REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

Ministère de la Communication, des Télécommunications, des Postes et de l'Economie numérique

STRATÉGIE NATIONALE DE CYBERSÉCURITÉ DU SÉNÉGAL (SNC2022)

Novembre 2017

SOMMAIRE

SIGLES ET ABREVIATIONSACRONYMES

ADIE- Agence De l'Informatique de l'Etat

APIX - Agence nationale pour la Promotion des Investissements et des Grands Travaux

ANSD- Agence Nationale de la Statistique et de la Démographie

ARTP - Autorité de Régulation des Télécommunications et des Postes

BNLC - Brigade Nationale de Lutte contre la Cybercriminalité

CNC - Commission Nationale de Cryptologie

DDoS – Distributed Deny of Service (Dénis de Services Distribués)

DIC - Division des Investigations Criminelles

DSC - Division Spéciale de Cybersécurité (ex BNLC)

IIC - Infrastructures d'Information Critiques

IGC - Infrastructure de Gestion des Clés

CERT – Computer Emergency Response Team

CSIRT - Computer Security Incident Response Team

CERT/ CSIRT- Centre de veille, d'alerte et de réaction aux attaques informatiques

MAESE - Ministère des Affaires étrangères et des Sénégalais de l'Extérieur

MCTPEN - Ministère de la Communication, des Télécommunications, des Postes et de L'Economie Numérique

MEFP - Ministère de l'Economie, des Finances et du Plan

MESRI- Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation

MFA - Ministère des Forces Armées

MEN - Ministère de l'Education Nationale

MINT - Ministère de l'Intérieur

MJ - Ministère de la Justice

PSE - Plan Sénégal Emergent

PSSI-ES - Politique de Sécurité des Systèmes d'Information de l'Etat du Sénégal.

SGPR - Secrétariat Général de la Présidence de la République

SN2025 - Sénégal Numérique 2025

SNC2022 - Stratégie Nationale de Cybersécurité 2022

TIC - Technologies de l'Information et de la Communication

RÉSUMÉ ANALYTIQUE

Dans sa volonté de réussir le défi de son développement, le Sénégal a adopté le Plan Sénégal Emergent (PSE), une stratégie nationale qui rompt avec les approches des dernières décennies et inscrit le Sénégal dans une nouvelle trajectoire de développement économique et social. Ce nouvel élan du Sénégal, décliné en une vision d' « Un Sénégal émergent en 2035 », mise sur la transformation structurelle de son économie.

En droite ligne de cette vision et entre autres efforts majeurs, le Sénégal entend mettre à profit les avancées technologiques et particulièrement les technologies de l'information et de la communication (TIC) comme l'un des moteurs clés de cette transformation.

C'est dans ce contexte que le Sénégal a adopté « Sénégal numérique 2025 » (SN2025), sa stratégie nationale de transformation du Sénégal en une société numérique. Dans cette optique, la SN2025 s'appuie sur trois prérequis :

- le cadre juridique et institutionnel ;
- le capital humain ;
- la **confiance numérique**.

Au vu du troisième prérequis susmentionné (« la confiance numérique ») de la SN2025, il apparait que, pour tous les acteurs, la protection des infrastructures, des systèmes d'information et des utilisateurs et, par là, la protection du cyberespace dans son ensemble, constitue un pilier essentiel des ambitions que le Sénégal se donne pour le numérique.

Pour garantir cette confiance numérique, le Gouvernement du Sénégal devra s'assurer qu'il dispose des cadres, outils, connaissances, ressources et capacités nécessaires afin non seulement d'éliminer les vulnérabilités des systèmes d'information existant au Sénégal, mais aussi d'assurer une veille des cybermenaces, de prévenir les actes de cybercriminalité et de les réprimer.

Aussi, l'instruction présidentielle (**https://www.sec.gouv.sn/-PSSI-ES-.html)** relative à la politique de sécurité des systèmes d'information de l'Etat du Sénégal (PSSI-ES), est prise pour fixer les principes et les règles à mettre en application pour assurer un niveau de sécurité optimal des systèmes d'information de l'Etat dans le respect des lois et règlements en vigueur.

La présente « Stratégie nationale de Cybersécurité 2022 » (SNC2022) articule la vision et les objectifs stratégiques du Sénégal en matière de cybersécurité, traduisant par là un soutien constant aux priorités et aux objectifs de la SN2025.

La SNC2022 comprend les éléments clés suivants :

- une évaluation du contexte stratégique de la cybersécurité au Sénégal, y compris les menaces actuelles et futures ;

- la vision du Gouvernement sur la cybersécurité et les objectifs stratégiques à atteindre;

- les principes généraux, les rôles et les responsabilités pouvant renforcer ladite stratégie ;

- le cadre logique pour sa mise en œuvre.

La vision du Sénégal pour la cybersécurité s'intitule **« En 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous ».**

Afin de mettre en œuvre cette vision, le Gouvernement du Sénégal s'emploiera à atteindre les cinq objectifs stratégiques suivants :

1. *Objectif stratégique 1: renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal ;*

2. *Objectif stratégique 2: protéger les infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal ;*

3. *Objectif stratégique 3: promouvoir une culture de la cybersécurité au Sénégal;*

4. *Objectif stratégique 4 : renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs ;*

5. *Objectif stratégique 5 : participer aux efforts régionaux et internationaux de cybersécurité.*

Dans la mise en œuvre de la SNC2022, le Gouvernement du Sénégal appliquera les principes relatifs à :

- l'État de droit ;
- la responsabilité partagée ;
- l'approche basée sur les risques ;
- l'accès universel au cyberespace et sa pleine exploitation ;
- la collaboration et la coopération entre toutes les parties prenantes.

Pour ce faire, **le Gouvernement du Sénégal mettra en place une structure nationale de la cybersécurité** chargée de jouer un rôle moteur dans les questions de cybersécurité et de conduire la mise en œuvre et la coordination des initiatives relatives à la cybersécurité pour le Sénégal.

1 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 Sénégalais. En effet, le Gouvernement du Sénégal développe activement l'usage généralisé des TIC dans la vie quotidienne au Sénégal, à travers ses différentes initiatives nationales telles que décrites dans sa stratégie SN2025. Ces initiatives entraînent une remarquable transformation du Sénégal 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 Sénégal de bénéficier d'un quotidien économiquement plus riche.

La transformation numérique du Sénégal 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 Sénégal et limiterait les bénéfices de cette transformation.

Étant donné que les TIC sont davantage intégrées dans tous les domaines de la vie, le Sénégal est inévitablement confronté à des cybermenaces grandissantes où les acteurs malveillants continuent d'exploiter lses 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 Sénégal.

La SNC2022 s'est inspirée des priorités définies dans le PSE, de l'instruction présidentielle n°003/PR en date du 03 janvier 2017 sur la PSSI-ES, ainsi que des objectifs de la SN2025, en proposant une approche globale où les particuliers, le secteur privé ainsi que les institutions gouvernementales jouent pleinement leur rôle. En effet, ces acteurs garantiront le développement d'un secteur dynamique de cybersécurité et d'une base de compétences qui permettront au Sénégal de rester à jour et d'assurer un suivi effectif de l'environnement évolutif des cybermenaces. Cette SNC2022 articule également la détermination et l'engagement du Sénégal à contrer les cybermenaces présentes et futures.

2 Contexte et portée de la SNC2022

2.1 Le contexte de la stratégie

Depuis 2004, le Sénégal a libéralisé le secteur des télécommunications et mis en place un cadre législatif et réglementaire visant la croissance des TIC dans un environnement sécurisé, rendant ainsi plus visibles l'ampleur et l'impact de l'évolution technologique au Sénégal. En effet, les tendances et les opportunités observées ont alors rapidement augmenté depuis lors avec l'apparition rapide de nouvelles technologies, de services et d'applications issus de l'Internet. Ces développements ont aussi donné lieu à de grandes opportunités de croissance économique et sociale pour le Sénégal et continueront d'offrir des avantages considérables aux sociétés connectées.

Comme pour tous les autres pays, la transformation numérique du Sénégal donnera alors lieu à un recours croissant aux réseaux et aux systèmes d'information. Cependant, cette tendance donnera inévitablement aussi plus de possibilités aux individus ou groupes d'individus malveillants pour compromettre ces réseaux et systèmes d'information. Les cyberactivités ne connaissant aucune frontière, les cybercriminels continuent d'intensifier leurs efforts et d'augmenter leurs capacités de cibler les systèmes et les réseaux des particuliers et des organisations à travers le monde, y compris au Sénégal.

2.1.1 Les menaces

2.1.1.1 La cybercriminalité

La présente SNC2022 considère deux formes d'infractions comme constitutives de cybercriminalité :

- les infractions qui ne peuvent être commises qu'à travers l'usage des TIC (sachant que ces technologies peuvent constituer aussi bien l'outil de réalisation de l'infraction que la cible de l'infraction) tels que le développement et la distribution de logiciels malveillants en vue de gains financiers et autres;

- les infractions traditionnelles perpétrées ou aggravées par l'usage des TIC.

Les cybercrimes et cyberdélits perpétrés au sein du Sénégal ou contre le Sénégal ont souvent une motivation financière. Les auteurs de ces infractions peuvent avoir leur résidence au Sénégal comme dans tout autre pays. Cependant, même lorsqu'il qu'il y a des signalements de cas de cybercriminalité et que des responsables sont identifiés, il est très souvent difficile pour les forces de l'ordre ainsi que leurs homologues internationaux de poursuivre les auteurs, notamment, lorsque ceux-ci se trouvent dans des juridictions aux capacités limitées et/ou dans des juridictions sans aucun accord de collaboration avec le Sénégal ; ceci, malgré le fait que le Sénégal dispose entre autres, de divisions spécialisées dans la lutte contre la cybercriminalité au sein de la Police et de la Gendarmerie nationale, chacune ayant des ressources humaines qualifiées et des moyens techniques afin d'aider les enquêtes sur les cybercrimes ou cyberdélits.

A la complexité de la menace cybercriminelle à laquelle est confrontée le Sénégal s'ajoute le crime organisé agissant à travers le « dark web ». En plus d'être vulnérable aux logiciels malveillants et aux attaques sophistiquées affectant les systèmes et les réseaux des

particuliers et des organisations, le Sénégal est exposé à des attaques de plus en plus agressives telles que les « ransomware » et les dénis de services distribués « DDoS ».

Outre les menaces engendrées par les groupes issus de la criminalité organisée, il existe également une forme plus courante de cybercriminalité moins sophistiquée mais plus commune, menée contre les particuliers et les organisations. L'usurpation et l'escroquerie par le mobile illustrent cette forme de cybercriminalité à cibler des individus et des organisations à travers les transactions financières.

Bien que le Sénégal dispose de la Loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité, celle-ci soulève des questions et porte en elle-même des insuffisances, limitant ainsi son efficacité. Par exemple, il figure dans cette loi des références partielles au Code pénal et au Code de procédure pénale qui, eux-mêmes, ne sont pas mis à jour par rapport au milieu et aux tendances observées au Sénégal.

2.1.1.2 L' « hacktivisme »

Les groupes d'hacktivistes sont en général motivés par un calendrier politique et social et opèrent de façon décentralisée. Ils ont par conséquent tendance à attaquer leurs cibles dans l'intérêt de causes spécifiques ou en réponse à des revendications apparentes. Malgré le fait que la plupart des attaques d'hacktivistes sont perturbantes de par leur nature et incluent des attaques telles que DDoS et des détournements de sites Internet, peu d'attaques hacktivistes ont infligé jusqu'ici des dégâts importants et durables à leurs cibles.

2.1.1.3 Les menaces internes

Les menaces internes constituent un des plus gros risques pour toutes les organisations, y compris celles au Sénégal. Les employés des organisations ayant accès aux systèmes et aux données critiques sont eux-mêmes une menace, car pouvant causer des dommages financiers et des dommages à la réputation à travers le vol de données sensibles. Ces employés peuvent également utiliser leur connaissance de l'organisation dans le but de permettre ou de perpétrer une attaque visant à perturber le bon fonctionnement de leur organisation. Outre ces actes délibérés, les employés peuvent causer des dommages par inadvertance du fait de leur ignorance des procédures de sécurité de l'organisation, notamment par le téléchargement des contenus non sûrs, l'usage de périphériques infectés, ou en ouvrant du courriel d'hameçonnage. Ces employés peuvent également devenir des victimes d'actes d'ingénierie sociale à travers lesquels ils donnent alors par ignorance accès à leurs réseaux ou exécutent des instructions aux apparences inoffensives mais profitant aux cybercriminels. A cet égard, la Présidence de la République agissant par l'intermédiaire de la Commission Nationale de Cryptologie (CNC) a pris les devants et a prescrit des mesures détaillées relatives à la politique de sécurité des systèmes d'information de l'Etat du Sénégal (PSSI-ES).

