BÉNIN RÉVÉLÉ
LE NOUVEAU DÉPART

STRATÉGIE NATIONALE DE
SÉCURITÉ NUMÉRIQUE

" Un cyberespace sécurisé et attrayant pour une économie numérique florissante "

DESCRIPTIF DU DOCUMENT	
Titre du document	Stratégie Nationale de Sécurité Numérique
Version du document	1.5
Date d'approbation	06 - Mai - 2020
Auteurs	MND, ANSSI, UIT

PREFACE

Sous l'impulsion du Président de la République, le Bénin a démarré la mise en œuvre de sa transformation digitale à un moment charnière de sa marche vers le développement. Aujourd'hui, plus de **80% des béninois** font usage des communications électroniques et **près de la moitié (45%)** sont des utilisateurs journaliers des nombreux services liés à l'Internet.

Le numérique fait sa révolution en Afrique et notre pays se veut être un centre d'innovations dans cette révolution globale. L'ambition du Gouvernement du Bénin est de positionner notre pays comme la référence en matière de plateformes de services numériques en Afrique de l'Ouest à l'horizon 2021 et de faire des technologies de l'information et de la communication le principal levier de son développement socio-économique.

Notre stratégie nationale de sécurité numérique reflète cette vision du gouvernement. Première stratégie réalisée suivant le guide de l'Union Internationale des Télécommunications, elle ambitionne de garantir un cyberespace sécurisé pour une économie numérique florissante. Déclinée sur une période de trois années, cette stratégie se veut ambitieuse : créer des compétences béninoises en matière de cybersécurité, protéger les systèmes d'information critiques, mettre en place un cadre réglementaire attrayant, renforcer la lutte contre la cybercriminalité, promouvoir la confiance numérique sont autant d'axes sur lesquelles entend œuvrer la stratégie. A travers un plan d'actions détaillé, elle engage de nombreux acteurs et implique divers responsables aussi bien de la société civile que du gouvernement.

J'ai la conviction que la mise en œuvre de notre stratégie de sécurité numérique changera profondément le secteur du numérique au Bénin en renforçant la sécurité au sein de nos projets numériques et en bâtissant une confiance numérique encore plus forte. Elle stimulera également la création de nouveaux métiers et de nouvelles opportunités d'emploi. Ce sont au total quarante-sept actions clés à mener pour gagner le combat du développement économique par la confiance numérique et l'innovation.

Cette stratégie dénote aussi de l'engagement du gouvernement à rassurer les partenaires nationaux et internationaux quant à la protection des données personnelles et d'entreprises. Par conséquent, son adoption est la preuve que le gouvernement béninois reconnait l'importance capitale d'un cyberespace sécurisé pour tous, aussi bien pour les citoyens qui accèdent aux services numériques que pour les entreprises qui chaque jour font avancer notre économie.

En ma qualité de Ministre du Numérique et de la Digitalisation, je m'engage à œuvrer avec tous les acteurs de l'écosystème, nos partenaires internationaux et les membres de la société civile afin que l'implémentation de cette stratégie soit une pleine réussite et fasse du Bénin, un champion africain du développement numérique.

Aurelie I. ADAM SOULE ZOUMAROU

Ministre du Numérique et de la Digitalisation

SOMMAIRE

INTRODUCTION

Les Technologies de l'Information et de la Communication (TIC) se développent rapidement et sont de plus en plus intégrées dans le quotidien des Béninois. En effet, le Gouvernement du Bénin développe activement l'usage généralisé des TIC dans la vie quotidienne au Bénin, à travers ses différentes initiatives nationales telles que décrites dans sa déclaration de politique sectorielle. Ces initiatives entraînent une remarquable transformation du Bénin en une société numérique où les secteurs public et privé utilisent de plus en plus les TIC dans la fourniture des biens et services, entreprennent des transactions et partagent l'information, ce qui permet aux personnes à travers le Bénin de bénéficier d'un quotidien économiquement plus riche.

La transformation numérique du Bénin entraînera la création de nouvelles dépendances non seulement vis-à-vis des systèmes, des données, des infrastructures et du cyberespace, mais aussi dans la fourniture des services critiques. Toute perte de confiance aux systèmes pourrait avoir des répercussions néfastes sur la digitalisation du Bénin et limiterait les bénéfices de cette transformation.

Étant donné que les TIC sont davantage intégrées dans tous les domaines de la vie, le Bénin à l'instar des autres pays ayant atteint un niveau élevé d'usage du numérique est inévitablement confronté à des cybermenaces grandissantes où les acteurs malveillants continuent d'exploiter les vulnérabilités. Ces acteurs malveillants emploient des méthodes et des instruments de plus en plus sophistiqués pour accéder illégalement à des systèmes d'information, subtiliser, altérer ou encore détruire des données personnelles ou institutionnelles publiques ou privées.

Dès lors, protéger ces systèmes et ces informations devient alors une priorité nationale pour le Bénin.

Le Programme d'Actions du Gouvernement (PAG), se basant sur le rapport de la grande rencontre du numérique tenue au Bénin en 2016 et dénommée eNNOV Bénin 2021 a définie pour le secteur de l'économie numérique les projets phares qui une fois mise en œuvre, garantiront le développement d'un secteur du numérique dynamique, sécurisé et surtout assure la confiance des citoyens.

CONTEXTE

Le Bénin a choisi la voie du développement numérique comme un socle pour le développement économique et social. Des travaux ont été initiés depuis plusieurs années afin de bâtir une stratégie et entamer de grands chantiers d'infrastructures et de réformes structurelles et réglementaires. Cette stratégie a commencé à se concrétiser par : l'interconnexion avec la fibre sous-marine, la connexion des différents sites et localités par fibre optique, la forte pénétration de l'Internet filaire et radio, la restructuration du secteur des télécommunications, la création de nouvelles structures comme l'ADN, l'ASSI, l'ANSSI, le lancement du grand projet de Datacenter et le développement d'une multitude d'applications sectorielles en ligne.

	T4_2018	T1_2019	T2_2019	T3_2019	T4_2019
Parc Internet FAI	27 093	26 601	22 824	25 996	25 489
Parc Internet Mobile	5 429 698	5 390 444	6 273 986	6 319 090	6 499 553
TOTAL[1]	5 456 791	5 417 045	6 296 810	6 345 086	6 525 042

Tableau 1: Parc Internet au Bénin (2019)-ARCEP

Opérateurs	T4_2018	T1_2019	T2_2019	T3_2019	T4_2019
MTN	5 183 061	5 485 689	5 656 957	5 881 606	5 972 405
MOOV	4 278 811	4 346 089	4 353 919	4 547 510	4 377 442
Parc d'abonnés mobiles	9 461 872	9 831 778	10 010 876	10 429 116	10 349 847
Croissance	-3,90	3,76%	1,79%	4,01%	-0,77%
Taux de pénétration[2]	83,27%	82,00%	82,78%	85,50%	84,12%

Tableau 2: Taux de pénétration du mobile au Bénin.

Il est clair que l'État dispose d'une grande volonté politique pour développer l'économie numérique et transformer le pays en une plateforme régionale en matière de services digitaux et pour développer un modèle économique durable.

Le 20 Avril 2018, le Chef de l'Etat a promulgué le code du numérique du Bénin (loi n° 2017-20), disposant ainsi d'un cadre réglementaire complet et à jour en termes de réglementation du secteur des TIC, permettant au Bénin de se positionner dans le

https://arcep.bj/wp-content/uploads/2020/02/Tableau-de-bord-Internet-au-31-D%C3%A9cembre-2019.pdf
https://arcep.bj/wp-content/uploads/2020/02/Tableau-de-bord-mobile-au-31-D%C3%A9cembre-2019.pdf

cercle des pays africains qui disposent d'un arsenal juridique apte à réguler le développement du numérique.

La démocratisation de l'Internet et le développement de nouvelles technologies comme l'Internet des objets, la Blockchain, l'Intelligence Artificielle, le Big Data, etc... exigent au Bénin, à l'instar de tout pays ayant choisi la voie du développement technologique, d'épouser rapidement ces tendances qui ne sont pas sans risques puisque entrainant une plus grande ouverture et exposant inévitablement le pays à des menaces et à des pratiques indésirables.

Cependant, le développement technologique induit une croissance saisissante des cybermenaces, qui risquent parfois de mettre en cause ce choix national, surtout que ce développement couvre de plus en plus de secteurs économiques, sociaux, politiques, culturels et même religieux.

Le Bénin ayant opté pour le développement technologique, assume son choix et décide d'élaborer son plan national pour protéger : les données et les systèmes d'information critiques, les citoyens ainsi que leurs données personnelles, et les entreprises publiques comme privées. Il s'agit de la Stratégie Nationale de Sécurité Numérique (SNSN) qui a pour objectif de définir un cadre national pour protéger les usages numériques au Bénin et pour accompagner la transformation digitale du pays, tout en ayant la sécurité numérique comme la pierre angulaire des choix technologiques opérés.

La technologie transforme les sociétés et également les pratiques criminelles, en offrant un éventail de possibilités, d'outils et de techniques parfois plus faciles que ceux du monde réel. Conscient de ces changements, le Bénin a élaboré cette stratégie, en impliquant toutes les parties prenantes et suivant une approche holistique. Une stratégie qui repose sur la politique de la bonne gouvernance et sur la valorisation du capital humain et qui accentue les efforts et les investissements sur la protection des systèmes critiques et vitaux.

L'État Béninois se veut garant de cette transformation vers l'économie numérique et mise sur l'ancrage de la confiance numérique pour que tous les Béninois adoptent les usages numériques sans crainte.
L'élaboration de la stratégie nationale commence par l'étude de l'écosystème numérique du Bénin et des pratiques actuelles. Elle couvre ensuite l'étude de l'état de l'art en termes de menaces, pour arriver à identifier les opportunités et les objectifs et en définir des axes de développement et le plan d'actions associé.

1 LE DIAGNOSTIC DU SECTEUR DE LA SECURITE NUMERIQUE

Le développement technologique induit une hausse des cybermenaces qui est due aux facteurs ci-après :

- **L'exposition des systèmes** qui s'ouvrent sur des réseaux externes et essentiellement sur Internet,
- **La complexification 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 même 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 mettre en cause leurs données par simple ignorance,
- **La démocratisation de la technologie** joue aussi au profit des criminels qui y trouvent des outils faciles et accessibles pour commettre leurs crimes.

Au Bénin, ces facteurs sont présents depuis des années et font en sorte que la cartographie des menaces et des attaques observées est en train de changer continuellement.
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 mettre en œuvre les moyens nécessaires pour identifier ces menaces et les évaluer de façon régulière et prendre les contre-mesures appropriées.
Néanmoins, les cybermenaces les plus importantes identifiées au niveau du cyberespace béninois sont comme suit :

- **La cyber-escroquerie :** qui s'illustre sous plusieurs formes et devenant de plus en plus inquiétante, allant de l'arnaque, aux extorsions, 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 Interpole et trend Micro). Ceci n'est pas dû seulement aux pratiques de cybercriminels Béninois, mais aussi à un grand nombre d'étrangers ayant trouvé au Bénin un refuge pour perpétrer leurs forfaits. Les bandes de criminels 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 et facilitateur pour commettre des crimes. Ces crimes peuvent aller du vol d'argent ou de données, de l'atteinte à la vie privée des citoyens, des fraudes, jusqu' au viol, trafic de drogue, trafic d'armes, etc. Cet état de choses peut mettre en cause la confiance des citoyens

dans les nouvelles technologies et risque de constituer de sérieuses entraves au développement numérique du pays.

- **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, le phénomène des infections virales qui touche aussi bien les simples utilisateurs que les entreprises, permettant parfois d'utiliser 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.) et entrainant fréquemment le blacklisting des adresses IPs béninoises. Ces incidents sont dans la plupart des cas, originaires de réseaux étrangers, mais ayant infecté des systèmes béninois exposés et manquants de protection.

- **Les menaces en relation avec les réseaux sociaux** : il s'agit d'une tendance inquiétante qui touche les citoyens en permettant de faciliter 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 où les informations peuvent circuler très rapidement. Ce phénomène peut avoir 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 même des incidents de chantage des officiels, sont généralement liés aux réseaux sociaux.

- **Les fraudes bancaires** : étant donné les enjeux financiers majeurs, les criminels s'attaquent très souvent aux moyens de paiement pour voler de l'argent aux institutions financières et aussi 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 aussi les fraudes dues aux acteurs internes. Ce genre de fraude se développe en parallèle avec le développement des moyens de paiement et des services bancaires en ligne menant à des pertes financières directes.
- **Les attaques contre les infrastructures critiques** : il s'agit d'une menace qui ne cesse de s'amplifier avec le développement technologique de ces infrastructures qui deviennent de plus en plus connectées, plus exposées et traitant des données de plus en plus critiques.

Sans oublier le caractère vital de certaines infrastructures où les cyber-attaques pourraient avoir un impact sur la société ou sur l'économie, voire même sur la sécurité nationale. Le choix du développement numérique qu'a pris le Bénin, exige que cette menace fasse l'objet d'une très grande considération dans la stratégie. Les systèmes d'information de l'État, les banques, les opérateurs de télécommunication, le secteur de l'énergie, le secteur du transport, etc. sont tous concernés par ce type de menace qui peut se traduire par des arrêts d'activité pouvant causer des perturbations économiques ou sociales, des vols de données sensibles, des pertes financières, ou même par l'atteinte à la sécurité nationale.

D'autres menaces seront également prises en considération par la stratégie comme le manque d'expertise en sécurité numérique, l'absence de structures privées spécialisées en sécurité numérique, l'absence de formations académiques spécialisées au niveau des universités, le faible niveau de sensibilisation chez les usagers de la technologie, le manque d'engagement de certains acteurs, la faiblesse des moyens financiers alloués à la protection des systèmes, etc.
Le diagnostic du secteur induit l'analyse FFOM suivant :

FORCE

- Une grande volonté politique pour développer la sécurité numérique comme un socle pour le développement de l'économie numérique,
- Une grande implication des parties prenantes à mettre en œuvre la stratégie,
- Présence de structures compétentes comme l'OCRC, l'ANSSI, l'ASSI, l'ADN,
- Présence d'un cadre légal déjà en vigueur, complet et très pertinent avec des orientations stratégiques,
- Présence d'un fort leadership représenté par la Présidence de la République et l'ANSSI.

FAIBLESSE

- Expertise peu abondante dans le domaine de la sécurité numérique,
- Faible niveau de considération de la sécurité numérique au sein des projets,
- Faible niveau de la culture de la sécurité numérique,
- Absence de budget au niveau des institutions concernées par la mise en œuvre du plan d'actions de la stratégie.

OPPORTUNITÉS

- Développer la confiance numérique,
- Assurer la souveraineté numérique,
- Promouvoir les services en ligne comme un des piliers de l'économie numérique,
- Bâtir le capital humain dans le domaine de la sécurité numérique,
- Créer des opportunités d'entreprenariat et d'emplois par la création d'entreprises dans le domaine de la sécurité numérique,
- Créer un pôle régional d'expertises qui fournira des opportunités pour exporter le savoir-faire béninois.

MENACES

- Manque d'engagement des parties prenantes devant impacter la mise en œuvre,
- Limitation des moyens financiers,
- Impact lent des projets en relation avec le développement des compétences,
- Manque de visibilité sur les menaces, les incidents vécus et sur l'état d'avancement des projets technologiques.

2 DEFIS ET ENJEUX

Défis et Enjeux

Au regard de l'analyse diagnostique qui prend en compte les problèmes majeurs, les forces, faiblesses, les menaces et les opportunités, il se dégage d'importants défis et enjeux qui doivent être relevés afin d'assurer efficacement la sécurité numérique.

Défis de la stratégie nationale de sécurité numérique

En dépit des efforts fournis par l'Etat, des défis demeurent pour assurer le maintien ou le perfectionnement de la sécurité numérique. Parmi les plus urgents, il convient de citer :

1. La nécessité de rétablir la confiance numérique pour les citoyens, les entreprises et les organes de l'État dans le cyberespace béninois

Le diagnostic a fait ressortir l'insuffisance des moyens nécessaires pour prévenir, traiter les cyberattaques et gérer de façon optimale les menaces identifiées. Les dispositifs actuellement mis en place ne sont pas fondés sur des piliers solides pour assurer la confiance numérique pour les citoyens, les entreprises et les organes de l'État dans le cyber espace béninois

2. L'inadaptabilité des capacités techniques et des moyens au regard des innovations et des ingénieries dont l'évolution est très rapide en matière de la sécurité numérique

La capacité technique, les moyens utilisés en matière de sécurité numérique se révèlent parfois caducs ou limités au regard des évolutions et des innovations très rapides dans ce domaine. Il s'en suit une contrainte à lever pour une bonne adéquation entre les capacités techniques et les moyens de sécurisation du numérique d'une part et l'évolution de la technologie d'autre part.

3. L'institutionnalisation des normes et des mesures en matière de sécurité numérique

L'adaptation au numérique suppose non seulement le renforcement et le perfectionnement des capacités technologiques mais aussi l'amélioration continue du cadre légal, la mise en place des normes et mesures en matière de sécurité numérique. Malgré l'effort du Gouvernement en adoptant le code du numérique, l'application effective de ce code et son appropriation tardent à rentrer dans les cultures. L'institutionnalisation des normes et des mesures en matière de sécurité numérique demeure un défi à relever.

Enjeux de la stratégie nationale de la sécurité numérique

Les enjeux de la stratégie nationale de sécurité numérique résident dans les garanties données par l'Etat pour permettre aux entreprises, aux organisations et aux individus d'exploiter en toute confiance les avantages du numérique. Ainsi, il s'agira pour l'Etat d'inscrire la sécurité numérique au rang des priorités de l'Etat et favoriser l'innovation pour répondre aux défis posés par la sécurité de son cyberespace.

1. L'inscription de la sécurité numérique au rang des priorités de l'Etat

Les évolutions actuelles dans le monde s'accordent sur la nécessité d'assurer la sécurité numérique. Dès lors, la sécurité numérique doit être portée au rang des priorités de l'Etat. La réalisation de cet enjeu exige que l'on révise la gestion tradition de la sécurité numérique en adoptant une méthode moderne du développement des capacités institutionnelles et techniques ainsi qu'un investissement adéquat.

2. Le renforcement de la recherche et l'innovation en matière d'adaptabilité aux nouvelles technologies de développement de la sécurité numérique

L'enjeu de la recherche et l'innovation en matière d'adaptabilité aux nouvelles technologies de développement de la sécurité numérique imposent de s'intéresser aux incidences de la modernité :

i) le management et les modes de régulation ;

ii) l'identification des menaces pour les entreprises et les organisations ;

iii) la protection des données des individus

3 LA VISION

Un cyberespace sécurisé et attrayant pour une économie numérique florissante.

Les axes de développement et le plan d'actions serviront de fil directeur et de catalyseur pour l'atteinte des objectifs qui concourent à cette vision. Les objectifs stratégiques se présentent comme suit :

- Renforcer la protection des systèmes d'information nationaux et des infrastructures critiques nationales,
- Accompagner et consolider la transformation numérique des infrastructures d'importance vitale,
- Renforcer la protection des services et des échanges électroniques,
- Renforcer les moyens de protection nécessaires pour protéger les données de l'État, les opérateurs économiques et les citoyens,
- Protéger l'identité numérique des citoyens,
- Assurer la confiance numérique et promouvoir l'usage des nouvelles technologies,
- Développer les compétences en matière de sécurité numérique,
- Développer la coopération internationale et l'intégration régionale des actions du Bénin en matière de sécurité numérique,
- Développer les capacités du Bénin à répondre aux incidents majeurs de sécurité numérique et à mitiger les risques qui en découlent,
- Intensifier la sensibilisation sur les risques et menaces liés au numérique,
- Promouvoir l'amélioration continue du cadre légal et mettre en place la régulation, les normes et politiques en matière de sécurité numérique

4 THEORIE DU CHANGEMENT

Théorie du changement : raison d'être et changements

Du diagnostic stratégique et de la vision ci-dessus exposés, il ressort que la raison d'être de la Stratégie Nationale de Sécurité Numérique (SNSN) dénote de la faible capacité technique de l'Etat à protéger ses propres systèmes d'information, ses citoyens et les organisations jugées critiques des menaces et des risques liés à l'insécurité numérique en vue d'établir une confiance totale dans l'exploitation d'un cyberespace sécurisé et attrayant pour une économie numérique florissante.

Ainsi, la mise en œuvre de la SNSN devrait permettre d'obtenir des changements ci-après :

1. à court terme :

- l'institutionnalisation des règles, des normes et des mesures en matière de sécurité numérique dans la culture des organisations et des individus ;
- la sécurisation des systèmes d'information de l'Etat ;
- le renforcement institutionnel pour favoriser la lutte contre la cybercriminalité

2. à moyen terme :

- la réduction du phénomène de la cybercriminalité ;
- le renforcement des capacités techniques en matière d'investigation numérique et dans la lutte contre les cyber-attaques ;
- le développement de la recherche-action, de l'innovation, de la sécurité numérique dans le milieu universitaire et des principaux opérateurs économiques ;

3. à long terme :

- l'exploitation d'un cyberespace attrayant en toute sécurisé pour une économie numérique florissante ;
- une prise de conscience totale des acteurs à tous les niveaux sur la cybercriminalité ;
- l'adoption des bonnes pratiques de la sécurité numérique

L'exploitation d'un cyberespace attrayant en toute sécurité, en tout temps et en tout lieu pour une économie numérique florissante suppose que la volonté déjà manifeste du Gouvernement se matérialise par la mise à disposition des ressources conséquentes pour la réalisation des extrants. En dépit de la disponibilité des ressources, il est important de ne pas occulter l'appropriation de la SNSN par les différents acteurs et leur engagement à l'atteinte des objectifs de cette stratégie.
En effet, la prise de conscience de l'importance de la sécurité numérique est nécessaire à l'obtention des changements souhaités. A titre d'exemple, la mise en conformité des entreprises aux standards et l'adoption des bonnes pratiques en matière de sécurité, doivent désormais intégrer la culture de ces organisations.

