STRATEGIE NATIONALE DE CYBERSECURITE

2019-2022

Relever le défi de la transformation digitale.

Table de matière

Liste des acronymes

4G	Quatrième génération des réseaux de télécommunication
APB	Association des Processionnels des Banques
API	Application Programming Interface
ARE	L'Autorité de Régulation
BCM	Banque Centrale de Mauritanie
BMCI	Banque Marocaine pour le commerce et l'industrie
BNM	Banque nationale Mauritanie
CEH	Certified Ethical Hacker
CERT	Computer Emergency Response Team
DAE	Direction de l'Administration Electronique
DDoS	Distributed Denial of Service
DGTIC	Direction Générale des Technologies de l'Information et de la Communication
DNS	Domain Name Service
DoS	Denial of Service
DIPVT	Direction des Infrastructures, de la Promotion et de la Veille Technologique
DSI	Directeur du Système d'Information
EMV	Europay Mastercard Visa
FIRST	Forum of Incident Response an Security Team
GCA	Global Cybersecurity Agenda
GIMTEL	Groupement Interbancaire de Monétique et des Transactions Electroniques
ICT/TIC	Technologies de l'Information et de la Communication
IP	Internet Protocol
IPV6	Internet Protocol version 6
IPS	Intrusion Prevention System
IT	Information Technology
IXP	Internet eXchange Point
NTP	Network Time Protocol
MDN	Ministère de la Défense Nationale
MESRSTIC	Ministre de l'Enseignement Supérieur, de la Recherche Scientifique et des Technologies de l'Information et de la Communication
MEN	Ministère de l'éducation nationale
MID	Ministre de l'Intérieur et de la Décentralisation
MJ	Ministère de la justice
OIC-CERT	Organization of Islamic Conference - Computer Emergency Response Team
PCI/DSS	The Payment Card Industry Data Security Standard
PME	Petites et Moyennes Entreprises
PMI	Petites et Moyennes Industries
PKI	Public Key Infrastructure
RIMCERT	RIM Computer Emergency Response Team
RSSI	Responsable de la Sécurité du Système d'Information
SEIM	Security Event and Information Management

SMS	Short Message System
SMSI	Système de Management de la Sécurité de l'Information
SPAM	Stupid Pointless Annoying Messages
TIC	Technologie de l'Information et de la Communication
UIT	Union Internationale des Télécommunications
WAF	Web Application Firewall
WARCIP	West Africa Regional Communications Infrastructure Project

1- Résumé exécutif

Le développement technologique en Mauritanie prend une avancée très importante et s'introduit considérablement dans tous les secteurs et toutes les formes de vie des citoyens, ce qui fait de la protection des infrastructures technologiques, des données de l'Etat, des entreprises et des citoyens un enjeu très important. Des efforts importants sont à fournir pour garantir la confiance numérique et pour accompagner cette transformation digitale que vit la Mauritanie.

C'est dans cette optique que l'Etat Mauritanien a décidé de tracer sa stratégie en cybersécurité et de se doter d'un plan d'action national pour atteindre les objectifs fixés.

Les objectifs qui ont été définis par cette nouvelle stratégie visent à sécuriser les infrastructures critiques de l'Etat et surtout les services électroniques en cours de développement, de doter les entreprises de moyens de protection, de promouvoir la cybersécurité, de développer les compétences, le cadre juridique et la sensibilisation des usagers.

Il s'agit d'une stratégie pour doter les différentes parties prenantes de moyens pour se protéger contre des menaces en évolution continue et qui risquent de mettre en cause tout le processus de développement. Ces menaces tournent essentiellement autour des éventuelles attaques qui touchent les institutions ou les infrastructures critiques de l'Etat, des attaques virales, des attaques portant atteinte aux données des citoyens sans oublier les fraudes bancaires.

Pour traiter ces menaces et atteindre les objectifs fixés, cinq axes de travail ont été définis ; tous les efforts de l'Etat et des différentes parties prenantes vont se concentrer sur ces orientations stratégiques jusqu'à l'année 2022. Ces axes couvrent la protection des systèmes d'information nationaux et gouvernementaux, la protection des infrastructures critiques, le développement des compétences, la sensibilisation, le développement du cadre juridique et réglementaire, le développement de partenariat public-privé au tour de la cybersécurité et la collaboration internationale.

Le document de la stratégie est un document vivant et évolutif. Chaque projet et action définie est muni d'indicateurs pour mesurer l'atteinte des objectifs à la performance des services et afin de pouvoir assurer un suivi et de redresser les orientations en cas d'insuffisance. Des révisions régulières de la stratégie sont également prévues selon un modèle défini ici.

La stratégie stipule aussi la création d'un modèle de gouvernance pour amorcer une dynamique multisectorielle et s'assurer de la bonne exécution des projets de cybersécurité. Ce modèle repose essentiellement sur la création d'une entité managériale de haut niveau qui a la charge de valider et adopter les plans d'action dans ce domaine, d'une agence nationale de cybersécurité et des équipes de traitement des urgences informatiques (CERT), sans oublier les autres entités opérationnelles qui sont impliquées implicitement dans tous les efforts de l'Etat.

2- Executive Summary

The technology development in Mauritania is taking a major step forward and is being introduced considerably in all sectors and all forms of life of citizens, which makes the protection of ICT infrastructures and all data belonging to the government, public and private companies and citizens a very important issue. Significant efforts are needed to ensure digital trust and to go along with this digital transformation in Mauritania.

With taking this into consideration that the Mauritanian State has decided to draw up its cybersecurity strategy and to adopt a national action plan to achieve the objectives set.

The objectives set out in this new strategy are aimed at securing the national critical infrastructures and especially the electronic services under development, providing enterprises with means of protection, promoting cybersecurity, developing skills, updating the legal framework and the promoting users awareness.

It is a strategy to equip different stakeholders with the means to protect themselves against continuously changing threats, which may jeopardize the entire development process. These threats turn mainly around possible attacks on critical institutions or infrastructures, malware attacks, attacks on citizens' data and banking fraud.

To address these threats and meet the set objectives, five lines of work have been defined; all the efforts of the government and the various stakeholders will concentrate on these strategic orientations until the year 2022. These axes cover the protection of national and government information systems, protection of critical infrastructures, awareness raising, the development of the legal and regulatory framework, the development of public-private partnerships in cybersecurity and international collaboration.

The strategy document is a living and evolving document. Each project and action defined is provided with performance indicators to measure the fulfilment of the objectives in order to be able to follow up and to correct the orientations in the event of insufficiency. Regular reviews of the strategy are also planned according to a model defined here.

The strategy also calls for the creation of a governance model to initiate a multi sectoral dynamic and ensure that cybersecurity projects are properly implemented. This model is essentially based on the creation of a high-level managerial body responsible for validating and adopting action plans, a national cybersecurity agency and computer emergency response team (CERT) , without forgetting the other operational entities that are implicitly involved in all the national efforts.

3- Contexte général

La Mauritanie connait un développement remarquable du secteur des TIC. L'Etat apporte son soutien au secteur privé pour assurer le développement des infrastructures et met l'accent sur de nouveaux axes de développement dans le domaine des technologies de l'information et de la communication. Ces technologies constituent actuellement un axe de développement focal et transversal pour accroitre la croissance des autres secteurs et le développement économique du pays.

Suite à la mise en œuvre, de la stratégie nationale de développement des TIC pour la période 2012-2016, des activités importantes ont étés réalisées. Les progrès se sont accélérés, la demande en débit a explosé avec les réseaux sociaux, et la généralisation des échanges de vidéo. Le numérique a envahi tous les domaines de la vie quotidienne à l'organisation des entreprises ou des administrations. L'internet des objets, le traitement massif des données issues des échanges numériques changent progressivement les modèles. Il faut que les Etats adaptent leur organisation et leur gouvernance pour tirer parti de ces développements au lieu d'en subir les conséquences.