2.1.1.4 Le cyberterrorisme et l'extrémisme

Les tendances globales suggèrent que les groupes terroristes continuent à envisager l'exécution de cyberattaques contre leurs pays cibles. De plus, les groupes terroristes continuent à utiliser l'Internet pour le recrutement et la radicalisation des individus, que ce soit contre le Sénégal ou contre d'autres pays. Le Sénégal pourra devenir un jour une cible pour ces groupes et doit donc prendre conscience de cette menace. Malgré le fait que les attaques physiques restent une priorité des groupes terroristes, avec la numérisation rapide des

économies et des sociétés à travers le monde, la probabilité de la survenance de groupes terroristes hautement qualifiés techniquement ou d'acteurs solitaires pouvant lancer des cyberattaques dévastatrices contre des nations cibles accroit également. La réputation du Sénégal pourrait également en souffrir s'il s'avérait que des acteurs solitaires issus du Sénégal sont impliqués dans des attaques contre des pays tiers. Tout ceci peut constituer une menace majeure pour le Sénégal et ses intérêts à l'avenir et il est ainsi impératif que le Sénégal considère cette menace dans sa stratégie.

2.1.1.5 Les menaces directes et indirectes des États

Les tendances actuelles liées aux cyberespionnage et aux cyberattaques indiquent entre autres que les pays se prennent de plus en plus pour cibles, deviennent les cibles d'acteurs soutenus par des États recherchant à pénétrer les systèmes et les réseaux d'États à des fins politiques, technologiques ou économiques. Pour cela, il est essentiel que le Sénégal prenne conscience de cette menace émergente et prenne des mesures pour l'atténuer.

2.1.2 Les vulnérabilités

Les tendances et prévisions au niveau mondial[1] indiquant la rapide prolifération à venir de l'« Internet des objets », ainsi que l'engagement du Sénégal pour une digitalisation de son économie et de sa société, suggèrent qu'il y aura de nouvelles vulnérabilités pouvant être exploitées et davantage d'attaques de grande envergure. En effet, considérant l'accroissement des dispositifs et des processus interconnectés ou connectés à l'Internet, les vulnérabilités auxquelles sera confronté le Sénégal incluront celles issues de l'absence de dispositifs de sécurité non seulement au niveau des équipements, mais aussi les menaces envers les systèmes interconnectés essentiels à la société.

Avec l'augmentation des vulnérabilités des réseaux, des systèmes et des logiciels, il devient urgent pour les pays de développer de bonnes pratiques et des processus de cybersécurité dans tous les secteurs. Cette nécessité s'est précisée après les récentes attaques à grand retentissement observées dans le monde entier, telles que l'attaque « Wannacry » en 2017, qui a affecté plusieurs gouvernements et entreprises à travers le monde. Considérant que la plupart des cyberattaques sont issues de l'exploitation de vulnérabilités connues et pouvant être facilement résolues, il est impératif que chaque pays prenne des mesures afin d'encourager les individus, les entreprises et les institutions à prendre les mesures nécessaires et faire les investissements adéquats pour réduire ces vulnérabilités.

Ceci est cohérent avec la situation actuelle au Sénégal où, malgré les efforts consentis, il persiste un manque de compétences et de connaissances pour traiter globalement des besoins de la cybersécurité des secteurs privé et public. En effet, outre les techniciens informatiques, la majorité des employés et des fonctionnaires de la plupart des organisations des secteurs privé et public au Sénégal ne mesurent pas suffisamment la portée des cybermenaces et n'y sont pas suffisamment sensibilisés. Certaines grandes organisations du secteur privé, telles que les banques et les opérateurs de télécommunications disposent, elles, d'une certaine connaissance de la cybersécurité et ont tendance à privilégier le développement d'une culture tournée vers la cybersécurité chez leurs employés, notamment concernant les pratiques à haut risque. Par contre, plusieurs organisations, et notamment celles proposant des services financiers, ne prennent pas toujours les mesures à la dimension

[1] *Roundup Of Internet Of Things Forecasts And Market Estimates*, 2016 - https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#368ddbb9292d

des vulnérabilités. Considérant qu'il n'existe aucun programme de sensibilisation coordonné au niveau national visant tous les secteurs de la société sénégalaise, le public n'est pas suffisamment sensibilise sur les questions de la cybersécurité.

Une vulnérabilité importante, actuellement observée au Sénégal, est liée aux insuffisances dans le domaine des compétences et aptitudes spécialisées nécessaires pour se tenir informé des évolutions du paysage cybernétique, ainsi que des technologies adéquates pour gérer les risques et les menaces qui y sont associés. Il est impératif que le Sénégal comble ces insuffisances.

Par ailleurs, plusieurs organisations des secteurs public et privé au Sénégal ainsi que les particuliers, ont tendance à utiliser des systèmes qui continuent à fonctionner avec des versions de logiciel obsolètes ou non protégées. Dans beaucoup cas, l'on constate l'emploi des logiciels qui ne sont plus supportés par les fournisseurs et pour lesquels les régimes de protection n'existent plus. Un logiciel non protégé ou obsolète souffre généralement de vulnérabilités que les auteurs de cybermenaces recherchent et exploitent.

2.2 La portée de la stratégie

La SNC2022 articule la vision et les objectifs stratégiques du Sénégal en matière de cybersécurité, ainsi qu'un engagement à soutenir de façon continue les priorités nationales en promouvant la transformation numérique du Sénégal. La SNC2022 vise à guider les actions de l'Etat concernant la cybersécurité tout en proposant une vision aux sénégalais, y compris aux organismes des secteurs privé et public, tout comme aux institutions universitaires, à la société civile et à d'autres parties prenantes.

La SNC2022 couvre le Sénégal dans son ensemble et énonce des actions visant tous les secteurs de l'économie et l'ensemble des couches de la société sénégalaise, y compris les institutions gouvernementales, les organismes du secteur privé et les particuliers. Par conséquent, le Gouvernement s'efforcera de garantir que la stratégie soit mise en œuvre pour le bien de tous. La SNC2022 vise également l'amélioration continue de la cybersécurité à tous les niveaux pour le bien commun, et précise le contexte dans lequel le Sénégal s'engage au niveau international afin de développer un cyberespace sûr et sécurisé.

La stratégie considère la cybersécurité comme la protection des systèmes d'information (logiciels, équipements et infrastructures), des données qui y sont incluses ainsi que des services qu'ils fournissent ou sur lesquels ils s'appuient, contre tout accès, modification, entrave, destruction ou usage illicites. Cela inclut des actes intentionnels ou non, issus de manquements lors de l'application des bonnes pratiques ou des procédures de sécurité.

La SNC2022 comprend les éléments clés suivants :

- une évaluation du contexte stratégique de la cybersécurité au Sénégal, y compris les menaces actuelles et futures ;
- la vision du Gouvernement quant à la cybersécurité et les objectifs stratégiques à atteindre ;
- les principes généraux, les rôles et les responsabilités pouvant renforcer ladite stratégie ;

- le cadre logique pour sa mise en œuvre.

3 L'APPROCHE

L'approche du Gouvernement pour répondre aux cybermenaces auxquelles le Sénégal est confronté s'appuie sur une vision et des objectifs stratégiques précis. Cette approche vient renforcer toutes les activités relatives à la cybersécurité entreprises au Sénégal par des particuliers, des organisations des secteurs public et privé et de la société civile ainsi que du monde universitaire.

3.1 Énoncé de la vision

La vision stratégique proposée constitue une représentation du futur souhaité pour le Sénégal. Elle est à la fois rationnelle, englobante et prospective. Elle découle d'une analyse faite de la situation de référence en matière de cybersécurité[2] et définit le cap pour les différents objectifs stratégiques de développement. Au regard de ce qui précède la vision se décline comme suit :

« En 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous »

3.2 Objectifs stratégiques

Afin de réaliser cette vision, le Gouvernement du Sénégal s'emploiera à atteindre les cinq objectifs stratégiques suivants :

1. *Objectif stratégique 1: renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal ;*

2. *Objectif stratégique 2: protéger les infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal ;*

3. *Objectif stratégique 3: promouvoir une culture de la cybersécurité au Sénégal;*

4. *Objectif stratégique 4 : renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs ;*

5. *Objectif stratégique 5 : participer aux efforts régionaux et internationaux de cybersécurité.*

3.3 Les principes directeurs

Dans la réalisation des objectifs susmentionnés, le Gouvernement du Sénégal appliquera les principes suivants :

[2] Situation de référence du Sénégal en matière de cybersécurité, par les experts de l'Université d'Oxford, mars 2016.

1. **La primauté du droit**: La SNC2022 sera mise en œuvre en conformité avec les lois en vigueur au Sénégal et les normes internationales, de façon à protéger les droits des Sénégalais.

2. **La responsabilité partagée**: La SNC 2022 garantira que tous les intervenants de l'écosystème de la cybersécurité au Sénégal (tels que l'administration publique, les entreprises et autres organisations ainsi que les particuliers) s'engagent à protéger leurs informations et les systèmes d'information afin d'assurer leur résilience, ainsi que pour aider à sécuriser les informations et les systèmes d'information des autres parties prenantes.

3. **Une approche basée sur les risques** : Le Gouvernement du Sénégal s'engage à ce que tous les intervenants de l'écosystème de la cybersécurité au Sénégal (tels que l'administration publique, les entreprises et autres organisations ainsi que les particuliers) adoptent une approche basée sur les risques dans l'évaluation et le suivi des menaces, dans la réponse aux incidents relatifs au cyberespace, ou dans la réalisation d'activités de cybersécurité.

4. **L'accès universel au cyberespace, et la pleine exploitation du cyberespace**: Le Gouvernement du Sénégal œuvrera pour garantir que tous les intervenants de l'écosystème de la cybersécurité du Sénégal (tels que l'administration publique, les entreprises et autres organisations, et les particuliers) jouissent pleinement du cyberespace et l'exploitent entièrement, afin de stimuler un développement socioéconomique plus étendu au Sénégal.

5. **La coopération et la collaboration entre les parties prenantes**: Le Gouvernement du Sénégal reconnaît les rôles et les responsabilités des différents intervenants dans la protection des intérêts sénégalais dans le cyberespace et s'engage à collaborer et coopérer avec l'ensemble des parties prenantes de l'écosystème de la cybersécurité au Sénégal (telles que l'administration publique, les entreprises et autres organisations ainsi que les particuliers), avec les organisations hors du Sénégal, ainsi qu'avec les organisations internationales afin de protéger le Sénégal dans le cyberespace.

3.4 Approche d'ensemble pour la réalisation des objectifs stratégiques

Afin que toutes les actions de cybersécurité soient autant que possible harmonisées, l'approche suivante orientera l'implémentation de la SNC2022.
Dans la mise en œuvre de la SNC2022, le Gouvernement du Sénégal développera de façon proactive les moyens et les instruments nécessaires permettant aux secteurs public et privé, à la société civile et à toute personne vivant au Sénégal d'être à l'abri des cybermenaces. Il doit également garantir que tous les acteurs précités puissent développer de manière dynamique, les compétences et la capacité à protéger leurs systèmes d'information ainsi que les informations proprement dites.

4 LES OBJECTIFS A ATTEINDRE

Les éléments suivants constituent les « objectifs spécifiques » et les « actions » à mettre en œuvre à l'horizon 2022, afin d'atteindre les « objectifs stratégiques » sus-énumérés et d'obtenir les résultats souhaités. Ils s'appuient sur les principes identifiés ci-dessus et s'alignent avec l'approche susmentionnée :

4.1 Objectif stratégique 1 : renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal

Il est nécessaire d'améliorer le cadre légal et réglementaire actuel du Sénégal, afin de permettre une gestion effective des cybermenaces et de la lutte contre la cybercriminalité, tout en garantissant que les nouvelles opportunités issues de la transformation numérique du Sénégal deviennent des atouts de son économie.

En outre, un cadre institutionnel est nécessaire pour garantir une gouvernance effective de la cybersécurité au Sénégal, renforcée par des fonctions et rôles clairs, ainsi que des responsabilités et des processus bien définis.

4.1.1 Objectif spécifique 1.1 : renforcer le cadre juridique de la cybersécurité

Au fur et à mesure que le Sénégal continue sa transformation en une société numérique telle que définie dans la SN2025, il devra à la fois lutter contre divers types de cybercrimes et cyberdélits et protéger ses cyber intérêts. En outre, vu l'évolution rapide et continue du paysage cybernétique, le Sénégal aura besoin de revoir régulièrement ses dispositifs législatifs et réglementaires afin de garantir que ceux-ci sont à jour et reflètent les tendances émergentes.

