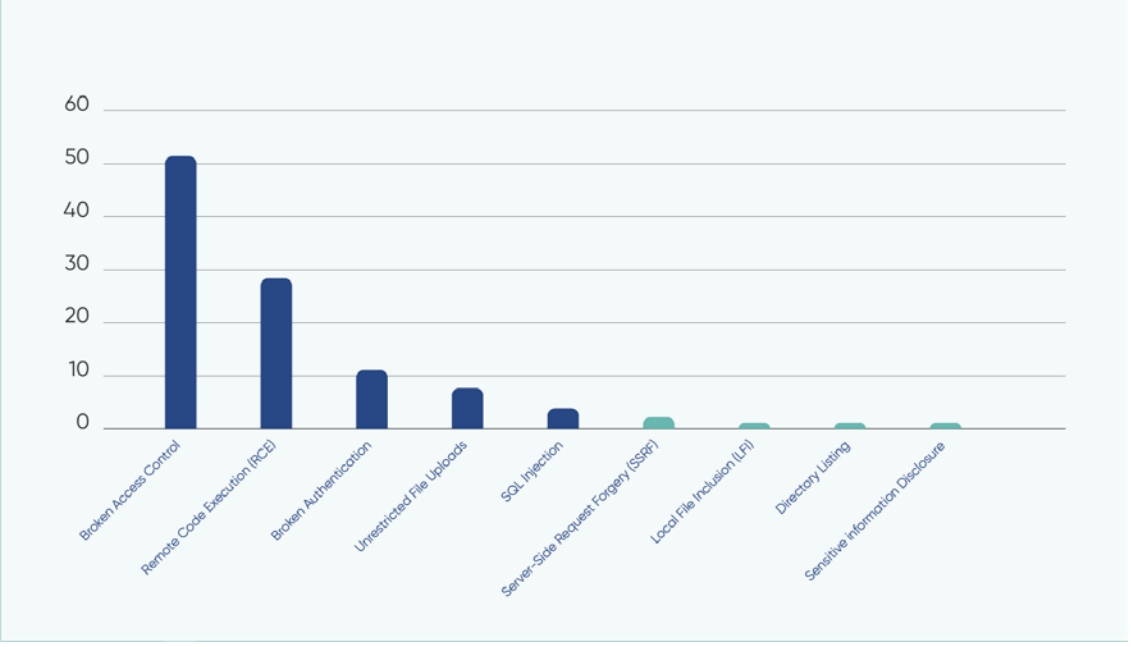


Figure 2 : Occurrences des vulnérabilités à risque critique

La hiérarchie des vulnérabilités critiques montre à la fois une continuité et un déplacement des priorités.

Le **contrôle d'accès défaillant** conserve la première place, ce qui confirme la persistance des enjeux liés aux habilitations et aux parcours applicatifs sensibles.

La **Remote Code Execution** occupe désormais une place plus élevée dans la collecte 2025, signalant une attention particulière à porter aux composants exposés, aux versions logicielles et aux surfaces d'exécution.

À l'inverse, la **divulgation d'informations sensibles**, très visible dans les données consolidées de 2021 à 2024, ne figure plus parmi les cinq premières vulnérabilités critiques de l'année, tandis que le **téléversement non contrôlé de fichiers** apparaît comme un risque applicatif à surveiller de plus près.

b. Répartition sectorielle des vulnérabilités critiques

Une analyse approfondie des données a permis d'identifier les secteurs ayant été touchés par les vulnérabilités critiques :

Vulnérabilités	Secteurs les plus touchés
Broken Access Control	Service Public : 30 ; Finance : 07 ; Enseignement : 05 ; Numérique/Santé : 04 ; Transport : 03 ; Télécommunications : 02.
Remote Code Execution	Service Public : 13 ; Finance/Numérique : 08 ; Télécommunications/Transport/Agriculture : 01.
Broken Authentication	Service Public : 08 ; Finance/Numérique/Santé : 01.
Unrestricted File Upload	Service Public : 06 ; Enseignement/Finance : 01.
SQL Injection	Service Public : 03 ; Agriculture/Enseignement : 01

Il est à noter que :



le Service Public concentre systématiquement le plus grand nombre de failles critiques ;



les secteurs Finance, Numérique et Digitalisation, et dans une moindre mesure le secteur Transport, présentent aussi une forte exposition aux risques critiques ;



le secteur de l'Enseignement, bien que moins attendu, reste concerné par des faiblesses de base, notamment les configurations insuffisamment sécurisées et les expositions d'informations.

La continuité sectorielle avec les données 2021-2024 est nette : les secteurs Service public, Finance, Numérique et Digitalisation, Transport et Enseignement demeurent les principaux espaces d'exposition, même si l'intensité et la nature des vulnérabilités varient selon les années.

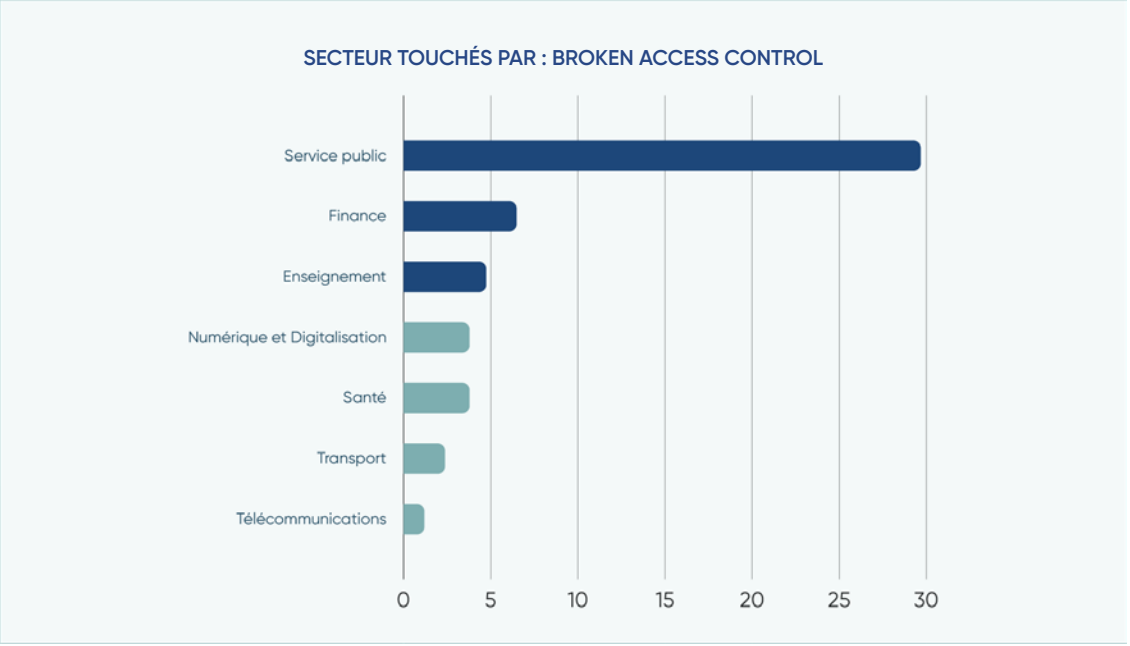


Figure 3 : Secteurs touchés par : «Broken Access Control»

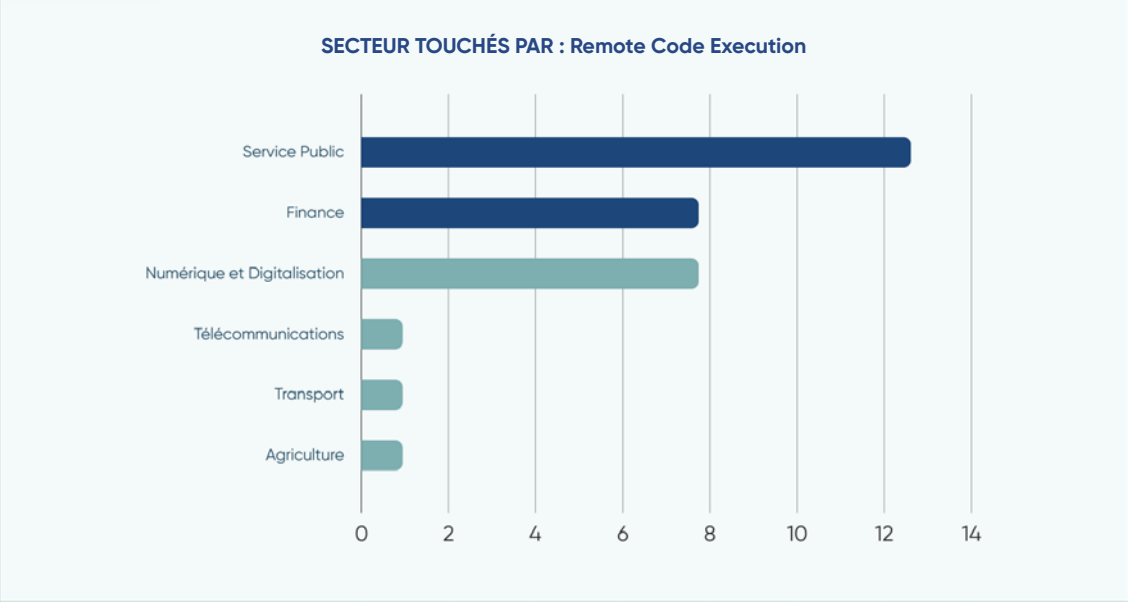


Figure 4 : Secteurs touchés par : «Remote Code Execution»

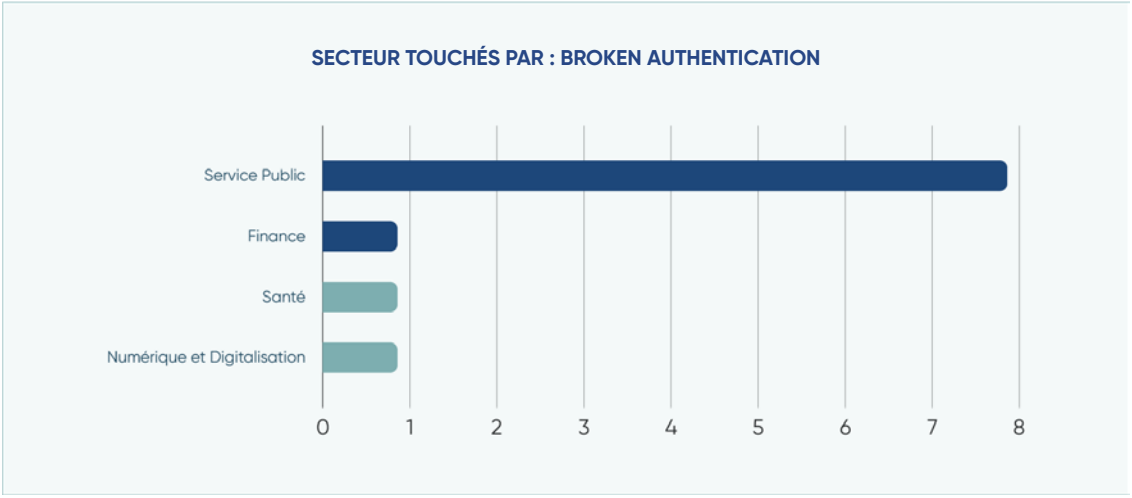


Figure 5 : Secteurs touchés par : «Broken Authentication»