Avec tout développement technologique et avec toute ouverture vers des moyens de communication diverses, les risques augmentent et exposent d'avantage les systèmes de l'Etat et des opérateurs économiques a des risques majeurs et aux tentations des malfaiteurs qui cherchent à profiter de ces nouveaux enjeux.

Conscient de ces risques, l'Etat mauritanien, a décidé d'élaborer sa stratégie pour assurer la sécurité de ses systèmes d'information, mettre en place des systèmes résiliant faces aux différentes menaces et prendre part aux initiatives mondiales de lutte contre la cybercriminalité. Ces dernières ont pour objectifs de doter tous les acteurs des moyens de protections et de disposer d'un socle solide pour le développement technologique et le renforcement de la confiance dans l'utilisation des nouveaux services.

Pour ce faire, l'Etat mauritanien, en partenariat avec l'Union Internationale des Télécommunications, entame l'élaboration d'une stratégie nationale de cybersécurité. L'UIT joue un rôle important dans l'assistance des pays, surtout africains, pour développer leur capacité en termes de cybersécurité et pour la mise en place de structures opérationnelles comme les CERTs.

La stratégie développée est basée sur une méthodologie qui prend en considérant l'étude de l'existant en termes de menaces, de développement technologique, de la structuration du cyberespace national, de la législation en vigueur, des expériences internationales et régionales et surtout de bonnes pratiques de l'UIT. L'étude de l'existant a pu dégager le niveau de maturité des entreprises, les pratiques de sécurité, le niveau d'expertise et le niveau de sensibilisation des usagers des nouvelles technologies.

4- Le cyberespace mauritanien

L'Internet a été introduit en Mauritanie en 1996, actuellement on compte 3 opérateurs télécoms qui sont: **Mauritel**, **Mattel** et **CHINGUITEL**. Le taux de pénétration mobile dépasse les 100%, et la pénétration du fixe est de 3%. Avec 712 465 connexions internet, le taux de couverture moyen est de 17.10%. Presque 40% de la population accède à Internet soit via le mobile ou les lignes Internet avec une bande passante internationale de 100 Gb/s, utilisée au tour de 30%. Le nombre de site web hébergé en Mauritanie est de l'ordre de 1500, mais, beaucoup de sites nationaux sont hébergés à l'étranger.

La Mauritanie vit une croissance économique importante, où les nouvelles technologies de l'information et de la communication constituent un socle pour ce développement. Ceci étant visible via les différents projets lancés dans différents secteurs :

- Le secteur des télécoms vit un développement de ses moyens technologiques, avec une forte pénétration, avec le lancement de nouveaux services et la préparation au passage à la 4G et à l'IPV6.
- Le secteur bancaire est aussi un acteur essentiel dans le développement technologique par le biais des différents services en ligne offerts aux citoyens, à travers la technologie et la forte connectivité (développement de l'e-Banking).
- Le gouvernement met l'accent sur les nouvelles technologies et investit massivement pour actualiser l'administration et se rapprocher d'avantage des citoyens ; ceci est visible via divers projets comme :
    - L'interconnexion des capitales régionales (projet WARCIP),
    - Le point d'échange internet (IXP),
    - La modernisation du gestionnaire du .mr et du DNS national,
    - Le projet de cloud privé de l'Etat,
    - L'étude pour la mise en place d'une autorité de certification,
    - Le projet e-gov et modernisation de l'administration,
    - Le projet d'open-data,
    - La modernisation du réseau du ministère de l'intérieur par l'interconnexion des wilayas, et la mise en place de nouveaux moyens de communication et d'échange,
    - Le projet e-santé (cybersanté),
    - Le projet e-éducation,
    - L'augmentation de la bande passante internationale,
    - Le projet de développement de l'e-Commerce,
    - Le lancement du projet de mise en place de nouvelles technopoles,
    - Le développement du secteur privé et des PPP,
    - Etc.

Ce développement considérable apporte plus de connectivité, plus de services et plus d'exposition à des risques cybernétiques. La volonté de l'Etat doit être accompagnée par des mesures de protection pour garantir la confiance numérique et assurer un développement plus efficace et plus rapide. Il serait important de considérer la cybersécurité comme l'un des piliers de la stratégie nationale de l'État et de dédier des lignes budgétaires pour la cybersécurité

La Direction Centrale du Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et des Technologies de l'Information et de la Communication (DGTIC) est un des principaux acteurs pour le développement des TIC en hébergeant le Datacenter du gouvernement avec la majorité des applications. Les principaux services offerts par la DGTIC sont : hébergement des sites et systèmes d'information, fourniture des outils de collaboration (messagerie, gestion électronique des documents), développement des sites web et des sites intranet, assistance à la maitrise d'ouvrage déléguée, élaboration des cahiers des charges, définition des normes et standards, support de deuxième niveau. Selon le décret organisant le ministère la Direction Générale des Technologies de l'Information et de la Communication a pour attributions :

- **Définir** et mettre en œuvre la stratégie nationale en matière d'administration électronique ou « e-gouvernement » ;
- **Assurer** la maîtrise d'ouvrage des projets informatiques de l'Administration à caractère transversal ainsi que la maîtrise d'ouvrage déléguée des projets à caractère sectoriel ;

- **Mener** et promouvoir, en coordination avec les administrations concernées, les actions permettant à l'Administration de se doter d'un dispositif cohérent de traitement et de diffusion de l'information répondant aux normes internationales en matière de qualité, de sécurité, de performance et de disponibilité ;
- **Évaluer** les besoins dû en matière de réseaux, d'équipement et d'application de technologies de l'information et de la communication ;
- **Élaborer** les normes et les standards nationaux dans le domaine des technologies de l'information et de la communication ;
- **Définir** le cadre juridique des technologies de l'information et de la communication.

Le développement d'une stratégie de cybersécurité, nécessite l'implication d'un certain nombre d'acteurs qui joueront un rôle essentiel dans l'élaboration de la stratégie et dans sa mise en œuvre.

Les principales parties prenantes ayant un rôle important dans le développement de la cybersécurité sont :

• **Parlement**
• **Premier ministère**
• **Ministre de l'Enseignement Supérieur, de la Recherche Scientifique et des technologies de l'information et de la communication (MESRSTIC)**
• **Ministre de l'Intérieur et de la décentralisation (MID)**
• **Direction Générale des Technologies de l'Information et de la Communication (DGTIC)**
• **RIM Computer Emergency Response Team (RIMCERT)**
• **Ministère de l'éducation nationale (MEN)**
• **Banque Centrale de Mauritanie (BCM)**
• **Ministère du Pétrole, de l'énergie et des Mines (MPEMs) et grand pôle industriel étatique**
• **Ministère de la défense nationale (MDN)**
• **Ministère de la justice (MJ)**
• **Les opérateurs de télécommunication**
• **Les associations du domaine des TIC**
• **Association des professionnels des banques (APB)**
• **Ministère de l'économie et des finances**
• **L'Autorité de régulation (ARE)**
• **Ministère de santé**
• **Secteur privé**
• **Le Groupement Interbancaire de Monétique et des Transactions Electroniques (GIMTEL)**
• **Ministère des affaires étrangères et de la Coopération**

5- Etude des menaces

Le cyberespace mauritanien fait face à des menaces importantes pouvant mettre en péril l'intégrité des systèmes et peuvent aussi mettre en cause la confiance numérique. L'étude des menaces a pu dégager les principaux facteurs suivants :

- **Attaques sur les sites web institutionnels**, qui constituent une préoccupation majeure vu l'ampleur de ce phénomène et vu l'existence d'une menace locale surtout de la part des groupes de hacking mauritanien qui ne cesse de chercher des failles pour attaquer ces sites. D'autres parts, la difficulté de sécuriser ces applications rend leur degré de vulnérabilité assez

élevé. Ces sites web s'apprêtent à développer des services en ligne transactionnels ce qui les rend plus importants à être protégés.

- **Malwares**, qui sont un fléau classique et qui touche tous les systèmes généralement connectés à Internet. L'absence de mesure de protection rudimentaire expose directement les systèmes, et parfois même avec la présence d'une protection antivirale les infections peuvent avoir lieu. Ces informations sont aussi causées par une imprudence des usagers et l'absence d'une conscience sur les risques.
- **Attaques contre les systèmes d'information des infrastructures critiques**, il s'agit d'une menace qui pose un risque important surtout avec le développement que connait la majorité des secteurs critiques, avec plus d'inter-connectivité et d'ouverture. Attaquer une infrastructure critique peut impacter l'économie ou même les installations physiques, et critiques.
- **Attaques aux systèmes d'information des deux secteurs public et privé,** qui sont généralement exposés et ne disposant pas d'un niveau de sécurité adéquat, ce qui les rend très vulnérables et sujets d'incidents.
- **Menaces en relation avec les nouveaux moyens de communication** (messagerie IP, sites de médias sociaux, …) qui ont remplacé les moyens traditionnels mais apportant plus d'exposition des données sensibles contre des attaques d'interception et de divulgation. Ces nouveaux médias exposent également les données privées des usages qui font face à leur tour à des risques de vol d'identité ou d'information personnelle.

⇨ D'autres menaces viennent en second lieu :

- **Manque d'experts et de compétences en cybersécurité**, il s'agit d'une menace exprimée par plusieurs parties prenantes vu l'absence de cabinet ou de professionnel pour les aider et les conseiller et vu aussi l'absence de spécialiste dans les entreprises. Face à ce manque les entreprises seront incapables de faire face aux différents défis de sécurisation des systèmes d'information. Ce manque est du généralement à l'absence de formation académique et la rareté de l'offre de formation professionnelle sur le marché local.
- **Phénomène de SPAM**, qui sont aussi un fléau international touchant toutes les entreprises et qui constitue presque 50% des emails échangés en Mauritanie. Les SPAM posent un problème pour les fournisseurs de service email en saturant les espaces de stockage et en consommant massivement les bandes passantes. Les SPAM permettent aussi la circulation des malwares et de certaines attaques d'ingénierie sociale. D'autre part, la circulation massive des spam peut être due à la présence d'un nombre important de machines infectées, ceci risque aussi de faire atteinte à la réputation des IPs mauritanienne et de les avoir blacklistées dans d'autres pays. Les SAPM doivent disposer d'un traitement spécial sur le plan technique et légal.
- **Atteinte aux Données privées des citoyens**, qui est considérée comme menace importante vu qu'elle peut impacter des données sensibles et vu qu'elle risque de mettre en cause la confiance des utilisateurs dans les nouvelles technologies. Certaines attaques de ce type ont été réalisées et qui ont eu un impact assez fatal. Ce genre de menace est généralement dû à la présence de système de traitement de données vulnérables et exposées sur Internet, sans oublier les fuites de données qui peuvent être perpétuées par des personnes internes à l'entreprise.

⇨ D'autres menaces moins importantes mais à considérer :

- **Croissance des Botnets**, il s'agit d'un type d'infection qui permet de transformer les machines en robot d'attaques. Les bots peuvent être utilisé pour envoyer des spam, voler des données, ou lancer des attaques DDoS ce qui risque de consommer inutilement la bande passante nationale et internationale voire même les saturer. La présence de botnet est généralement causée par l'absence de moyen de protection antivirale.
- **Violation des cartes de crédit**, un risque majeur pour les banques et pour les différents moyens de paiement, malgré que la majorité des cas observés est en relation avec des fraudes contre

des cartes étrangères. Toutefois, la présence de ces pratiques pose un risque sur les moyens de paiement mauritaniens.

- **Cyber terrorisme**, même si ce phénomène n'est pas très développé, il peut être considéré comme étant une menace importante vu les moyens offerts par les nouvelles technologies aux groupes de terroristes.

6- Les besoins en terme de sécurité de l'information

Les différentes entreprises ont des besoins spécifiques par rapport à la stratégie, qui sera un cadre qui va les aider à bien cadrer leur projet et de les aider à trouver les ressources nécessaires. Parmi les besoin à développer on peut citer :

- **Développer les compétences et ce en impliquant l'université pour créer des cursus académiques spécialisés en sécurité ou d'ajouter la composante sécurité dans les cursus actuels,**
- **Développer l'offre de formations professionnelles en poussant les bureaux de formation pour développer plus de modules de formations et avec l'implication de l'Etat pour faire des incitations et pour subventionner. Les formations doivent cibler les responsables des entreprises et aussi les consultants du secteur privé.**
- **Développer l'usage de l'open source comme une alternative aux solutions commerciales assez couteuses. Ceci va nécessiter l'implication de l'Etat pour pousser les entreprises du secteur privé à développer une offre pour l'installation, la maintenance et la formation et aussi par le développement de programme de sensibilisation et d'incitation sur l'usage de l'open source.**
- **Développer le cadre légal pour permettre aux entreprises et aux citoyens de disposer de moyens pour se protéger contre les cybercrimes, les arnaques et les fraudes. Ceci va nécessiter la mise à niveau du cadre légal et la formation des juristes et les autorités de force publique.**
- **Développer la coordination entre les différents intervenants nationaux et avec les entités internationales par la mise en place de moyens de partage et d'échange et par la mise en place d'un cadre de confiance.**
- **L'implication des hauts responsables afin qu'ils soient sensibilisés sur la question de la sécurité et qu'ils soient impliqués, ceci garantira le succès de la stratégie.**
- **Disposer d'un modèle de gouvernance simple basé sur le renforcement des structures actuelle comme la DGTIC et penser à créer à long terme une nouvelle entité spécialisée en cybersécurité.**
- **Développer la sensibilisation chez les citoyens et les employés en développant un programme national impliquant les acteurs qui peuvent aider comme les médias et les associations.**
- **Inciter les entreprises à développer leur niveau de sécurité et ce en développant un référentiel qui décrit le niveau de sécurité minimal et en mettant en place un moyen pour contrôles l'application de ces mesures.**
- **Lancer une structure de veille pour informer et alerter les entreprises en cas de menaces.**
- **Définir la politique de sécurité décrivant les règles à appliquer pour protéger le patrimoine informationnel et la mise en place de structure de suivi et d'audit.**
- **Etablir le CIRT national qui va servir comme de point de contact de confiance et de coordination centrale pour la cybersécurité visant à identifier, défendre, répondre et gérer les menaces cybernétiques.**

7- Les Opportunités apportées par la stratégie

La stratégie apporte plusieurs opportunités de développer touchant plusieurs axes, parmi ces opportunités on peut citer :

1. **Promouvoir la société numérique, en considérant que le développement de la cybersécurité aiderait à booster le développement de la société numérique, assurer la confiance numérique et encouragera d'avantage les différents opérateurs à y investir.**
2. **Promouvoir l'inclusion financière numérique, le commerce électronique et le commerce en général, en considérant que le commerce électronique est une base fondamentale pour le développement économique en Mauritanie. Le développement de la sécurité encouragera les investisseurs dans ce domaine et donnera plus de garantit par rapport à la sécurité des différentes transactions en ligne. On parle aujourd'hui de toute une économie numérique basée sur les services en ligne et sur des moyens de communication sophistiqués.**
3. **Promouvoir l'administration électronique, ceci est un élément essentiel pour le développement technologique en Mauritanie. Certes, la sécurité est un élément essentiel pour le développement de ces services afin de garantir une meilleure stabilité des systèmes et une résistance aux attaques, surtout que les services administratifs en ligne sont très souvent sujets d'attaques. Le développement de la cybersécurité assurera certainement le développement des services de l'e-administration.**
4. **Promouvoir l'e-banking, surtout que toutes les banques sont en train de développer de nouveau service de consultant et préparer pour les services transactionnels. En absence de mesure de sécurité, les services transactionnels risquent de faire face à des fraudes ce qui met en cause la confiance et la pérennité des systèmes. La cybersécurité chez le secteur bancaire devra être développé pour promouvoir les services bancaires en ligne.**
5. **Protéger l'information et l'infrastructure de l'information dans le cyberespace, certainement la stratégie sera une opportunité pour évaluer les pratiques de protection et de proposer des approches de protection des informations et des systèmes d'information. La stratégie met en œuvre les dispositifs nécessaires pour renforcer les capacités des différents secteurs pour prévenir et répondre aux menaces cybernétiques.**
6. **Construire un cyberespace sécurisé et résilient pour les citoyens, les entreprises et le gouvernement en réduire le degré de vulnérabilités et en minimisant les dégâts qui peuvent être causés par les incidents cybernétiques.**

8- Les objectifs de la stratégie

Certains objectifs à atteindre ont été fixé au niveau de cette stratégie, tous les axes et le plan d'action ont été conçus pour concrétiser ces objectifs durant la période spécifiée:

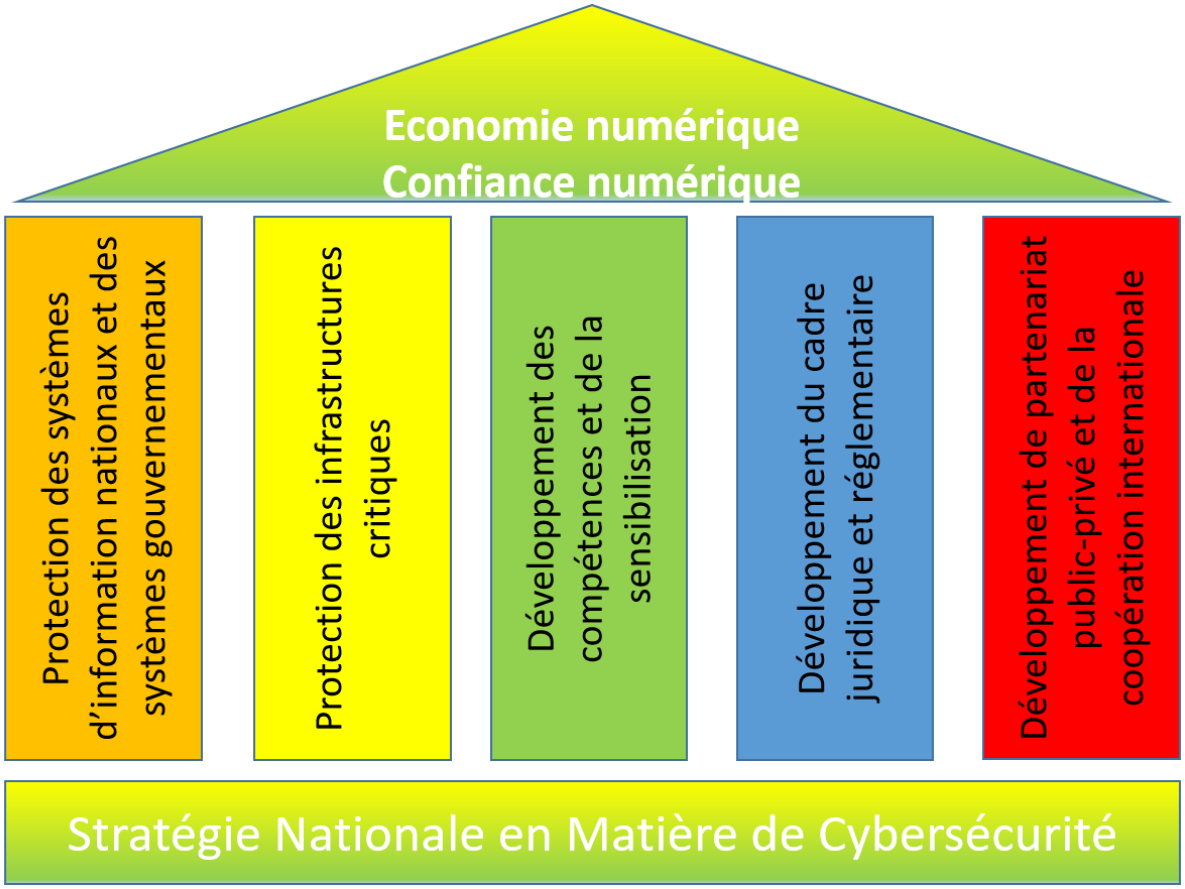
Les objectifs de la stratégie sont :

1. **Sécuriser les infrastructures TIC critiques de l'Etat et privé et les tendre résistantes aux menaces, surtout pour les services de l'e-gouvernement, de l'administration électronique,**
2. **Protéger les PME en les dotant des moyens de protection adéquats,**
3. **Développer les compétences,**
4. **Renforcer le cadre juridique et de lutte contre la cybercriminalité,**
5. **Renforcer la sécurité des infrastructures vitales nationales et garantir la disponibilité, la fiabilité et la confidentialité des échanges de données dans le cyberespace**
6. **Développer la collaboration entre les partie-prenantes pour sécuriser les systèmes d'information**
7. **Promouvoir la qualité des services de télécommunication et de l'IT**
8. **Combattre les cybercrimes et développer les capacités du pays pour répondre aux incidents majeurs.**

9- Les axes stratégiques

Pour ’atteindre les objectifs et développer les opportunités, la stratégie devra se baser sur des axes de travail qui ont été discuté et analysé avec les différentes parties prenantes. Pour cela, cinq axes ont été considérés :

1. **Protection des systèmes d’information nationaux et des systèmes gouvernementaux.**
2. **Protection des infrastructures critiques.**
3. **Développement des compétences et de la sensibilisation.**
4. **Développement du cadre juridique et réglementaire.**
5. **Développement de partenariat public-privé et de la coopération internationale.**



Pour développer les opportunités considérées et pour atteindre les objectifs tout en considérants les menaces et les spécificités de l’environnement en Mauritanie, les axes stratégiques vont permettre de développer le programme de cybersécurité.

Il est a noté que les axes stratégique identifiés vont couvrir les objectifs définis :

Axe stratégique	Objectifs à atteindre
1. Protection des systèmes d’information nationaux et des systèmes gouvernementaux.	• Sécuriser les infrastructures TIC critiques de l’Etat et privé et les rendre résistantes aux menaces, surtout pour les services de l’e-gouvernement, de l'administration électronique, • Protéger les PME en les dotant des moyens de protection adéquats

	• Promouvoir la qualité des services de télécommunication et de l'IT
2. Protection des infrastructures critiques.	• Sécuriser les infrastructures TIC critiques de l'Etat et privé et les tendre résistantes aux menaces, surtout pour les services de l'e-gouvernement, de l'administration électronique. • Renforcer la sécurité des infrastructures vitales nationales et garantir la disponibilité, la fiabilité et la confidentialité des échanges de données dans le cyberespace. • Promouvoir la qualité des services de télécommunication et de l'IT.
3.Développement des compétences et de la sensibilisation.	• Développer les compétences. • Protéger les PME en les dotant des moyens de protection adéquats.
4.Développement du cadre juridique et réglementaire.	• Renforcer le cadre juridique et de lutte contre la cybercriminalité. • Combattre les cyber-crimes et développer les capacités du pays pour répondre aux incidents majeurs.
5.Développement de partenariat public-privé et de la coopération internationale.	• Développer la collaboration entre les partie-prenantes pour sécuriser les systèmes d'information. • Intégrer la Mauritanie dans les initiatives internationales dans le domaine de la cyber sécurité.

Protection des systèmes d'information nationaux et des systèmes gouvernementaux

Il s'agit de mettre en place les dispositifs organisationnels et techniques pour mettre à niveau les systèmes d'information nationaux et ceux du gouvernement :

- **Etablir une classification des entreprises publiques selon leur criticité et selon la criticité de leurs systèmes d'information,**
- **Développer un référentiel de sécurité pour indiquer aux entreprises le niveau de sécurité minimal auquel ils doivent se conformer, tout en instaurant un mécanisme d'audit de conformité, ce référentiel devra être appliqué sur les entreprises publiques et les entreprises privées sensibles selon la classification en vigueur (Axe Protection des Infrastructures Critiques).**
- **Instaurer un mécanisme d'audit périodique et obligatoire pour vérifier la conformité des entreprises par rapport au référentiel de sécurité. Cet audit doit viser à mettre en place, au niveau des établissements et des entreprises, un processus interne d'identification, de traitement et de suivi des risques auxquels est exposée l'information relevant de leur autorité. Un tel processus doit être officialisé et prendre appui sur la connaissance des différentes menaces et de leur impact potentiel sur l'organisation,**
- **Inciter les entreprises à déployer des solutions de protection open source, tout en poussant le secteur privé à assurer le service nécessaire pour assister les entreprises dans leur projet,**
- **Organiser, au moins annuellement, un séminaire de sensibilisation des organismes publics, sur la cybersécurité afin de prendre en compte au quotidien la sécurité informatique par les employés de l'État. Ces derniers, en tant que principal maillon de la chaîne de protection, doivent être conscients des risques de sécurité de l'information auxquels ils sont exposés et s'approprier les meilleures façons de se prémunir contre eux,**
- **Développer et publier des guides pour assister les entreprises publiques et privées à appliquer les bonnes pratiques de sécurité,**
- **Désigner des responsables de sécurité de systèmes d'information dans toutes les entreprises et qui auront pour rôle de gérer tous les projets de sécurité et de veiller à l'application de toutes les obligations,**
- **Développement de mécanisme de sécurisation des échanges électroniques à l'instar du SMS Banking et payement mobile. Ces mécanismes doivent se baser sur une analyse des risques, de développement de guide de bonne pratique et d'assistance pour la mise en œuvre des technologies de protection,**
- **Mettre en place une équipe commune d'experts issue des différents ministères pour le suivi des grands projets technologiques et pour s'assurer de la prise en considération des règles de sécurité adéquates,**
- **Mise en place d'une autorité de certification électronique pour la sécurisation des échanges en lignes, pour fournir des services d'identification, d'authentification et de signature électronique pour les entreprises et les citoyens et pour implémenter le projet d'identifiant unique.**
- **Assister les établissements bancaires pour se doter de la certification PCI/DSS,**

- **Veiller à la mise en place de moyens de protection adéquats pour la protection des données à caractère privé (Autorité de Protection des Données à Caractère Personnel, Guide de Bonne Conduite, Guide technique, Processus de déclaration et de contrôle),**
- **Renforcer les capacités nationales de réponse aux incidents et développement de la coordination et du partage de l'information et ce par :**
    - **La mise en place du CERT national : RIMCERT pour assurer les services de traitement d'incident, de veille, de supervision, etc.**
    - **Mise en place d'un plan de coordinations nationale et international pour la lutte contre les cyber-attaques,**
    - **Renforcement des capacités du ministère de l'intérieur et de la défense pour la lutte contre les cyber-attaques,**
    - **Mettre en place une entité de coordination, de collecte et de partage de données au sein du secteur bancaire.**
- **Mettre en place une PKI nationale pour la protection des échanges en ligne, pour la protection des documents électroniques et les différents services.**

Protection des infrastructures critiques

Il s'agit de mettre en place les dispositifs organisationnels et techniques pour assurer la sécurité des systèmes d'information appartenant aux infrastructures critiques afin d'accompagner leur développement technologique :

- **Réaliser un inventaire et une classification des infrastructures critiques publiques et privées incluant les opérateurs de systèmes industriels et énergétiques vitaux, les banques, les opérateurs télécom, etc.**
- **Développer un référentiel de protections spécifiques à chaque catégorie,**
- **Mettre en place un Framework de suivi et d'analyse des risques, basé sur des audits périodiques pour vérifier la conformité des entreprises critiques par rapports aux dispositions du référentiel de protection,**
- **Déployer les moyens de protection adéquats en fonction des risques encourus,**
- **Organiser des workshops, des formations et des opérations blanches,**
- **Mettre en place une plateforme d'échange et de partage entre les opérateurs critiques pour échanger les informations relatives aux cyber-menaces et préparer les plans de réponses adéquats,**
- **Sécurisation de l'infrastructure DNS national, pour garantir sa disponibilité et résilience avec la mise en œuvre des bonnes pratiques comme le DNSsec.**
- **Sécurisation du point d'échange Internet (IXP) considéré comme étant un point névralgique pour l'Internet Mauritanie et aussi pour les télécommunications.**
- **Programmer la migration vers le protocole IPV6 afin de profiter de la meilleure sécurité est le gros avantage de ce protocole. Contrairement à son prédécesseur, le nouveau protocole incorpore les technologies universelles de cryptage end- to-end et de vérification de l'intégrité utilisé par les VPN. Il a également des capacités de sécurisation qui rendent plus difficiles les attaques du type man-in-the-middle. IPv6 va certes renforcer la sécurité des réseaux des agences gouvernementales, mais il faut au préalable prendre**

une décision concernant son adoption et définir la stratégie de transition du protocole IPv4 à celui IPv6.

- **Développement de moyens de lutte contre les SPAM considérés comme un fléau perturbateur, et en en dotant les opérateurs et fournisseurs d'outils de filtrage, en adaptant le cadre légal de lutte contre les SPAM et surtout le développement de la coordination entre les opérateurs nationaux et les opérateurs internationaux.**

Développement des compétences et de la sensibilisation

La cybersécurité est un domaine d'expertise qui nécessite d'avoir des spécialistes bien formés capables de réponde aux besoins des entreprises. L'expertise est nécessaire pour travailler au sein des entreprises comme elle est nécessaire pour les prestataires de services pour assurer diverses prestations comme les audits, les tests intrusifs, les investigations sur incident, le développement sécurisé d'application, la mise en place du système de management de la sécurité, le développement de politique et des procédures, le développement de plan de continuité d'activité, la sensibilisation, la formation, etc. Pour ce, la stratégie dédie tout un axe pour le développement des compétences qui va veiller à :

- **Lancement d'un diplôme spécialisé en sécurité des systèmes d'information mastère spécialisé au niveau de l'université et un diplôme d'ingénieur informaticien spécialise en cybersécurité,**
- **Intégration de cours de sécurité au niveau des formations d'informaticiens,**
- **Créer un cursus de formation pour les responsables de la sécurité des entreprises citriques et ceux du gouvernement,**
- **Allocation de fond pour subventionner des formations de formateurs en cybersécurité, conformément aux dispositions de la loi sur la société de l'information,**
- **Inciter les sociétés de prestation de service à former leurs consultants et à développer leur offre de sécurité tout en visant les certifications internationales,**
- **Inciter les laboratoires de recherche en IT à développer des thématiques au tour de la cybersécurité,**

⇨ **Sur le volet de sensibilisation :**

- **Développer un programme national de sensibilisation en impliquant tous les acteurs potentiels et couvrant le maximum de publics cibles,**
- **Etablissement de partenariats avec les associations de la société civiles travaillant sur les TIC, les former et leur fournir du contenue afin d'organiser des compagnes de sensibilisation d'une manière autonome ou conjointement avec le RIMCERT,**
- **Lancement d'émission radio/télé pour la sensibilisation du grand public,**
- **Organisation d'un workshop de sensibilisation pour les hauts décideurs,**
- **Développement de contenu de sensibilisation,**
- **Promouvoir les évènements sur la cybersécurité,**
- **Lancement d'un groupe de travail sur la protection des enfants en ligne (Online Child Protection) en collaboration avec l'Union International des Télécommunications et les instances en charge de la protection de l'enfance.**
- **Lancement d'un forum national sur la sensibilisation.**

Développement du cadre juridique et réglementaire

Le cadre légal actuelle est déjà assez riche, d'autres textes important sont en cours d'adoption et des conventions internationales ont été déjà ratifiées. Cet axe principal veillera à :

- **L'information de tous les intervenants et même le grand public sur l'arsenal juridique en relation avec la cybersécurité,**
- **Mise en place des structures de suivi pour ces nouvelles lois : cybercriminalité, protection des données personnelles, sécurité des transactions électroniques, etc.**
- **Formation des juristes sur les nouvelles technologies, sur les aspects techniques des lois, et sur les nouvelles procédures judiciaires,**
- **Mettre en place un centre d'investigation et de criminologie,**
- **Ratifier la convention de l'Union Africaine sur la cyber-sécurité et la protection des données à caractère personnel**
- **Intégrer la convention de Budapest sur la cybercriminalité**
- **Veiller à l'application des engagements de l'Etat issue des ratifications de conventions et veiller à l'application des dispositions de ces conventions.**
- **Elaborer les différents décrets d'application du Cadre juridique de la Société Mauritanienne de l'Information et en particulier, ceux en relation avec les lois sur la cybercriminalité, la protection des données à caractère personnelles et les transactions électroniques.**
- **Etablir un cadre de coopération et d'échange entre les instances techniques (RIMCERT, DGTIIC, etc.) et les autorités de force publique, tout en développant des relations étroites,**
- **Développer les relations de coopération avec les entités internationales de lutte contre la cybercriminalité, et surtout l'interpole,**
- **Développer une nouvelle règlementation pour instaurer l'audit obligatoire pour les entreprises publiques et pour les infrastructures critiques tout en considérant les référentiels de sécurité,**
- **Développer une nouvelle règlementation pour instaurer l'obligation de déclaration des incidents critiques,**
- **Mettre en place les dispositifs nécessaires pour l'écoute légale surtout pour les nouvelles technologies comme la voix sur IP (Il faut une cadre légal : Lawfull Interception (qui peut accompagner la loi de lutte contre la cybercriminalité ou sous forme d'une loi à part, Il faut disposer de solutions techniques à déployer chez les opérateurs, il est possible d'imposer ces solutions pour les opérateurs en donnant l'accès à leur réseau téléphonique et Data, mais il faudra disposer de solution technique pour faire les recherches. Ceci est un besoin pour le Ministère de l'Intérieur et de la Décentralisation et aussi le Ministère de la Défense, donc il est possible de disposer d'une unité technique indépendante des deux ministères qui agira comme un centre d'expertise).**
- **On peut également le joindre au projet de centre d'investigation.**
- **Elaborer une directive sur la sécurité de l'information gouvernementale. En énonçant des obligations de haut niveau à l'égard des organismes publics, cette directive renforcera**

l'encadrement de la sécurité de l'information gouvernementale, contribuant ainsi à l'atteinte des cibles fixées dans le cadre de l'approche stratégique. Elle contribuera également à l'instauration d'une gestion optimale du risque d'atteinte à l'information gouvernementale et à l'accroissement de la confiance des citoyens et des entreprises quant à la sécurité de l'information qu'ils confient à l'État.

- **Mise en place d'un cadre gouvernemental de gestion de la sécurité de l'information. Celui-ci sert de complément aux dispositions de la nouvelle directive, en précisant l'organisation fonctionnelle de la sécurité de l'information au sein de l'appareil gouvernemental ainsi que les rôles et responsabilités en la matière. Il sert également à définir et à préciser les mandats de divers comités et tables de concertation soutenant les travaux gouvernementaux en matière de sécurité de l'information.**
- **Mise en place d'un cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information. Ce cadre présente une approche novatrice de gestion des risques et des incidents susceptibles de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peuvent avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux en matière de la protection des renseignements personnels qui les concernent et de respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.**

Développement de partenariat public-privé et de la coopération internationale
La collaboration entre le secteur public et privé est essentielle pour faire face aux menaces et pour mettre à niveau la sécurité du cyberespace. Cet axe donnera plus de priorité à ce vol et veillera à : - **Développer un cadre de partenariat entre les structures de sécurité et les opérateurs télécom pour la lutte contre les cyber-attaques,** - **Développer un cadre de partenariat entre les structures de sécurité et le secteur bancaire pour la lutte contre les fraudes et les attaques,** - **Développer des partenariats avec les éditeurs technologiques pour développer une offre de sécurité adaptée au contexte national,** - **Développer un partenariat avec le secteur privé pour l'assister à développer son offre de sécurité,** - **Développer un partenariat avec les associations des TIC pour le développement du programme national de sensibilisation,** - **Faire adhérer le RIMCERT aux réseaux internationaux de collaboration pour le traitement des incidents comme le FIRST, OIC-CERT, AfricaCERT, etc.** - **Adhérer à l'initiative et aux efforts de l'Union Internationale des Télécommunication pour la protection des enfants en ligne,** - **Rejoindre le réseau des autorités de certification électroniques afro-africaines (the Arab-African e-Certification Authorities Network),** - **Etudier et adhérer activement dans les initiatives régionales et internationales pour le développement des bonnes pratiques de sécurité, des standards et des conventions, en faisant part des groupes de travails et en étudiant et adoptant les recommandations. A l'instar de : FIRST, OIC-CERT, AfricaCERT, ITU-COP, ITU-GCA, convention de Budapest sur la cybercriminalité, convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel, cadre juridique pour l'harmonisation du carde légale et réglementaire du secteur des TIC dans les pays de l'Union du Maghreb Arabe, Convention de la Commission Européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, OIF, etc.**

10-Modèle de gouvernance

La stratégie propose généralement un modèle de gouvernance en vue d'assurer sa bonne gestion et pour permettre à tous les plans d'action qui vont en découler d'atteindre leurs objectifs.

Il s'agit d'un modèle adapté au contexte mauritanien en tenant compte du rôle joué par la DGTIC en tant que point focal et pionnière dans le domaine de la cybersécurité. Vu son emplacement, la DGTIC peut jouer le rôle de coordinateur entre les différents intervenants et ce en l'appuyant par l'implication directe de toutes les parties prenantes. La DGTIC constitue, à travers ce modèle, le responsable de la mise en œuvre de la Stratégie pour le MESRSTIC.

Le modèle de gouvernance proposé, est inspiré aussi des différentes expériences similaires comme celles de la France et de la Tunisie et aussi des bonnes pratiques en voguer essentiellement celles de l'UIT. Le modèle de gouvernance vise à définir les rôles et les responsabilités de chaque entité et de définir les interactions entre elles.

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

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

- La définition des objectifs annuels,
- La mise à jour de la stratégie,
- La mise en œuvre de la stratégie,
- Le contrôle et la mesure de performance,
- L'amélioration continue.

L'adoption de la Bonne Gouvernance comme principe de base de gestion de la stratégie nationale en matière de cybersécurité permet :

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

Idéalement le modèle de gouvernance doit être constitué de quatre entités principales :

- L'entité managériale ;
- L'entité de suivi ;
- L'entité de contrôle, de surveillance et d'analyse des performances ;
- Les entités opérationnelles.

Entité managériale	Description : Il s'agit de l'entité de plus haut niveau qui devra disposer de l'autorité, du leadership et affirmer son engagement en faveur de la cybersécurité pour : • S'assurer que la stratégie de la cybersécurité est bien établie et qu'elle est cohérente avec les orientations stratégiques du pays;

	• S'assurer que les ressources nécessaires (humaine et financière) pour mettre en œuvre la stratégie et la politique générale sont disponibles ; • Communiquer sur l'importance de la stratégie de cybersécurité et son apport pour la politique générale du pays ; • S'assurer que la stratégie de cybersécurité produit les résultats escomptés; • Orienter et soutenir les responsables des différents projets, qui font partie du plan d'action, pour qu'ils contribuent efficacement à la mise en œuvre de la stratégie ; • Encourager l'investissement dans la cybersécurité ; • Pousser les différentes parties prenantes à travailler et collaborer ensemble ; • Disposer de l'appui politique pour la mise en œuvre de la politique ; • Assurer l'amélioration continue de la stratégie grâce à la revue périodique.
	Composition: **Scénario-1 :** - Comité interministériel présidé par le Premier Ministre et incluant : o Le Ministre de la Justice, o Le Ministre de la Défense, o Le Ministre de l'Intérieur et de la décentralisation, o Le Ministre de l'Economie et des Finances, o Le Président de l'Autorité de Régulation (ARE), **Scénario-2 :** - DGTIC représentée par son directeur général en tant que président de cette entité, - Des représentants des ministères : o Ministère de la Défense, o Ministère de l'Intérieur et de la décentralisation, o Ministère de la Justice, o Ministère de l'économie et des finances, - Un représentant de l'Autorité de Régulation (ARE), - Un représentant du secteur privé personnifiant les opérateurs télécom et les fournisseurs de service.
L'entité de suivi	Description : Une entité désignée en tant que représentant de l'entité managériale, avec l'autorité et les responsabilités nécessaires pour s'assurer que les actions qui découlent de la stratégie sont effectivement établies, mises en œuvre et maintenues. Ce comité remonte des rapports au comité managérial et il a comme rôle de: • Définir et faire valider par le comité managérial la stratégie du cybersécurité ; • Maintenir la stratégie du cybersécurité ; • Elaborer et maintenir le plan d'action relatif à la stratégie du cybersécurité ; • Garantir l'obtention des résultats escomptés ; • Empêcher ou limiter les résultats indésirables ; • Elaborer le rapport annuel de la cybersécurité ;

	• Analyser les risques et les nouvelles tendances ;
	• Assurer une mise à jour annuelle de l'évaluation du risque ;
	• Assurer le suivi de tous les indicateurs de performance ;
	• Jouer le rôle de centre de Coordination entre les différents intervenants ;
	• Jouer le rôle de hub d'information en cas d'attaque massive ;
	• Reporter au comité de managérial :
	  ○ les performances de la stratégie ;
	  ○ L'état d'avancement des actions décidées ;
	  ○ Les modifications des enjeux externes et internes pertinents pour la cybersécurité ;
	  ○ Les retours d'information des parties intéressées ;
	  ○ Les opportunités d'amélioration continuent ;
	  ○ Les nouvelles tendances en matière de risque et de technologies ;
	• Assurer la veille réglementaire, méthodologique et technique afin d'adapter en permanence la stratégie de la cybersécurité aux différentes évolutions ;
	Réaliser les opérations de communication et de sensibilisation pour toutes les parties prenantes.

	<u>Composition:</u> Cette entité est représentée par la DGTIC et le RIMCERT en faisant appel à tout spécialise qui peut apporter de l'aide au travail de l'entité. Elle doit inclure des représentants de : • Ministère de la Défense, • Ministère de l'Intérieur et de la décentralisation, • Ministère de la Justice, • Ministère de l'économie et des finances, • Autorité de Régulation (ARE), • Les opérateurs télécom et les fournisseurs de service.
Les entités opérationnelles	Cette entité est constituée des responsables des projets et des actions découleront de la stratégie nationale en matière de cybersécurité. Il s'agit en fait des entités opérationnelles publiques et privées qui seront chargées d'exécuter un ou plusieurs volets de la stratégie. Chaque entité opérationnelle reporte au comité de suivi et sera responsable de : • Accomplir les actions dont elle est responsable convenablement ; • Informer le comité de suivi sur les mesures de performance montrant le bon fonctionnement des actions ; • Mentionner au comité de suivi les nouvelles tendances des menaces dans le périmètre dont elle est responsable ; • Faciliter le travail de l'entité d'audit pour accomplir sa mission d'audit annuel ; • Proposer des actions d'amélioration ; • Suivre les actions correctives qui lui sont associées ; • S'assurer que toutes les structures, sous sa responsabilité, sont conscientes et comprennent bien la stratégie ainsi que son apport. S'assurer que toutes les mises à jour et que toutes les révisions des objectifs de la stratégie sont réalisées ;

	S'inspirer de ce modèle de gouvernance et l'appliquer particulièrement pour la gestion des grands projets dans le but de vérifier que les actions soient effectuées convenablement.
	<u>Composition:</u> Liste des entités opérationnelles : - Le CERT, - L'entité de cybercriminalité au niveau du ministère de l'intérieur, - L'entité de cyberdéfense (ministère de défense), - Les infrastructures critiques, - Toute entité qui sera désignée ou créée par le comité stratégique pour appliquer une partie du plan d'action.

I. Agence Nationale de la cybersécurité

Afin d'assurer une meilleure gouvernance et de s'assurer que les objectifs de la stratégie seront atteints, il est important de créer une agence spécialisée dans la sécurité des systèmes d'information pour agir comme un point focal, pour la coordination et pour agir comme une entité de suivi. Au départ la DGTIC jouera ce rôle mais à moyens terme il faudra renforcer le modèle et mettre en place cette structure spécialisée. Cette structure aura permettra de :

- Assurer les rôles de l'entité de suivi,
- Coordonner entre tous les interlocuteurs,
- Etre en charge du suivi la sécurité des systèmes gouvernementaux,
- Etre en charge de suivi de la sécurité des infrastructures critiques,
- Piloter l'axe de sensibilisation et de développement de compétences,
- Assurer la coordination avec les entités internationales,
- Veiller à l'application de la législation à l'instar de l'audit obligatoire,
- Agir comme entité technique pour les autorités juridiques et judiciaires,
- Chercher les fonds pour le financement des projets,
- Créer l'entité de traitement d'incident : le RIMCERT.

II. Le RIMCERT

C'est une entité opérationnelle qui agira comme étant une entité focale pour le traitement des incidents et pour la coordination, le RIMCERT est une entité qui va démarrer au sein de la DGTIC et qui sera rattaché par la suite à l'Agence national de cybersécurité une fois créée. Le RICMCERT aura les rôles suivants :

- Conduire une activité de veille pour identifier les menaces potentielles et alerter les parties concernées,
- Faciliter le partage de données relatives aux incidents, menaces, vulnérabilités, bonnes pratiques, etc.
- Conduire des travaux communs de recherches pour étudier les risques, les menaces, etc.
- Agir comme étant un hub de communication et surtout durant les périodes de crises.
- Collaborer avec tous les intervenants (Opérateurs Télécom, Banques, infrastructure critique, Justice, Police, media, etc.),

- Développer la sensibilisation de formation, pour les entreprises publiques, privées et pour le grand public,
- Coordonner avec d'autres CERT,
- Assurer la collecte et le partage de données entre toutes les parties prenantes.

Le CERT mettra en place un certain nombre de service pour assurer sa mission. Les services à fournir s'articulent autour des thèmes suivant :

  - Le traitement d'incident,
  - La coordination,
  - La veille,
  - La sensibilisation,
  - L'audit,
  - La définition et mise à jour des politiques nationales de cybersécurité.

III. Maintien et amélioration continue

Un des principes du management de la qualité est l'amélioration continue. La qualité doit devenir un des objectifs permanents de la stratégie, elle doit assurer l'amélioration de la performance globale.

D'autre part, la révision de la stratégie est nécessaire afin de l'adapter avec les évolutions du contexte national et international et d'ajuster les objectifs ainsi que les projets en fonction d'un certain nombre d'indicateurs. **La stratégie mauritanienne en cybersécurité sera révisée chaque 3 ans**, et ce en :

- Préparation d'un rapport triennal sur l'état d'avancement par le comité de suivi, indiquant les évolutions ainsi que les obstacles rencontrés,
- Préparation de rapports techniques sur les nouveaux besoins ou sur les tendances internationales par les entités opérationnelles,
- Présentation de ces rapports au comité managérial ainsi que les recommandations d'améliorations ou de changements,
- Le comité managérial révise et valide les propositions.

11-Plan d'action

Le tableau suivant présente les actions qui découlent de la stratégie, pour chaque action on a défini :

- Une priorité,
- Un ou plusieurs responsables sur l'exécution,
- Un indicateur de mesure de performance pour assurer le suivi et s'assurer de la bonne exécution par rapport aux objectifs.

Définition des priorités :

- 1 : action à réaliser avant mi-2020,
- 2 : action à réaliser avant 2022,
- 3: action à réaliser avant Juin 2022.

	ACTION	PRIORITE	RESPONSABLE	INDICATEUR DE MESURE
	PROTECTION DES SYSTEMES D'INFORMATION NATIONAUX ET DES SYSTEMES GOUVERNEMENTAUX			
1	Développer une classification des entreprises publiques selon leur criticité et la criticité de leurs systèmes d'information.	2	DGTIC	DELAIS DE 6 MOIS
2	Développement d'un référentiel de sécurité.	1	DGTIC	DELAIS DE 12 MOIS
3	Lancement d'une compagne de sensibilisation sur l'usage de l'open source des entreprises à déployer des solutions de protection open source.	3	DGTIC	COUVRIR 80% DES ENTREPRISES PUBLIQUES
4	Développer et publier des guides sur les bonnes pratiques de sécurité	3	RIMCERT	DEVELOPPER 5 GUIDES PAR AN
5	Créer un réseau de responsables de sécurité de systèmes d'information	1	DGTCI	NOMMER DES RSSI DANS 100% DES ENTREPRISES ORGANISER UN MEETING PAR AN
6	Créer un comité de pilotage d'experts issue des différents ministères pour le suivi des grands projets technologiques	2	MESRSTIC	DELAIS DE 6 MOIS
7	Création d'une autorité de certification électronique pour la sécurisation des échanges en lignes	2	DGTIC	ENTITE OPERATIONNELLE DANS 18 MOIS
8	Organisation d'un séminaire avec le secteur bancaire sur la certification PCI/DSS	3	RIMCERT	UN SEMINAIRE EN 2020
9	Développement d'un référentiel pour la protection des données à caractère privé	2	DGTIC	DELAIS 6 MOIS APRES LA PROMULGATION DE LA LOI
10	Mise ne place d'un réseau de collaboration pour la réponse aux incidents, la coordination et le partage de l'information	3	RIMCERT	ORGANISATION D'UNE REUNION ANNUELLE
11	Mise en place du CERT national : RIMCERT	1	DGTIC	OPERATIONNEL EN 2019
12	Mise en place d'une unité au sein du ministère de l'intérieur et de la défense pour la lutte contre les cyber-attaques	2	MID MD	CREATION EN 2020

13	Mise en place une entité de coordination, de collecte et de partage de données au sein du secteur bancaire.	2	BCM APB RIMCERT	CREATION EN 2020
	PROTECTION DES INFRASTRUCTURES CRITIQUES			
14	Réalisation d'un inventaire et une classification des infrastructures critiques	2	DGTIC	DELAIS MI-2020
15	Développement d'un référentiel de protections spécifiques à chaque catégorie et d'un Framework de suivi et d'analyse des risques	3	DGTIC MINISTERE DE L'ENERGIE	DELAIS MI-2021
16	Organisation des workshops, des formations et des opérations blanches	3	DGTIC MINISTERE DE L'ENERGIE TELCOS BCM	WORKSHOP ANNUEL
17	Mise en place d'une plateforme d'échange et de partage entre les opérateurs critiques	3	DGTIC MINISTERE DE L'ENERGIE TELCOS BCM	DELAIS 2022
	DEVELOPPEMENT DES COMPETENCES ET DE LA SENSIBILISATION			
18	Lancement d'un diplôme spécialisé en sécurité des systèmes d'information	2	MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE	DEMARRAGE 2020/2021
19	Intégration de cours de sécurité au niveau des formations d'informaticiens	3	MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE	DEMARRAGE 2020/2021
20	Création un cursus de formation pour les responsables de la sécurité des entreprises citriques et ceux du gouvernement	2	DGTIC	3 FORMATIONS PAR AN
21	Allocation de fond pour subventionner des formations de formateurs en cybersécurité	2	DGTIC	FOND POUR COUVRIR 3 FORMATION PAR AN
22	Incitation des laboratoires de recherche en IT à développer des thématiques au tour de la cybersécurité	3	MINISTRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE	LANCEMENT DE 5 PROJETS AVANT 2022
23	Développement d'un programme national de sensibilisation	1	DGTIC	DELAIS DE 12 MOIS
24	Lancement d'émission radio/télé pour la sensibilisation du grand public	2	DGTIC	1 EMISSION RADIO EN 2019 1 EMISSION TV EN 2020
25	Organisation d'un workshop de sensibilisation pour les hauts décideurs	1	MESRSTIC DGTIC	AVANT LA FIN DE 2019
26	Développement de contenu de sensibilisation	1	DGTIC	3 SUPPORT EN 2010

				5 NOUVEAUX SUPPORT PAR AN
27	Lancement d'un forum national sur la sensibilisation	1	DGTIC MESRSTIC	ORGANISATION D'UN FORUM PAR AN A PARTIR DE 108
	DEVELOPPEMENT DU CADRE JURIDIQUE ET REGLEMENTAIRE			
28	Formation des juristes sur les nouvelles technologies, sur les aspects techniques des lois, et sur les nouvelles procédures judiciaires	1	MINISTERE DE LA JUSTICE	FORMATION DE 25 JURISTES PAR AN
29	Mettre en place un centre d'investigation et de criminologie	2	MINISTERE DE LA JUSTICE MINISTERE DE L'INTERIEUR	MIS EN PLACE AVANT FIN 2020
30	Développer la nouvelle réglementation relative à l'audit obligatoire et à l'obligation de déclaration d'incidents.	2	MINISTERE DE LA JUSTICE	AVANT 2022
31	Mettre en place les le système pour l'écoute légale	1	MINISTERE DE LA JUSTICE MINISTERE DE L'INTERIEUR	MIS EN PLACE AVANT FIN 2020
	DEVELOPPEMENT DE PARTENARIAT PUBLIC-PRIVE AU TOUR DE LA CYBERSECURITE			
32	Développement d'un cadre de partenariat entre les structures de sécurité et les opérateurs télécom pour la lutte contre les cyber-attaques	3	DGTIC OPERATEUR TELECOM	DEVELOPPEMENT D'UNE CONVENTION EN 2020
33	Développement d'un cadre de partenariat entre les structures de sécurité et le secteur bancaire pour la lutte contre les fraudes et les attaques	2	DGTIC BCM APB	DEVELOPPEMENT D'UNE CONVENTION EN 2020
34	Développement un partenariat avec les associations des TIC pour le développement du programme national de sensibilisation	2	DGTIC	LANCEMENT DE PARTENARIAT EN 2020
35	Faire adhérer le RIMCERT dans des réseaux internationaux de collaboration (FIRST, OIC-CERT, AfricaCERT, etc)	2	DGTIC	ADHESION AVANT MI-2020 AU FIRST ADHESION AVANT FIN-2019 AU OIC-CERT ET AFRICACERT
36	Créer une Agence Nationale de Cybersécurité	3	MESRSTIC	OPERATIONNELLE EN 2022