Résultats attendus :

4.1.1.1 Le Sénégal dispose d'un cadre législatif et règlementaire à jour, à la fois aligné sur les développements du cyberespace et sur les normes internationales, lui permettant de combattre effectivement les cyber-activités malveillantes visant le pays ou qui sont perpétrées depuis son territoire.

4.1.1.2 Le cadre législatif et réglementaire sénégalais prévoit des unités judiciaires et de sécurité disposant des outils et des technologies appropriés pour mener à bien leurs missions de lutte contre la cybercriminalité.

Actions :

4.1.1.1 Effectuer une analyse des déficits du cadre législatif et réglementaire des TIC, et élaborer des instruments adéquats pour améliorer le cyber environnement et lutter contre la cybercriminalité.

4.1.1.2 Souscrire aux conventions internationales et régionales relatives à la cybercriminalité et la cybersécurité.

4.1.1.3 Examiner et améliorer les dispositions législatives et règlementaires sur les pouvoirs de procédure en matière d'investigations d'actes de cybercriminalité pour prévenir, réagir et poursuivre les auteurs de ces actes plus efficacement.

4.1.1.4 Renforcer le cadre législatif et réglementaire en matière de protection des données et l'aligner aux normes internationales.

4.1.2 Objectif spécifique 1.2 : renforcer le cadre institutionnel pour assurer une gouvernance efficace de la cybersécurité

Face à la complexité croissante des menaces et défis de la cybersécurité, le Gouvernement du Sénégal se devra d'assurer un leadership fort et une gouvernance effective. Pour cela, il est essentiel que le Gouvernement établisse un cadre institutionnel qui encourage et permette une coordination rapide et prompte des activités de la cybersécurité accompagnée d'une approche cohérente et structurée. Ce cadre articulera et attribuera un ensemble de fonctions relatives à la gouvernance de la cybersécurité dans notre pays, comprenant : la revue périodique de la SNC2022, des conseils et un leadership stratégiques, le suivi des initiatives sur la cybersécurité, la coordination nationale de la détection et de la réponse aux cyber-incidents, et la préparation des organisations privées et publiques, notamment celles possédant ou exploitant des systèmes d'information au Sénégal.

Résultats attendus :

4.1.2.1 Une structure de gouvernance opérationnelle centralisée et adéquate est créée.

4.1.2.2 Une approche nationale cohérente et efficace pour le développement, la mise en œuvre et la coordination des activités de cybersécurité au Sénégal, est effective.

Actions :

4.1.2.1 Mettre en place une structure nationale de cybersécurité, laquelle mènera la mise en œuvre de la SNC2022 et sera responsable du développement et de la coordination des activités nationales relatives à la cybersécurité.

4.1.2.2 Mettre en place le CERT/ CSIRT national sous forme d'unité au sein de la structure nationale de cybersécurité, avec des fonctions et responsabilités précises, y compris la réponse aux incidents.

4.1.2.3 Identifier les institutions pertinentes des secteurs public et privé et en constituer un comité consultatif sur la cybersécurité dont le but sera de fournir des conseils stratégiques à la structure nationale de la cybersécurité.

4.1.2.4 Mettre en place un centre de commandement et de contrôle pour la cyberdéfense.

4.1.2.5 Renforcer le pouvoir des forces de défense et de sécurité, ainsi que leurs ressources en matière de lutte contre la cybercriminalité, notamment dans l'usage effectif d'outils d'investigation et d'établissement de preuves en cas de crimes ou délits commis à partir d'instruments numériques ou de réseaux informatiques.

4.1.2.6 Élaborer une stratégie de cyberdéfense qui décrit l'approche nationale face aux cybermenaces envers la sécurité nationale.

4.1.3 Objectif spécifique 1.3 : établir des normes de cybersécurité, des lignes directrices et un cadre opérationnel et technique

Le Sénégal développera et édictera des normes et adoptera des lignes directrices et des structures opérationnelles qui garantiront que les organisations des secteurs public et privé et notamment les propriétaires et operateurs d'infrastructures d'information critiques (IIC), ainsi

que les citoyens, adoptent les bonnes pratiques et des mesures communes dans le domaine de la cybersécurité. Ces pratiques et mesures devront se fonder sur la définition nationale de la cybersécurité au Sénégal.

Résultats souhaités :

4.1.3.1 Des normes de cybersécurité compréhensibles et appropriées sont édictées, ainsi que des lignes directrices, un cadre opérationnel et technique, des processus et des procédures sont établis et sont respectés au Sénégal.

Actions :

4.1.3.1 Edicter un ensemble de normes sur la cybersécurité, prenant en compte les normes internationales et adaptées au niveau national, entre autres pour les logiciels et le développement de leur code source.

4.1.3.2 Mettre en place un cadre opérationnel et technique chargé d'édicter les normes de cybersécurité et du suivi de leur application.

4.1.3.3 Promouvoir la sensibilisation et la mise en œuvre des normes dans les secteurs public et privé, surtout pour les PME.

4.2 Objectif stratégique 2 : renforcer la protection des infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal

Les systèmes et les réseaux qui composent le cyberespace doivent être en mesure de fonctionner pendant ou après tout cyber-incident. C'est pourquoi la protection des systèmes et des réseaux de l'Etat et celle des IIC sont une priorité absolue pour le Gouvernement. Le Gouvernement œuvrera à garantir que les IIC, les systèmes d'information du Sénégal dans leur ensemble puissent résister aux cyberattaques. Pour cela, il sera impératif que les organismes du secteur privé et particulièrement leurs gérants et leurs conseils d'administration soient non seulement conscients de leurs responsabilités et de leurs obligations, mais disposent aussi du support approprié pour leur permettre de mettre en place des mesures adéquates pour répondre aux cybermenaces.

4.2.1 Objectif spécifique 2.1 : assurer la protection des infrastructures d'information critiques et sécuriser les systèmes d'information du Sénégal

Pour assurer la protection des IIC et sécuriser les systèmes d'information du Sénégal, il est nécessaire que le Gouvernement ait au préalable une compréhension des niveaux de vulnérabilités de ceux-ci.

Résultats attendus :

4.2.1.1 Un état des lieux exhaustif des vulnérabilités et des niveaux de sécurité des IIC et des systèmes d'information du Sénégal est disponible.

4.2.1.2 La création et l'application de mesures indispensables pour améliorer et mettre en valeur la sécurité des IIC et des systèmes d'information du Sénégal sont effectives.

4.2.1.3 La capacité des opérateurs et des propriétaires d'IIC et systèmes d'information pour gérer les cybermenaces et cyber incidents est améliorée.

Actions :

4.2.1.1 Etablir un répertoire des IIC et des systèmes d'information du Sénégal.

4.2.1.2 Définir les cadres, les procédures et les processus nécessaires en matière de cybersécurité pour toute institution possédant ou gérant des IIC et les systèmes d'information du Sénégal.

4.2.1.3 Etablir un cadre de gestion des vulnérabilités des IIC et des systèmes d'information de l'Etat afin d'en promouvoir un suivi régulier.

4.2.1.4 Effectuer des tests et autres activités de surveillance réguliers des IIC et des systèmes d'information du Sénégal.

4.2.1.5 Définir des exigences minimales en matière de sécurité des IIC et des systèmes d'information du Sénégal.

4.2.2 Objectif spécifique 2.2 : maintenir un suivi permanent des cybermenaces et une gestion des risques

Le nombre et la gravité des cybermenaces et cyberrisques auxquels s'exposent les particuliers et les organisations au Sénégal continuent de croitre. La structure nationale de cybersécurité sera chargée de coordonner au plan national la gestion de ces cybermenaces et risques, actuels ou émergents.

Résultats attendus :

4.2.2.1 Une approche nationale coordonnée et une mise en œuvre pour la gestion d'incidents, soutenues par un état des lieux des cybermenaces, sont adoptées.

4.2.2.2 Une meilleure compréhension de la taille et de l'échelle des cybermenaces existe désormais au Sénégal suite à la signalisation des cyber-incidents à la structure nationale de cybersécurité.

4.2.2.3 Le Sénégal a une gestion plus complète, efficace et efficiente des cyber-incidents résultant de l'attribution d'un mandat centralisé de signalement des incidents et de réponse à la structure nationale de cybersécurité.

Actions :

4.2.2.1 Définir des exigences minimales dans la tenue de répertoires d'incidents nécessaires à leur analyse.

4.2.2.2 Surveiller, analyser, gérer en continu les menaces et les risques, atténuer, préparer, intervenir et faire le retour d'incidents.

4.2.2.3 Mettre en place un registre national des risques, les réglementations et les directives nationales afin de promouvoir l'évaluation et la gestion des risques.

4.2.2.4 Créer et continuellement actualiser un répertoire des incidents cybernétiques, évaluer ces incidents et proposer des solutions.

4.2.2.5 Mettre en place des procédures de protection des informations et des procédures de gestion des risques.

4.2.2.6 Concevoir et mettre en œuvre des scénarii et programmes de simulation d'incidents de cybersécurité à utiliser lors des exercices nationaux.

4.2.2.7 Mettre en place des mesures nationales de gestion des crises, effectuer des tests périodiques au moyen d'exercices de cyberattaques et évaluer les enseignements tirés de ces exercices afin d'améliorer ces mesures.

4.2.2.8 Créer et continuellement actualiser un plan d'urgence de cybersécurité qui décrit les rôles et les responsabilités de la structure nationale de cybersécurité, des forces de défense et de sécurité en cas de cyberattaques.

4.3 Objectif stratégique 3 : promouvoir une culture de la cybersécurité au Sénégal

La réussite d'un Sénégal numérique s'appuiera sur la confiance des organisations et des particuliers en matière des services en ligne. Le Gouvernement devra alors travailler avec les secteurs public et privé afin d'augmenter la connaissance et la compréhension des cybermenaces auxquelles sont confrontés le Sénégal et les sénégalais. En effet, si un nombre d'organisations, notamment celles du secteur bancaire et du secteur des télécommunications, prennent déjà des mesures pour se protéger, ces organisations demeurent minoritaires.

4.3.1 Objectif spécifique 3.1 : sensibiliser tous les groupes concernés ainsi que le grand public sur les risques de sécurité dans le cyberespace.

Le Gouvernement procédera à des campagnes de sensibilisation ciblant autant le public que les organisations sur les risques en matière de cybersécurité et les façons de se protéger. Pour ce faire, il adoptera diverses approches pour optimiser l'impact de ces campagnes et travaillera au besoin en partenariat avec d'autres organisations, en particulier celles offrant à leur clientèle des interfaces sujettes aux cybermenaces.

Résultats attendus :

4.3.1.1 Les bonnes pratiques sont adoptées par les particuliers et les organisations, afin que le nombre, la sévérité et l'impact des cyberattaques fructueuses qui ont lieu au Sénégal soient continuellement réduits.

4.3.1.2 Les organisations et les particuliers comprennent l'importance de la cybersécurité, leurs responsabilités et obligations, ainsi que les mesures qu'ils doivent adopter pour se protéger, favorisant une culture généralisée de la cybersécurité au Sénégal.

Actions :

4.3.1.1 Effectuer une étude nationale pour déterminer le niveau de sensibilisation à la cybersécurité sur tous les pans de la société et mettre en place un programme national de sensibilisation pour couvrir les différents groupes-cibles.

4.3.1.2 Vulgariser les bonnes pratiques en matière de cybersécurité.

4.3.1.3 Mener des formations obligatoires en matière de cybersécurité pour les hauts fonctionnaires et les membres de conseils d'administration du secteur privé afin d'améliorer leur compréhension des risques et menaces et comment atténuer ceux-ci.

4.3.2 Objectif spécifique 3.2 : Mettre en place un environnement de confiance fiable pour la fourniture des services gouvernementaux en ligne et des transactions électroniques

La vulgarisation des services en ligne, et notamment les services gouvernementaux en ligne et les transactions électroniques constituent des éléments important de la transition vers un Sénégal numérique. Pour atteindre cet objectif, le Gouvernement devra relever le défi crucial de la sécurité de ces services au Sénégal. En effet, un niveau minimal de sécurité devra être mis en place afin que les particuliers et les organisations au Sénégal puissent recourir aux services numériques et les utiliser en toute confiance. Pour ce faire, le Gouvernement mettra en place des mesures de sécurité spécifiques à ces services afin de stimuler la confiance en ceux-ci. Ces mesures incluent entre autres les éléments suivants :

- **l'authentification**, qui consiste en la validation de l'identité d'un individu ou d'une entité ;
- **la confidentialité** relative à la protection de l'information afin que seules les parties autorisées puissent y accéder ;
- **l'intégrité**, donnant l'assurance que les données non pas été modifiées ou falsifiées;
- **la non-répudiation**, permettant que soit fournie une attestation de participation à une action ou transaction.