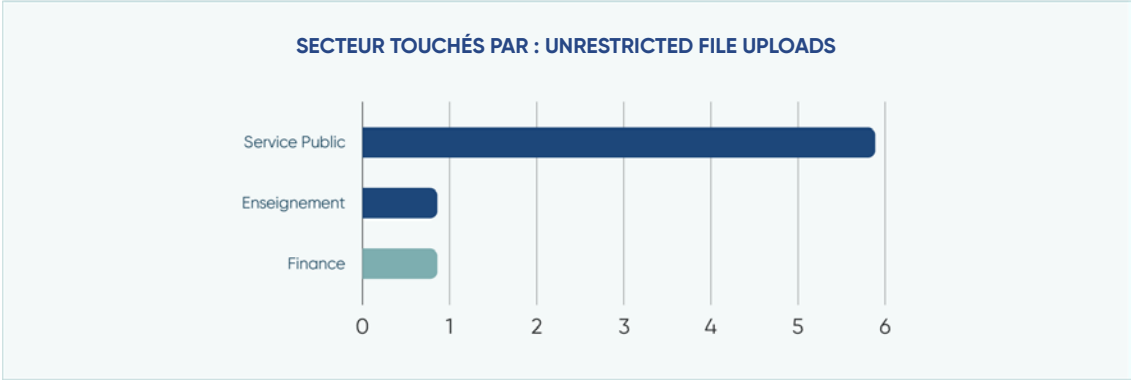


Figure 6 : Secteurs touchés par : «Unrestricted File Uploads»

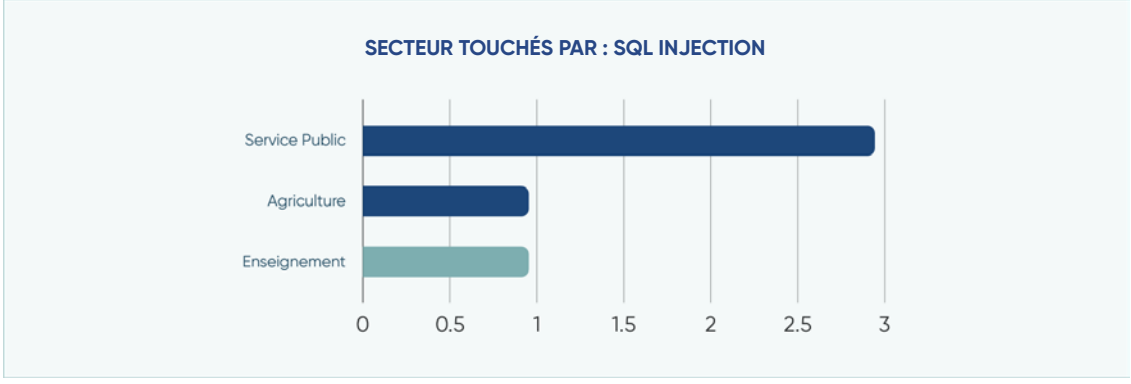


Figure 7 : Secteurs touchés par : «SQL Injection»

En ce qui concerne la classification des vulnérabilités par secteur, tous niveaux de risque confondus, les cinq secteurs les plus concernés par les vulnérabilités recensées sont :

Service Public : **234** | Finance : **81** | Numérique et Digitalisation : **44** | Transport : **28** | Enseignement : **26**

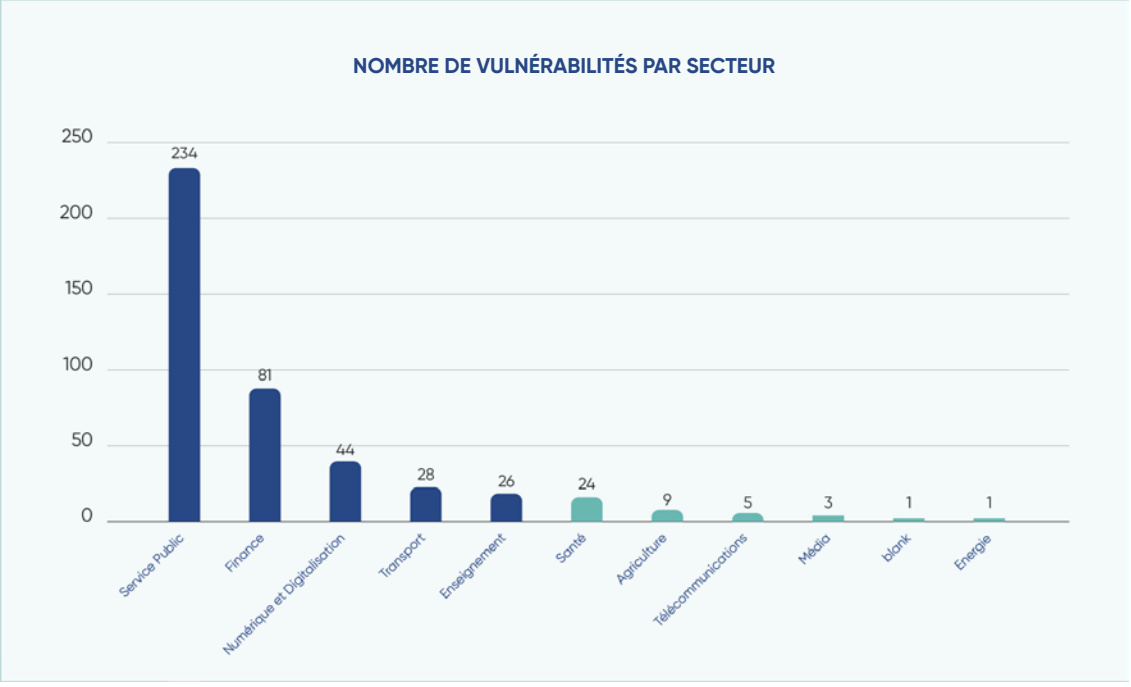


Figure 8 : Nombre de vulnérabilités par secteur

53% Des secteurs sont touchés par des vulnérabilités

Les secteurs **Service Public** et **Finance** sont à eux seuls touchés par plus de **69% des vulnérabilités recensées**.

À eux seuls, les secteurs **Service public** et **Finance** représentent plus de 69 % des vulnérabilités recensées.

c. Évolution des vulnérabilités

Au regard des données collectées au cours de l'année 2025, la situation de la cybersécurité dans les institutions publiques béninoises reste préoccupante. La comparaison avec l'exercice précédent montre une progression du nombre de vulnérabilités identifiées : trois cent soixante-quinze (375) en 2024 contre quatre cent cinquante-six (456) en 2025, soit quatre-vingt-un (81) cas supplémentaires.

Cette hausse peut traduire à la fois l'élargissement de la surface numérique, une meilleure capacité de détection et la persistance de faiblesses de sécurité non corrigées. Elle confirme aussi que la réduction du risque ne dépend pas seulement de l'identification des vulnérabilités, mais de la capacité des entités à organiser, suivre et vérifier les remédiations.

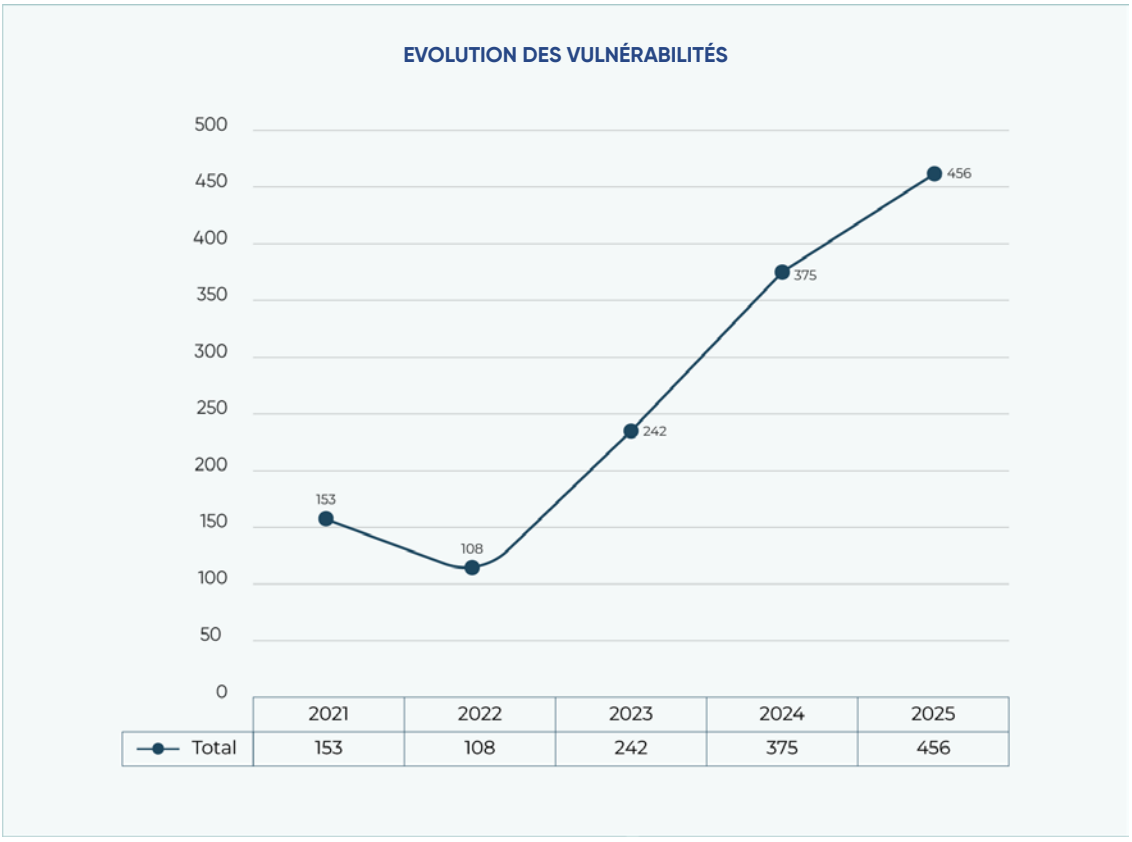


Figure 9 : Évolution des vulnérabilités de 2021 à 2025

d. Causes des vulnérabilités

Les vulnérabilités recensées trouvent principalement leur origine dans les causes suivantes :

- **Mauvaise configuration des paramètres de sécurité :** cent trente-neuf (139) occurrences ;
- **Mauvaise implémentation des contrôles adéquats :** soixante-dix (70) occurrences ;
- **Mauvaise gestion des rôles et des permissions :** soixante-cinq (65) occurrences ;
- **Version du logiciel non à jour :** soixante-deux (62) occurrences ;
- **Exposition de fichiers sensibles sans restriction d'accès :** quarante-six (46) occurrences.

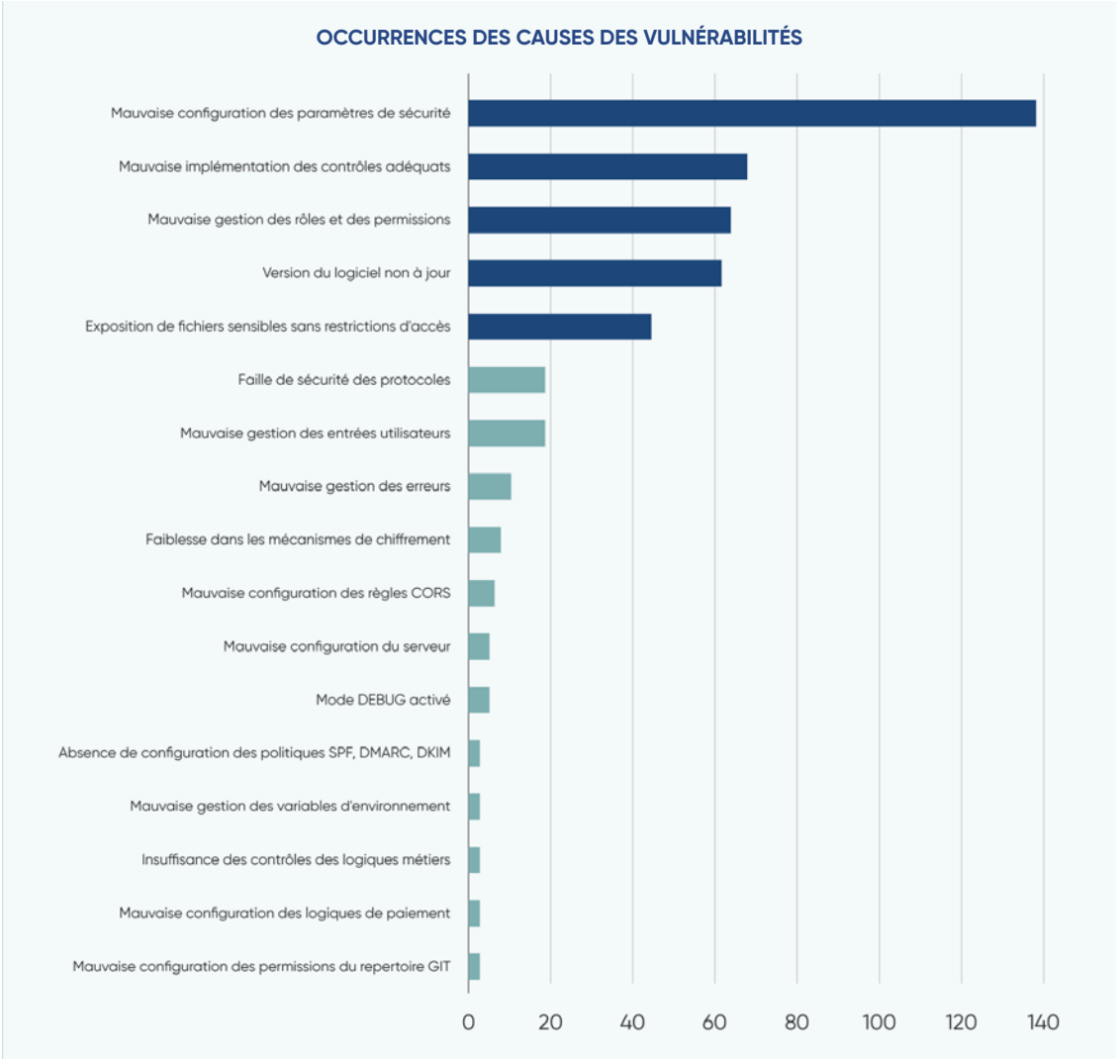


Figure 10 : Occurrences des causes des vulnérabilités

Cette augmentation du nombre de vulnérabilités peut s'expliquer par une combinaison de facteurs techniques et organisationnels :

- l'augmentation du nombre de plateformes et de services numériques exposés ;
- le maintien en production de systèmes anciens ou insuffisamment durcis ;
- l'absence ou l'insuffisance de pilotage cyber structuré dans certaines entités ;
- des ressources limitées pour appliquer, suivre et vérifier les correctifs nécessaires ;
- la maintenance irrégulière de certaines applications, laissant perdurer des failles connues.

Au-delà des vulnérabilités techniques, les données collectées en 2025 mettent également en lumière l'ampleur des fuites de mots de passe, autre indicateur majeur de l'exposition des systèmes d'information.

8. Analyse des fuites de mots de passe

Les fuites de mots de passe constituent l'un des signaux les plus préoccupants de l'année 2025. Elles résultent généralement de la réutilisation d'identifiants, d'infections par logiciels malveillants, de pratiques de partage non sécurisées ou d'une gestion insuffisante des comptes.

a. Répartition des cas de fuites de mots de passe par secteur

La collecte 2025 recense neuf cent soixante-dix-sept (977) cas, un niveau supérieur aux huit cent trente-deux (832) cas consolidés sur la période 2021-2024. Cette évolution fait des identifiants exposés un marqueur prioritaire de risque opérationnel, principalement dans les secteurs suivants :

- **Finance :** quatre cent quarante-deux (442) cas ;
- **Service Public :** quatre cent vingt-huit (428) cas ;
- **Santé :** cinquante-sept (57) cas ;
- **Numérique et Digitalisation :** trente (30) cas ;
- **Enseignement :** quatorze (14) cas.

La répartition sectorielle évolue également : le Service public concentre légèrement moins de cas que la Finance en 2025. Ce basculement invite à traiter les fuites d'identifiants comme un risque transversal de continuité des services publics, et non comme une problématique limitée aux environnements financiers.



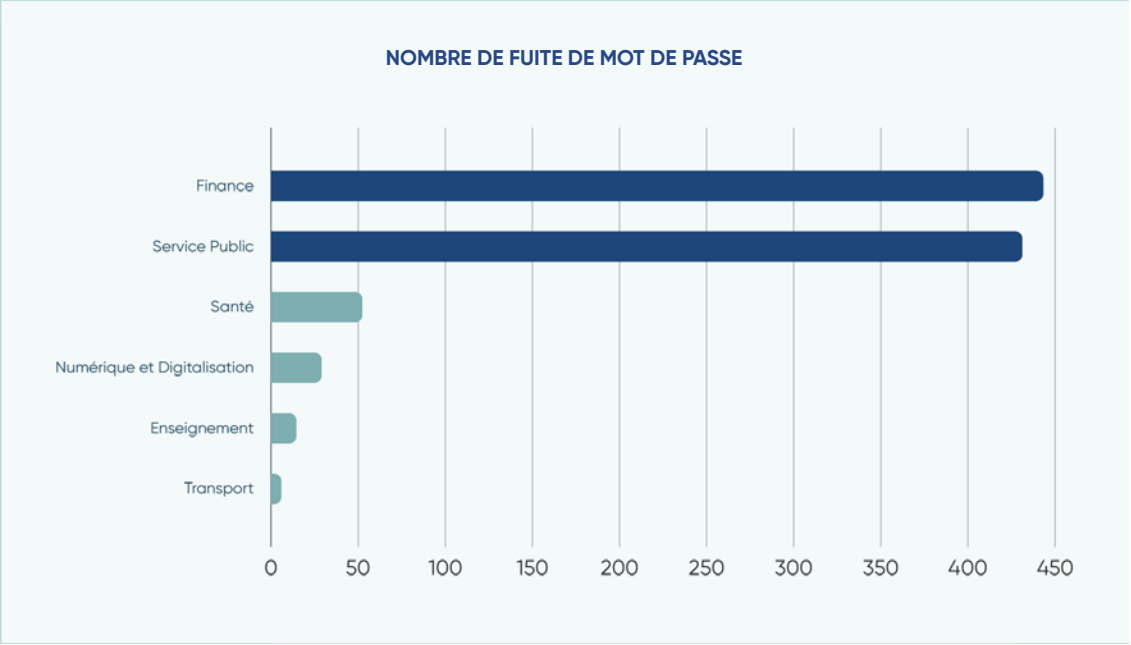


Figure 11 : Nombre de fuites de mots de passe par secteur

32% Des secteurs sont touchés par des fuites de mots de passe

Ces fuites constituent souvent des vecteurs d'intrusion majeurs, facilitant les attaques ciblées, l'usurpation d'identité ou encore les campagnes d'hameçonnage.

b. Causes des fuites de mots de passe

Les identifiants peuvent être compromis selon différents mécanismes, dont certains ne résultent pas directement d'une attaque contre le système d'information de l'organisation concernée. L'encadré ci-dessous présente les principaux scénarios conduisant à l'exposition d'identifiants afin d'en faciliter la compréhension.

Enregistrement des mots de passe dans le navigateur

Les navigateurs proposent d'enregistrer localement les identifiants afin de faciliter les connexions. Lorsqu'un poste de travail est compromis par un logiciel malveillant spécialisé dans le vol d'informations (Infostealer), ces identifiants peuvent être récupérés et utilisés

pour accéder à des services professionnels, sans qu'une compromission des serveurs de l'organisation ne soit nécessaire.

Réutilisation d'un même mot de passe

L'utilisation d'un même mot de passe sur plusieurs services accroît le risque de compromission. Lorsqu'un service tiers est victime d'une fuite de données, les identifiants divulgués peuvent être réutilisés par des attaquants pour tenter d'accéder à d'autres comptes appartenant au même utilisateur.

Saisie des identifiants sur un service non sécurisé

La saisie d'identifiants sur une application insuffisamment sécurisée, utilisant par exemple une connexion non chiffrée ou ne présentant pas les garanties de sécurité nécessaires, peut conduire à l'interception ou à la collecte de ces informations par un acteur malveillant.

Exposition de fichiers de configuration ou de dépôts de code

L'exposition accidentelle de fichiers de configuration (ex : .env, config.php), de sauvegardes, de dépôts Git ou d'autres ressources contenant des secrets applicatifs peut révéler des identifiants, des clés d'API, des jetons d'authentification ou des mots de passe de bases de données. Ces informations peuvent ensuite être exploitées par un attaquant pour compromettre directement les systèmes d'information ou faciliter des attaques ultérieures.

Hameçonnage (Phishing)

L'utilisateur est incité à renseigner volontairement ses identifiants sur une page frauduleuse reproduisant l'apparence d'un service légitime. Cette technique, fondée sur l'ingénierie sociale, demeure l'un des principaux vecteurs de compromission des comptes utilisateurs.

c. Les failles qui rendent l'hameçonnage possible

Les campagnes d'hameçonnage exploitent rarement un seul facteur de vulnérabilité. Elles tirent parti de faiblesses techniques, organisationnelles et humaines qui facilitent le vol d'identifiants et la compromission des systèmes d'information. Si l'hameçonnage repose avant tout sur des techniques d'ingénierie sociale, son efficacité est largement favorisée par des faiblesses techniques récurrentes observées au cours de l'année 2025. Les analyses menées ont notamment mis en évidence :

- **Absence de configuration des politiques SPF, DKIM et DMARC :** permet l'usurpation de l'identité d'un domaine et facilite l'envoi de courriels frauduleux paraissant légitimes ;
- **Domain Spoofing et Network Spoofing :** rendent crédible l'usurpation d'un domaine ou

d'un flux réseau afin de tromper les utilisateurs ;

- **Weak Password :** favorise les attaques par force brute, par dictionnaire ou l'exploitation d'identifiants déjà compromis ;

- **Broken Authentication :** des mécanismes d'authentification insuffisamment sécurisés ou ne mettant pas en place plusieurs facteurs d'authentification, permettent la compromission de comptes utilisateurs ;

- **Broken Password Reset :** des procédures de réinitialisation de mot de passe mal conçues peuvent conduire à une prise de contrôle de compte.

- **Brute Force OTP :** l'absence de limitation des tentatives sur les codes à usage unique (OTP) peut permettre le contournement de l'authentification multifacteurs.

d. Impact des identifiants exposés

Les identifiants exposés constituent un facteur majeur de compromission des systèmes d'information. Une fois récupérés par un acteur malveillant, ils peuvent être utilisés pour accéder à des comptes légitimes, usurper l'identité d'utilisateurs, diffuser des campagnes d'hameçonnage ou faciliter des fraudes ciblées.

Plus d'un tiers des incidents traités en 2025 (35 %) résulte directement d'une compromission d'identité. Cette corrélation met en évidence que les 977 identifiants exposés recensés ne constituent pas uniquement un indicateur d'exposition, mais représentent un risque opérationnel susceptible de conduire à des compromissions effectives des systèmes d'information.

En alimentant directement plusieurs compromissions, ces identifiants exposés permettent d'établir le lien avec les incidents effectivement traités par le bjCSIRT en 2025, dont l'analyse est présentée ci-après.

9. Analyse des Incidents

a. Causes des incidents

Les incidents observés sur les systèmes d'information ou sur les infrastructures d'information des institutions officielles et OIIC en 2025 montrent que les compromissions ne relèvent pas uniquement de failles techniques. Elles résultent aussi d'une mauvaise hygiène numérique et de lacunes techniques, organisationnelles et humaines. Les causes les plus fréquentes sont les suivantes :

Causes prédominantes :

- **Manque de sensibilisation du personnel (6 cas) :** des erreurs humaines telles que les clics sur des liens frauduleux, le partage d'identifiants ou la mauvaise appréciation d'un message suspect facilitent certaines compromissions ;
- **Sensitive Information Disclosure (4 cas) :** des messages d'erreur, fichiers de configuration, journaux ou identifiants sont exposés ou transmis sans mécanismes de protection suffisants ;
- **Mauvaise implémentation des contrôles adéquats (3 cas) :** des mécanismes essentiels, tels que le contrôle d'accès, la validation des entrées, le filtrage ou la journalisation, sont absents ou appliqués de manière incomplète ;
- **Mauvaise gestion des accès (3 cas) :** des droits excessifs, des comptes inactifs non supprimés ou l'absence de contrôle granulaire favorisent les accès non autorisés ;
- **Correctifs de sécurité non appliqués (2 cas) :** des vulnérabilités connues restent exploitables faute de processus de mise à jour formalisé et suivi.

Autres causes :

- **Plugin malveillant** (2 cas) ;
- **Utilisation de logiciel obsolète** (1 cas) ;
- **Non-respect de l'hygiène numérique** (1 cas) ;
- **Cyberattaque ciblée** (1 cas).

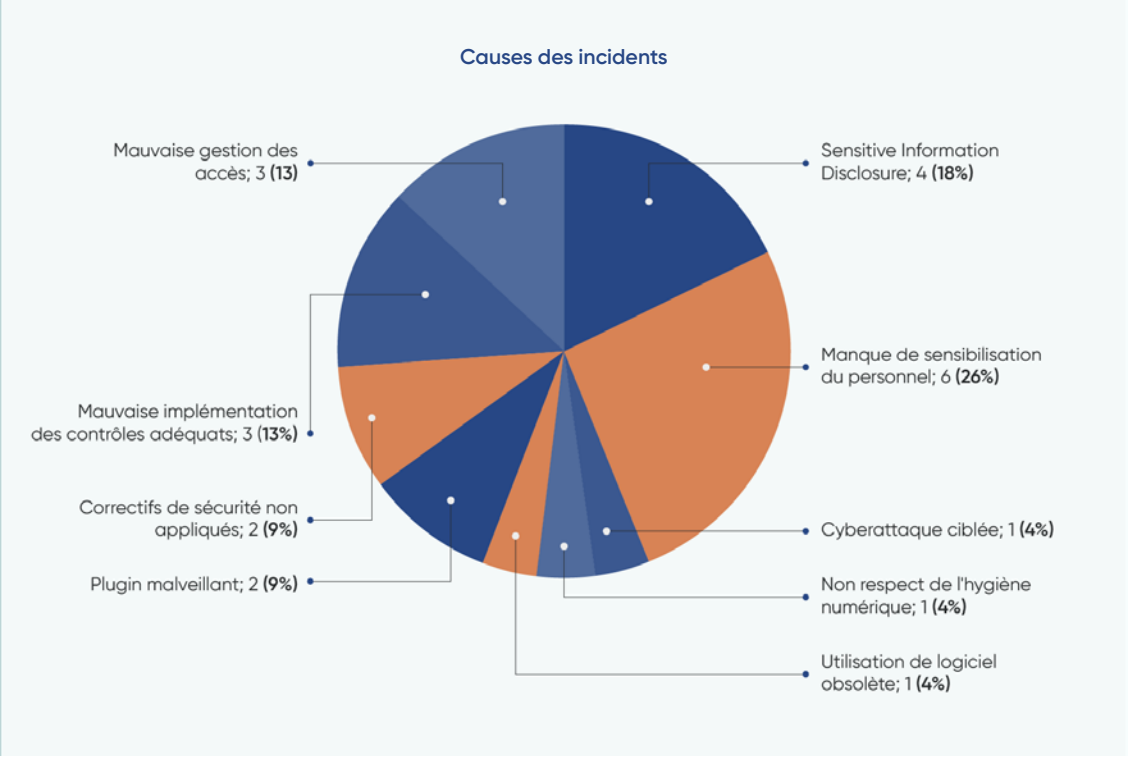
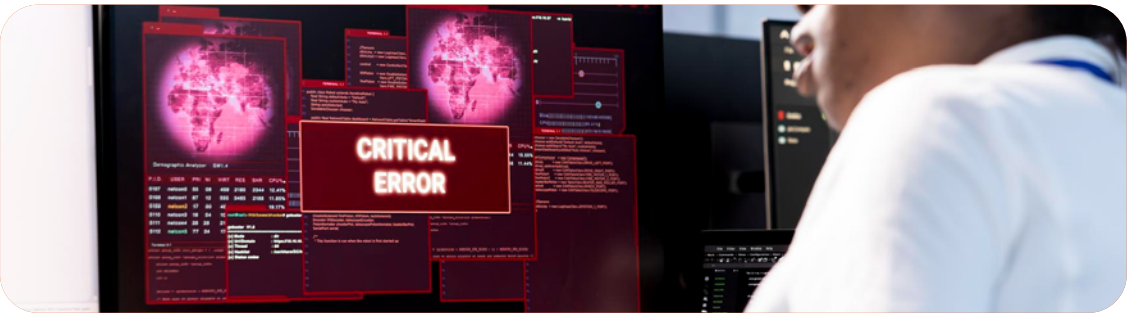


Figure 12 : Causes des incidents de cybersécurité

b. Types des incidents répertoriés

La typologie des incidents recensés permet de mieux comprendre les modes opératoires les plus visibles en 2025. Les cas remontés concernent principalement le phishing, les compromissions de serveurs, les infections par logiciels malveillants, les défacements et les accès non autorisés. Par rapport aux données consolidées de 2021 à 2024, où les malwares, les piratages de sites web et les botnets occupaient une place centrale, la collecte 2025 met davantage en évidence les attaques reposant sur l'humain, les identifiants et les faiblesses de configuration.



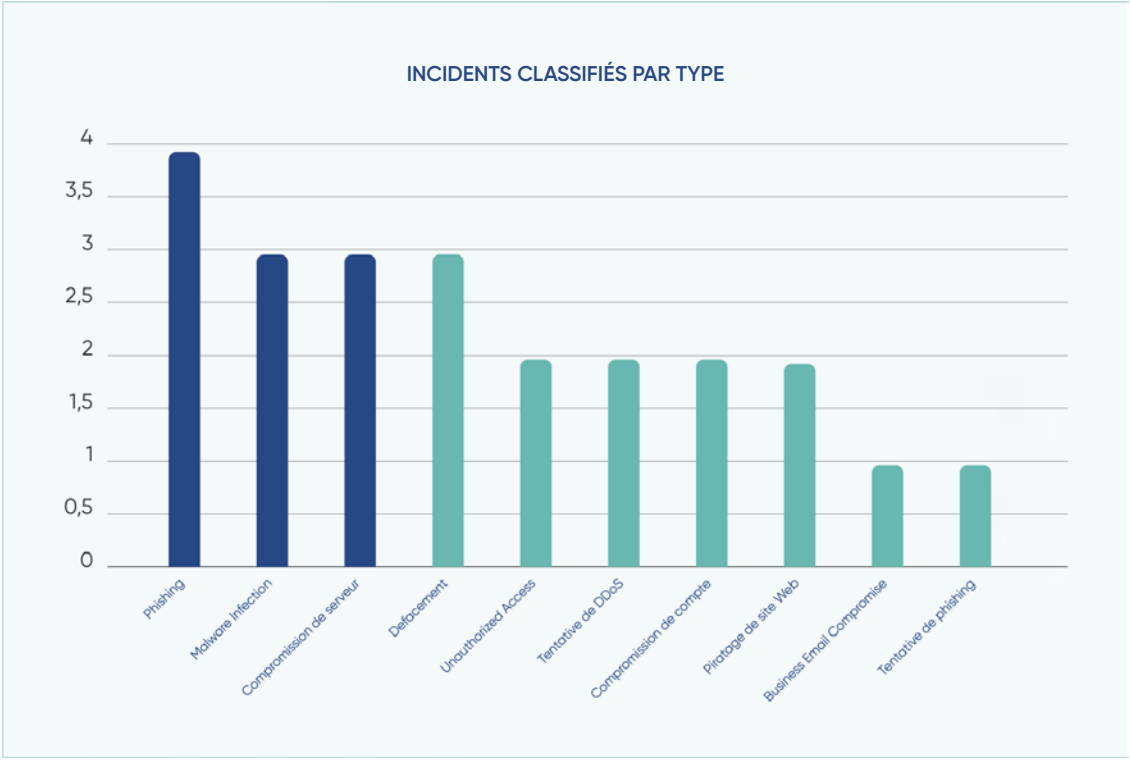


Figure 13 : Incidents de cybersécurité classifiés par type

Incidents les plus fréquents :

- **Phishing (4 cas) :** messages frauduleux conçus pour tromper les utilisateurs et obtenir des identifiants, informations sensibles ou accès non autorisés ;
- **Malware Infection (3 cas) :** introduction de codes malveillants via des pièces jointes, téléchargements non fiables ou périphériques amovibles compromis ;
- **Compromission de serveur (4 cas) :** prise de contrôle ou accès non autorisé à un serveur à la suite d'une faille exploitée, d'un mot de passe faible ou d'une configuration défaillante ;
- **Défacement (3 cas) :** modification non autorisée du contenu de sites web, généralement à la suite d'une compromission applicative ou de failles de sécurité non corrigées ;

- **Unauthorized Access (2 cas) :** accès illégitime à des comptes, applications ou ressources critiques résultant d'un vol d'identifiants ou d'une gestion insuffisante des habilitations.

Autres incidents :

- **Tentative de DDoS** (2 cas) ;
- **Compromission de compte** (2 cas) ;
- **Piratage de site web** (2 cas) ;
- Utilisation de comptes non autorisés, tentative d'escalade de privilèges, injection SQL, etc.

Ces incidents montrent que les attaquants exploitent d'abord les faiblesses les plus accessibles : identifiants exposés, absence de contrôle fort, défaut de supervision ou manque de sensibilisation. La tendance 2025 rappelle ainsi que la sécurité applicative et la sécurité des usages doivent être traitées ensemble.

Plusieurs mesures auraient permis de réduire fortement la probabilité ou l'impact de ces incidents à savoir :

- la mise en œuvre systématique de l'authentification multifacteur ;
- la limitation et la surveillance des tentatives de connexion ;
- le renforcement régulier des campagnes de sensibilisation ;
- la détection précoce d'activités suspectes à partir des journaux et solutions de supervision.

c. Classification des types d'attaques par secteur

Les données confirment que les attaques ne touchent pas les entités de manière uniforme. Certaines menaces, comme l'hameçonnage ou les infections par logiciels malveillants, se concentrent sur des secteurs dont les données, services ou usages numériques présentent un intérêt particulier pour les attaquants.

Phishing

Ce type d'attaque consiste à tromper les utilisateurs au moyen de messages, courriels ou sites frauduleux afin de les inciter à divulguer des informations sensibles, telles que des identifiants de connexion ou des données personnelles.

- **Finance (3 cas) :** secteur particulièrement sensible en raison de la sensibilité des données traitées et de l'impact potentiel d'une compromission sur la crédibilité institutionnelle ;

- **Service Public (1 cas) :** secteur stratégique, porté par la dématérialisation des services et la forte visibilité des plateformes administratives.

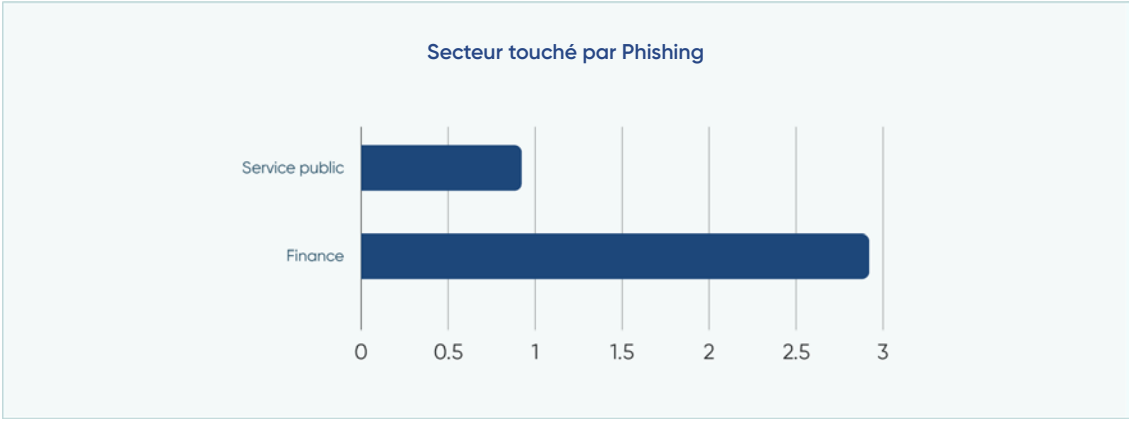
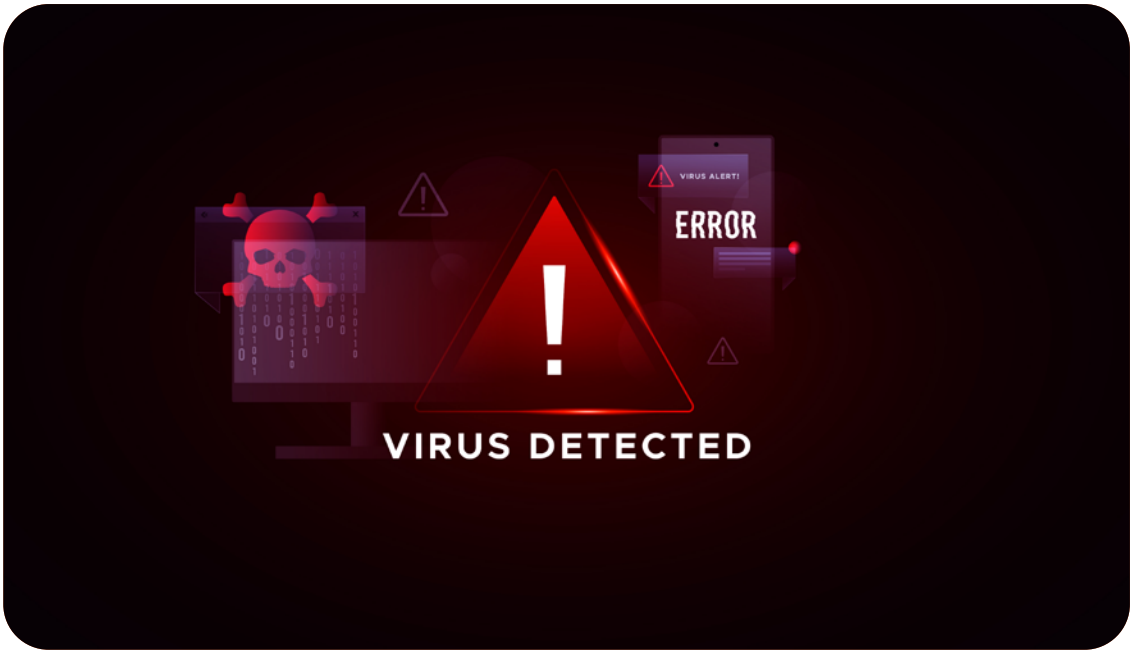


Figure 14 : Secteurs touchés par : Phishing

Infections par logiciels malveillants



Les attaques de type infections par logiciels malveillants ont touché plusieurs secteurs, avec une concentration particulière sur :

- **Finance (1 cas) :** Le secteur financier, très ciblé pour ses données sensibles, est exposé aux trojans bancaires, ransomwares et autres malwares furtifs ;

- **Numérique et Digitalisation (1 cas) :** Cas d'infection généralement associés à des configurations de sécurité insuffisantes ou des utilisateurs non sensibilisés et non formés ;

- **Service Public (1 cas) :** Cas d'infection observé via l'utilisation de périphériques externes, le téléchargement de logiciels provenant de sources non fiables ou l'ouverture de pièces jointes infectées, favorisés par une faible maturité des mécanismes de filtrage et de protection.

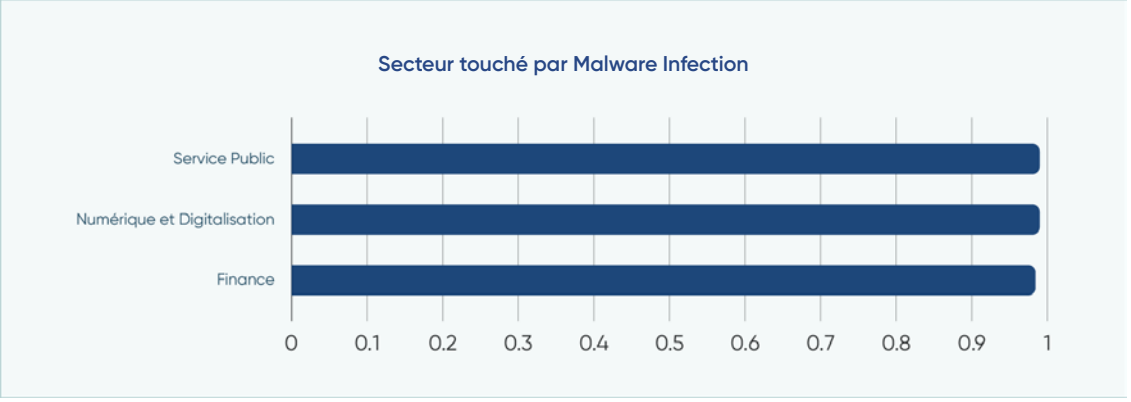


Figure 15 : Secteurs touchés par : Malware Infection

Ces constats rappellent l'importance du filtrage, du contrôle des périphériques, de la mise à jour centralisée des solutions de protection et de l'isolement réseau pour limiter la propagation d'un code malveillant.

d. Évolution des attaques



Figure 16 : Évolution des attaques de 2021 à 2025

L'évolution des attaques doit être interprétée avec nuance. Elle renseigne à la fois sur la pression exercée par les menaces, sur la maturité de détection et sur la capacité des entités à remonter les incidents. Elle révèle un déplacement vers des incidents liés aux comptes, aux accès, à l'hameçonnage et à l'exploitation de faiblesses applicatives ciblées.

Les variations observées peuvent donc traduire simultanément une amélioration du signalement et une pression continue sur les systèmes publics et les infrastructures critiques. Elles confirment l'intérêt d'un suivi annuel : chaque collecte permet de vérifier si les risques déjà connus se maintiennent, diminuent ou se recomposent autour de nouveaux vecteurs d'attaque.

Au-delà du volume d'incidents, les causes récurrentes restent lisibles : configurations insuffisantes, correctifs non appliqués, gestion des accès perfectible et sensibilisation inégale. Ces facteurs montrent que plusieurs incidents peuvent être évités par une discipline de sécurité plus régulière, documentée et suivie.

Si l'analyse des vulnérabilités, des fuites d'identifiants et des incidents dresse un état des lieux de la menace, elle ne suffit pas, à elle seule, à expliquer la persistance de ces risques. Le rapport examine à présent les écarts de conformité relevés au regard de la PSSIE, qui éclairent une partie des causes structurelles évoquées précédemment.

10. Les écarts de conformité à la PSSIE

Dans le cadre de la mise en œuvre opérationnelle de la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE), chaque année, l'ASIN, à travers son service conformité, mène des missions d'inspection visant à mesurer le niveau d'application de ladite politique. Ces évaluations permettent de déterminer les taux de conformité et de relever les écarts constatés dans les différentes institutions publiques.

Ainsi, à l'issue de l'année 2025, le panorama des écarts de conformité met en évidence un facteur clé expliquant la persistance des vulnérabilités et la répétition des incidents à savoir : le degré d'adhésion à la PSSIE.

Conçue pour encadrer la sécurité des systèmes d'information de l'État, cette politique définit des mesures structurantes en matière de gouvernance, de politiques internes, de contrôles techniques et de suivi des incidents.

Lorsque sa mise en œuvre demeure partielle, absente ou mal comprise, les environnements informatiques restent fragiles et exposés à des failles exploitables.

Depuis l'adoption de la PSSIE par le décret N° 2021-550 du 27 octobre 2021, l'ASIN a engagé une démarche proactive d'accompagnement, ciblant les structures dites prioritaires par des audits de conformité.

Ces audits ont permis d'établir un état des lieux précis de la sécurité des systèmes d'information, en identifiant les écarts et en calculant les taux de conformité, qui servent désormais de référence pour orienter les actions correctives et renforcer la résilience numérique de l'État.

a. Présentation de la démarche d'audit

La démarche d'audit mise en œuvre repose sur une approche structurée et fondée sur les risques, visant à apprécier le niveau de conformité du système d'information aux exigences applicables de la **Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)**.

L'évaluation s'appuie sur la **collecte, l'analyse et la corroboration d'éléments probants suffisants et appropriés**, au moyen de revues documentaires, d'entretiens avec les parties prenantes concernées et de vérifications ou tests destinés à confirmer la mise en œuvre effective des mesures de sécurité.

La démarche d'audit s'articule autour des quatre (04) étapes suivantes :

Étape	Description
1. Revue documentaire	Cette phase consiste à examiner les politiques, procédures, référentiels, documents d'architecture, rapports, registres, éléments de configuration et autres documents pertinents du système d'information. Elle vise à identifier les dispositions formalisées et à apprécier leur adéquation au regard des exigences de la PSSIE.
2. Entretiens	Des entretiens sont conduits avec les responsables et acteurs concernés afin de comprendre l'organisation, les processus, les pratiques et les dispositifs de sécurité effectivement mis en œuvre. Ils permettent également de préciser et de compléter les informations issues de la revue documentaire, ainsi que d'identifier les éventuels écarts entre les pratiques déclarées et les dispositions formalisées.
3. Vérifications et tests	Des vérifications et, lorsque cela est pertinent, des tests sont réalisés afin d'apprécier la mise en œuvre effective des mesures de sécurité. Ces travaux portent notamment sur l'examen d'éléments techniques, de configurations, de traces, de registres, d'échantillons ou de situations opérationnelles permettant d'étayer les constats d'audit.
4. Corroboration et évaluation	Les informations recueillies au cours des différentes phases font l'objet d'une corroboration croisée afin d'en apprécier la cohérence, la fiabilité et la suffisance. Cette étape permet de confirmer les éléments probants, de qualifier les éventuels écarts par rapport aux exigences applicables et d'établir le niveau de conformité et de maturité retenu pour chaque domaine évalué.

L'évaluation de la conformité ne se limite pas aux déclarations recueillies lors des entretiens. Les conclusions d'audit s'appuient, dans la mesure du possible, sur **un faisceau d'éléments probants provenant** de sources complémentaires.

Ainsi, une exigence est considérée comme effectivement satisfaite lorsque les éléments recueillis permettent de démontrer, de manière suffisamment fiable :

- l'existence de la mesure ou du dispositif attendu ;
- sa formalisation lorsque celle-ci est requise ;
- sa mise en œuvre effective ;
- et, lorsque cela est pertinent, son fonctionnement régulier et son suivi.

En l'absence d'éléments probants suffisants, la conformité ne peut être considérée comme démontrée sur la seule base d'une déclaration.

b. Panorama des écarts de conformité

Le graphique ci-dessous présente le nombre d'écarts relevés pour chacun des 18 domaines de la PSSIE, pour l'ensemble des structures auditées au cours de l'année 2025.

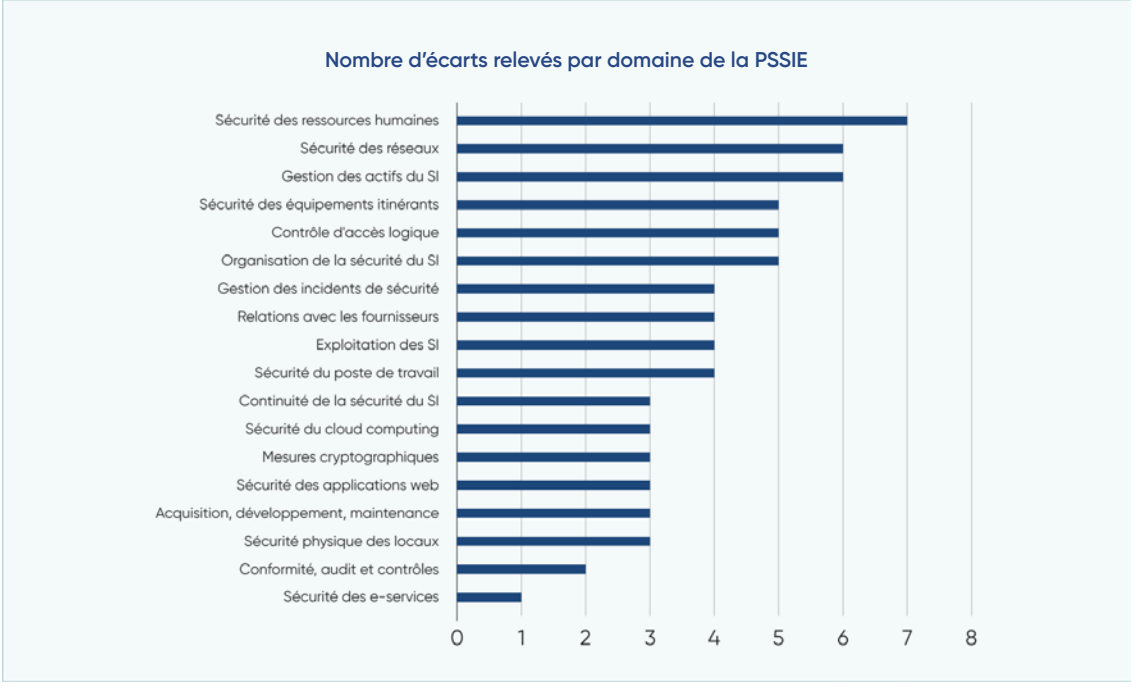


Figure 17 : Nombre d'écarts relevés par domaine de la PSSIE en 2025

c. Détail des écarts de conformité par domaine

Le tableau ci-dessous reproduit l'intégralité des écarts de conformité relevés par domaine de la PSSIE.

N°	Domaine de la PSSIE	Écarts de conformité relevés
1	**Organisation de la sécurité du système d'information**	• Absence de comité de sécurité du SI. • Absence de nomination formelle d'un RSSI. • Absence de charte administrateur définissant les rôles et responsabilités. • Absence de procédure de veille sécurité. • Absence de communication avec les groupes spécialisés en sécurité des SI.
2	**Sécurité des ressources humaines**	• La charte de bonne utilisation du SI n'est pas systématiquement signée par les utilisateurs. • Absence de procédure de gestion de la mobilité et des départs des collaborateurs. • Absence de procédure formelle de retrait des accès logiques et physiques. • Absence de procédure formelle relative au recrutement des rôles de confiance. • Absence de sensibilisation à l'hygiène numérique. • Les nouvelles recrues ne bénéficient pas de formations aux outils et procédures internes. • Absence de document définissant les sanctions en cas de violation des règles de sécurité.
3	**Gestion des actifs du système d'information**	• Absence d'inventaire exhaustif des actifs informationnels. • Absence d'identification formelle des propriétaires d'actifs. • Absence de classification et de catégorisation des actifs. • Absence de grille de classification des actifs du SI. • Absence de chiffrement des supports contenant des données sensibles. • Absence de procédure de gestion des mouvements des supports de données.

N°	Domaine de la PSSIE	Écarts de conformité relevés
4	**Contrôle d'accès logique au système d'information**	• Absence de politique de contrôle d'accès logique. • Absence de procédure de gestion des comptes utilisateurs. • Absence de revue périodique des habilitations. • Gestion insuffisante des comptes à privilèges. • Utilisation de comptes génériques ou partagés.
5	**Sécurité physique des locaux abritant les actifs SI**	• Absence de systèmes de contrôle d'accès aux zones sensibles. • Absence de procédure de gestion des visiteurs dans les locaux sensibles. • Insuffisance des dispositifs de protection contre l'incendie.
6	**Sécurité des réseaux informatiques**	• Absence de matrice des flux réseau. • Cloisonnement réseau insuffisant. • Absence de documentation des flux. • Équipements réseau obsolètes. • Insuffisance des mécanismes de filtrage réseau. • Absence de supervision des réseaux.
7	**Sécurité du poste de travail utilisateur**	• Droits administrateurs accordés aux utilisateurs. • Absence de chiffrement des postes de travail. • Absence de procédure de réaffectation des postes de travail. • Absence de politique d'utilisation des terminaux utilisateurs.
8	**Sécurité des équipements itinérants**	• Absence de chiffrement des équipements nomades. • Absence de filtres de confidentialité. • Absence de câble antivol pour les équipements mobiles. • Absence de procédure de gestion des pertes et vols d'équipements. • Protection insuffisante des données transportées sur les équipements nomades.

N°	Domaine de la PSSIE	Écarts de conformité relevés
9	**Sécurité liée à l'exploitation des SI**	• Absence de procédures formelles d'exploitation. • Journalisation insuffisante des événements de sécurité. • Absence de supervision des actifs critiques. • Absence d'évaluation périodique des vulnérabilités.
10	**Sécurité dans l'acquisition, le développement et la maintenance des SI**	• Absence de prise en compte formelle des exigences de sécurité dans les projets SI. • Absence de procédures de tests de sécurité avant mise en production. • Contrôles de sécurité insuffisants lors des développements applicatifs.
11	**Sécurité des e-services**	• Absence de méthode d'authentification grâce à la cryptographie à clef publique et aux signatures numériques offertes par la PKI nationale.
12	**Sécurité des applications web**	• Absence d'évaluation de sécurité des applications web. • Contrôles de sécurité insuffisants sur les applications exposées sur Internet. • Absence de tests d'intrusion périodiques.
13	**Mesures cryptographiques**	• Absence de politique de cryptographie. • Absence de procédures de protection des clés cryptographiques. • Utilisation insuffisante des mécanismes cryptographiques pour protéger les données sensibles.
14	**Relations avec les fournisseurs**	• Absence d'exigences de sécurité dans les contrats fournisseurs. • Absence d'accords de confidentialité (NDA). • Absence de journalisation des activités réalisées par les prestataires. • Absence d'évaluation des risques liés aux tiers

N°	Domaine de la PSSIE	Écarts de conformité relevés
15	**Sécurité du cloud computing**	• Absence d'encadrement de l'utilisation des services cloud. • Absence d'évaluation des risques liés au cloud computing. • Contrôles de sécurité insuffisants sur les services cloud utilisés.
16	**Gestion des incidents de sécurité**	• Absence de procédure de signalement des incidents. • Absence de procédure de réponse aux incidents. • Absence de registre des incidents de sécurité. • Absence de mécanisme formel de suivi et de traitement des incidents.
17	**Gestion de la continuité de la sécurité du SI**	• Absence de plan de continuité de la sécurité du SI. • Absence de PCA/PRA. • Absence de redondance des systèmes critiques.
18	**Conformité, audit et contrôles de sécurité**	• Absence de charte d'audit de sécurité formalisée. • Absence de suivi interne de la conformité à la PSSIE.

d. Analyse des écarts de conformité relevés

Un déficit de formalisation

La majorité des écarts relevés (plus de 9 constats sur 10) se traduit par une « absence » : absence de politique, de procédure, de charte, de comité ou de dispositif formel. Ce constat indique que l'un des freins à la conformité avec la PSSIE est un déficit de gouvernance et de formalisation des processus de sécurité.

Une gouvernance à fonder en priorité

Les domaines « Organisation de la sécurité du système d'information » ; « Sécurité des ressources humaines » ; « Gestion des actifs du système d'information » et « Contrôle d'accès logique au système d'information » concentrent à eux seuls 23 écarts, soit près d'un tiers du total. L'absence de comité de sécurité, de RSSI nommé et de charte administrateur prive les entités d'un pilotage formel de la sécurité, ce qui explique en partie la récurrence des écarts dans les autres domaines. En effet, sans gouvernance claire, les politiques et procédures ont plus de mal à être définies, portées et maintenues dans la durée.

Des risques opérationnels et de résilience à ne pas sous-estimer

Les domaines « Sécurité des réseaux informatiques » (6 écarts) et « Gestion des actifs du système d'information » (6 écarts) figurent parmi les plus impactés après la gouvernance et les ressources humaines. À cela s'ajoutent les thématiques « Incidents & Continuité » et « Poste de travail & Itinérance » (7 et 9 écarts). L'absence conjointe de procédure de réponse aux incidents, de registre des incidents et de plan de continuité (PCA/PRA) constitue un point d'attention particulier : en cas d'incident de sécurité avéré, les entités auditées ne disposent aujourd'hui d'aucun dispositif formel de détection, de réponse ou de reprise d'activité.

Une gouvernance des tiers et du cloud encore émergente

Les relations avec les fournisseurs et l'usage du cloud computing totalisent sept (07) écarts, marqués par l'absence quasi générale d'exigences de sécurité contractuelles, d'accords de confidentialité et d'évaluation des risques liés aux tiers. Cela reflète un risque croissant à mesure que l'entité externalise des services ou des infrastructures, l'absence de cadre de gouvernance des tiers expose à des risques dont la maîtrise échappe largement au périmètre interne.

e. Panorama des taux de conformité

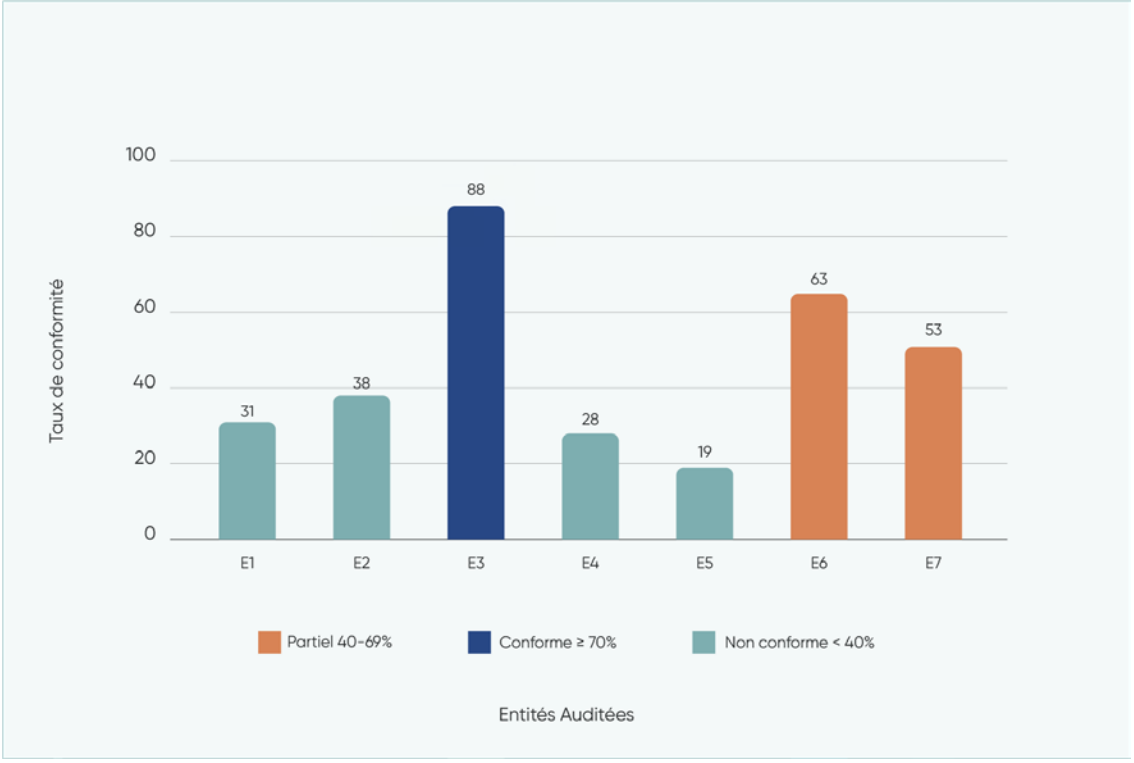


Figure 18 : Vue d'ensemble des taux de conformité

Globalement, d'après le graphique ci-dessus, les taux de conformité des entités auditées sur l'année 2025 varient de 19 % à 88 %.

En appliquant le seuil de conformité de 70 %, seulement une (01) entité sur sept (07) est conforme, soit 14,3 % du panel audité. E3 est la seule à franchir ce cap avec 88 % de taux de conformité. Les 85,7 % d'entités restantes demeurent en situation de non-conformité.

Parmi ces entités non conformes, trois (E2, E6 et E7) affichent néanmoins des taux compris entre 40 % et 69 %, traduisant une conformité partielle avec respectivement 38 %, 63 % et 53 %. Les trois entités restantes (E1, E4, E5) se situent en deçà des 40 %, reflétant une mise en œuvre très insuffisante des exigences de la PSSIE.

Cela montre que la mise en conformité est globalement faible et que la majorité des exigences de la PSSIE ne sont pas respectées

11. Recommandations spécifiques

Les recommandations spécifiques formulées ci-après découlent directement de l'analyse consolidée des constats relevés au sein des entités auditées en 2025 :

Renforcer la formalisation du dispositif de sécurité

Il est recommandé de mettre en place un socle documentaire de sécurité formel, cohérent et maintenu dans le temps, couvrant notamment les politiques, procédures, chartes, référentiels et processus nécessaires à la mise en œuvre des exigences de la PSSIE.

À cet effet, les entités devraient prioritairement :

- élaborer ou actualiser leur Politique de Sécurité des Systèmes d'Information (PSSI) ;
- formaliser les procédures relatives aux principaux processus de sécurité, notamment la gestion des accès, des incidents, des actifs, des changements, des sauvegardes et de la continuité d'activité ;
- établir les chartes nécessaires, notamment la charte utilisateur et la charte d'administration des systèmes d'information ;
- définir les responsables, propriétaires et contributeurs associés à chaque processus de sécurité ;
- mettre en place un mécanisme de revue périodique, de validation et de mise à jour de la documentation ;
- assurer la traçabilité de l'approbation et de la diffusion des documents de sécurité auprès des parties prenantes concernées.

L'objectif est de passer d'une logique de conformité fondée sur l'existence ponctuelle de documents à un système documentaire vivant, intégré au fonctionnement courant de l'organisation.

Établir en priorité une gouvernance formelle de la sécurité de l'information

Compte tenu de la concentration des écarts dans les domaines liés à l'organisation de la sécurité, aux ressources humaines, aux actifs et au contrôle des accès, il est recommandé de prioriser la mise en place d'un dispositif de gouvernance clairement défini.

Cette gouvernance devrait notamment prévoir :

- la désignation formelle d'un responsable de la sécurité des systèmes d'information (RSSI) ou d'une fonction équivalente ;
- la création ou la formalisation d'un comité de sécurité de l'information, doté d'un mandat, de responsabilités et d'une fréquence de réunion définis ;
- la formalisation des règles applicables aux comptes privilégiés et aux administrateurs systèmes, notamment à travers une charte ;
- la mise en place d'un mécanisme de pilotage des risques de sécurité, permettant de suivre les risques, les plans d'action, les incidents et les écarts de conformité ;
- l'intégration des enjeux de sécurité dans les processus de décision, de gestion des projets et de transformation numérique.

La gouvernance doit constituer le premier niveau de maîtrise permettant d'assurer que les politiques, procédures et mesures de sécurité sont effectivement définies, déployées, contrôlées et maintenues dans le temps.

Renforcer la maîtrise des risques opérationnels et la résilience

Au regard du nombre d'écarts affectant les réseaux, les actifs, les postes de travail ainsi que la gestion des incidents et la continuité d'activité, il est recommandé de renforcer prioritairement les capacités de prévention, de détection, de réponse et de reprise face aux incidents de sécurité.

Les entités devraient notamment :

- formaliser un processus de gestion des incidents de sécurité, précisant les modalités de détection, qualification, escalade, traitement, communication et clôture ;
- mettre en place un registre centralisé des incidents de sécurité permettant d'assurer leur traçabilité et leur analyse ;
- définir les rôles et responsabilités des différents intervenants dans la réponse aux incidents ;
- réaliser des exercices périodiques de gestion de crise et de réponse aux incidents afin d'évaluer l'efficacité du dispositif ;
- élaborer et maintenir un Plan de Continuité d'Activité (PCA) et un Plan de Reprise d'Activité (PRA) proportionnés aux risques identifiés ;
- identifier les actifs et services critiques, leurs dépendances ainsi que les exigences de

- disponibilité et de reprise associées ;
- renforcer la gestion du cycle de vie des actifs, notamment leur inventaire, leur classification, leur affectation et leur mise au rebut ;
- renforcer les mesures de sécurité relatives aux réseaux et aux postes de travail, notamment en matière de supervision, de durcissement, de mise à jour et de protection contre les menaces.

L'objectif est de faire évoluer les entités d'une posture principalement préventive et documentaire vers une capacité effective de résilience, leur permettant de limiter l'impact d'un incident et de rétablir rapidement les services critiques.

Structurer la gouvernance des tiers et des services cloud

Compte tenu du recours aux fournisseurs, prestataires et services cloud, il est recommandé de mettre en place un cadre de gestion des risques liés aux tiers, intégré au cycle de vie des relations contractuelles.

Ce dispositif devrait notamment prévoir :

- une évaluation préalable des risques de sécurité associés aux fournisseurs et prestataires critiques ;
- la définition de critères de sécurité applicables à la sélection et à la qualification des tiers ;
- l'intégration d'exigences de sécurité dans les contrats, notamment en matière de confidentialité, de protection des données, de contrôle d'accès, de notification des incidents, de sauvegarde, de continuité et de réversibilité ;
- la formalisation d'accords de confidentialité (NDA) lorsque la nature des informations échangées le justifie ;
- la définition de responsabilités claires entre l'entité et le fournisseur selon le principe de responsabilité partagée, particulièrement pour les services cloud ;
- la réalisation périodique d'évaluations ou de revues de sécurité des fournisseurs présentant un niveau de criticité élevé ;
- l'intégration des risques liés aux tiers dans le registre des risques de l'organisation et dans les mécanismes de suivi du risque résiduel ;
- la définition de mesures de réversibilité et de sortie afin de limiter la dépendance à un fournisseur et de garantir la continuité des services critiques.

L'enjeu est de faire évoluer la gestion des fournisseurs d'une approche essentiellement contractuelle et opérationnelle vers une véritable gouvernance du risque tiers, permettant de maintenir un niveau de maîtrise acceptable lorsque tout ou partie des services, infrastructures ou données sont externalisés.

Ces recommandations spécifiques, ciblées sur les écarts constatés lors des audits, doivent s'accompagner de mesures transversales, valables pour l'ensemble des structures publiques, indépendamment de leur niveau de conformité actuel.

12. Recommandations globales

Au-delà des mesures correctives directement associées aux constats relevés, il s'avère nécessaire de renforcer certaines mesures à caractère transversal, susceptibles de favoriser durablement l'amélioration du niveau de sécurité des systèmes d'information au sein des structures publiques.

Ces recommandations portent principalement sur la gouvernance, les moyens budgétaires, le renforcement des capacités, la surveillance des systèmes d'information et l'amélioration continue du niveau de sécurité.

À ce titre, il est recommandé aux structures publiques de :

- **Poursuivre les actions de sensibilisation des hauts dirigeants** aux enjeux de cybersécurité, afin de renforcer leur implication dans la gouvernance de la sécurité de l'information et de favoriser une prise de décision intégrant systématiquement les enjeux de risque numérique ;

- **Poursuivre les démarches visant à institutionnaliser la fonction de RSSI** au sein de l'architecture organisationnelle type des ministères et institutions de l'État, en veillant à garantir son positionnement, son indépendance fonctionnelle et la clarification de ses responsabilités ;

- **Poursuivre l'opérationnalisation de la fonction RSSI** au sein des entités assujetties à la PSSIE, notamment par la formalisation de ses missions, de ses responsabilités, de ses moyens d'action et de ses modalités d'interaction avec les autres fonctions de l'organisation ;

- **Renforcer les capacités des RSSI et des équipes impliquées dans la sécurité des systèmes d'information**, au moyen de programmes réguliers de formation, de perfectionnement et de partage d'expérience adaptés à l'évolution des menaces et des exigences réglementaires ;

- **Prévoir une ligne budgétaire dédiée à la cybersécurité et à la mise en conformité avec la PSSIE** au sein des entités concernées. Cette allocation devrait permettre de financer de manière prévisible les actions de remédiation, les audits, la formation, les dispositifs techniques de sécurité et les mesures de maintien en condition de sécurité ;

- **Mettre en place ou renforcer les dispositifs de surveillance des systèmes d'information**, notamment à travers la centralisation et l'analyse des journaux d'événements, la mise en place d'alertes de sécurité en temps réel et le déploiement de tableaux de bord permettant au RSSI et aux instances de gouvernance de disposer d'une visibilité régulière sur le niveau de sécurité du SI ;

- **Renforcer les politiques et mécanismes de contrôle des accès**, notamment par l'application d'exigences de robustesse des mots de passe, la revue périodique des habilitations, l'application du principe du moindre privilège, la gestion rigoureuse des comptes à privilèges et, lorsque cela est techniquement et opérationnellement possible, le déploiement de l'authentification multifacteur ;

- **Intégrer durablement la cybersécurité dans les dispositifs de formation continue** du personnel technique et non technique. Cette démarche devrait être complétée par l'organisation ou la participation régulière à des exercices de simulation de gestion de crise cyber, afin de tester la capacité des entités à coordonner leur réponse face à un incident majeur ;

- **Instituer un dispositif d'audit périodique de la sécurité des systèmes d'information**, avec une cible d'au moins un audit annuel pour les entités présentant un niveau de criticité ou d'exposition élevé. Les recommandations issues des audits devraient faire l'objet d'un plan d'action formalisé, assorti de responsables, d'échéances et d'indicateurs de suivi, afin de s'assurer de leur mise en œuvre effective ;

- **Renforcer le suivi et la prise en compte des alertes de sécurité émises par le bjCSIRT**, en veillant à leur diffusion auprès des responsables concernés, à leur qualification et à la mise en œuvre des mesures correctives ou préventives appropriées dans les délais compatibles avec le niveau de criticité de la menace ;

- **Mettre en place un mécanisme de pilotage consolidé de la conformité et de la maturité en cybersécurité**, permettant de suivre périodiquement l'évolution des niveaux de conformité à la PSSIE, l'état d'avancement des plans de remédiation, les incidents de sécurité, les risques résiduels et les principaux indicateurs de sécurité.

La mise en œuvre de ces recommandations devrait s'inscrire dans une démarche d'**amélioration continue**, articulant gouvernance, ressources, compétences, mesures techniques et contrôle. L'enjeu n'est donc plus uniquement de résorber les écarts de conformité constatés, mais de permettre aux structures publiques de disposer d'un **dispositif de sécurité durable, piloté par le risque et capable de s'adapter à l'évolution de la menace cyber**.

À terme, cette approche doit permettre de faire de la conformité à la PSSIE non pas un exercice ponctuel lié aux audits, mais un **processus permanent de maîtrise des risques et d'amélioration de la résilience numérique de l'administration publique.**

13. Conclusion

L'édition 2025 du rapport met en perspective l'état de la cybersécurité observé en 2025 au sein du périmètre couvert par le bjCSIRT. Après un premier exercice consacré aux données consolidées de 2021 à 2024, cette nouvelle collecte annuelle permet d'observer plus finement les continuités et les évolutions du risque. Elle montre un environnement numérique en croissance, exposé à des risques persistants, mais aussi mieux documenté grâce aux efforts de collecte, d'analyse et de réponse menés par l'ASIN.

Les vulnérabilités recensées rappellent que la réduction du risque repose d'abord sur des pratiques régulières : configuration maîtrisée, gestion rigoureuse des accès, mise à jour des systèmes, supervision et sensibilisation. La permanence du contrôle d'accès défaillant, la progression des vulnérabilités exploitables à distance et le niveau élevé des fuites d'identifiants confirment la nécessité d'une posture active et anticipative.

Les constats relatifs à la conformité rappellent enfin que la cybersécurité ne se limite pas aux outils techniques. Elle exige une gouvernance claire, des responsabilités établies, des contrôles suivis et une culture de sécurité portée par chaque entité.

Ce rapport doit donc être utilisé comme un instrument de pilotage et d'action. Il invite les décideurs, responsables techniques et parties prenantes à renforcer la coordination, à prioriser les remédiations et à inscrire durablement la cybersécurité au cœur de la résilience numérique nationale.



Annexe

Évaluation des risques associés aux vulnérabilités

Le bjCSIRT évalue la criticité des vulnérabilités identifiées en s'appuyant sur la méthodologie d'évaluation OWASP.

Le niveau de risque est déterminé à partir de deux dimensions : l'impact potentiel et la probabilité d'occurrence. La relation utilisée est la suivante : **Risque = Impact x Probabilité**.

Impact

Les impacts technique et commercial d'une vulnérabilité sont échelonnés en termes de gravité comme suit :

Elevé	Modéré	Faible

Elevé : les vulnérabilités à impact élevé sont des vulnérabilités ayant des conséquences négatives graves sur la confidentialité, l'intégrité, la disponibilité ou la non-répudiation des systèmes d'information, des données qu'ils hébergent ou qui y transitent, ainsi que le métier qui les utilise. Ces conséquences peuvent être la compromission du système d'information, la perte d'intégrité ou de la confidentialité des données jugées sensibles, l'indisponibilité partielle ou totale du service.

Modéré : les vulnérabilités à impact modéré sont des vulnérabilités ayant des conséquences négatives certaines pouvant perturber le bon fonctionnement des systèmes d'information et des données qu'ils hébergent.

Faible : les vulnérabilités à impact faible sont des vulnérabilités ayant des conséquences mineures sur les systèmes d'information si elles venaient à être exploitées.

Probabilité d'occurrence

La **probabilité de découverte et d'exploitation** (dénommée ci-après probabilité d'occurrence) d'une vulnérabilité est échelonnée comme suit :

Elevé	Probable	Faible

Élevé : vulnérabilité facile à découvrir et à exploiter.

Probable : il existe une certaine probabilité qu'un attaquant pertinent puisse découvrir cette vulnérabilité et arrive à l'exploiter.

Faible : vulnérabilité difficile à découvrir et surtout à exploiter. Son exploitation requiert un attaquant expérimenté qui cible particulièrement la plateforme.

Risques associés

À partir de l'impact et de la probabilité d'occurrence, nous arrivons à la matrice de classification du risque ci-après :

RISQUES ASSOCIES AUX VULNERABILITES				
IMPACT	ÉLEVÉ	Modéré	Élevé	Critique
	MODÉRÉ	Faible	Modéré	Élevé
	FAIBLE	Note	Faible	Modéré
		FAIBLE	PROBABLE	ÉLEVÉ
		PROBABILITE		

Cette matrice sert de référence pour qualifier le niveau de risque associé aux vulnérabilités identifiées.



Rapport annuel de vulnérabilités et d'incidents

Vulnérabilités, incidents et écart de conformité
du cyberespace béninois.

Suivez-nous sur nos
canaux digitaux

@asinbenin