5 ORIENTATIONS STRATEGIQUES

Les orientations stratégiques

OS 1 : Protection des systèmes d'information et des infrastructures critiques

Étant donné qu'il s'agit de systèmes critiques appartenant à l'État et au secteur privé et qui, en cas de dysfonctionnement, peuvent avoir un impact important sur la stabilité de l'État ; Ce genre de systèmes est généralement une cible privilégiée des attaquants et nécessitent une attention particulière d'un point de vue protection et résilience.

Cet axe stratégique vise à mettre en place les instruments nécessaires pour assurer un bon niveau de protection des systèmes d'information et les infrastructures critiques. Il s'agira d'identifier ces systèmes, de les classifier et de définir le niveau de protection requis pour chaque catégorie tout en instaurant un cadre de conformité qui veillera à ce que les exigences soient bien respectées par tous les opérateurs de ces systèmes d'information et des infrastructures critiques.

Les objectifs spécifiques de cet axe sont :

- Veiller à la mise en place d'un cadre normatif national pour le renforcement des capacités sécuritaires des entreprises critiques,

- Inciter les entreprises à se conformer aux standards et à adopter les bonnes pratiques en matière de sécurité,

- Veiller à ce que les entreprises opérant des infrastructures vitales disposent d'un bon modèle de gouvernance en interne, aussi au niveau sectoriel et au niveau national. Tout en renforçant le rôle que peut jouer l'ANSSI comme catalyseur,

- Encourager les partenariats public-privé pour favoriser la collaboration en matière de protection des infrastructures critiques,

- S'assurer que les entreprises aient accès aux technologies de protection des systèmes d'information,

- Promouvoir l'utilisation des solutions open-source,

- Veiller à ce que la sécurité numérique soit considérée dans tous les projets nationaux à caractère technologique.

OS 2 : Lutte contre la cybercriminalité et développement du cadre juridique et règlementaire

Le Bénin dispose d'un cadre juridique assez complet surtout après la promulgation du code du numérique qui couvre plusieurs aspects en matière de sécurité numérique. Cette stratégie vise aussi à promouvoir l'application du code numérique. Cet axe stratégique vise à doter le Bénin d'un environnement juridique complet qui comprend les lois, les décrets d'application, les réglementations. Les objectifs spécifiques relatifs à cet axe stratégique :

- Renforcer le cadre juridique et judiciaire pour la lutte contre la cybercriminalité,

- Veiller à ce que les magistrats se spécialisent en cybercriminalité et en nouvelles technologies,

- Veiller à renforcer la coopération régionale et internationale dans la lutte contre la cybercriminalité,

- Veiller à ce que les politiques de sécurité locales aient un poids d'imposition et prévoir des sanctions légales en cas de défaillance,

- Renforcer les capacités techniques en matière d'investigation numérique et dans la lutte contre les cyber-attaques.

OS 3 : Développement des compétences et de la culture de la sécurité numérique

La stratégie nationale de Sécurité numérique ne peut se mettre en place de manière efficiente et pérenne que moyennant des compétences locales, qui sont actuellement peu abondantes et qu'il faut absolument développer. Sans ces compétences et sans l'expertise en sécurité numérique, la stratégie trouvera du mal à se concrétiser et restera toujours dépendante de l'expertise étrangère. Pour des raisons évidentes de souveraineté, certains sujets sensibles devraient être traités par une expertise béninoise.

Il s'agit de développer un réseau de spécialistes et d'experts en sécurité numérique apte à répondre aux différents besoins exprimés par les entreprises et l'État. Ces professionnels serviront dans les entreprises privées et publiques et aussi au sein des prestataires de services privés auxquels feront appel les entreprises pour faire des études, des audits, de l'assistance, de la formation, etc.

Le développement de ce réseau de spécialistes devra se baser sur un programme impliquant l'État, les universités et aussi le secteur privé.

Il s'agit de mettre en œuvre un programme de développement de compétences en sécurité numérique à travers la création de cursus académiques ainsi que la stimulation et l'incitation du secteur privé à investir dans ce créneau de formations.

Le développement de compétences passe aussi par la stimulation des activités de recherche et développement en matière de sécurité numérique, afin d'accroitre et de pérenniser les capacités scientifiques, techniques, industrielles et humaines.

Spécifiquement, le développement de compétences vise à :

- Créer d'une synergie avec les universités pour les impliquer davantage dans la stratégie et jouer un rôle fondamental pour le développement des compétences,

- Veiller à rapprocher le milieu académique de l'entreprise pour mieux orienter les formations universitaires vers les besoins réels du marché,

- Incitation des acteurs du secteur privé à investir dans le développement d'offres de formations et de certifications internationales,

- Encourager la recherche et le développement autour de la sécurité numérique dans le milieu universitaire et aussi au niveau des principaux opérateurs économiques,

- Encourager l'innovation et l'entreprenariat dans la sécurité numérique,

- Veiller à ce que les entreprises aient un accès à des formations de haut niveau et que les personnes qui seront chargées de gérer les programmes de sécurité soient bien habilitées à le faire.

D'autre part, le développement de la sécurité numérique passe obligatoirement par le changement de comportement des utilisateurs qui sont en première ligne face aux cybermenaces. Le constat montre que le niveau de sensibilisation est très faible voire même absent.

Il s'agit de développer une nouvelle culture nécessitant une grande implication de plusieurs parties prenantes et surtout des hauts décideurs qui ont aussi besoin d'être sensibilisés sur la question de la sécurité en premier lieu. Cette nouvelle culture passe par le développement d'un programme national de sensibilisation en sécurité numérique englobant le plus d'acteurs possible.

Le développement de la culture de sécurité numérique est tout d'abord la responsabilité de l'État mais aussi des entreprises, de la société civile, des médias, universités et écoles.

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

- Veiller à ce que les principaux acteurs soient impliqués pour appuyer les efforts de sensibilisation, comme les universités, les écoles, les associations, les médias, etc.

- S'assurer que les actions de sensibilisation couvrent le maximum d'utilisateurs de la technologie en organisant des séminaires, des workshops, des compétitions, etc.

- Veiller à ce que les programmes de sensibilisation touchent toutes les catégories d'utilisateurs y compris les enfants, les parents, les professionnels, les étudiants, etc.

- Veiller à ce que les décideurs et les hauts responsables soient bien informés et sensibilisés à la question de la sécurité.

OS 4 : Promotion de la confiance numérique

La sécurité numérique est un facteur essentiel pour le développement de la confiance numérique en mettant en place les mécanismes nécessaires pour protéger les consommateurs de technologies et services en ligne. La sécurité est un des piliers de la confiance numérique pour s'assurer de l'adhésion des entreprises et des citoyens dans le processus de transformation numérique du pays.

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 de transactions en ligne sans oublier le cadre juridique adéquat qui va favoriser la confiance dans les échanges. Sans la sécurité numérique, la confiance ne peut pas se développer, et l'économie non plus. De plus, la stratégie sera un outil essentiel pour l'application du code du numérique.

Les objectifs spécifiques identifiés pour cet axe sont :

- Renforcer la sécurité des services en ligne offerts par le secteur public et le secteur privé, en s'assurant que le niveau de protection soit conforme aux standards en vigueur,

- Améliorer la réputation du cyberespace béninois tout en s'assurant que ses utilisateurs soient identifiés de manière fiable,

- Accélérer l'adoption des services dématérialisés en garantissant la sécurité des transactions grâce aux services de confiance électronique,

- Veiller à instaurer un cadre de qualité relatif à la protection des données,

- Veiller à renforcer les moyens de protection des données personnelles.

OS 5 : Coordination nationale et coopération internationale

L'espace numérique du Bénin ne peut pas se dissocier du cyberespace mondial, les menaces auxquelles font face les pays du monde sont nécessairement des menaces qui peuvent toucher aussi l'espace béninois. Cependant, la protection de l'espace numérique du Bénin doit se reposer sur une coopération avec les pays de la région et aussi de la communauté internationale compétente en la matière.

D'autre part, la protection des systèmes d'information, des services et même des données des citoyens nécessite l'implication de plusieurs parties prenantes qui doivent disposer d'un cadre formel de coopération et de partage de données.

La coopération nationale et internationale est un axe important pour atteindre les objectifs de la stratégie, cependant on peut distinguer les objectifs spécifiques suivants :

- Veiller à ce que le Bénin adhère aux conventions régionales et internationales, et en tire des bénéfices pour sa propre sécurité ;

- Veiller à ce que le Bénin participe activement dans les initiatives techniques : ITU, FIRST, Interpol, GFCE, etc. ;

- Renforcer la coopération entre les parties prenantes nationales pour la protection du cyberespace national et pour la lutte contre les cyber-attaques ;

- Mettre en place un cadre formel de coopération favorisant le partage d'information et la coordination pour la lutte contre les cyber-attaques.

6 LES OBJECTIFS STRATEGIQUES ET LES OPPORTUNITES

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. 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 va favoriser la confiance dans les échanges. Sans la sécurité numérique, la confiance ne peut pas se développer, et l'économie non plus. 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 et même 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 et surtout à le défendre 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 dans l'Afrique de l'Ouest, qui sera reconnue pour la qualité et l'innovation.
- **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 ainsi que 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 sur 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.

Le but du développement de la stratégie est de créer l'environnement propice à la mise en œuvre des plans de développement numérique, économique et social définis par le Bénin et ce en étroite ligne avec la vision ci-dessus mentionnée.

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'actions.

7 LES ACTIONS

Au total quarante-sept (47) actions ont été retenues dans le plan d'actions de la stratégie. Quelques-unes de ses actions majeures sont :

Au titre de la gouvernance :

- Valider et adopter la stratégie ;
- Créer le conseil national de la sécurité numérique ;
- Organiser un workshop national pour présenter la stratégie.

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

- Lancer une étude de classification des systèmes d'information et des infrastructures critiques du Bénin.
- Créer le conseil national de la sécurité numérique ;
- Définir la politique de sécurité des systèmes d'information de l'État ;
- Définir la politique de protection des infrastructures critiques ;
- Mettre en place un cadre d'analyse des risques ;

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

- Développer une politique de lutte contre la cybercriminalité ;
- Former des magistrats spécialistes en cybercriminalité et en nouvelles technologies ;

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

- Inciter la création de cursus académiques spécialisés dans la sécurité numérique ;
- Inclure des cours basiques de sécurité dans les cursus scolaires de l'enseignement secondaire ;
- Créer un mécanisme d'incitation pour la formation professionnelle, à la certification internationale et la formation de formateur ;
- Inciter l'entreprenariat et la création des startups dans le domaine de la sécurité numérique ;

- Lancer un portail pour la sensibilisation et l'information des utilisateurs du cyberespace ;
- Détecter et former les talents en cybersécurité ;
- Mettre en œuvre un programme pour la protection des enfants en ligne.

Au titre de la promotion de la confiance numérique :

- Définir un référentiel de sécurité pour la protection des e-services ;
- Inciter les entreprises fournissant des e-services à se certifier selon les standards internationaux ;
- Régulation et promotion de l'activité des prestataires de service de confiance électronique ;
- Mise en œuvre du programme de protection des données personnelles ;
- Mettre en place un cadre de régulation de la cryptologie ;
- Elaborer un cadre de certification/qualification des produits et services de sécurité ;
- Elaborer un Référentiel Général de Sécurité.

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

- Mettre en œuvre un programme pour le renforcement de la coopération régionale et internationale dans la lutte contre la cybercriminalité ;
- Lancer un cadre national de partenariat pour la protection du cyberespace national et la lutte contre les cyber-attaques, prévoir des exercices de simulation (cyber- drill) et promouvoir le partage d'information ;
- Inciter les secteurs critiques et le privé à créer des CSIRTs.

8 LES PARTIES PRENANTES ET LE MODELE DE GOUVERNANCE

La stratégie est transversale, son application nécessite donc l'implication de toutes les parties prenantes du secteur public, du secteur privé et aussi de la société civile. Le modèle de gouvernance décrit clairement les rôles et les responsabilités des différentes entités de gouvernance.

La mise en œuvre de la stratégie nécessite l'implication de tout le monde, mais surtout des principaux intervenants qui sont :

- La Présidence de la République,
- Le Parlement,
- Les Ministères:
    - Ministère du Numérique et de la Digitalisation,
    - Ministère en charge de la Défense Nationale
    - Ministère de l'Intérieur et de la Sécurité Publique,
    - Ministère de la Justice et de la Législation,
    - Ministère de l'Energie,
    - Ministère de l'Économie et des Finances,
    - Ministère de l'Enseignement Supérieur et de la Recherche Scientifique,
    - Ministère des Enseignements Secondaire, Technique et de la Formation Professionnelle,
    - Ministère des Enseignements Maternel et Primaire,
    - Ministère des affaires étrangères et de la coopération,
    - Ministère des Infrastructures et du Transport,
- Les agences et les entités de l'État :
    - ANSSI,
    - ASSI,
    - ADN,
    - APDP,
    - ABSU-CEP,
    - OCRC,
    - CRIET,
    - ANIP,
    - ARCEP,
- Les acteurs du secteur privé :
    - 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,
- Le développement de la stratégie,
- La mise en œuvre de la stratégie,
- Le contrôle et la mesure de performance,
- Et l'amélioration continue.

Le modèle de gouvernance doit garantir une gestion aussi efficace que possible dans la durée tout en prenant bien en compte les intérêts stratégiques de l'État et du secteur privé.

Il s'agit en fait de définir une entité décisionnelle et de planification, une entité d'exécution et une entité de contrôle. Il est indispensable que ces entités soient séparées pour assurer la bonne gouvernance et ceci surtout en séparant les organes en couches stratégique, tactique et opérationnelle. Cela constitue le fondement d'un bon modèle de gouvernance.

Les principes de gouvernance :

- Efficacité,
- Transparence,
- Responsabilité.

L'adoption de la bonne gouvernance comme principe de base de gestion de la stratégie nationale de sécurité numérique permet :

- Une gestion efficace et efficiente des ressources ;
- Une meilleure information des parties prenantes ;
- Une viabilité Économique, Sociale et Financière.

Il s'agit d'un modèle adapté au contexte béninois prenant en considération le rôle joué par l'ANSSI en tant qu'agence en charge de la sécurité numérique. Vu son positionnement, l'ANSSI peut jouer le rôle de coordinateur entre les différents intervenants tout en s'assurant de l'implication directe de toutes les parties prenantes.

L'application de ce modèle va dépendre directement des efforts à entreprendre par l'ANSSI pour convaincre toutes les autres parties prenantes et en plus elle va dépendre fortement de l'implication du gouvernement ainsi que de l'autorité qui sera donnée aux différentes entités de ce modèle

Le modèle proposé est constitué essentiellement de trois entités principales :

- L'entité managériale
- L'entité de pilotage ;
- Les entités opérationnelles..

Le modèle de gouvernance vise essentiellement à :

- Définir les rôles et les responsabilités de chaque entité ;
- Définir les interactions entre elles ;

L'entité managériale : Conseil National de la Sécurité Numérique (CNSN)

Description et rôles

Il s'agit de l'entité de plus haut niveau qui disposera de l'autorité, du leadership et affirmera son engagement en faveur de la sécurité numérique pour :

- S'assurer que la stratégie nationale de Sécurité numérique est bien établie et qu'elle est cohérente avec les orientations stratégiques du pays ;
- S'assurer que les ressources nécessaires pour mettre en œuvre la stratégie et la politique générale sont disponibles ;
- Communiquer sur l'importance de la stratégie de sécurité du numérique et son apport pour la politique générale du pays ;
- S'assurer que la stratégie de la sécurité numérique produit les résultats escomptés ;
- Orienter et soutenir les responsables des différents projets, qui font partie du plan d'actions, pour qu'ils contribuent efficacement à la mise en œuvre de la stratégie ;
- Pousser les différentes parties prenantes à travailler et collaborer ensemble ;
- Disposer de l'appui politique pour la mise en œuvre de la stratégie ;
- Assurer l'amélioration continue de la stratégie grâce à la revue périodique.

Composition proposée

- La Présidence de la République,
- L'ANSSI,
- L'ANSSI se charge du secrétariat de cette entité
- Des représentants des ministères:
    - Ministère du Numérique et de la Digitalisation,
    - Ministère en charge de la Défense Nationale,
    - Ministère de l'Intérieur et de la Sécurité Publique, représenté au travers de l'OCRC,
    - Ministère de la Justice et de la Législation, représenté au travers de la CRIET,
    - Ministère de l'Énergie,
    - Ministère de l'Économie et des Finances, représenté au travers du CENTIF,
    - L'ARCEP.