Plus spécifiquement, le Gouvernement développera entre autres l'intégration d'une infrastructure de gestion des clés (IGC), la norme IPv6 et les minima de sécurité dans la conception et le déploiement des services gouvernementaux en ligne et des transactions électroniques. Des activités du Gouvernement sénégalais quant à cet objectif sont alignées sur les initiatives pertinentes définies par le SN2025, telles que l'architecture d'entreprise gouvernementale ou le système de paiement électronique d'impôts et de droits de douane.

Résultats attendus :

4.3.2.1 Les exigences de contrôle et les minima de cybersécurité sont intégrés dans les services gouvernementaux en ligne et les transactions électroniques, lesquels sont utilisés en toute confiance par les organisations et les personnes au Sénégal ou depuis l'étranger.

Actions :

4.3.2.1 Encourager l'utilisation des fonctions de sécurité de l'IGC, et notamment la confidentialité, l'authentification et l'intégrité pour créer des environnements fiables et sécurisés pour les services gouvernementaux en ligne et les transactions électroniques.

4.3.2.2 Mener à bien la transition du protocole IPv4 au protocole IPv6.

4.3.2.3 Assurer la prééminence des exigences de sécurité minimales dans le développement des services gouvernementaux en ligne et des transactions électroniques pour promouvoir la confiance numérique.

4.3.3 Objectif spécifique 3.3 : promouvoir l'usage des services gouvernementaux en ligne et des transactions électroniques

Le Gouvernement reconnaît pleinement l'importance du développement de la connaissance et de l'octroi d'information sur les aspects de la sécurité de ces services dans l'accroissement de la confiance. Pour cela, le Gouvernement s'attèlera à diffuser la bonne information sur la sécurité de ces services afin de permettre aux organisations et aux personnes des choix et des décisions informées quant à l'utilisation desdits services. Pour comprendre pleinement les préoccupations des personnes et des organisations au Sénégal et y répondre, le Gouvernement mettra en place des points de contact fiables qui veilleront à la collecte d'informations sur les préoccupations utilisateurs et à déterminer si les dispositifs de sécurité de ces services répondent à ces préoccupations. Le Gouvernement s'assurera également que l'information sur ces dispositifs de sécurité soit présentée aux utilisateurs de ces services dans un format et dans la langue de leurs choix. En somme, le Gouvernement encouragera une communication effective entre les utilisateurs, les organisations et le gouvernement pour maintenir la confiance en ces services.

Résultats attendus :

4.3.3.1 La confiance dans l'utilisation des services gouvernementaux en ligne et des transactions électroniques au Sénégal est établie.

Actions :

4.3.3.2 Mettre en place les points de contact nationaux pour la cybersécurité dont le rôle sera, entre autres, la collecte d'informations sur les préoccupations des usagers des services gouvernementaux en ligne et des transactions électroniques, d'apporter des réponses à ces préoccupations et de promouvoir l'utilisation de ces services.

4.3.3.3 Informer le public sur les mesures de cybersécurité mises en place pour les services gouvernementaux en ligne et les transactions électroniques.

4.4 Objectif stratégique 4 : renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs

Des ressources humaines compétentes et qualifiées en cybersécurité seront nécessaires pour l'émergence d'un écosystème innovateur et dynamique dans cette branche spécifique des TIC. A présent, le Sénégal connait des insuffisances en matière de cybersécurité autant dans l'éducation que dans les programmes de formations professionnelles, le développement personnel et les parcours de carrière spécialisés en cybersécurité. Pour y remédier, le Gouvernement fera du développement des compétences et d'une expertise critique en cybersécurité au Sénégal une priorité majeure.

4.4.1 Objectif spécifique 4.1 : renforcer les capacités et les connaissances techniques en matière de cybersécurité

Pour la réalisation de cet objectif, le Gouvernement mettra sur pied un programme national de renforcement des capacités en cybersécurité, afin de sécuriser les IIC, les systèmes d'information et les réseaux d'accès à l'Internet au Sénégal.

Résultats attendus :

4.4.1.1 Le Sénégal dispose de compétences et d'expertise pour surveiller, analyser et gérer en continu les menaces et les risques ainsi que pour l'atténuation, la préparation, l'intervention et le retour d'incidents.

Actions :

4.4.1.1 Évaluer régulièrement les capacités et les connaissances techniques du CERT/ CSIRT national et des institutions étatiques afin de traiter les faiblesses identifiées.

4.4.1.2 Former et orienter régulièrement le personnel du CERT/CSIRT national afin qu'il puisse faire face aux cyberattaques les plus sophistiquées.

4.4.1.3 Former et orienter périodiquement le personnel des institutions étatiques afin qu'il ait la capacité et les connaissances pour préparer, protéger, intervenir et effectuer les retours d'incidents.

4.4.1.4 Établir des exigences de base en ce qui concerne la formation sur la cybersécurité pour les secteurs privé et public.

4.4.2 Objectif spécifique 4.2 : renforcer les capacités et les connaissances techniques nécessaires à l'application effective des textes législatifs et réglementaires

Les organes chargés de l'application des lois développeront les capacités et les compétences nécessaires pour mettre en œuvre les cadres législatif et règlementaire et pour poursuivre les auteurs d'actes de cybercriminalité commis par ou contre toute personne ou organisation au Sénégal.

Résultats attendus :

4.4.2.1 Les organismes chargés de l'application des lois au Sénégal ont les capacités et les compétences nécessaires pour traiter les cas de cybercriminalité.

Actions :

4.4.2.1 Former et orienter en continu le personnel des services de sécurité et les autorités judiciaires afin de renforcer leurs capacités et leurs connaissances techniques pour traiter des cas de cybercriminalité.

4.4.2.2 Mettre en place les formations obligatoires liées aux investigations numériques et à la manipulation des preuves pour le personnel des services de sécurité, des autorités judiciaires et autres organisme œuvrant dans la détection et la poursuite d'actes de cybercriminalité.

4.4.3 Objectif spécifique 4.3 : Assurer une bonne adéquation formation/emploi en cybersécurité

Vu le rôle et les responsabilités partagées entre le milieu académique, la société civile, le secteur public et le secteur privé dans la réponse au déficit de compétences dans le domaine de la cybersécurité au Sénégal, le Gouvernement adoptera une approche nationale cohérente au développement de ces compétences afin d'accroitre l'expertise technique locale en matière

de cybersécurité. En partenariat avec toutes les parties prenantes, le Gouvernement devra accroitre de façon significative le nombre de professionnels de la cybersécurité issus du système éducatif Sénégalais ayant les compétences requises pour répondre aux besoins actuels.

Résultats attendus :

4.4.3.1 Il existe des programmes nationaux d'éducation et de formation comportent le volet cybersécurité aux niveaux préscolaire, primaire, secondaire et universitaire

4.4.3.2 La cybersécurité est reconnue comme une filière avec des voies d'admission et des parcours de carrière clairement définis.

4.4.3.3 La cybersécurité est un élément essentiel de la formation continue de tous les acteurs.

Actions :

4.4.3.1 Élaborer un programme coordonné au niveau national sur l'éducation et la formation en cybersécurité, qui comporte un volet secondaire et universitaire sous la responsabilité des ministères concernés ;

4.4.3.2 Promouvoir les carrières en cybersécurité.

4.4.3.3 Évaluer et actualiser les programmes et la documentation pour les niveaux préscolaire, primaire, secondaire et universitaire pour y intégrer les notions de cybersécurité sous la responsabilité des ministères en charge de l'enseignement.

4.4.3.4 Elaborer des conventions de partenariat entre les universités et grandes écoles nationales et/ou étrangères, le secteur public et le secteur privé pour mettre au point des programmes d'études, de recherche et de stages en cybersécurité.

4.4.4 Objectif spécifique 4.4 : promouvoir le développement du secteur de la cybersécurité au Sénégal

Le Gouvernement stimulera la croissance d'un secteur innovant dans le développement de produits fiables de cybersécurité au sein duquel les professionnels et les organisations bénéficieront du soutien, des compétences et des investissements requis pour prospérer. A cet effet, le Gouvernement renforcera les initiatives déjà en cours dans le cadre de la stratégie SN2025, telles que le développement de parcs de technologies numériques, notamment celui de Diamniadio, ou encore « Startup Sénégal ».

Résultats attendus :

4.4.4.1 Une augmentation significative des investissements chez les prestataires et structures de cybersécurité est acquise.

4.4.4.2 Il existe une croissance annuelle du secteur de la cybersécurité et de sa contribution au PIB.

4.4.4.3 Un soutien du Gouvernement de façon proactive aux prestataires et structures de cybersécurité locales à travers diverses mesures dont, entre autres, la commande publique et les mesures d'incitation, est acquis.

Actions :

4.4.4.4 Promouvoir les investissements locaux et étrangers dans le secteur de la cybersécurité au Sénégal et proposer des mesures d'incitation.

4.4.4.5 Réaliser des études sur l'impact de la cybercriminalité sur l'économie sénégalaise.

4.4.4.6 Soutenir les entreprises locales spécialisées dans le développement et la fourniture de solutions de cybersécurité.

4.5 Objectif stratégique 5 : participer aux efforts régionaux et internationaux de cybersécurité

Compte tenu de la nature transfrontalière du cyberespace, une collaboration régionale et internationale sur les questions de cybersécurité sera essentielle pour le Sénégal dans ses efforts de renforcement de la confiance numérique. Pour cette raison, le Gouvernement fera également de sa participation aux efforts régionaux sur la cybersécurité une priorité. En plus, le Gouvernement s'engage à collaborer avec ses partenaires partout dans le monde pour répondre aux questions de cybersécurité, apportant ainsi sa contribution à l'émergence d'un cyberespace global plus sûr.

4.5.1. Objectif spécifique 5.1 : renforcer la coopération internationale sur les questions liées à la cybersécurité

Le Gouvernement du Sénégal cherchera à renforcer sa collaboration et sa contribution sur les questions de cybersécurité, notamment dans la lutte contre la cybercriminalité, en soutenant la coopération internationale en cybersécurité , en prenant sa place dans le cyber-écosystème global, ou encore en promouvant un comportement responsable de la part des sénégalais.

Résultats attendus :

4.5.1.1 Une participation efficace et active du Sénégal dans les activités régionales et internationales de cybersécurité.

4.5.1.2 Une collaboration bilatérale et multilatérale renforcée sur les questions de cybersécurité.

Actions :

4.5.1.1 Coordonner la participation du Sénégal et renforcer sa collaboration avec les autres États et partenaires régionaux et internationaux sur la cybersécurité, notamment dans la lutte contre la cybercriminalité.

4.5.1.2 Participer activement aux activités régionales et internationales de cybersécurité notamment dans la lutte contre la cybercriminalité.

5 GESTION ET SUIVI DE L'EXÉCUTION DE LA SNC2022

5.1 Rôles et responsabilités

Le Gouvernement du Sénégal est pleinement conscient du caractère essentiel d'une gouvernance et d'un cadre institutionnel en matière de cybersécurité reposant sur la responsabilité collective de toutes les parties prenantes afin de protéger les systèmes d'information, les réseaux, les installations critiques, les données et les utilisateurs. Cette section définit clairement les rôles et responsabilités des acteurs clés de la mise en œuvre de la SNC2022.

Les **personnes** résidant au Sénégal ont pour responsabilité d'adopter toutes les mesures raisonnables pour sécuriser les données, les logiciels, le matériel informatique et les systèmes qui leur appartiennent ou qu'ils utilisent dans leur vie professionnelle ou privée. Cela est essentiel pour le Sénégal du fait que les personnes représentent une portion significative du Sénégal dans le cyberespace et peuvent constituer une ligne efficace de protection dans le cyberespace contre les acteurs malveillants, mais aussi une vulnérabilité.

Les **organisations** au Sénégal ont une connectivité et des technologies intégrées dans leurs opérations ; elles possèdent et opèrent des systèmes numériques, fournissent des services numériques et détiennent des données personnelles. Par conséquent, elles ont une responsabilité dans la protection des ressources qu'elles détiennent et emploient et doivent assurer la continuité et la sécurité des services numériques qu'elles offrent. En cela, il est impératif que les entreprises et autres organisations usent de toutes les normes et mesures pratiques pour protéger toutes les données personnelles en leur possession, ainsi que pour asseoir leur sécurité et leur capacité de résistance et de reprise après tout sinistre subit par leurs systèmes ou leurs services.

Le **Gouvernement du Sénégal** a pour responsabilité de protéger ses citoyens contre tout dommage et de remettre tout criminel à la justice. Il a également pour responsabilité de protéger le Sénégal contre les cybermenaces contre sa sécurité nationale et ses infrastructures critiques. En plus, étant lui-même prestataire de services numériques et par là détenteur de données, le Gouvernement doit d'adopter des mesures strictes pour protéger ces données ainsi que ses systèmes d'information. Pour ce qui est des IIC du Sénégal dans la fourniture des services essentiels au niveau national, et bien que certains de ces IIC ou services peuvent être détenus ou opérés par le secteur privé, le Gouvernement est en fin de compte responsable de s'assurer de la résilience nationale et de la continuité des services et fonctions essentielles sur tout le Sénégal. Le Gouvernement a également pour devoir de fournir des conseils et des informations aux organisations et aux citoyens sur ce qu'ils doivent faire pour se protéger en ligne et édicter les normes auxquelles les organisations doivent se plier. Par ailleurs, le Gouvernement doit également diriger la création d'un environnement favorable à un cyber secteur dynamique et innovant au Sénégal dans lequel son système éducatif produit les ressources humaines capables de répondre aux besoins présents et futurs de cybersécurité au Sénégal. En somme, le Gouvernement du Sénégal est responsable de la mise en œuvre de la stratégie nationale de cybersécurité. **Un comité de suivi et d'évaluation** présidée par ***le ministère en charge du numérique*** sera créé pour entreprendre le suivi et l'évaluation effectifs de la mise en œuvre de la SNC2022 afin d'évaluer et de résoudre toute entrave opérationnelle rencontrée, mais aussi, afin de déterminer l'impact et les résultats à long terme de la SNC2022.

Les **services habilités notamment de police judiciaire (police, gendarmerie, douane) et les organismes judiciaires** collaboreront selon les besoins avec les partenaires bilatéraux et multilatéraux pour renforcer leurs actions dans l'investigation, la mise en déroute et la poursuite en justice des actes de cybercriminalité.

Les **forces nationales de défense (les armées)** sont chargées de défendre le Sénégal contre les cybermenaces dirigées vers la souveraineté et à la sécurité nationales et enquêteront sur toutes les menaces relevant du domaine de la défense (cyberterrorisme, guerre cybernétique, etc.) Les forces nationales de défense, à travers le centre national de commande et de contrôle de la cyberdéfense, sont responsables des systèmes de sécurisation des informations et des infrastructures utilisées pour la défense nationale et travailleront en collaboration avec la structure nationale de cybersécurité pour soutenir la protection et la prévention contre les cyber incidents au niveau national, ainsi que l'atténuation de leurs effets et les retours d'incidents.

La structure nationale de cybersécurité sera établie comme l'organe central pour la cybersécurité au Sénégal chargé de diriger l'exécution de la SNC2022. Elle sera responsable de la planification, de la coordination et de la mise en œuvre des initiatives de cybersécurité au Sénégal. La structure assurera la protection, la prévention, l'atténuation et le rétablissement en cas de cyber incidents sur tout le Sénégal et fournira des conseils et de l'assistance aux organisations au Sénégal. La structure coordonnera la protection des IIC et des systèmes d'information publics et privés au Sénégal. Elle développera et assurera la conformité de ceux-ci aux politiques, orientations, normes et bonnes pratiques. En bref, la structure servira de voix nationale et de centre d'expertise sur la cybersécurité. **Un Comité de pilotage pour la structure** sera créé pour mettre sur pied La structure nationale de cybersécurité

Le **comité consultatif national sur la cybersécurité** sera créé pour fournir des conseils stratégiques sur le développement et la mise en œuvre d'initiatives nationales en matière de cybersécurité.

Les **organisations de la société civile** du Sénégal collaboreront avec les autres parties prenantes de l'écosystème de cybersécurité du Sénégal pour assurer la transparence et la responsabilité des organisations des secteurs public et privé, pour renforcer la relations entre ces organisations et les particuliers et pour aider à sensibiliser la société sénégalaise aux questions de cybersécurité.

Le milieu académique collaborera avec la société civile, le secteur public et le secteur privé pour faciliter le développement des capacités et de l'expertise en cybersécurité, contribuant ainsi aux besoins actuels et futurs en professionnels compétents et avertis pour la cybersécurité. Le milieu académique collaborera également avec la société civile, le secteur public et le secteur privé pour mener à bien la recherche et le développement concernant la cybersécurité.

Les **propriétaires et les opérateurs des infrastructures d'information critiques (IIC) et des systèmes d'information du Sénégal** seront responsables de la protection de leurs systèmes d'information et, par conséquent, devront mettre en œuvre toutes les mesures nécessaires pour protéger ceux-ci contre les cybermenaces. Ils devront s'assurer de leur conformité par rapport aux normes, directives, processus, procédures et cadres établis par le gouvernement du Sénégal en matière de cybersécurité.

5.2 Suivi et évaluation

Du fait de l'évolution constante des cybermenaces, le Gouvernement est pleinement conscient que pour une mise en œuvre réussie de la SNC2022, il est impératif de lui adjoindre un cadre de suivi et d'évaluation. Un suivi et une évaluation entrepris de façon effective permettra, entre autres, d'élaborer de nouvelles mesures ou de modifier des mesures existantes.

Sur ce volet important, le Gouvernement adoptera l'approche suivante :

5.2.1.1 L'établissement d'objectifs de performance spécifiques, mesurables et réalisables dans des délais déterminés pour diverses parties prenantes responsables de la mise en œuvre des actions de la SNC2022.

5.2.1.2 L'élaboration de plans d'actions annuels pour chaque projet, définissant les résultats attendus, l'approche quant à la réalisation de ces résultats, ainsi que l'identification des ressources nécessaires pour garantir la réussite de leur mise en œuvre. Ces plans reposeront sur des objectifs, des indicateurs de performance et des délais fixés dans le cadre logique de mise en œuvre de la SNC2022.

5.2.1.3 L'adoption, dans les trois (3) mois suivant le lancement de la SNC2022, d'un plan général de suivi et d'évaluation basé sur l'approche proposée.

5.2.1.4 Le suivi et l'évaluation proprement dits des objectifs et indicateurs de performance tels qu'établis dans le cadre logique de mise en œuvre et la production de rapports d'évaluation provisoires.

5.2.1.5 Des examens périodiques contenant les évolutions dans la réalisation des résultats attendus, les mesures correctives, ainsi que les impacts à long terme de la SNC2022, dont :

- Des examens annuels ;
- Un examen à moyen terme à la fin de la 2ème année de la mise en œuvre de la SNC2022 ;
- Un examen à long terme à la fin de la 4ème année de la SNC2022.

CONCLUSION

L'évolution rapide du cyberespace comporte des avantages considérables pour l'accélération du développement économique du Sénégal. Cependant, le cyberespace recèle aussi de vulnérabilités et d'une cybercriminalité croissante qui mettent en péril non seulement la confiance numérique au Sénégal, mais la vision même d'un « Sénégal numérique 2025 ».

La SNC2022 articule l'approche et l'engagement au niveau national à éliminer ces vulnérabilités liées aux IIC et aux systèmes d'information au Sénégal, et à combattre la cybercriminalité de façon efficace. Dans cette approche, le Sénégal s'engage à être proactif face aux cybermenaces actuelles et futures en se dotant des capacités adéquates .

En effet, une mise en œuvre effective de la SNC2022 améliorera le niveau de maturité du Sénégal en termes de cybersécurité, grâce non seulement à une meilleure compréhension et

à une meilleure gestion des vulnérabilités, des menaces, des risques et des incidents liés au cyberespace, mais aussi à la croissance du secteur de la cybersécurité avec une expertise et des produits locaux hautement compétitifs.
A l'horizon 2022, tous les acteurs de la société feront alors bon usage du cyberespace, en exploitant toutes ses potentialités et en toute confiance.

ANNEXE A - CADRE LOGIQUE DE MISE EN ŒUVRE DE LA SNC2022

Cette annexe présente les éléments clés nécessaires à une mise en œuvre optimale de ladite stratégie :

- Objectif stratégique : l'objectif substantiel à long terme qui contribue à la réalisation de la vision ;
- Objectif spécifique : les étapes nécessaires pour atteindre chaque Objectif stratégique ;
- Stratégies / Actions : les activités à entreprendre pour atteindre les objectifs spécifiques ;
- Éléments livrables / Résultats : Les produits obtenus suite aux actions entreprises;
- Agence et assistance principale de mise en œuvre : Les institutions ou organes ayant une responsabilité principale dans la gestion de la réalisation de chaque objectif et ceux qui assureront les services de soutien.
- Echéance : Période durant laquelle les Éléments livrables / Résultats seront produits et/ou les Stratégies ou Actions seront mises en œuvre.
- Indicateurs clés de performance : Les indicateurs, mesures de données et tendances qui doivent être suivis pour évaluer les états d'avancement dans la mise en œuvre de la stratégie.
- Sources de financement : Identification des structures de financement possibles de la mise en œuvre de la stratégie.

Objectif stratégique 1 : renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal

Objectif spécifique 1.1 : renforcer le cadre juridique de la cybersécurité

Résultats attendus :

- Le Sénégal dispose d'un cadre législatif et règlementaire à jour, à la fois aligné sur les développements du cyberespace et sur les normes internationales, lui permettant de combattre effectivement les cyber-activités malveillantes visant le pays ou qui sont perpétrées depuis son territoire.
- Le cadre législatif et réglementaire sénégalais prévoit des unités judiciaires et de sécurité disposant des outils et des technologies appropriés pour mener à bien leurs missions de lutte contre la cybercriminalité

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Echéance	Indicateurs clés de performance	Sources possibles de financement	Coût estimatif (XOF)

1.1.1 Effectuer une analyse des déficits du cadre législatif et réglementaire des TIC, et élaborer des instruments adéquats pour améliorer le cyber environnement et lutter contre la cybercriminalité.	PRIMATURE MCTPEN CNC	Une étude identifiant des déficits dans le cadre législatif et réglementaire des TIC en matière de cybersécurité. Instruments adéquats pour améliorer le cyber environnement et lutter contre la cybercriminalité.	Juin 2018	Ampleur de la révision de cadre législatif et réglementaire ; Adoption d'Instruments adéquats pour améliorer le cyber environnement et lutter contre la cybercriminalité ; L'amélioration de l'effectivité du de cadre législatif et réglementaire ;	PRIMATURE MCTPEN	35 000 000
1.1.2 Souscrire aux conventions internationales et régionales relatives à la cybercriminalité et la cybersécurité.	PRIMATURE, MCTPEN	Conventions internationales et régionales relatives à la cybercriminalité et la cybersécurité.	Décembre 2018	Ampleur de la mise en oeuvre des conventions internationales et régionales relatives à la cybercriminalité et la cybersécurité. Effectivité des conventions internationales et régionales relatives à la cybercriminalité et la cybersécurité.	PRIMATURE ;	10 000 000

1.1.3 Examiner et améliorer les dispositions législatives et règlementaires sur les pouvoirs de procédure en matière d'investigations d'actes de cybercriminalité pour prévenir, réagir et poursuivre les auteurs de ces actes plus efficacement	PRIMATURE MJ MFA MINT	Dispositions législatives et règlementaires sur les pouvoirs de procédure en matière d'investigations d'actes de cybercriminalité	Juin 2018	Effectivité des dispositions législatives et règlementaires Ampleur d'application des dispositions législatives et règlementaires Ampleur d'amélioration des dispositions législatives et règlementaires	PRIMATURE MJ	35 000 000

1.1.4 Renforcer le cadre législatif et réglementaire en matière de protection des données et l'aligner aux normes internationales.	PRIMATURE ; MCTPEN ; MJ ; CDP Structure nationale de cybersécurité	Cadre législatif et réglementaire en matière de protection des données	Septembre 2018	Effectivité du cadre législatif et réglementaire en matière de protection des données Ampleur d'application du cadre législatif et réglementaire en matière de protection des données Nombre d'organisations adoptant et implémentant le cadre législatif et réglementaire en matière de protection des données	PRIMATURE ; MCTPEN ; MJ ; Structure nationale de cybersécurité	25 000 000

Objectif spécifique 1.2 : renforcer le cadre institutionnel pour assurer une gouvernance efficace de la cybersécurité

Résultats attendus

- Une structure de gouvernance opérationnelle centralisée et adéquate est créée.
- Une approche nationale cohérente et efficace pour le développement, la mise en œuvre et la coordination des activités de cybersécurité au Sénégal, est effective.

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Echéance	Indicateurs clés de performance	Sources possibles de financement	Coût estimatif (XOF)
1.2.1 Mettre en place une structure nationale de cybersécurité, laquelle mènera la mise en œuvre de la SNC2022 et sera responsable du développement et de la coordination des activités nationales relatives à la cybersécurité.	PRIMATURE SGPR MCTPEN	structure nationale de cybersécurité opérationnelle	Septembre 2018	Promulgation de texte Opérationnalisation de la structure nationale de cybersécurité	PRIMATURE SGPR MCTPEN	950 000 000
1.2.2 Mettre en place le CERT/CSIRT national sous forme d'unité au sein de la structure nationale de cybersécurité, avec des fonctions et responsabilités précises, y compris la réponse aux incidents	PRIMATURE SGPR MCTPEN	CERT / CSIRT national sous forme d'unité au sein de la structure nationale de cybersécurité	Décembre 2018	Promulgation de texte Opérationnalisation de la structure nationale de cybersécurité	PRIMATURE SGPR MCTPEN	

1.2.3 Identifier les institutions pertinentes des secteurs public et privé et en constituer un comité consultatif sur la cybersécurité dont le but sera de fournir des conseils stratégiques à la structure nationale de la cybersécurité.	PRIMATURE MCTPEN	comité consultatif sur la cybersécurité	Décembre 2018	Promulgation de texte Opérationnalisation du Comité	PRIMATURE MCTPEN	15 000 000
1.1.4 Mettre en place un centre de commandement et de contrôle pour la cyberdéfense	PRIMATURE Min Forces Armées (MFA)	Un centre de commandement et de contrôle pour la cyberdéfense	Décembre 2018	Promulgation de texte Opérationnalisation du centre de commandement et de contrôle pour la cyberdéfense	PRIMATURE Min Forces Armées (MFA) ;	900 000 000

1.2.5 Renforcer le pouvoir des forces de défense et de sécurité, ainsi que leurs ressources en matière de lutte contre la cybercriminalité, notamment dans l'usage effectif d'outils d'investigation et d'établissement de preuves en cas de crimes ou délits commis à partir d'instruments numériques ou de réseaux informatiques	MFA ; MJ; MINT ADIE	Mandat et rôle des forces de défense et de sécurité en matière de lutte contre la cybercriminalité, notamment dans l'usage effectif d'outils d'investigation et d'établissement de preuves en cas de crimes	Promulgation de texte : Décembre 2018	Promulgation de texte Ampleur d'application du texte	MFA ; MJ ; MINT	35 000 000
1.2.6 Élaborer une stratégie de cyberdéfense qui décrit l'approche nationale face aux cybermenaces envers la sécurité nationale.	PRIMATURE MFA	Stratégie nationale de cyber-défense	Décembre 2018	Ampleur de la mise en œuvre de la Stratégie nationale de cyber-défense	PRIMATURE MFA	3 5 000 000

Objectif spécifique 1.3 : établir des normes de cybersécurité, des lignes directrices et un cadre opérationnel et technique

Résultats attendus

- Des normes de cybersécurité compréhensibles et appropriées sont édictées, ainsi que des lignes directrices, un cadre opérationnel et technique, des processus et des procédures sont établis et sont respectés au Sénégal

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Échéance	Indicateurs clés de performances	Sources possibles de financement	Couts Estimatif Par An (XOF)
1.3.1 Edicter un ensemble de normes sur la cybersécurité, prenant en compte les normes internationales et adaptées au niveau national, entre autres pour les logiciels et le développement de leur code source.	structure nationale de cybersécurité MCTPEN CNC ADIE	un ensemble de normes sur la cybersécurité, prenant en compte les normes internationales et adaptées au niveau national	Décembre 2018	Ampleur de la mise en œuvre de l'ensemble de normes sur la cybersécurité	Structure nationale de cybersécurité ; MCTPEN	15 000 000
1.3.2 Mettre en place un cadre opérationnel et technique chargé d'édicter les normes de cybersécurité et du suivi de leur application.	MCTPEN ; Secteur privé ; Structure nationale de cybersécurité	Un cadre opérationnel et technique chargé d'édicter les normes de cybersécurité et du suivi de leur application.	Décembre 2018	Ampleur de la mise en œuvre d'un cadre opérationnel et technique	MCTPEN ; Secteur privé ; Structure nationale de cybersécurité	10 000 000

1.3.3 Promouvoir la sensibilisation et la mise en œuvre des normes dans les secteurs public et privé, surtout pour les PME	MCTPEN ; Secteur privé ; Structure nationale de cybersécurité	Un programme national pour promouvoir l'adaptation et l'adoption des normes de cybersécurité	Juin 2019	Ampleur de la mise en œuvre de l'ensemble de normes sur la cybersécurité Nombre d'organisations adoptant et implémentant l'ensemble de normes sur la cybersécurité	MCTPEN ; Secteur privé ; Structure nationale de cybersécurité	10 000 000

Objectif stratégique 2 : renforcer la protection des infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal

Objectif spécifique 2.1 : assurer la protection des infrastructures d'information critiques et sécuriser les systèmes d'information du Sénégal

Résultats attendus

- Un état des lieux exhaustif des vulnérabilités et des niveaux de sécurité des IIC et des systèmes d'information du Sénégal est disponible.
- La création et l'application de mesures indispensables pour améliorer et mettre en valeur la sécurité des IIC et des systèmes d'information du Sénégal sont effectives.
- La capacité des opérateurs et des propriétaires d'IIC et systèmes d'information pour gérer les cybermenaces et cyber incidents est améliorée

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Échelle de temps	Indicateurs clés de performances	Sources et mécanismes possibles de financement	Couts Estimatif Par An (XOF)

2.1.1 Etablir un répertoire des IIC et des systèmes d'information du Sénégal.	ARTP ; ADIE CNC Structure nationale de cybersécurité	Répertoire des IIC et des systèmes d'information du Sénégal.	Septembre 2018	Fréquence des exercices d'évaluation fondés sur les risques destinés à identifier des IIC et des systèmes d'information du Sénégal. Fréquence d'actualisation du répertoire des IIC et des systèmes d'information du Sénégal.	ARTP ; ADIE Structure nationale de cybersécurité	25 000 000
2.1.2 Définir les cadres, les procédures et les processus nécessaires en matière de cybersécurité pour toute institution possédant ou gérant des IIC et les systèmes d'information du Sénégal	ADIE ; Structure nationale de cybersécurité	Les cadres, les procédures et les processus nécessaires en matière de cybersécurité pour les IIC et des systèmes d'information	Septembre 2018	Ampleur de la mise en œuvre la mise les cadres, les procédures et les processus nécessaires en matière de cybersécurité	ADIE ; Structure nationale de cybersécurité	25 000 000

2.1.3 Etablir un cadre de gestion des vulnérabilités des IIC et des systèmes d'information de l'Etat afin d'en promouvoir un suivi régulier.	ADIE ; CERT /CSIRT	Un répertoire des vulnérabilités cadre de gestion et divulgation des vulnérabilités	Décembre 2018	Ampleur de la mise en œuvre du cadre de gestion et divulgation des vulnérabilités Fréquence de l'actualisation du répertoire des vulnérabilités Fréquence des divulgations de vulnérabilités	ADIE ; CERT/CSIRT (structure nationale de cybersécurité)	25 000 000
2.1.4 Effectuer des tests et autres activités de surveillance réguliers des IIC et des systèmes d'information du Sénégal.	ADIE ; CERT/ CSIRT	Tests et autres activités de surveillance réguliers des IIC et des systèmes d'information	Décembre 2018	Nombre des tests et autres activités de surveillance menées Fréquences des tests et autres activités de surveillance menées Efficacité des tests et autres activités de surveillance ;	ADIE ; CERT/CSIRT (structure nationale de cybersécurité)	25 000 000

2.1.5 Définir des exigences minimales en matière de sécurité des IIC et des systèmes d'information du Sénégal.	ADIE CNC Structure nationale de cybersécurité	Exigences minimales en matière de sécurité des IIC et des systèmes d'information	Décembre 2019	Ampleur de la mise en œuvre des exigences minimales en matière de sécurité des IIC et des systèmes d'information	ADIE CNC Structure nationale de cybersécurité	25 000 000

Objectif spécifique 2.2 : maintenir un suivi permanent des cybermenaces et une gestion des risques

Résultats attendus

- Une approche nationale coordonnée et une mise en œuvre pour la gestion d'incidents, soutenues par un état des lieux des cybermenaces, sont adoptées.
- Une meilleure compréhension de la taille et de l'échelle des cybermenaces existe désormais au Sénégal suite à la signalisation des cyber-incidents à la structure nationale de cybersécurité.
- Le Sénégal a une gestion plus complète, efficace et efficiente des cyber-incidents résultant de l'attribution d'un mandat centralisé de signalement des incidents et de réponse à la structure nationale de cybersécurité.

Stratégies/ Actions	**Agence et assistance principale de mise en œuvre**	**Éléments livrables/ Résultats**	**Échéance**	**Indicateurs clés de performances**	**Sources possibles de financement**	**Couts Estimatif (XOF)**

2.2.1 Définir des exigences minimales dans la tenue de répertoires d'incidents nécessaires à leur analyse	ADIE; MINT:; MFA CERT/ CSIRT	Exigences minimales dans la tenue de répertoires d'incidents	Décembre . 2018	Nombre d'entités adoptant et mettant en œuvre les exigences de signalisation des incidents de cyber sécurité Analyse et conclusions fiables sur les incidents de cyber sécurité	ADIE; MINT: MFA CERT/ CSIRT	25 000 000
2.2.2 Surveiller, analyser et gérer en continu les menaces et les risques, atténuer, préparer, intervenir et faire le retour d'incidents	ADIE; CERT/ CSIRT	Mesures d'atténuation des menaces et des risques et de résolution des incidents	Décembre 2018	Fréquence des mises à jour des répertoires nationaux des risques et d'incidents; Fréquence de l'élaboration et de l'application de mesures d'atténuation des menaces et risques et de résolution	ADIE; Structure nationale de cybersécurité	25 000 000

2.2.3 Mettre en place un registre national des risques, les réglementations et les directives nationales afin de promouvoir l'évaluation et la gestion des risques	ADIE; CERT/CSIRT	Répertoire national des risques, les réglementations et les directives nationales	Juin 2018	Fréquence des mises à jour de répertoire national des risques	ADIE; Structure nationale de cybersécurité	25 000 000
2.2.4 Créer et continuellement actualiser un répertoire des incidents cybernétiques, évaluer ces incidents et proposer des solutions	ADIE; CERT/CSIRT	Répertoire des incidents cybernétiques	Septembre 2018	Fréquence des mises à jour des répertoires nationaux des risques et d'incidents ; Fréquence de l'élaboration et de l'application de mesures d'atténuation des menaces et risques et de résolution	ADIE; CERT/CSIRT	25 000 000
2.2.5 Mettre en place des procédures de protection des informations et des procédures de gestion des risques	CERT/CSIRT	Des procédures de protection des informations et des procédures de gestion	Septembre 2018	Ampleur de la mise en œuvre des procédures de protection des informations et des procédures de gestion	ADIE; Structure nationale de cybersécurité	25 000 000

2.2.6 Concevoir et mettre en œuvre des scénarii et programmes de simulation d'incidents de cybersécurité à utiliser lors des exercices nationaux	CERT/CSIRT	Des scénarios et programmes de simulation d'incidents de cyber	Décembre 2018	Utilisation des scénarios et programmes de simulation des incidents de cyber sécurité lors d'exercices à l'échelle nationale	Structure nationale de cybersécurité	25 000 000
2.2.7 Mettre en place des mesures nationales de gestion des crises, effectuer des tests périodiques au moyen d'exercices de cyberattaques et évaluer les enseignements tirés de ces exercices afin d'améliorer ces mesures	CERT/CSIRT	Des mesures nationales de gestion des crises	Décembre 2018	Ampleur de la mise en œuvre des mesures nationales de gestion des crises	Structure nationale de cybersécurité	25 000 000

2.2.8 Créer et continuellement actualiser un plan d'urgence de cybersécurité qui décrit les rôles et les responsabilités de la structure nationale de cybersécurité, des forces de défense et de sécurité en cas de cyberattaquess	MFA MINT CSIRT	Un plan d'urgence de cybersécurité	Décembre 2018	Fréquence des mises à jour du plan d'urgence de cybersécurité; Effectivité de plan d'urgence de cybersécurité Nombre d'exercices d'entraînement en ligne	MFA ; Structure nationale de cybersécurité	25 000 000

Objectif stratégique 3 : promouvoir une culture généralisée de la cybersécurité au Sénégal

Objectif spécifique 3.1 : sensibiliser tous les groupes concernés ainsi que le grand public sur les risques de sécurité dans le cyberespace

Résultats attendus

- Les bonnes pratiques sont adoptées par les particuliers et les organisations, afin que le nombre, la sévérité et l'impact des cyberattaques fructueuses qui ont lieu dans le pays puissent être continuellement réduits.
- Les organisations et les particuliers comprennent l'importance de la cybersécurité, leurs responsabilités et obligations, ainsi que les mesures qu'ils doivent adopter pour se protéger, favorisant une culture généralisée de la cybersécurité au Sénégal

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Echéance	Indicateurs clés de performances	Sources possibles de financement	Couts Estimatif (XOF)
3.1.1 Effectuer une étude nationale pour déterminer le niveau de sensibilisation à la cybersécurité sur tous les pans de la société et mettre en place un programme national de sensibilisation pour couvrir les différents groupes-cibles.	MCTPEN CNC Structure nationale de cybersécurité ANSD	Étude au niveau national du niveau de sensibilisation à la cybersécurité sur tous les segments de la société. Programme national de sensibilisation visant tous les groupes d'utilisateurs, en particulier ceux qui sont les plus vulnérables.	Septembre 2018 ;	Niveau de sensibilisation Nombre / fréquence des campagnes de cybersécurité Effectivité des campagnes Étendue de l'évaluation des niveaux nationaux de sensibilisation de cybersécurité	MCTPEN CNC Structure nationale de cybersécurité ANSD	15 000 000

3.1.2 Vulgariser les bonnes pratiques en matière de cybersécurité.	Société civile Structure nationale de cybersécurité Secteur privé MCTPEN CNC	Feuille de route nationale pour inculquer une culture de la cybersécurité au Sénégal. Publication / diffusion des pratiques exemplaires en matière de cybersécurité sur de multiples canaux de communication	Juin 2018 ;	Feuille de route nationale pour inculquer une culture de la cybersécurité au Sénégal. Fréquence de publication / diffusion des pratiques exemplaires en matière de cybersécurité sur de multiples canaux de communication	Société civile Structure nationale de cybersécurité Secteur privé MCTPEN CNC	15 000 000

3.1.3 Mener des formations obligatoires en matière de cybersécurité pour les hauts fonctionnaires et les membres de conseils d'administration du secteur privé afin d'améliorer leur compréhension des risques et menaces et comment atténuer ceux-ci	MCTPEN MESRI MEN CNC Structure nationale de cybersécurité	Formation obligatoire de cybersécurité pour les représentants de rang élevé au sein du gouvernement, les législateurs de haut rang et les membres du comité de gouvernance et de direction des organisations du secteur privé	Juin 2018 ;	Ampleur des connaissances des hauts fonctionnaires et les membres de conseils d'administration du secteur privé Nombre de hauts fonctionnaires et les membres de conseils d'administration prenant part aux formations Effectivité des formations obligatoires en matière de cybersécurité pour les hauts fonctionnaires et les membres de conseils d'administration du secteur privé Fréquence des formations obligatoires en matière de cybersécurité pour les hauts fonctionnaires et les membres de conseils d'administration du secteur privé	MCTPEN MESRI MEN CNC Structure nationale de cybersécurité	20 000 000

Objectif spécifique 3.2 : mettre en place un environnement de confiance fiable pour la fourniture des services gouvernementaux en ligne et des transactions électroniques

Résultats attendus

- Les exigences de contrôle et les minima en cybersécurité sont intégrés dans les services gouvernementaux en ligne et les transactions électroniques, lesquels sont utilisés en toute confiance par les organisations et les personnes au Sénégal ou depuis l'étranger

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Échéance	Indicateurs clés de performances	Sources possibles de financement	Couts Estimatif (XOF)
3.2.1 Encourager l'utilisation des fonctions de sécurité de l'infrastructure de gestion des clés, et notamment la confidentialité, l'authentification et l'intégrité pour créer des environnements fiables et sécurisés pour les services gouvernementaux en ligne et les transactions électroniques	Structure nationale de cybersécurité CNC ADIE	Plan de mise en œuvre de l'infrastructure de gestion des clés (IGC)	Juin 2018 ;	Nombres des services gouvernementaux en ligne et des transactions électroniques intégrant l'utilisation des IGC	Structure nationale de cybersécurité CNC ADIE ARTP	60 000 000

3.2.2 Mener à bien la transition du protocole IPv4 au protocole IPv6.	ARTP ADIE Structure nationale de cybersécurité MCTPEN	Plan de transition du protocole IPv4 au protocole IPv6.	Décembre 2018 ;	Ampleur de la mise en œuvre du Plan de transition du protocole IPv4 au protocole IPv6	ARTP ADIE Structure nationale de cybersécurité MCTPEN	50 000 000
3.2.3 Assurer la prééminence des exigences de sécurité minimales dans le développement des services gouvernementaux en ligne et des transactions électroniques pour promouvoir la confiance numérique	Structure nationale de cybersécurité ADIE Toutes les parties prenantes concernées	exigences de sécurité minimales dans le développement des services gouvernementaux en ligne et des transactions électroniques.	Juin 2018 ;	Nombre des services services gouvernementaux en ligne et des transactions électroniques adoptant et mettant en œuvre les exigences de sécurité minimales	Structure nationale de cybersécurité ADIE Toutes les parties prenantes concernées	50 000 000

Objectif spécifique 3.3 : promouvoir l'usage des services gouvernementaux en ligne et des transactions électroniques

Résultats attendus

- La confiance dans l'utilisation des services gouvernementaux en ligne et des transactions électroniques au Sénégal est établie

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Échéance	Indicateurs clés de performances	Sources possibles de financement	Couts Estimatif (XOF)

3.3.1 Mettre en place les points de contact nationaux pour la cybersécurité dont le rôle sera, entre autres, la collecte d'informations sur les préoccupations des usagers des services gouvernementaux en ligne et des transactions électroniques, d'apporter des réponses à ces préoccupations et de promouvoir l'utilisation de ces services	structure nationale de cybersécurité ADIE	Points de contacts de « Confiance »	Déc. 2018	Étendue de la collecte et de l'analyse des informations sur les préoccupations de sécurité des personnes et des organisations en ce qui concerne les services électroniques publics et commerciaux Étendue de la confiance dans les services électroniques publics et commerciaux stimulée chez les personnes et les organisations	Structure nationale de cybersécurité ADIE	50 000 000
3.3.2 Informer le public sur les mesures de cybersécurité mises en place pour les services gouvernementaux en ligne et les transactions électroniques.	Structure nationale de cybersécurité ADIE	Programme de partage des informations sur les mesures de cybersécurité mises en place pour les services gouvernementaux en ligne et des transactions électroniques	Septembre 2018	Effectivité du partage des informations Fréquence de du partage des informations Ampleur du partage des informations	Structure nationale de cybersécurité ADIE	30 000 000

Objectif stratégique 4 : renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs

Objectif spécifique 4.1 : renforcer les capacités et les connaissances techniques de en matière de cybersécurité

Résultats attendus

- Le Sénégal dispose de compétences et d'expertise pour surveiller, analyser et gérer en continue les menaces et les risques ainsi que pour l'atténuation, la préparation, l'intervention et le retour d'incidents

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Échéance	Indicateurs clés de performances	Sources possibles de financement	Couts Estimatif (XOF)
4.1.1 Évaluer régulièrement les capacités et les connaissances techniques du CERT /CSIRT) national et des institutions étatiques afin de traiter les faiblesses identifiées	Structure nationale de cybersécurité Autres parties prenantes concernées	L'évaluation des capacités et les connaissances techniques du CSIRT national et des institutions étatiques	décembre 2018	Nombres des programmes de renforcement des faiblesses identifiées Fréquence / Effectivité des évaluations de capacité et d'expertise technique Effectivité des programmes répondant aux manques et aux points faibles	Structure nationale de cybersécurité Autres parties prenantes concernées	25 000 000

4.1.2 Former et orienter régulièrement le personnel du CERT/CSIRT national afin qu'il puisse faire face aux cybermenaces les plus sophistiquées.	CERT/ CSIRT Structure nationale de cybersécurité	Programme national de formation du personnel CERT/CSIRT	décembre 2018	Ampleur de la mise en œuvre du Programme national de formation du personnel du CERT/CSIRT Effectivité du Programme national de formation du personnel du CERT/CSIRT Nombre d'incidents / attaques / menaces / risques évités / mitigés en conséquence directe de programme national de formation du personnel du CERT/CSIRT	CERT/CSIRT Structure nationale de cybersécurité	25 000 000

4.1.3 Former et orienter périodiquement le personnel des institutions étatiques afin qu'il aie la capacité et les connaissances pour préparer, protéger, réagir et rétablir en cas d'incidents.	Parties prenantes concernées	Programme Périodique de formation pour le personnel des institutions étatiques	décembre 2018	Ampleur de la mise en œuvre du Programme Périodique de formation pour le personnel des institutions étatiques Effectivité de Programme Périodique de formation pour le personnel des institutions étatiques Nombre d'incidents, d'attaques, de menaces et de risques évités/atténués grâce au développement de capacité et les connaissances	Parties prenantes concernées	10 000 000
4.1.4 Établir des exigences de base en ce qui concerne la formation sur la cybersécurité pour les secteurs privé et public.	MENN MESRI	Exigences de base pour la formation sur la cybersécurité	en décembre 2018	Nombre des programmes de formation adoptant et mettant en œuvre les exigences de base pour la formation sur la cybersécurité	MEN MESRI	5 000 000

Objectif spécifique 4.2 : renforcer les capacités et les connaissances techniques nécessaires à l'application effective des textes législatifs et réglementaires

Résultats attendus

- Les organismes chargés de l'application des lois au Sénégal ont les capacités et les compétences nécessaires pour traiter les cas de cybercriminalité

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Echéance	Indicateurs clés de performances	Sources possibles de financement	Couts Estimatif (XOF)

4.2.1 Former et orienter en continu le personnel des services de sécurité et les autorités judiciaires afin de renforcer leurs capacités et leurs connaissances techniques pour traiter des cas de cybercriminalité.	MJ MINT MFA MEFP	Programme de formation pour le personnel des services de sécurité et les autorités judiciaires afin de renforcer leurs capacités et leurs connaissances techniques pour traiter des cas de cybercriminalité	décembre 2018	Ampleur de la mise en œuvre du Programme de formation pour le personnel des services de sécurité et les autorités judiciaires Effectivité du Programme de formation pour le personnel des services de sécurité et les autorités judiciaires Nombre d'incidents / attaques / menaces / risques évités / mitigés grâce au développement de capacités et connaissances techniques des services de sécurité et les autorités judiciaires	MJ MINT MFA MEFP	100 000 000

4.2.2 Mettre en place les formations obligatoires liées aux investigations numériques et à la manipulation des preuves pour le personnel des services de sécurité, des autorités judiciaires et autres organisme œuvrant dans la détection et la poursuite d'actes de cybercriminalité.	Toutes les parties prenantes concernées Gendarmerie / Police / Armée	Programme de formation sur les investigations numériques et à la manipulation des preuves	décembre 2018	Ampleur de la mise en œuvre du Programme de formation sur les investigations numériques et à la manipulation des preuves Effectivité du Programme de formation sur les investigations numériques et à la manipulation des preuves Nombre d'incidents / attaques / menaces / risques évités / mitigés grâce au développement de capacités et connaissances techniques sur les investigations numériques et la manipulation des preuves	Toutes les parties prenantes concernées Gendarmerie / Police / Armée	10 000 000

Objectif spécifique 4.3 : Assurer une bonne adéquation formation/emploi en cybersécurité

Résultats attendus

- Il existe des programmes nationaux d'éducation et de formation comportent le volet cybersécurité aux niveaux pré-scolaire, primaire, secondaire et universitaire.
- La cybersécurité est reconnue comme une filière avec des voies d'admission et des parcours de carrière clairement définis.
- La cybersécurité est un élément essentiel de la formation continue de tous les acteurs.

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Échéance	Indicateurs clés de performances	Sources possibles de financement	Couts Estimatif (XOF)
4.3.1 Élaborer un programme coordonné au niveau national sur l'éducation et la formation en cybersécurité qui comporte un volet secondaire et universitaire sous la responsabilité des ministères concernés ;	MEN MESRI	Un programme national sur l'éducation et la formation en cybersécurité	décembre 2018	Ampleur de la mise en œuvre du programme national sur l'éducation et la formation en cybersécurité Effectivité du programme national sur l'éducation et la formation en cybersécurité	MEN MESRI	20 000 000

4.3.2 Promouvoir les carrières en cybersécurité.	MEN MESRI MCTPEN	Programme national de niveau qualification en matière de cybersécurité	décembre 2018	La cybersécurité est reconnue comme une filière avec des voies d'admission et des parcours de carrière clairement définis ; Ampleur de la mise en œuvre du programme national des métiers en matière de cybersécurité	MEN MESRI MCTPEN	20 000 000

4.3.3 Évaluer et actualiser les programmes et la documentation pour les niveaux préscolaire, primaire, secondaire et universitaire pour y intégrer les notions de cybersécurité	MENMESRI	Les programmes et documentation aux niveaux préscolaire, primaire, secondaire et universitaire actualisé avec les notions de cyber sécurité	décembre 2018	Ampleur de l'actualisation du programmes et documentation aux niveaux préscolaire, primaire, secondaire et universitaire actualisé avec les notions de cyber sécurité Ampleur d'utilisation des Les programmes aux niveaux pré-scolaire, primaire, secondaire et universitaire actualisé avec les notions de cyber sécurité Nombre de diplômés des programmes scolaires avec les compétences requises en matière de cybersécurité Effectivité de l'actualisation des programmes et documentation	MEN MESRI	30 000 000

4.3.4 Elaborer des conventions de partenariat entre les universités et grandes écoles nationales et/ou étrangères, le secteur public et le secteur privé pour mettre au point des programmes d'études, de recherche et de stages en cybersécurité	MEN MESRI MCTPEN CNC Universités	Nouveaux programmes d'études et de stages en cybersécurité Partenariats entre le gouvernement, le secteur privé et le milieu académique pour prendre en charge la participation des organisations et des individus dans les programmes d'études, de recherche et de stages en cybersécurité	décembre 2018	Nombres des nouveaux programmes d'études et de stages sur la cybersécurité Nombre d'étudiants/de diplômés des nouveaux programmes d'études et de stages Ampleur de la participation à des projets et des activités de recherche nationaux et internationaux sur la cyber sécurité ; Nombre de partenariats créés pour soutenir la participation à des projets et des activités de recherche nationaux et internationaux sur la cybersécurité ;	MEN MESRI MCTPEN	50 000 000

Objectif spécifique 4.4 : promouvoir la croissance du secteur de la cybersécurité au Sénégal

Résultats attendus

- Une augmentation significative des investissements chez les prestataires et structures de cybersécurité est acquise.
- Il existe une croissance annuelle du secteur de la cybersécurité et de sa contribution au PIB.
- Le Gouvernement soutient de façon proactive les prestataires et sociétés de services de cybersécurité locales à travers diverses mesures dont, entre autres, la commande publique et les mesures d'incitation, est acquis..

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Échéance	Indicateurs clés de performances	Sources possibles de financement	Couts Estimatif (XOF)

4.4.1 Promouvoir les investissements locaux et étrangers dans le secteur de la cybersécurité au Sénégal et proposer des mesures d'incitation.	MEFP MESRI MPIPDTE MCTEN APIX Structure nationale de cybersécurité Banques	Programme d'incitation pour promouvoir des investissements dans le secteur de la cybersécurité	e Septembre 2018	Ampleur de la mise en œuvre du Programme d'incitation pour promouvoir des investissements dans le secteur de la cybersécurité Effectivité du Programme d'incitation pour promouvoir des investissements dans le secteur de la cybersécurité Nombre de bénéficiaires du Programme d'incitation pour promouvoir des investissements dans le secteur de la cybersécurité	MEFP MESRI APIX Banques Structure nationale de cybersécurité	60 000 000

4.4.2 Réaliser des études sur l'impact de la cybercriminalité sur l'économie sénégalaise.	Structure nationale de cybersécurité	Publication des résultats des études sur l'impact de la cybercriminalité sur l'économie sénégalaise	juin 2019	Fréquence / mises à jour des études sur l'impact de la cybercriminalité sur l'économie sénégalaise Ampleur des investissements sur la cybersécurité grâce au des résultats des études	Structure nationale de cybersécurité	25 000 000
4.4.3 Soutenir les entreprises locales spécialisées dans le développement et la fourniture de solutions de cybersécurité.	MEFP MESRI APIX MCTPEN Banques Structure nationale de cybersécurité	Programme de financement et d'incitation pour les entreprises locales spécialisées dans le développement et la fourniture de solutions de cybersécurité.	septembre 2018	Nombre d'entreprises participant au programme de financement et d'incitation pour les entreprises locales Effectivité du programme de financement et d'incitation pour les entreprises locales Ampleur de la mise en œuvre du programme de financement et d'incitation pour les entreprises locales	MEFP MESRI APIX Banques MCTPEN	80 000 000

Objectif stratégique 5 : participer aux efforts régionaux et internationaux de cybersécurité

Objectif spécifique 5.1 : renforcer la collaboration bilatérale et multilatérale sur les questions liées à la cybersécurité

Résultats attendus

- Une participation efficace et active du Sénégal dans les activités régionales et internationales de cybersécurité.
- Une collaboration bilatérale et multilatérale renforcée sur les questions de cybersécurité.

Stratégies/ Actions	Agence et assistance principale de mise en œuvre	Éléments livrables/ Résultats	Échéance	Indicateurs clés de performances	Sources possibles de financement	Couts Estimatif (XOF)

5.1.1 Coordonner la participation du Sénégal et renforcer sa collaboration avec les autres États et partenaires régionaux et internationaux sur la cybersécurité notamment dans la lutte contre la cybercriminalité	SGPR MAESE Structure nationale de cybersécurité MCTPEN ARTP	Programme de coordination de la participation du Sénégal et sa collaboration avec les autres États et partenaires régionaux et internationaux sur la cybersécurité et la lutte contre la cybercriminalité Protocoles d'entente et de collaboration signés avec les partenaires cibles, sur la cybersécurité et la lutte contre la cybercriminalité	septembre 2018	Ampleur de la mise en œuvre du Programme de coordination de la participation du Sénégal et sa collaboration avec les autres États et partenaires régionaux et internationaux Effectivité du Programme de coordination de la participation du Sénégal et sa collaboration avec les autres États et partenaires régionaux et internationaux Ampleur de la mise en œuvre des cadres appropriés Effectivité de Mise en Œuvre des cadres appropriés Fréquence des partages de l'information sur les menaces potentielles à travers les liens ou réseaux internationaux; Nombre des menaces potentielles à partir de l'information provenant des liens ou réseaux internationaux	SGPR MAESE Structure nationale de cybersécurité MCTPEN ARTP	5 000 000

5.1.2 Participer activement aux activités régionales et internationales de cybersécurité notamment dans la lutte contre la cybercriminalité	SEC GÉN PRÉSIDENCE MAESE Structure nationale de cybersécurité MCTPEN MINT MJ MFA ARTP	Plan d'engagement régional et international dans le domaine de la cybersécurité et la lutte contre la cybercriminalité Fonds pour la participation plus active dans les activités sur la cybersécurité et la lutte contre la cybercriminalité Participation dans des forums internationaux clés sur la cybersécurité et la lutte contre la cybercriminalité. Publication des résultats / leçons tirés de la participation à des activités internationales et régionales sur la cybersécurité et la lutte contre la cybercriminalité.	septembre 2018	Ampleur de la mise en œuvre du plan d'engagement régional et international dans le domaine de la cybersécurité et la lutte contre la cybercriminalité Ampleur de l'utilisation des fonds pour la participation plus active dans les activités sur la cybersécurité et la lutte contre la cybercriminalité Ampleur de la participation dans des forums internationaux clés sur la cybersécurité et la lutte contre la cybercriminalité. Effectivité des résultats / leçons tirés de la participation à des activités internationales et régionales sur la cybersécurité et la lutte contre la cybercriminalité.	SEC GÉN PRÉSIDENCE MAESE Structure nationale de cybersécurité MCTPEN MINT MJ MFA ARTP	15 000 000

ANNEXE B – PROJETS PRIORITAIRES

Pour les coûts estimatifs et l'échéance, se référer à l'Annexe A.

Objectif stratégique 1: renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal
1. **Établissement et mise en opération de la structure nationale de cybersécurité pour le Sénégal** 2. Renforcement du cadre juridique de la cybersécurité
Objectif stratégique 2: renforcer la protection des infrastructures d'information critiques (IIC) et les systèmes d'information de l'Etat du Sénégal
3. Projet d'identification et de protection des infrastructures d'information critiques (IIC)
Objectif stratégique 3: promouvoir une culture de cybersécurité au Sénégal
4. Elaboration d'une feuille de route nationale pour promouvoir une culture de cybersécurité au Sénégal 5. Mise en place d'un programme national de sensibilisation visant tous les groupes d'utilisateurs, en particulier ceux qui sont les plus vulnérables. 6. Programme de formation à la cybersécurité pour les autorités du gouvernement, des autres institutions de la République et les membres des conseils d'administration des organisations du secteur privé et du public.
Objectif stratégique 4 : renforcer les capacités et les connaissances techniques en cybersécurité dans tous les secteurs
7. Programme de formation et de renforcement de capacité nationale à la cybersécurité 8. Normes règlementaires et minimales dans la formation et l'éducation à la cybersécurité 9. Programme de coordination nationale sur l'éducation en matière de cybersécurité et de développement des compétences 10. Programme incitatif national pour promouvoir les investissements dans le secteur de la cybersécurité
Objectif stratégique 5 : participer aux efforts régionaux et internationaux de cybersécurité.
11. Plan d'engagement régional et international dans le domaine de la cybersécurité notamment dans la lutte contre la cybercriminalité 12. Mise en place d'un fonds national pour une participation active dans les activités de cybersécurité notamment dans la lutte contre la cybercriminalité.

ANNEXE C – GLOSSAIRE

- Authentification: L'authentification pour un système informatique est un processus permettant au système de s'assurer de la légitimité de la demande d'accès faite par une entité (être humain ou un autre système) afin d'autoriser l'accès de cette entité à des ressources du système (systèmes, réseaux, applications) conformément au paramétrage du contrôle d'accès.

- Cconfidentialité : le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé

- Cyberattaque : un acte malveillant envers un dispositif informatique via un réseau cybernétique

- Cybercriminalité: les actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible..

- Cybersécurité : l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques connectés directement ou indirectement à un réseau des états et des organisations (avec un objectif de disponibilité, intégrité & authenticité, confidentialité, preuve & non-répudiation).

- Cyberespace : le cyberespace est l'environnement global de l'interconnexion des systèmes d'information et de communication. Le cyberespace est plus large que le monde informatique et contient également les réseaux informatiques, systèmes informatiques, medias et données numériques, qu'ils soient physiques ou virtuels.

- Dénis de services distribués (« DDoS » : un type d'attaque rendant un service inaccessible aux bénéficiaires habituels du service. Il s'agit d'ne technique perturbant fortement le fonctionnement normal du système par un grand nombre de requêtes.

- Hameçonnage : L'hameçonnage (appelés également «phishing») est une approche détournée utiliser pour vous pousser à révéler des informations personnelles, comme des mots de passe ou des numéros de carte de crédit, de sécurité sociale ou de compte bancaire..

- Incident cybernétique : un événement représentant réellement ou potentiellement une menace à un dispositif, un ordinateur ou un réseau connecté à Internet et / ou aux données traitées, stockées ou transmises sur ces données et qui peuvent demander une réponse afin de mitiger les conséquences.

- Ingénierie sociale : fait référence à des pratiques de manipulation psychologique à des fins d'escroquerie. Les pratiques de Ingénierie sociale exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles pour permettre d'obtenir

quelque chose de la personne ciblée (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.)

- Intégrité : L'intégrité d'un système est un principe selon lequel un système informatique est protégé contre les dysfonctionnements, les agressions et les attaque.

- Internet : le réseau informatique mondial accessible au public. C'est un réseau de réseaux, à commutation de paquets, sans centre névralgique, composé de millions de réseaux aussi bien publics que privés, universitaires, commerciaux et gouvernementaux, eux-mêmes regroupés en réseaux autonomes .

- l'Internet des objets : est une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

- Logiciel malveillant : tout type de logiciel essayant de nuire à un système informatique, sans le consentement de l'utilisateur. En effet, logiciel malveillant englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces

- Cybermenaces: tout ce qui est capable de compromettre la sécurité de, ou de provoquer des dommages aux dispositifs, ordinateurs, logiciels ou réseaux connectés à Internet, toutes les données qu'ils contiennent ainsi que les services qu'ils fournissent ou sous-tendent.

- Non-répudiation : signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message

- Ransomware: est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un ransomware chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Un ransomware peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent.

- Résilience : la capacité d'un système d'information à résister à une panne ou à une cyberattaque et à revenir à son état initial après l'incident

- Risques : sont les conséquences d'une atteinte aux données, sans atteinte au système d'information et/ou les conséquences d'une atteinte au système d'information.

- Vulnérabilité : une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient