STRATEGIE NATIONALE DE SECURITE NUMERIQUE

2023-2026

Un cyberespace sécurisé et attrayant pour une économie numérique florissante

PREFACE

Sous l'égide éclairée du Président de la République, le Bénin a franchi des étapes significatives dans sa transformation digitale, capitalisant sur les fondations solides établies pendant la première phase du Programme d'Action du Gouvernement (PAG1). Aujourd'hui, la mise en œuvre de la première Stratégie Nationale de Sécurité Numérique du Bénin (SNSN), initiée suivant les directives de l'Union Internationale des Télécommunications (UIT), nous a permis de nous rapprocher davantage de nos objectifs ambitieux d'inclusion numérique et de protection du cyberespace national. Plus de 80% des Béninois sont désormais connectés à l'univers numérique, et une majorité impressionnante utilise quotidiennement Internet, témoignant de l'efficacité de notre approche inclusive et avant-gardiste.

Le numérique continue sa révolution en Afrique, et le Bénin s'est fermement positionné comme un hub d'innovations dans cette révolution globale. Notre ambition, clairement énoncée, de faire du Bénin la référence en matière de plateformes de services numériques en Afrique de l'Ouest, se concrétise chaque jour. Les technologies de l'information et de la communication, pierre angulaire de notre développement socio-économique, ont été transformées, portées par une stratégie qui a su créer des compétences locales en cybersécurité, protéger nos infrastructures d'information critiques, et mettre en place un cadre réglementaire attractif et sécurisé.

Aujourd'hui, en réaffirmant notre engagement vers une mise à jour de cette stratégie, je m'adresse à vous avec une conviction renouvelée. La première phase de notre stratégie a profondément changé le paysage numérique au Bénin, renforçant la sécurité de nos infrastructures numériques et établissant une confiance digitale sans précédent. Elle a stimulé la création de nouveaux métiers et ouvert des horizons d'opportunités d'emploi inédits à notre jeunesse.

En intégrant vingt-cinq (25) nouvelles actions clés, pour la période 2023-2026, nous avons posé les jalons d'une économie dynamisée par la confiance numérique et l'innovation. Cette stratégie actualisée et en parfaite adéquation avec les défis et les opportunités actuels, continue de témoigner de l'engagement du Gouvernement à protéger les données personnelles et celles des entreprises. Elle est la preuve vivante de notre reconnaissance de l'importance vitale d'un cyberespace sécurisé pour chaque citoyen, chaque entreprise et pour la nation toute entière, qui contribue à faire avancer notre économie.

En tant que Ministre du Numérique et de la Digitalisation, je réitère mon engagement à travailler en synergie avec tous les acteurs de l'écosystème, nos partenaires internationaux et la société civile, pour que cette nouvelle phase soit un succès retentissant et consolide la position du Bénin en tant que leader africain du développement numérique dans un cyberespace sécurisé.

Aurelie I. ADAM SOULE ZOUMAROU

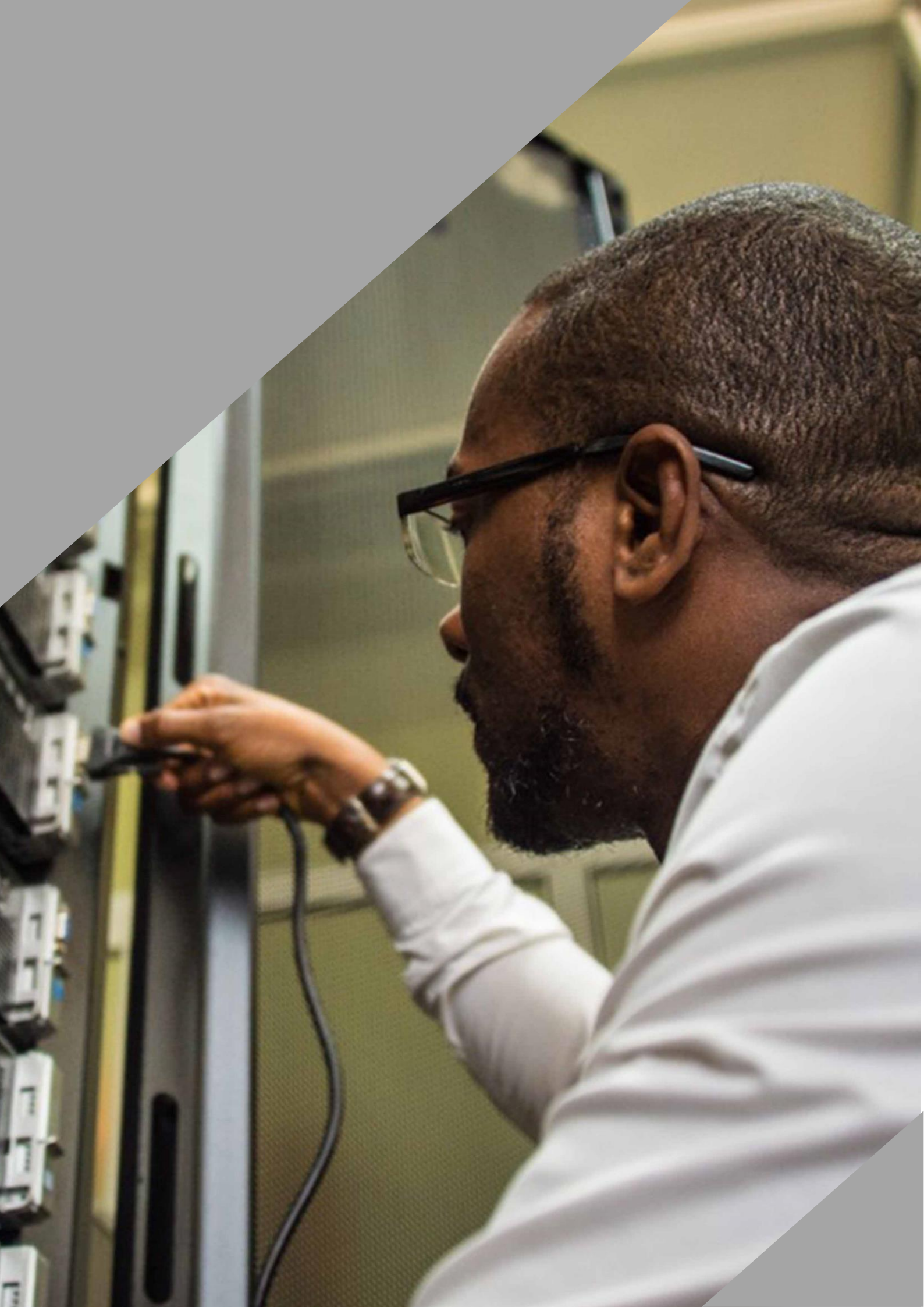
SOMMAIRE

INTRODUCTION

À l'ère de la transformation numérique fulgurante, le Bénin a fait des avancées considérables dans l'intégration des Technologies de l'Information et de la Communication (TIC) dans la vie quotidienne de ses citoyens. Sous la direction éclairée du Gouvernement, une métamorphose remarquable du Bénin en une société numérique est constatée à travers l'adoption des TICs dans le quotidien des Béninois. Grâce aux efforts déployés dans le cadre du Programme d'Action du Gouvernement (PAG 1 & 2), il est remarqué une prolifération exponentielle de l'usage des TICs dans les secteurs public et privé avec à la clé, plusieurs dizaines de services publics dématérialisés.

Ces avancées, tout en étant sources d'opportunités, ont également révélé de nouvelles dépendances vis-à-vis des systèmes, des données et des infrastructures numériques, soulevant ainsi la question cruciale de leur sécurité. L'expérience béninoise dans cette transformation numérique, jalonnée de succès, a confronté l'écosystème à des cybermenaces croissantes, avec des acteurs malveillants employant des méthodes sophistiquées.

Face à ces défis, la protection des systèmes et informations devient une priorité nationale, soulignant l'importance capitale d'un cyberespace sécurisé. La mise à jour de la Stratégie Nationale de Sécurité Numérique du Bénin (SNSN) pour couvrir la période (2023-2026) reflète cette ambition. Elle vise non seulement à consolider les acquis d'une transformation numérique réussie, mais à anticiper et neutraliser les menaces actuelles et émergentes, assurant ainsi la pérennité et la confiance dans l'usage du numérique.



1. CONTEXTE

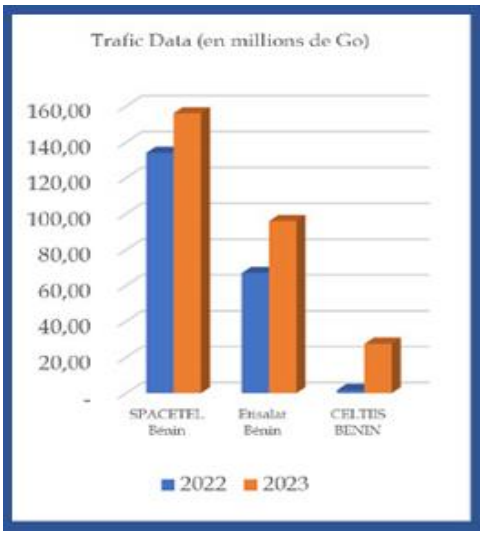
Embrassant résolument la digitalisation de l'administration publique et des services aux populations, le Bénin a fait le choix stratégique de placer le développement numérique au cœur de son essor économique et social. Depuis plusieurs années, des efforts soutenus ont été déployés pour élaborer une stratégie robuste, ponctuée par la mise en place d'infrastructures de pointe et l'adoption de réformes structurelles et réglementaires essentielles. Les fruits de cette stratégie sont déjà visibles et multiples. Nous notons par exemple l'interconnexion à la fibre sous-marine, l'extension du réseau de fibre optique reliant divers sites et localités du pays, l'augmentation significative de la disponibilité de l'Internet filaire et sans fil, et la restructuration de manière stratégique du secteur des télécommunications.

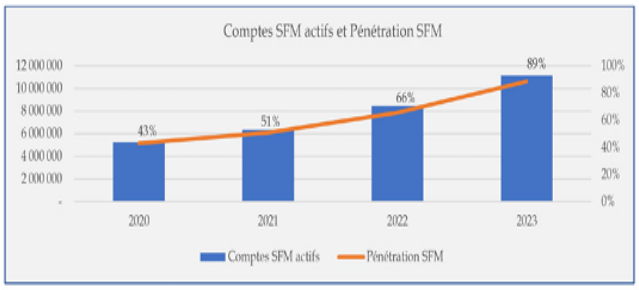
La création en 2022 de l'Agence des Systèmes d'Information et du Numérique (ASIN), par la fusion d'autres entités clés telles que l'ADN[1], l'ASSI[2] et l'ANSSI[3], marque un jalon important, renforçant notre cadre institutionnel pour le développement du secteur du numérique. Par ailleurs, le lancement ambitieux du Datacenter National de type TIA-942 et Tier III, et le développement d'une variété d'applications sectorielles en ligne telles que le portail national des services publics, témoignent de la progression constante du pays vers une économie numérique dynamique et intégrée. Ces initiatives illustrent l'engagement à transformer le Bénin en un écosystème numérique florissant, en phase avec les standards internationaux et répondant aux aspirations du peuple.

Les données statistiques fournies dans le rapport annuel d'activités de l'année 2023 de l'Autorité de Régulation des Communications Electroniques et de la Poste du Bénin (ARCEP Bénin) viennent conforter cette volonté manifeste de révolutionner le numérique. Ainsi, le trafic Internet mobile continue sa croissance exponentielle avec un volume de 280 millions de Go en 2023, soit une croissance de 37,8% par rapport à 2022. Le nombre de comptes associés aux services financiers mobiles a atteint 11 171 087 clients en 2023, soit un accroissement de 32% par rapport à 2022. Le taux de pénétration des services financiers via la téléphonie mobile a atteint 89% au 31 décembre 2023 contre 66% en 2022. Ces chiffres mettent en exergue le

[1] Agence pour le Développement du Numérique
[2] Agence des Services et Systèmes d'information
[3] Agence Nationale de la Sécurité des Systèmes d'Information

changement d'habitude de consommation des services numériques par la population.





Source : Rapport annuel d'activités 2023, ARCEP.

2. POINT DE MISE EN ŒUVRE DE LA SNSN 2020-2023

Le 06 mai 2020, le Gouvernement béninois a approuvé en Conseil des Ministres, la première Stratégie Nationale de Sécurité Numérique (SNSN) couvrant la période 2020-2023. Cette stratégie nationale traduit la vision de l'Etat de bâtir une confiance numérique forte et dénote aussi de son engagement à rassurer ses partenaires nationaux et internationaux. La mise en œuvre de cette stratégie a permis de sécuriser les processus de digitalisation de l'administration publique et renforcer le service aux citoyens et aux entreprises par la généralisation des e-services et la mise en place du réseau national de l'administration (RNA).

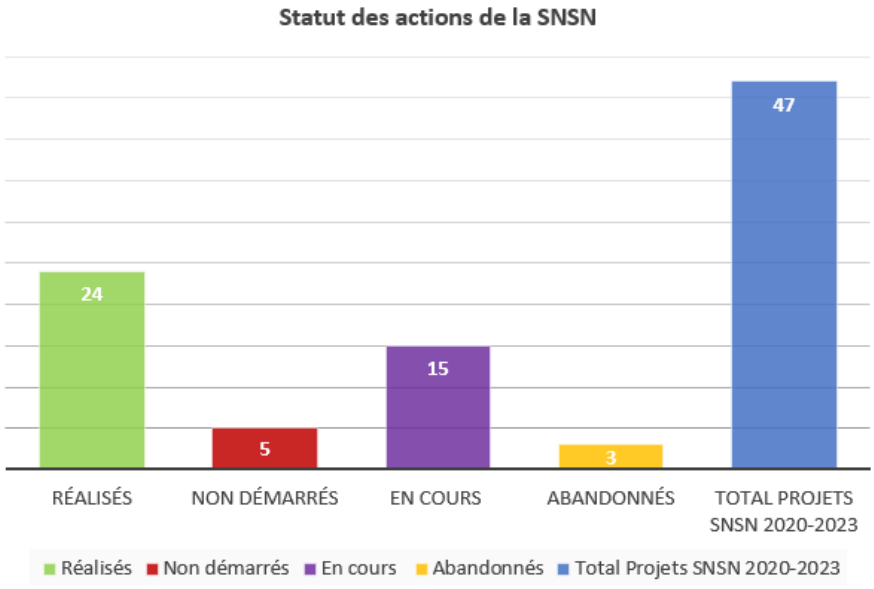
La première version de la stratégie compte quarante-sept (47) actions réparties sur cinq (05) axes et planifiées sur trois (03) années. Sa mise en œuvre a considérablement contribué à améliorer le niveau de sécurité global du cyberespace national. L'évaluation de l'implémentation de ces quarante-sept (47) actions au cours de l'atelier organisé en avril 2023 indique un taux de réalisation global de 71% des projets. Le détail des statistiques se présente comme suit :

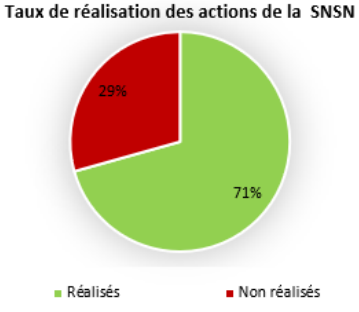
- vingt-quatre (24) projets complétés
- cinq (05) projets non démarrés
- quinze (15) projets en cours
- trois (03) projets abandonnés.

La mise en œuvre de la stratégie a permis au Bénin de se hisser à la 6ème place africaine et 56ème dans le classement international d'après le rapport du Global Cybersecurity Index (GCI) publié en juin 2021, par l'Union Internationale des Télécommunications. D'autres données statistiques mettent en exergue la progression remarquable du pays et justifient de la volonté de l'Etat béninois à poursuivre son œuvre de promotion de la cybersécurité. Ainsi, le National Cyber Security Index (NCSI) positionne le Bénin à la 58ème place, dans son rapport de septembre 2023.

Il est prévu que le nouveau classement fournira un meilleur positionnement du Bénin sur l'échiquier international. Ceci suscitera davantage un intérêt auprès des acteurs internationaux et les investisseurs dans le domaine du numérique sur le potentiel technologique et humain du Bénin.

La stratégie a bénéficié globalement d'une mobilisation satisfaisante des ressources financières nécessaires à sa mise en œuvre, même si ces ressources peuvent être augmentées pour une meilleure efficacité.





3. LE DIAGNOSTIC DU SECTEUR DE LA SECURITE NUMERIQUE

L'adoption généralisée du numérique et le développement technologique induit une hausse des cybermenaces due aux facteurs ci-après :

- L'exposition des systèmes qui s'ouvrent sur des réseaux externes et essentiellement sur Internet
- la complexité des environnements technologiques par la superposition de plusieurs couches applicatives, parfois hétérogènes et assez difficiles à maîtriser
- l'enrichissement des systèmes par l'acquisition massive des données dont le degré de sensibilité varie entre des données personnelles et des données économiques, voire des données critiques de l'État
- la vulgarisation de la technologie et le taux de pénétration de l'Internet qui font en sorte que les simples citoyens qui accèdent à la technologie, s'exposent davantage et risquent de compromettre leurs données par simple ignorance
- la démocratisation de la technologie joue aussi au profit des cybercriminels qui y trouvent des outils faciles et accessibles pour commettre leurs crimes
- les systèmes d'intelligence artificielle amplifiant les cybermenaces notamment les escroqueries et manipulations de contenu, les faux comptes et bots, les attaques de phishing améliorées, les cyberattaques automatisées, et l'évasion de la sécurité.

Au Bénin, ces facteurs sont présents et font en sorte que la cartographie des menaces et des attaques observées est en perpétuelle changement. Mais la difficulté actuelle pour l'Etat est de trouver le dispositif adéquat pour identifier ces menaces, les évaluer de façon régulière et prendre les contre-mesures appropriées.

Le but de la stratégie est de déployer les moyens nécessaires pour anticiper les cybermenaces et garantir un niveau de sécurité acceptable pour les usagers du numérique au plan national.

Néanmoins, les cybermenaces les plus importantes identifiées au niveau du cyberespace béninois se déclinent comme suit :

- La cyber-escroquerie : qui s'illustre sous plusieurs formes et devenant de plus en plus inquiétante, allant de l'arnaque aux sextorsions, aux chantages,

jusqu'aux crimes rituels par des cybercriminels qui y ont trouvé un moyen pour faciliter leurs crimes tout en restant relativement anonymes. A cause de ce phénomène, le Bénin a été classé en 2018 parmi les pays Africains ayant un taux de cyber-escroquerie élevé (Source : Rapport Interpol et Trend Micro). Ceci n'est pas seulement dû aux pratiques de cybercriminels Béninois, mais à un grand nombre d'étrangers ayant trouvé au Bénin un refuge pour perpétrer leurs forfaits. Les bandes de cybercriminels ont également eu recours à Internet pour recruter des jeunes afin de les impliquer dans des opérations de crimes organisés. Le fléau de la cyber-escroquerie inquiète du fait que les criminels ont trouvé un terrain favorable pour commettre leurs crimes.

- Les cyber-attaques : il s'agit de pratiques observées depuis des années mais qui risquent de s'accentuer avec le développement numérique du pays. On peut citer les attaques contre les sites web institutionnels par des dégradations de pages web essentiellement dues à des défaillances techniques et à la non-application des bonnes pratiques de protection. Il y a aussi le phénomène des infections virales qui touche aussi bien les simples utilisateurs que les entreprises. Il favorise l'utilisation des systèmes infectés sur le réseau béninois en tant que relais pour lancer des attaques contre des systèmes dans d'autres pays (DDoS, pourriels, hameçonnages, etc.). Cette situation entraîne fréquemment le blacklisting des adresses IPs béninoises.
- Les menaces en relation avec les réseaux sociaux : il s'agit d'une tendance inquiétante qui touche les citoyens et facilitant certains fléaux sociaux et pratiques marginales comme la diffamation, le chantage, les infox, la propagande. Il est à signaler aussi les menaces en relation avec le vol de comptes, la falsification de comptes, le vol de données, etc. Le phénomène des infox trouve un bon refuge sur les réseaux sociaux où le contrôle est plus difficile et les informations peuvent circuler très rapidement. Ce phénomène peut entraîner des répercussions sociales, politiques et même sécuritaires. Certains incidents de falsification de photos, de contrefaçon de documents, de fuites de documents officiels, ou des incidents en rapport avec des personnalités politiques, voire des incidents de chantage des officiels, sont généralement liés aux réseaux sociaux.
- Les fraudes bancaires : étant donné les enjeux financiers majeurs, les cybercriminels s'attaquent très souvent aux moyens de paiement pour voler

de l'argent aux institutions financières et aux citoyens utilisant ces systèmes. C'est une menace qui ne cesse de se développer dans la sous-région, y compris au Bénin. En outre, plusieurs pratiques sont observées comme les fraudes aux cartes bancaires, les attaques par hameçonnage, l'usage de techniques d'ingénierie sociale, sans oublier les fraudes dues aux acteurs internes.

- Les attaques contre les infrastructures d'information critiques : il s'agit d'une menace croissante avec le développement technologique de ces infrastructures qui deviennent de plus en plus connectées, plus exposées et traitant des données assez critiques ; sans oublier le caractère vital de certaines infrastructures où les cyberattaques pourraient avoir un impact important sur la société ou l'économie, voire la sécurité nationale. Le choix du développement numérique qu'a fait le Bénin, exige que cette menace fasse l'objet d'une très grande considération dans la stratégie.

  D'autres enjeux sont également pris en considération par la stratégie comme le manque d'expertise en sécurité numérique, le faible niveau de maturité et le nombre insuffisant de structures privées spécialisées offrant des services de sécurité numérique. A cela s'ajoute l'insuffisance d'offre de formations spécialisées au niveau des universités, et le faible niveau de sensibilisation chez les usagers du numérique. Enfin, il est à noter le manque d'engagement de certains acteurs et la faiblesse des moyens financiers alloués à la protection des systèmes.

Le diagnostic du secteur induit l'analyse FFOM suivante :

Les forces :

- Engagement politique fort : le Gouvernement du Bénin a manifesté une volonté politique inébranlable pour développer la sécurité numérique. Cette détermination est essentielle car elle constitue un pilier majeur pour l'épanouissement de l'économie numérique, garantissant un engagement soutenu au plus haut niveau de l'État.
- Implication active des parties prenantes : la mise en œuvre réussie de la première version de la stratégie témoigne d'une implication remarquable des différentes parties prenantes. Cette collaboration étendue englobe les secteurs gouvernementaux, privés, les fournisseurs de services de sécurité

numérique (FSSN) et la société civile, créant un écosystème synergique pour la réalisation des objectifs de la stratégie.

- Résultats concrets de la première phase : l'implémentation de la première version de la stratégie a produit des avancées significatives, notamment dans le développement des compétences, la régulation et l'amélioration de la sécurité numérique. Ces résultats démontrent non seulement l'efficacité de la stratégie mais aussi la capacité du Bénin à progresser dans un domaine complexe et en rapide évolution.
- Création de l'ASIN : la création de l'Agence des Systèmes d'Information et du Numérique (ASIN) a marqué un jalon important. Cette entité a prouvé son expertise et son engagement pour l'implémentation de la stratégie nationale de sécurité numérique, en jouant un rôle pivot dans sa mise en œuvre et dans la coordination des efforts de cybersécurité à l'échelle nationale et internationale. A cela s'ajoute la création en novembre 2023 du Centre National d'Investigations Numériques (CNIN) qui a pour but de lutter contre la criminalité liée aux technologies de l'information et de la communication, et de contribuer en relation avec les organismes compétents, à la cybersécurité du Bénin.
- Cadre légal et réglementaire solide : le Bénin bénéficie d'un cadre légal pertinent, aligné sur des orientations stratégiques claires. Ce cadre constitue une base solide pour la régulation et la promotion de la sécurité numérique. Il s'agit entre autres du code du numérique du Bénin, la stratégie nationale de sécurité numérique (SNSN 2020-2023), la politique de sécurité des systèmes d'information de l'Etat (PSSIE), la politique de protection des infrastructures d'information critiques (PPIIC).
- Leadership clair et visionnaire : la présence d'un leadership fort, incarné par la Présidence de la République, le Ministère du Numérique et de la Digitalisation, le Ministère de l'Economie et des Finances, l'ASIN et le CNIN, offre une direction claire et une vision stratégique pour la sécurité numérique. Ce leadership est essentiel pour orienter les efforts nationaux vers des objectifs cohérents et surmonter les défis liés à la cybersécurité.

Les faiblesses :

- Manque d'expertise locale expérimentée : le secteur de la sécurité numérique au Bénin fait face à une pénurie d'expertise locale, exacerbée par le départ massif de professionnels qualifiés vers l'étranger. Cette situation crée un défi en matière de maintien des cadres expérimentés dans le pays.
- Implication limitée du secteur privé et des fournisseurs de services de sécurité numérique : le niveau d'engagement du secteur privé dans la stratégie de sécurité numérique reste modeste. Il en est de même pour les fournisseurs de services de sécurité numérique (FSSN). Cette faible participation limite les perspectives de partenariats public-privé et la contribution de l'Etat aux innovations.
- Faible priorité accordée à la sécurité numérique dans les projets : la sécurité numérique n'est souvent pas suffisamment intégrée ou considérée comme une priorité dans la planification et l'exécution des projets numériques. Cette lacune peut accroître la vulnérabilité des infrastructures et des données.
- Concentration sur les grandes structures : la stratégie actuelle se focalise principalement sur les grandes entreprises et les structures gouvernementales, laissant ainsi en marge les petites et moyennes entreprises (PME) qui forment l'essentiel du tissu économique national. Cette approche limite l'efficacité globale de la stratégie car ne couvrant pas un segment significatif du marché.
- Culture de la sécurité numérique insuffisante : le niveau de sensibilisation et de compréhension de la sécurité numérique parmi le grand public et au sein des entreprises est relativement bas. Cette faiblesse rend le cyberespace national vulnérable aux cyberattaques et aux pratiques de sécurité inadéquates.
- Contraintes budgétaires : l'insuffisance des ressources budgétaires affectées aux structures responsables de la mise en œuvre du plan d'action de la stratégie nationale de sécurité numérique constitue un enjeu majeur. La faiblesse du financement adéquat peut entraver la réalisation effective des initiatives et des mesures prévues.

Les opportunités :

- Renforcement de la confiance numérique : la mise en œuvre effective de la nouvelle version (2023-2026) de la stratégie offre une occasion unique de

renforcer la confiance numérique, essentielle pour encourager l'adoption des technologies numériques par les citoyens et les entreprises et garantir un cyberespace sécurisé.

- Affirmation de la souveraineté numérique : la stratégie peut contribuer à assurer la souveraineté numérique du Bénin, permettant au pays de contrôler et de sécuriser ses propres infrastructures numériques et données, un aspect crucial dans le contexte mondial actuel.
- Promotion des services en ligne : en développant des services en ligne sécurisés et fiables, le Bénin peut considérablement améliorer l'accès aux services gouvernementaux et privés, stimulant ainsi l'économie numérique.
- Développement du capital humain : investir dans la formation et le développement des compétences en sécurité numérique créera un réservoir de talents locaux, essentiel pour soutenir et maintenir les initiatives de cybersécurité.
- Stimulation de l'entrepreneuriat et de l'emploi : la croissance du secteur de la sécurité numérique peut générer de nouvelles opportunités d'entrepreneuriat et d'emploi, en particulier dans la création d'entreprises spécialisées dans ce domaine. C'est le cas des fournisseurs de services de sécurité numérique.
- Exportation du savoir-faire béninois : le Bénin a l'opportunité d'exporter son expertise en matière de cybersécurité, contribuant ainsi à l'affirmation de sa présence sur la scène internationale en tant que leader dans ce secteur.
- Etablissement d'un pôle régional d'expertise : en devenant un centre d'excellence régional en matière de sécurité numérique, le Bénin peut attirer des investisseurs et des partenariats, renforçant son rôle de leader dans la région.
- Collaboration et coopération internationale et partenariats : la stratégie offre la possibilité de développer des collaborations et coopérations internationales, favorisant le partage des connaissances et des ressources avec d'autres pays et organisations, afin de bénéficier de leur expertise.
- Innovation technologique : en mettant l'accent sur la sécurité numérique, le Bénin peut encourager l'innovation technologique, en particulier dans le développement de solutions de cybersécurité avancées.

Les menaces :

- Faible engagement des parties prenantes : un engagement insuffisant de la part des parties prenantes clés pourrait entraver la mise en œuvre efficace de la stratégie. Cela inclut les acteurs gouvernementaux, le secteur privé et la société civile, dont la participation active est cruciale.
- Absence de synergie entre les acteurs : le manque de coordination et de collaboration entre les différentes entités impliquées dans la mise en œuvre de la stratégie peut conduire à des efforts fragmentés et à une inefficacité globale, limitant la portée et l'impact de la stratégie.
- Contraintes budgétaires des entreprises : les limitations des ressources financières au sein des entreprises, en particulier des PME[4], peuvent les empêcher de se conformer pleinement à la législation en vigueur, ce qui représente un risque pour la sécurité numérique globale.
- Lenteur dans le développement des compétences : l'impact lent des initiatives liées au développement des compétences en matière de cybersécurité peut retarder la constitution d'une main-d'œuvre locale qualifiée, nécessaire pour répondre aux défis actuels et futurs.
- Fuite des compétences formées : le départ massif des professionnels expérimentés en sécurité numérique vers d'autres pays constitue une perte significative de capital humain essentiel pour la mise en œuvre et le maintien de la stratégie.
- Manque de visibilité sur les menaces et les progrès : un déficit d'informations et de données sur les menaces actuelles, les incidents de sécurité et l'avancement des projets technologiques peut entraver la capacité à répondre efficacement aux cybermenaces et à ajuster la stratégie en conséquence.

[4] PME : Petite et Moyenne Entreprise

4. DEFIS ET ENJEUX

L'analyse diagnostique de la situation actuelle, prenant en compte les problématiques majeures, les atouts, les faiblesses, ainsi que les menaces et opportunités, révèle que, malgré les progrès importants réalisés, des défis cruciaux persistent. Ces défis doivent être relevés afin de renforcer efficacement la sécurité numérique au Bénin.

5.1 Défis clés de la stratégie nationale de sécurité numérique

Il est important de noter que les défis en matière de sécurité numérique varient en fonction des facteurs tels que le niveau de développement technologique, le cadre législatif et réglementaire, et les ressources disponibles. Ainsi, les défis clés de la stratégie nationale de sécurité numérique du Bénin, s'articulent autour du renforcement de la confiance numérique, l'adaptation aux innovations technologiques, l'institutionnalisation des normes et mesures de sécurité.

5.1.1 Renforcer la confiance numérique

Malgré les avancées, la confiance numérique des citoyens, des entreprises et des institutions étatiques dans le cyberespace béninois nécessite une attention continue. Il est impératif d'accroître les ressources et les moyens de prévention, de traitement des cyber-risques, et de gestion optimale des menaces pour consolider cette confiance.

4.1.2. Adaptation aux innovations technologiques

L'évolution rapide dans le domaine de la sécurité numérique impose une mise à jour constante des capacités techniques et des moyens de protection. Les outils et stratégies actuels, bien que performants, peuvent s'avérer obsolètes face à cette évolution. Il est crucial d'aligner en permanence nos capacités techniques et nos ressources pour suivre les avancées technologiques et assurer une protection numérique efficace.

4.1.3. Institutionnalisation des normes et mesures de sécurité

L'effort gouvernemental, notamment l'adoption du code du numérique, la PSSIE et la PPIIC a été un pas significatif. Cependant, la mise en application effective de ces référentiels et leur intégration dans la culture numérique nationale demeurent un

défi. Il est essentiel de continuer à améliorer le cadre légal, d'implémenter des normes et des mesures en matière de sécurité numérique, et de veiller à leur institutionnalisation effective et leur adoption généralisée.

5.2 Principaux enjeux de la SNSN

La stratégie nationale de sécurité numérique vise principalement à offrir des garanties étatiques robustes, permettant aux entreprises, organisations et individus d'exploiter pleinement et en toute sécurité les potentialités du numérique. Il s'agit pour l'État de positionner la sécurité numérique comme une priorité absolue et de stimuler l'innovation pour relever efficacement les défis sécuritaires du cyberespace.

5.2.1 Priorisation de la sécurité numérique par l'État

La nécessité mondiale de renforcer la sécurité numérique exige que celle-ci soit élevée au rang de priorité nationale. Cet enjeu implique une révision de l'approche traditionnelle en matière de sécurité numérique, en faveur de méthodes modernes de développement des capacités institutionnelles et techniques, ainsi que d'un investissement adéquat et ciblé.

5.2.2 Stimulation de la recherche et de l'innovation pour l'adaptabilité aux nouvelles technologies

L'un des défis majeurs réside dans la recherche et l'innovation orientées vers l'adaptabilité aux nouvelles technologies de sécurité numérique, ainsi que la résolution des problèmes particuliers du Bénin. Cela inclut :

i) L'évolution des pratiques de management et des modes de régulation, adaptés aux réalités contemporaines

ii) l'identification précise et proactive des menaces pesant sur les entreprises et les organisations

iii) la protection efficace des données personnelles des individus, en réponse à l'évolution constante des risques et des vulnérabilités dans le cyberespace.

5. VISION

La stratégie révisée vise à capitaliser sur les bases solides établies précédemment, en orientant le développement et les actions futures vers des objectifs stratégiques renforcés et adaptés aux progrès déjà réalisés. Ces objectifs stratégiques se détaillent comme suit :

- consolidation de la protection des systèmes d'information nationaux et des infrastructures d'information critiques : s'appuyant sur les fondations déjà établies, cet objectif vise à renforcer davantage la sécurité des systèmes d'information nationaux et des infrastructures d'information critiques
- soutien et renforcement de la transformation numérique des infrastructures vitales : continuer à accompagner la transformation numérique tout en consolidant la sécurité des infrastructures d'information critiques
- amélioration de la sécurité des services et échanges électroniques : approfondir les mesures de protection pour les services et les échanges électroniques, en s'adaptant aux évolutions technologiques
- élargissement des moyens de protection des données : étendre et renforcer les moyens de protection des données de l'état, des opérateurs économiques et des citoyens
- protection avancée de l'identité numérique des citoyens : approfondir les mesures de protection de l'identité numérique des citoyens, en tenant compte des nouvelles menaces et opportunités du cyberespace
- assurance et promotion de la confiance numérique : renforcer la confiance numérique et promouvoir l'utilisation sécurisée des nouvelles technologies.
- développement et mise à jour continue des compétences en sécurité numérique : mettre l'accent sur le développement continu des compétences nationales en matière de sécurité numérique
- renforcement de la coopération internationale et intégration régionale : intensifier les efforts de coopération internationale et d'intégration régionale pour les actions de sécurité numérique
- capacité améliorée de réponse aux incidents majeurs de sécurité numérique : développer davantage les capacités de réponse aux incidents majeurs et de mitigation des risques associés

- intensification de la sensibilisation aux risques numériques : élever le niveau de sensibilisation aux risques et menaces liés au numérique
- promouvoir l'amélioration continue du cadre légal : mettre en place des régulations, normes et politiques adaptées en matière de sécurité numérique.

6. THEORIE DU CHANGEMENT

À partir du diagnostic stratégique et de la vision révisée, il est clair que l'objectif de la stratégie nationale de sécurité numérique est d'améliorer substantiellement la capacité technique de l'État à protéger ses systèmes d'information, ses citoyens, et les opérateurs d'infrastructures d'information critiques face aux menaces et risques liés à l'insécurité numérique. Cette stratégie vise à établir une confiance robuste dans l'exploitation d'un cyberespace sécurisé, propice au développement d'une économie numérique dynamique.

Pour que la mise en œuvre de la SNSN soit efficace, elle devrait induire les changements suivants :

À court terme :

- Institutionnalisation des normes de sécurité numérique : intégrer fermement les règles et normes de sécurité numérique dans la culture des organisations et des individus
- sécurisation des systèmes d'information de l'État : renforcer la protection des infrastructures informatiques gouvernementales et des infrastructures d'information critiques
- renforcement du cadre institutionnel de lutte contre la cybercriminalité : mettre en place des structures et des politiques efficaces pour lutter contre la cybercriminalité.

À moyen terme :

- Réduction de la cybercriminalité : diminuer significativement les incidents de cybersécurité. Il est à noter que le Bénin a fait une avancée très considérable en matière de lutte contre la cybercriminalité, en témoigne les statistiques ci-après (Source : Statistique OCRC).

Année	Nombre de plaintes relatives aux faits de cybercriminalité	Nombre de personnes interpellées
2020	2345	534
2021	2831	980
2022	2188	728
2023	3743	1450

Année	Nombre de plaintes relatives aux faits de cybercriminalité	Nombre de personnes interpellées
Total	11 107	3692

- renforcement des capacités techniques : améliorer les compétences en investigation numérique et en réponse aux cyber-attaques. Sur ce plan, le bjCSIRT a fourni des services de réponse consignés dans le tableau ci-dessous. (Source : Service bjCSIRT/ASIN).

Année	2020	2021	2022	2023
Nombre d'incidents de sécurité numérique traités	12	17	62	38

- développement de la recherche-action et de l'innovation : encourager la recherche et l'innovation en sécurité numérique dans les universités et parmi les acteurs économiques clés.

À long terme :

- Exploitation sécurisée du cyberespace pour une économie numérique florissante : assurer un environnement numérique sûr et attrayant pour stimuler l'économie numérique
- sensibilisation complète sur la cybercriminalité : élever la prise de conscience à tous les niveaux sur les enjeux de la cybercriminalité
- adoption des bonnes pratiques de sécurité numérique : promouvoir l'adoption généralisée de pratiques de sécurité efficaces.

La réalisation de ces objectifs implique une forte volonté gouvernementale se traduisant par l'allocation des ressources nécessaires. Toutefois, au-delà de la disponibilité des ressources, l'appropriation de la SNSN par tous les acteurs concernés et leur engagement envers ses objectifs sont cruciaux.

La prise de conscience de l'importance de la sécurité numérique est un prérequis fondamental. Par exemple, la conformité des entreprises aux standards de sécurité et l'adoption de bonnes pratiques deviendront des éléments intégrés dans la culture organisationnelle de ces entités. Ainsi, une approche d'accompagnement est

essentielle pour garantir que les changements sont non seulement mis en place, mais effectivement adoptés et maintenus sur le long terme.


XOXO
STREET WEAR
XOXO
USA

7. LES ORIENTATIONS STRATEGIQUES

Le Bénin a choisi le numérique comme levier du développement économique et social. Dans cette optique, la stratégie de la sécurité numérique ambitionne d'être un socle solide pour ce développement.

En ayant comme objectif de développer la sécurité numérique, cette stratégie apporte de véritables opportunités pour :

- Développer la confiance numérique, qui est un facteur prépondérant pour s'assurer de l'adhésion des entreprises et des citoyens dans le processus de transformation numérique du pays. En effet, la confiance numérique ne peut se développer qu'en mettant en place les moyens de protection des données et des échanges numériques, les moyens de traçabilité et de sécurisation des communications électroniques sans oublier le cadre juridique adéquat qui favorisera la confiance dans les échanges. Sans la sécurité numérique, la confiance ne peut pas se développer, de même que l'économie numérique. De plus, la stratégie sera un outil essentiel pour l'application du code du numérique.
- Assurer la souveraineté numérique qui est un enjeu majeur pour l'État. L'absence de maîtrise de la technologie, la dépendance technologique, et l'incapacité à protéger les systèmes d'information, les infrastructures et les données peuvent mettre en cause la souveraineté numérique, à fortiori, la souveraineté en général. Ainsi, la sécurité numérique est un moyen indispensable pour atteindre cette souveraineté, en veillant à construire un cyberespace sécurisé et résilient, par les moyens adéquats.
- Promouvoir les services en ligne comme un des piliers de l'économie numérique. Les services en ligne ne peuvent se développer qu'en assurant le niveau de protection adéquat. L'e-administration, l'e-gouvernement, l'e-commerce, l'e-banking, l'e-santé, l'e-agriculture, etc., sont tous des services qui ne peuvent prospérer sans une stratégie de sécurité numérique et une bonne gouvernance. Le développement des e-services peut faire du Bénin une plateforme de services numériques en Afrique de l'Ouest pour l'innovation numérique.
- Bâtir le capital humain dans le domaine de la sécurité numérique. La stratégie nationale de sécurité numérique servira de levier pour l'éclosion de

professionnels certifiés et de talents dans le domaine de la sécurité numérique, nécessaire pour la mise en œuvre de la politique de promotion du numérique au Bénin.

- Créer des opportunités d'entreprenariat et d'emploi par la création d'entreprises dans le domaine de la sécurité numérique, pour répondre aux besoins nationaux en termes de services, de recherche et développement, de formations, d'études, etc. Ceci favorisera également le développement des compétences en sécurité numérique pour créer un pôle régional d'expertises et fournira des opportunités pour exporter le savoir-faire. L'expertise est importante pour être plus compétitif à l'international et surtout dans le cadre de la coopération internationale.

La stratégie nationale de sécurité numérique est une bonne opportunité pour développer un environnement technologique résilient et performant. Elle offre également plusieurs autres opportunités de développement technologique et économique pour des secteurs autres que celui des technologies de l'information à l'instar du transport, de l'énergie, de la santé, de l'agriculture, de l'administration, du secteur bancaire, des télécommunications, de l'industrie, etc.

Pour atteindre les objectifs énumérés, profiter des opportunités qui en découlent et traiter les menaces identifiées, un ensemble d'axes de développement a été identifié. Chaque axe traitera un volet stratégique, duquel découlera un plan d'action.

8. LES OBJECTIFS STRATEGIQUES

Objectif Stratégique N°1 : Protection des systèmes d'information et des infrastructures d'information critiques

Compte tenu de l'importance cruciale des systèmes critiques, qui appartiennent aussi bien à l'État qu'au secteur privé, et du risque majeur que leur dysfonctionnement représente pour la stabilité nationale, une vigilance renforcée s'impose. Ces systèmes, souvent la cible d'attaques cyber, requièrent une protection et une résilience améliorées.

Dans cette optique, l'objectif de cet axe stratégique est de concevoir des mesures essentielles pour assurer une protection efficace des systèmes d'information et des infrastructures d'information critiques. Cela implique l'identification et la classification de ces systèmes, la détermination des niveaux de protection appropriés pour chaque catégorie, et l'établissement d'un cadre réglementaire qui garantissent la conformité des différents acteurs impliqués dans leur gestion. Les objectifs spécifiques de cet axe sont :

- fournir un soutien actif pour que les OIICs[5] atteignent la conformité totale avec les exigences de la PPIIC, assurant ainsi un niveau élevé de protection et de résilience des infrastructures d'information critiques
- assurer une assistance ciblée afin que les structures prioritaires du Gouvernement atteignent la conformité totale avec la PSSIE, renforçant ainsi la sécurité et l'intégrité des systèmes d'information étatiques
- renforcer et maintenir continuellement les capacités de protection du cyberespace béninois à travers les activités et les interventions du bjCSIRT (Centre de réponse aux incidents de sécurité informatique du Bénin), garantissant ainsi une réponse rapide et efficace aux incidents de cybersécurité
- établir une supervision efficace par la conduite d'activités de mise en conformité et d'inspection pour garantir l'application effective et le maintien continu des politiques de protection des infrastructures d'information

[5] Opérateurs d'Infrastructures d'Information Critiques

critiques, de même que la politique de sécurité des systèmes d'information de l'État du Bénin

- mettre en place un organe consultatif composé d'experts nationaux en sécurité numérique pour traiter des grandes questions de cybersécurité au plan national.

Objectif Stratégique N°2 : Lutte contre la cybercriminalité et développement du cadre juridique et réglementaire

Le Bénin dispose d'un cadre juridique assez mature surtout après la promulgation du code du numérique qui couvre plusieurs aspects en matière de sécurité numérique. Cette stratégie vise également à promouvoir l'application du code du numérique et des différentes conventions auxquelles le Bénin a adhéré en matière de lutte contre la cybercriminalité.

Cet axe stratégique vise à doter le Bénin d'un arsenal juridique complet qui comprend les lois, les décrets d'application, les réglementations et les politiques. Les objectifs spécifiques relatifs à cet axe stratégique sont :

- créer une infrastructure robuste et intégrée dédiée à la prévention, à la détection et à la lutte contre la cybercriminalité
- augmenter et maintenir les compétences pour une meilleure prise en charge des investigations pour des enquêtes numériques efficaces et concluantes
- accroître les compétences techniques et opérationnelles de tous les acteurs impliqués dans la lutte contre la cybercriminalité
- développer un plan national exhaustif et une stratégie pour combattre efficacement la cybercriminalité
- rendre pleinement opérationnel le Centre National d'Investigation Numérique (CNIN) afin qu'il remplisse efficacement ses missions.

Objectif Stratégique N° 3 : Développement des compétences et de la culture de la sécurité numérique

La mise en œuvre efficace et durable de la stratégie nationale de sécurité numérique dépend du renforcement des compétences locales en sécurité numérique. À l'heure actuelle, ces compétences sont insuffisantes et requièrent un développement intensif. En l'absence d'une expertise locale en sécurité numérique, la stratégie risque d'être dépendante de l'expertise internationale. De plus, pour garantir la

souveraineté nationale, il est impératif que les questions sensibles soient gérées par des experts béninois.

L'objectif est donc de forger un réseau local de spécialistes et d'experts en sécurité numérique, capables de satisfaire les exigences des entreprises et des entités gouvernementales. Ces professionnels seront des atouts tant pour le secteur public que privé, fournissant des services essentiels tels que les analyses, les audits, le support technique, la formation etc.

Pour y parvenir, il est nécessaire d'établir un programme collaboratif entre l'État, les institutions académiques et le secteur privé. Ce programme vise à développer des compétences en sécurité numérique par l'instauration de cursus universitaires dédiés, et en encourageant activement les investissements privés dans ce domaine de formation.

Parallèlement, il est essentiel de stimuler la recherche et le développement en sécurité numérique pour élargir et pérenniser le savoir-faire scientifique, technique, industriel et humain du Bénin dans ce secteur.

Spécifiquement, le développement de compétences vise à :

- stimuler la création et le développement de start-ups spécialisées dans le domaine de la sécurité numérique pour renforcer l'innovation et la compétitivité dans cet écosystème
- mettre en place un cadre idéal pour la recherche et le développement avancé en cybersécurité axé sur des domaines clés tels que la cryptologie, l'intelligence artificielle, la blockchain et l'informatique quantique pour soutenir les avancées technologiques du Bénin
- développer un creuset d'échange national pour rassembler tous les acteurs de la cybersécurité, facilitant ainsi le partage d'expertise, la collaboration et la coordination des efforts de sécurité numérique
- poursuivre le renforcement de capacités des Responsables de la Sécurité des Systèmes d'Information (RSSI), afin de répondre aux besoins croissants de compétences en sécurité informatique
- organiser des événements au niveau régional en cybersécurité au Bénin pour promouvoir la coopération, partager les meilleures pratiques et renforcer les capacités régionales en matière de lutte contre les menaces numériques.

L'enjeu est de cultiver une nouvelle mentalité de sécurité numérique qui requiert l'engagement actif de diverses parties prenantes, en particulier des dirigeants et décideurs qui doivent être éduqués sur les questions de cybersécurité. L'instauration de cette culture se traduit par la création d'un programme national de sensibilisation à la sécurité numérique impliquant un large éventail d'acteurs.

Les objectifs spécifiques en relation avec le développement de la sensibilisation sont :

- garantir l'engagement et la participation actifs des institutions éducatives, des associations civiles, professionnelles et des médias dans les campagnes de sensibilisation à la cybersécurité, afin de créer un front uni dans l'éducation au numérique sécurisé
- assurer que les initiatives de sensibilisation atteignent un large public utilisateur des technologies numériques, en organisant des événements tels que des séminaires, ateliers pratiques et compétitions, pour maximiser l'impact et la portée
- veiller à ce que les programmes de sensibilisation soient conçus de manière à englober toutes les catégories d'utilisateurs, y compris les enfants, les parents, les professionnels et les étudiants, afin d'adresser les besoins spécifiques de chaque groupe
- s'assurer que les décideurs et les hauts responsables reçoivent une information détaillée et une sensibilisation adéquate sur les enjeux de la sécurité numérique pour favoriser une prise de décision éclairée en matière de politiques et stratégies de cybersécurité.

Objectif Stratégique N°4 : Promotion de la confiance numérique

La cybersécurité constitue un élément clé pour établir la confiance dans l'écosystème numérique, grâce à l'implémentation de dispositifs adéquats assurant la protection des utilisateurs de technologies et services en ligne. Elle est l'un des fondements indispensables à l'instauration de cette confiance, nécessaire pour encourager l'engagement des entreprises et des citoyens dans la transformation numérique du pays.

La confiance dans le domaine numérique ne peut se concrétiser qu'à travers la mise en place de mesures efficaces pour la protection des données et des transactions

numériques, l'assurance d'une traçabilité fiable et la sécurisation des transactions en ligne. Cette confiance doit être soutenue par un cadre juridique mature encadrant tous les aspects du numérique. Autrement, la confiance reste précaire, ce qui peut entraver le développement économique.

Les objectifs spécifiques identifiés pour cet axe sont :

- encourager et soutenir les entreprises fournissant des services de confiance numérique pour qu'elles obtiennent des certifications selon les normes nationales et internationales, garantissant ainsi un niveau élevé de sécurité et de qualité dans leurs offres
- assurer la mise en œuvre rigoureuse des activités de conformité aux différents référentiels nationaux de sécurité tels que le référentiel FSSN, Crypto, PC-PKI, PSSIE, PPIIC, etc.
- consolider et maintenir les capacités de la PKI (Public Key Infrastructure) nationale pour renforcer la confiance dans les transactions et les communications numériques
- œuvrer à l'amélioration de la réputation du cyberespace béninois sur la scène internationale, en instaurant des normes élevées de sécurité et de fiabilité
- améliorer la réputation des domaines et des adresses IP du Bénin pour éviter le blacklisting, en renforçant ainsi la crédibilité du Bénin dans le cyberespace
- mettre en place un cadre formel pour la certification et la qualification des produits et services de sécurité numérique, afin de garantir leur conformité aux standards de qualité et de sécurité.

Objectif Stratégique N° 5 : Coordination nationale et coopération internationale

Le cyberespace béninois, intégré au contexte mondial, est sujet aux mêmes menaces auxquelles sont confrontées les autres nations. Il est donc impératif que la protection du cyberespace béninois s'appuie sur une collaboration étroite avec les pays voisins et la communauté internationale spécialisée dans ce domaine.

Par ailleurs, la sécurisation des systèmes d'information, des services en ligne et des données des citoyens requiert l'engagement de diverses parties prenantes, qui doivent opérer au sein d'un cadre formel facilitant la coopération et l'échange de données.

La coopération nationale et internationale est un pilier fondamental pour la réalisation des objectifs de la stratégie de sécurité numérique. Au sein de ce cadre, les objectifs spécifiques peuvent être définis comme suit :

- mettre en place des programmes d'échanges d'apprentissage avec des pays ayant une maturité avancée en matière de cybersécurité, pour acquérir des connaissances et des pratiques de pointe
- faciliter la création de centres de réponse aux incidents de sécurité informatique (CSIRT) dans différents secteurs stratégiques, pour renforcer la réponse aux menaces numériques à l'échelle sectorielle
- renforcer la cyberdiplomatie du Bénin, en engageant activement le dialogue et la collaboration avec d'autres nations sur les enjeux de cybersécurité
- développer des programmes de coopération bilatérale et multilatérale avec les pays de la région et former des coalitions pour une approche unifiée et efficace de la cybersécurité
- encourager les organismes internationaux à organiser des événements liés à la cybersécurité au Bénin, afin de promouvoir le pays comme un acteur clé dans le domaine
- planifier et exécuter des cyber-exercices à l'échelle nationale pour évaluer et améliorer la préparation et la réponse aux incidents de sécurité informatique
- développer un système national pour le partage d'informations sur les menaces de cybersécurité, facilitant ainsi la collecte, l'analyse et la diffusion de renseignements vitaux pour contrer les risques numériques.

10. LES ACTIONS

Au total vingt-cinq (25) actions ont été retenues dans le plan d'action de la stratégie révisée. Quelques-unes de ses actions majeures sont :

Au titre de la gouvernance :

- valider et adopter la stratégie nationale de sécurité numérique (2023-2026)
- vulgariser la stratégie auprès des différents acteurs nationaux concernés

Au titre de la protection des systèmes d'information et des infrastructures critiques:

- vulgarisation d'un cadre d'analyse des risques cyber
- accompagnement pour la revue des AOF[6] des ministères et entités publiques en vue de la création et de l'opérationnalisation de la fonction RSSI
- renforcement et maintenance des capacités de protection du cyberespace à travers le bjCSIRT
- accompagnement à l'atteinte de la conformité aux exigences de la PPIIC pour au moins 80% des OIICs
- accompagnement à l'atteinte de la conformité à la PSSIE pour au moins 80% des structures prioritaires
- renforcement des capacités du laboratoire de conformité au sein de l'ASIN pour contrôler l'application des référentiels de sécurité numériques au plan national
- mise en place d'un comité consultatif composé d'experts nationaux de la sécurité numérique

Au titre de la lutte contre la cybercriminalité et du développement du cadre juridique et règlementaire :

- ratification de la convention de Budapest et Malabo
- renforcement des capacités des acteurs intervenant dans la lutte contre la cybercriminalité
- organiser une rencontre régionale sur la lutte contre la cybercriminalité

[6] Attributions, Organisation et Fonctionnement

- opérationnalisation du CNIN[7]

Au titre du développement des compétences et de la culture de la sécurité numérique :

- incitation à l'entreprenariat et la création des start-ups dans le domaine de la sécurité numérique
- mise en place d'un centre de recherche et développement en cybersécurité (cryptologie, zero day, IA, blockchain, informatique quantique)
- formation certifiante au profit de soixante-quinze (75) RSSI sur trois (03) ans
- poursuite des activités de sensibilisation pour la protection de l'enfance en ligne
- mise en place d'un programme de Bug Bounty permanent

Au titre de la promotion de la confiance numérique :

- incitation des entreprises fournissant des services de sécurité numérique à se qualifier selon les référentiels nationaux de qualification
- mise en œuvre des activités de conformité aux différents référentiels de sécurité (FSSN, Crypto, PC-PKI, PSSIE, PPIIC, etc.)
- renforcement et maintenance des capacités de confiance numérique au travers de la PKI nationale
- développement d'un guide pour améliorer la réputation des domaines et des adresses IP afin d'éviter le blacklisting

Au titre de la coordination nationale et de la coopération internationale :

- organisation des learning expéditions vers les pays cybernétiquement plus matures
- accompagnement à la création de CSIRT/SOC sectoriels
- renforcement et poursuite de la cyberdiplomatie
- développement des programmes de coopération bilatérale et multilatérale avec les pays de la région et création des coalitions

[7] Centre National d'Investigations Numériques

11. LES PARTIES PRENANTES ET LE MODELE DE GOUVERNANCE

La stratégie adopte une approche globale et la réussite de son implémentation requiert la participation active de tous les acteurs impliqués, incluant le secteur public, le secteur privé et la société civile. Le modèle de gouvernance établi, détaille de manière explicite les rôles et responsabilités attribués aux différentes entités impliquées dans ce processus.

La mise en œuvre de la stratégie nécessite l'implication de tous, surtout des principaux intervenants qui sont :

- la Présidence de la République
- le Parlement
- les Ministères et institutions de la République
- les agences et les entités de l'État :
    - ASIN
    - CNIN
    - APDP
    - CRIET
    - ANIP
    - ARCEP
- les acteurs du secteur privé :
    - les fournisseurs de services de sécurité numériques qualifiés
    - les banques
    - les institutions de microfinances
    - les opérateurs télécoms
    - les fournisseurs d'accès à Internet
    - les industriels
    - le transport
    - l'enseignement privé
    - les intégrateurs et fournisseurs de technologie
    - les acteurs de la société civile intervenants dans le domaine du numérique au Bénin.

L'objectif principal du modèle de gouvernance est de mettre en place les structures nécessaires pour s'assurer de :

- la définition des objectifs
- la mise en œuvre de la stratégie

- le contrôle et la mesure de performance
- le développement de la stratégie
- l'amélioration continue.

Le modèle de gouvernance doit garantir une gestion aussi efficace que possible dans la durée tout en prenant compte des intérêts stratégiques de l'État et du secteur privé. Il s'agit de définir d'une part, une entité décisionnelle et d'autre part, une entité d'exécution. Il est indispensable que ces entités soient séparées pour assurer la bonne gouvernance, en dissociant les organes en couches stratégique, tactique et opérationnelle. Cela constitue le fondement d'un bon modèle de gouvernance axé sur les principes d'efficacité, de transparence et de responsabilité. L'adoption de la bonne gouvernance comme principe de base de gestion de la stratégie nationale de sécurité numérique permettra :

- une gestion efficace et efficiente des ressources
- une meilleure communication entre les parties prenantes
- une viabilité économique, sociale et financière.

Le modèle proposé est constitué essentiellement de deux (02) entités principales :

- l'entité de pilotage
- les entités opérationnelles.

L'entité de pilotage	
Description et rôles	Elle est une entité dont le rôle est de s'assurer que les actions qui découlent de la stratégie sont effectivement établies, mises en œuvre et maintenues. Cette entité a comme rôle de : • valider et faire adopter la stratégie nationale de sécurité numérique par le Gouvernement • mettre à disposition les ressources nécessaires à la mise en œuvre réussie de la stratégie • définir les orientations en vue de garantir l'obtention des résultats escomptés • s'assurer d'empêcher ou de limiter les résultats indésirables • valider le rapport annuel des actions de renforcement de lasécurité numérique • assurer le suivi de tous les indicateurs de performance • valider les performances de la stratégie rapportées par les entités opérationnelles, l'état d'avancement des actions décidées, les modifications des enjeux externes et internes pertinents pour la sécurité numérique • assurer la veille réglementaire, méthodologique et technologique afin d'adapter en permanence la stratégie nationale de sécurité numérique aux différentes évolutions.
Composition	Cette entité est composée ainsi qu'il suit : • MEF • MND • ASIN • CNIN
Positionnement	Cette entité dispose d'une communication directe avec le Conseil d'Administration de l'ASIN.

Les entités opérationnelles	
Description et rôles	Ces entités sont chargées de la mise en œuvre opérationnelle des actions de la stratégie nationale de sécurité numérique. Il s'agit en fait des entités publiques mettant en œuvre les activités gouvernementales dans le secteur du numérique et ayant une responsabilité dans la protection du cyberespace national. Elles rapportent à l'entité de pilotage et sont responsables de: • élaborer et maintenir le plan d'action relatif à la stratégie nationale de sécurité numérique • rapporter à l'entité de pilotage les mesures de performance montrant le bon fonctionnement des actions entreprises • proposer des actions d'amélioration pour une mise en œuvre réussie de la stratégie • jouer le rôle de centre de coordination entre les différents intervenants • s'assurer que toutes les structures concernées, sont conscientes et comprennent bien la stratégie ainsi que son apport • s'assurer que toutes les mises à jour et les révisions des objectifs de la stratégie sont réalisées • s'inspirer de ce modèle de gouvernance et l'appliquer particulièrement pour la gestion des grands projets dans le but de vérifier que les actions soient effectuées convenablement. • réaliser les opérations de communication et de sensibilisation pour toutes les parties prenantes • analyser les risques et les nouvelles tendances de cybersécurité.
Composition	La mise en œuvre opérationnelle de la stratégie est assurée conjointement par : - ASIN - CNIN Chacun étant responsable de son périmètre de compétence conformément à ses attributions, organisation et fonctionnement.

Positionnement	L'entité opérationnelle rend compte de ses activités à l'entité de pilotage.

CONCLUSION

La mise à jour de la stratégie nationale de sécurité numérique du Bénin sur la période 2023-2026 énonce les objectifs à atteindre et sera enrichie par un récapitulatif des mesures déjà en place, ainsi que par l'élaboration de plans d'action opérationnels. Pour chaque objectif stratégique, ces plans détailleront les actions spécifiques à réaliser, le calendrier de leur mise en œuvre et les parties prenantes responsables de leur exécution. Dans ce cadre, les universités et centres de recherche, reconnus comme des pôles d'excellence et détenant des savoir-faire spécialisés, seront sollicités pour apporter leur contribution à la réalisation des objectifs stratégiques. Cette stratégie est conçue pour évoluer et fera l'objet de révisions périodiques pour s'adapter aux nouveaux contextes et réalités. Ces révisions comprendront une réévaluation régulière des menaces et des risques, accompagnée de recommandations pour des mises à jour nécessaires de la stratégie.

12. LISTES DES SIGLES ET ABREVIATIONS

ADN	Agence pour le Développement du Numérique
ANIP	Agence Nationale d'Identification des Personnes
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASSI	Agence des Services et Systèmes d'Information
ASIN	Agence des Systèmes d'Information et du Numérique
ARCEP	Autorité de Régulation des Communications Electroniques et de la Poste
APDP	Autorité de Protection des Données Personnelles
bjCSIRT	Bénin Computer Security Incident Response Team
CSIRT	Computer Security Incident Response Team
CNIN	Centre National d'Investigations Numériques
DDoS	Distributed Denial of Service
FIRST	Forum of Incident Response and Security Team
FSSN	Fournisseurs de Services de Sécurité Numérique
GFCE	Global Forum on Cyber Expertise
ITU	International Telecommunication Union
MDC	Ministère du Développement et de la Coordination de l'Action Gouvernementale
MEF	Ministère de l'Economie et des Finances
MND	Ministère du Numérique et de la Digitalisation
NCSI	National Cyber Security Index
OCRC	Office Central de Répression de la Cybercriminalité
OIIC	Opérateurs d'Infrastructures d'Information Critiques
PKI	Public Key Infrastructure
RSSI	Responsable de la Sécurité du Système d'Information
PPIIC	Politique de Protection des Infrastructures d'Information Critiques
PSSIE	Politique de Sécurité des Systèmes d'Information de l'Etat
SNSN	Stratégie Nationale de Sécurité Numérique
TIC	Technologies de l'Information et de la Communication