Positionnement

Au vu de la constitution proposée, cette entité sera placée au plus haut niveau de la pyramide, et assurera une forte représentation du gouvernement. Le positionnement de cette entité est au niveau de la Présidence de la République.

L'entité de pilotage

Description et rôles

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 rapporte au Conseil National de la Sécurité Numérique et a comme rôle de :

- Définir et faire valider par le Conseil National de la Sécurité Numérique, la stratégie de sécurité numérique ;
- Maintenir la stratégie nationale de sécurité numérique ;
- Elaborer et maintenir le plan d'actions relatif à la stratégie nationale de sécurité numérique ;
- Garantir l'obtention des résultats escomptés ;
- Empêcher ou limiter les résultats indésirables ;
- Elaborer le rapport annuel de la sécurité numérique ;
- Analyser les risques et les nouvelles tendances ;
- Assurer une mise à jour annuelle de l'évaluation du risque ;
- Assurer le suivi de tous les indicateurs de performance ;
- Jouer le rôle de centre de coordination entre les différents intervenants ;
- Jouer le rôle de hub d'information en cas d'attaque ;
- Rapporter au comité managérial : les performances de la stratégie ; L'état d'avancement des actions décidées ; Les modifications des enjeux externes et internes pertinents pour la sécurité numérique ; Les retours d'information des parties intéressées ; Les opportunités d'amélioration continue ; Les nouvelles tendances en matière de risque ;
- Assurer la veille réglementaire, méthodologique et technologique afin d'adapter en permanence la stratégie nationale de sécurité numérique aux différentes évolutions ;
- Réaliser les opérations de communication et de sensibilisation pour toutes les parties prenantes.

Composition proposée

Cette entité et cette fonction seront assurées par l'ANSSI. Le Ministère du Numérique et de la Digitalisation assure le suivi continu et l'appui des actions de l'ANSSI dans ce sens.

Positionnement

Cette entité dispose d'une communication directe avec le conseil national de la sécurité numérique.

Les entités opérationnelles

Description et rôles

Ces entités sont constituées de responsables des projets et des actions qui découleront de la stratégie nationale de sécurité numérique. Il s'agit en fait des entités opérationnelles publiques et privées qui seront chargées d'exécuter un ou plusieurs volets de la stratégie.

Chaque entité opérationnelle rapporte à l'entité de suivi et sera responsable de :

- Accomplir les actions dont elle est responsable convenablement ;
- Rapporter à l'entité de suivi les mesures de performance montrant le bon fonctionnement des actions ;
- Mentionner à l'entité de suivi les nouvelles tendances des menaces dans le périmètre dont elle est responsable ;
- Faciliter le travail de l'entité d'audit pour accomplir sa mission d'audit annuel ;
- Proposer des actions d'amélioration ;
- Suivre les actions correctives qui lui sont associées ;
- S'assurer que toutes les structures, sous sa responsabilité, sont conscientes et comprennent bien la stratégie ainsi que son apport. S'assurer que toutes les mises à jour et que toutes 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.

Composition proposée

Liste des entités opérationnelles :

- L'ANSSI,
- L'ASSI,
- Le bjCSIRT,
- L'OCRC,
- L'ARCEP,
- Ministères: Finances, Energie, Santé, Education, Enseignement supérieur, Economie Numérique, Transport.
- Les infrastructures critiques privées et publiques,
- Toute entité qui sera désignée par le CNSN pour appliquer une partie du plan d'actions.

Positionnement

Il s'agit en fait des agences de l'Etat, des différents ministères et de toute autre entité impliquée dans la mise en œuvre de la stratégie.

CONCLUSION

La présente stratégie définit les objectifs qu'il importe d'atteindre. Elle sera complétée par un inventaire des mesures existantes et par des plans d'actions opérationnels qui devront pour chaque domaine décrire les mesures concrètes à mettre en œuvre suivant un calendrier déterminé ainsi que les acteurs appelés à contribuer à leur accomplissement. Dans ce contexte, les centres universitaires et de recherches, qui constituent des centres d'excellence et disposent de connaissances et compétences pointues, seront invités à contribuer à la réalisation des objectifs de la stratégie. La stratégie ci-avant décrite à vocation à évoluer dans le temps. Elle sera périodiquement révisée afin d'être adaptée, si besoin en était, aux nouvelles réalités. A cette fin, il sera périodiquement procédé à une réévaluation des menaces et des risques, accompagnée, si nécessaire, de propositions ayant pour objet d'actualiser la présente stratégie.

9 LISTE DES ABREVIATIONS

ABSUCEP	Agence Béninoise du Service Universel des Communications Electroniques et de la Poste
ADN	Agence pour le Développement du Numérique
ANIP	Agence Nationale de l'Identification des Personnes
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASSI	Agence des Services et Systèmes d'Information
ARCEP	Autorité de Régulation des Communications Electroniques et de la Poste
APDP	Autorité de Protection des Données à caractère Personnel
BJCSIRT	Bénin Computer Security Incident Response Team
CSIRT	Computer Security Incident Response Team
CNSN	Conseil National de la Sécurité Numérique
DDOS	Distributed Denial of Service
FIRST	Forum of incident Response and Security Team
GFCE	Global Forum on Cyber Expertise
ITU	International Telecommunication Union
PKI	Public Key Infrastructure
RSSI	Responsable de la Sécurité du Système d'Information
TIC	Technologies de l'Information et de la Communication

MINISTÈRE DU NUMÉRIQUE
ET DE LA DIGITALISATION

RÉPUBLIQUE DU BÉNIN

ANSSI AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN