Politique régionale de protection des infrastructures critiques de la CEDEAO

SECTION 1. INTRODUCTION 3
SECTION 2. OBJET 3
SECTION 3. DEFINITIONS 4
SECTION 4. CADRE DE PROTECTION DES INFRASTRUCTURES CRITIQUES ET DES SERVICES ESSENTIELS 5
SECTION 5. ROLES RESPECTIFS DE L'ETAT ET DES OPERATEURS 5
SECTION 6. DEMARCHE DE GESTION DES RISQUES 5
SECTION 7. IDENTIFICATION DES INFRASTRUCTURES CRITIQUES ET DES SERVICES ESSENTIELS ET DESIGNATION DES OPERATEURS 6
SECTION 8. OBLIGATIONS DES OPERATEURS 6
SECTION 9. MESURES DE PROTECTION 6
SECTION 10. SANCTIONS PENALES 7
SECTION 11. INTERDEPENDANCES DES INFRASTRUCTURES CRITIQUES ET SERVICES ESSENTIELS 7
SECTION 12. COORDINATION NATIONALE 7
SECTION 13. INTERDEPENDANCES ENTRE PAYS DE LA REGION ET COOPERATION REGIONALE 7
SECTION 14. SUIVI ET MISE A JOUR DE LA PRESENTE POLITIQUE REGIONALE 8
ANNEXE I : INFRASTRUCTURES ET SERVICES POUVANT ETRE CLASSES CRITIQUES OU ESSENTIELS 9
ANNEXE II : CRITÈRES D'IDENTIFICATION DES OPÉRATEURS D'INFRASTRUCTURES CRITIQUES ET DE SERVICES ESSENTIELS 11
ANNEXE III : MESURES POUVANT ETRE IMPOSEES AUX OPERATEURS D'INFRASTRUCTURES CRITIQUES ET DE SERVICES ESSENTIELS 12

SECTION 1. INTRODUCTION

Dans tout pays, un certain nombre de services matériels ou immatériels fournis par des opérateurs publics ou privés sont essentiels pour la Nation, et en particulier pour le fonctionnement de l'État, pour l'économie ou pour la santé, la sûreté, la sécurité et le bien-être de la population. Ces services reposent eux-mêmes sur un ensemble d'infrastructures, physiques ou numériques, ainsi que sur les données nécessaires à leur fonctionnement.

Il est donc de la plus haute importance, pour l'État, les opérateurs économiques et la population, de garantir la résilience et la sécurité de ces infrastructures critiques, services essentiels et données face à tous les risques et menaces qui pourraient en affecter la disponibilité ou l'intégrité.

En effet, la résilience et la sécurité des infrastructures critiques et services essentiels peuvent être affectées par des risques et des menaces de natures très diverses - pannes, accidents, malveillance, agressions physiques, attaques numériques, catastrophes naturelles, pandémies, etc. -, tous pouvant avoir un impact grave sur une Nation. Il importe donc que la protection de chaque infrastructure critique ou service essentiel prenne en compte l'ensemble des risques et menaces, physiques comme numériques, auxquels il peut être soumis.

Par ailleurs, certains services peuvent reposer sur des infrastructures et des données situées à l'étranger. Dans ce cas, la protection de ces services ne peut pas être totalement assurée dans le pays où ils sont fournis. Cela justifie que chaque État intègre dans sa démarche les services essentiels qui lui sont nécessaires autant que les infrastructures critiques situées sur son territoire. Ce type de situation justifie aussi l'approche régionale de la présente politique.

Dans la suite du présent document, les données seront considérées comme faisant partie des infrastructures qui les stockent, les traitent ou les transmettent.

SECTION 2. OBJET

La présente Politique régionale a pour objectif d'assurer la résilience et la sécurité, face aux divers risques et menaces qui pourraient en affecter le fonctionnement, des infrastructures et services de la région qui sont essentiels pour le fonctionnement de l'État, pour l'économie ou pour la santé, la sûreté, la sécurité et le bien-être de la population, notamment lorsque ces services et infrastructures ont un caractère transnational.

A cette fin, cette politique régionale :

- fixe le cadre normatif minimal que les États membres devraient adopter pour assurer la protection de leurs infrastructures critiques et services essentiels ;
- fournit des éléments de méthodologie et des critères pour identifier les infrastructures et services concernés dans les différents secteurs d'activité ;
- propose une liste de mesures préventives, réactives et proactives pouvant être mises en place ;
- prévoit les principes et modalités de la coopération entre les États membres ayant une interdépendance en matière de service essentiel ou d'infrastructure critique.

La présente Politique régionale doit s'entendre sans préjudice de la possibilité donnée à chaque État d'adopter les mesures nécessaires pour garantir la protection de ses intérêts essentiels et sa sécurité, assurer l'action publique et la sécurité publique et permettre la recherche, la détection et la poursuite d'infractions pénales.

SECTION 3. DEFINITIONS

Au sens de la présente Politique, on entend par :

Cybersécurité : l'ensemble des mesures et des actions destinées à protéger le cyberespace et les cyber-actifs contre les menaces associées ou susceptibles d'endommager son réseau et son infrastructure d'information. La cybersécurité vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues ;

Cybercriminalité : les activités criminelles dont les ordinateurs et systèmes informatiques constituent soit l'arme soit la cible principale. La cybercriminalité recouvre les délits habituels (fraude, contrefaçon et usurpation d'identité par exemple), les délits liés au contenu (distribution en ligne de matériel pédopornographique ou incitation à la haine raciale par exemple) et les délits spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service et logiciel malveillant par exemple) ;

Infrastructure critique : une infrastructure ou un processus public ou privé dont la destruction, l'arrêt, l'exploitation illégitime ou la perturbation pendant une période de temps définie pourrait entraîner soit des pertes de vies humaines, soit des pertes importantes pour l'économie, ou porter un préjudice considérable à la réputation de l'État ou de ses symboles de gouvernance. Dans cette définition, l'infrastructure comprend les réseaux et systèmes et les données physiques ou numériques indispensables pour fournir ce service. Cette expression peut faire référence à un système ou processus dont le fonctionnement est critique au sein de l'organisation ;

Infrastructure critique d'information : réseau de communication ou système d'information dont le dysfonctionnement ou une exploitation malveillante pourrait provoquer l'interruption totale ou partielle d'une infrastructure critique ou d'un service essentiel ;

Opérateur d'infrastructure critique : opérateur public ou privé qui opère une infrastructure critique ;

Protection des infrastructures critiques : l'ensemble des mesures et des actions destinées à protéger les infrastructures critiques de l'ensemble des risques et menaces susceptibles de provoquer l'interruption totale ou partielle des services essentiels qu'elles fournissent ;

Protection des infrastructures critiques d'information : cybersécurité des infrastructures critiques, c'est-à-dire l'ensemble des mesures et des actions destinées à protéger des cybermenaces les réseaux de communication et les systèmes d'information dont la perturbation ou l'arrêt pourrait provoquer l'interruption totale ou partielle d'une infrastructure critique ou d'un service essentiel ;

CSIRT (*Computer Security Incident Response Team*) : équipe chargée d'alerter sur les menaces, de prévenir les risques sur les systèmes d'information, de réagir en cas d'incident de sécurité et d'aider à en atténuer les effets ;

Service essentiel : un service dont l'interruption totale ou partielle pourrait avoir un impact grave sur le fonctionnement de l'État, sur l'économie du pays ou sur la santé, la sûreté, la sécurité et le bien-être de la population, ou une combinaison d'impacts de cette nature qui, pris individuellement, ne suffiraient pas à classer essentiel le service considéré ;

Opérateur de service essentiel : opérateur public ou privé qui fournit un service essentiel ;

Protection des services essentiels : l'ensemble des mesures et des actions destinées à protéger les services essentiels de l'ensemble des risques et menaces susceptibles de provoquer leur interruption totale ou partielle ;

Technologies de l'information et de la communications (TIC) : technologies employées pour recueillir, stocker, traiter et transmettre des informations, incluant les technologies qui impliquent l'utilisation d'ordinateurs ou de tout système de communication ou de télécommunication.

Système d'information : tout dispositif, isolé ou non, ou ensemble de dispositifs interconnectés assurant en tout ou partie un traitement automatisé de données en exécution d'un programme ;

Réseaux : ensemble des moyens assurant l'alimentation d'une infrastructure en produits ou services nécessaires à son fonctionnement (communications, énergie, logistique, etc.) ;

SECTION 4. CADRE DE PROTECTION DES INFRASTRUCTURES CRITIQUES ET DES SERVICES ESSENTIELS

Chaque État devrait adopter un cadre de protection des infrastructures critiques et des services essentiels pour tous les secteurs d'activité (activités de l'État, santé, énergie, transports, eau, banques, industrie, etc.) et en particulier les secteurs transverses (production et distribution électrique et services numériques), en fixant :

- les responsabilités au sein de l'État ;
- les critères et les modalités d'identification des infrastructures critiques et des services essentiels ;
- les modalités de désignation des opérateurs de services essentiels et d'infrastructures critiques ;
- les obligations de sécurité qui s'imposent à ces opérateurs.

Chaque État devrait identifier la ou les autorités chargées, pour les différents secteurs d'activité, :

- d'identifier les services essentiels et les infrastructures critiques ;
- de désigner les opérateurs correspondants ;
- d'élaborer les mesures de sécurité qui leur sont imposées ;
- de veiller à la coordination de l'action des autorités publiques qui doivent concourir à la sécurité des infrastructures critiques et des services essentiels ;
- de participer à la gestion de crise en cas d'incident grave affectant une infrastructure critique ;
- d'assurer la coordination de ces différentes tâches avec son ou ses homologues étrangers pour les infrastructures critiques transnationales.

Chaque État devrait mettre en place une structure chargée de veiller à la cohérence des démarches mises en œuvre par les diverses autorités nationales.

SECTION 5. ROLES RESPECTIFS DE L'ETAT ET DES OPERATEURS

Les opérateurs d'infrastructures critiques et de services essentiels sont responsables de leur protection. Néanmoins, l'État, garant de la sécurité de la Nation, a la responsabilité de garantir la sécurité des infrastructures critiques et des services essentiels du pays. Il doit en particulier identifier et désigner les opérateurs de services essentiels et d'infrastructures critiques, leur fixer des obligations de protection, en contrôler la bonne exécution et sanctionner les éventuels manquements.

Par ailleurs, la protection des infrastructures critiques et des services essentiels ne peut pas être assurée par les seuls opérateurs concernés, car ils n'ont ni la légitimité ni en général les connaissances et informations pertinentes pour intervenir en dehors de leur périmètre de responsabilité. L'État doit y prendre sa part, en apportant aux opérateurs ses instructions et son soutien, dans un étroit partenariat public-privé. Il devrait en particulier intervenir dans la prévention des menaces et dans la gestion de la situation en cas d'attaque physique ou numérique, notamment au moyen de ses autorités, de ses services de renseignement, de ses forces de l'ordre, du CSIRT national et de ses institutions judiciaires.

SECTION 6. DEMARCHE DE GESTION DES RISQUES

La protection des infrastructures critiques et services essentiels constitue une charge lourde au plan organisationnel, technique, humain et financier. Il convient donc de n'assurer une protection renforcée que pour les infrastructures et services réellement critiques ou essentiels, au juste niveau nécessaire.

Dans cette optique, une démarche de gestion des risques doit être mise en place pour l'application de la présente politique dans le but d'identifier les risques et menaces potentielles et de proportionner les efforts à la probabilité d'occurrence et à la gravité des impacts qu'ils pourraient provoquer sur la Nation.

Elle permettra notamment à chaque État :

- d'identifier et de désigner les infrastructures critiques, les services essentiels et les opérateurs publics et privés concernés ;
- de définir au juste niveau nécessaire les mesures destinées à protéger ces infrastructures et services face aux risques et menaces physiques et numériques susceptibles de causer un impact grave sur la Nation, et les mesures visant à minimiser les impacts potentiels.

SECTION 7. IDENTIFICATION DES INFRASTRUCTURES CRITIQUES ET DES SERVICES ESSENTIELS ET DESIGNATION DES OPERATEURS

La démarche doit commencer par l'identification des services essentiels, puis des infrastructures qui sont nécessaires pour fournir ces services ou qui sont critiques pour d'autres raisons. Une liste non limitative d'infrastructures et de services susceptibles d'être classés critiques ou essentiels, présentée par secteur d'activité, est fournie en annexe I.

La démarche doit se poursuivre par l'identification des opérateurs d'infrastructures critiques ou de services essentiels. Des critères-types sont proposés en annexe II. Ces opérateurs doivent ensuite faire l'objet d'une procédure formelle d'approbation et de désignation.

SECTION 8. OBLIGATIONS DES OPERATEURS

Une liste non limitative de mesures pouvant être imposées aux opérateurs d'infrastructures critiques et de services essentiels est proposée en annexe III.

Ces opérateurs devraient être contraints au minimum à :

- mettre en place au niveau de leur direction une structure destinée à organiser et prendre en compte la protection de leurs installations ;
- respecter des règles techniques et opérationnelles destinées à renforcer la sécurité physique et la cybersécurité de leurs installations ;
- déclarer rapidement aux autorités compétentes tout incident pouvant avoir un impact grave ;
- collaborer franchement et sans réserve avec les autorités en cas de nécessité.

Tout opérateur d'infrastructures critiques ou de services essentiels doit mettre en place et respecter les mesures de protection qui lui sont imposées. Il les décrit dans les documents suivants, qu'il soumet aux autorités compétentes chargées de la gestion de la cybersécurité dans chaque Etat membre :

- une cartographie de ses services essentiels ;
- un plan de sécurité de l'opérateur ;
- une politique de sécurité des systèmes d'information (PSSI) pour ce qui concerne la cybersécurité, mettant l'accent sur les systèmes d'information les plus critiques pour les services essentiels qu'il assure.

SECTION 9. MESURES DE PROTECTION

Une analyse de risque, basée sur des scénarios prenant en compte les divers risques et menaces identifiés, doit permettre d'élaborer des mesures de protection pour chaque opérateur ou type d'opérateur d'infrastructures critiques ou de services essentiels.

Ces mesures sont préventives, réactives et proactives et peuvent également être organisationnelles, opérationnelles, techniques ou juridiques.

Les mesures préventives doivent viser à prévenir et atténuer les risques et menaces, et à réduire autant que possible la gravité des impacts potentiels sur l'infrastructure ou le service concerné et sur la Nation. Les

mesures réactives doivent être planifiées et mises en œuvre en cas d'incident affectant l'infrastructure critique ou le service essentiel. Elles doivent permettre d'assurer la gestion de l'incident, jusqu'à la reprise normale de l'activité, et la gestion de la crise que cet incident provoque sur la Nation. Les mesures proactives visent à éviter la récurrence des incidents, en examinant les causes possibles des incidents survenus et en adoptant une approche permettant de détecter et contenir tout incident identique. Ne devaient être prises que des mesures réalistes pouvant avoir un effet concret sur les objectifs cités.

Les mesures destinées à protéger les infrastructures critiques et services essentiels des risques et menaces utilisant ou pesant sur les technologies de l'information et de la communication doivent être cohérentes avec la Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité.

Par ailleurs, les États membres doivent prendre en compte dans leur politique nationale les mesures de protection déjà prévues dans les règlements internationaux pour tous les secteurs clés (transport aérien, navigation maritime, transactions bancaires, etc.).

SECTION 10. SANCTIONS

Chaque État doit prévoir des sanctions, y compris des sanctions pénales et administratives le cas échéant, pour les opérateurs et autres parties ne respectant pas les mesures de protection.

Par ailleurs, le droit pénal devrait imposer, aux opérateurs et autres parties, des sanctions plus sévères (pénales et administratives) pour les infractions qui ont perturbé ou tenté de perturber le bon fonctionnement des infrastructures critiques et des services essentiels.

SECTION 11. INTERDEPENDANCES DES INFRASTRUCTURES CRITIQUES ET SERVICES ESSENTIELS

La démarche doit prendre en compte les interdépendances pouvant exister entre les infrastructures critiques et services essentiels. A titre d'exemple, tous les services et les infrastructures sont, sauf rares exceptions, dépendants des services de distribution électrique et de communications électroniques.

En conséquence, chaque État devrait mettre en place des mesures de contournement[1] pour éviter toute interruption de fonctionnement des infrastructures critiques et services essentiels qui pourrait provoquer un impact grave sur la Nation.

SECTION 12. COORDINATION NATIONALE

Chaque État devrait mobiliser l'ensemble des autorités et acteurs publics concernés, y compris notamment la structure responsable de la cybersécurité au niveau national, pour établir une politique nationale de protection des infrastructures critiques et des services essentiels et fixer la contribution de chacun à sa mise en œuvre, tant pour les mesures préventives que réactives.

Les autorités et acteurs publics devraient établir un dialogue avec les opérateurs d'infrastructures critiques et de services essentiels pour identifier les principales vulnérabilités, les mesures propres à les réduire et les délais raisonnables de la mise en œuvre de ces mesures.

SECTION 13. INTERDEPENDANCES ENTRE PAYS DE LA REGION ET COOPERATION REGIONALE

Les interdépendances entre pays ne cessent de croitre au sein de la CEDEAO, y compris notamment pour des services essentiels.

Aux services interdépendants, comme les télécommunications publiques, les transactions financières ou les transports aériens internationaux, s'ajoutent de plus en plus des infrastructures desservant plusieurs pays, par exemple dans les domaines des corridors routiers, de la connexion à l'Internet mondial, de l'électricité,

[1] Mise en place de générateurs électriques ou d'une redondance des liaisons électriques et électroniques, par exemple.

des mines, du gaz et le système d'information des polices d'Afrique de l'Ouest (SIPAO) en place dans tous les États membres de la CEDEAO .

Certains services peuvent être désignés comme services essentiels par tous les États membres concernés. D'autres, essentiels dans un pays, peuvent dépendre d'infrastructures situées dans un pays ne les identifiant pas comme critiques.

Face à cette double problématique, il convient de mettre en place un dialogue et une coopération entre les États membres de la région, s'appuyant sur une compréhension commune des enjeux et de mesures de protection similaires et suffisantes dans tous les pays.

Les États Membres ayant une interdépendance de services essentiels ou d'infrastructures critiques sont ainsi invités à établir une coopération entre leurs autorités compétentes visant à :

- Identifier les services essentiels et les infrastructures critiques à caractère transnational, ainsi que la nature de leurs interdépendances ;
- Prendre en compte autant que possible les besoins des autres États membres dans la désignation de leurs infrastructures critiques ;
- Harmoniser les mesures de protection imposées aux opérateurs concernés ;
- Échanger des informations sur les menaces et les risques et prendre de manière coordonnée les éventuelles mesures complémentaires nécessaires pour répondre à une menace ou à un risque croissant ou imminent ;
- Coordonner les mesures à prendre en cas de crise liée à une infrastructure critique transnationale.

SECTION 14. SUIVI ET MISE A JOUR DE LA PRESENTE POLITIQUE REGIONALE

La Commission de la CEDEAO mettra en place un comité de suivi de la présente politique. Le comité de suivi, composé de Commission de la CEDEAO et d'un représentant de haut niveau fourni par chaque État membre se réunira au moins une fois par an pour assurer dans le temps le suivi des dispositions de la présente politique régionale et proposer les évolutions qui seraient nécessaires.

ANNEXE I :

Infrastructures et services pouvant être classés critiques ou essentiels

La démarche d'identification des opérateurs d'infrastructures critiques et de services essentiels doit considérer la liste non limitative des infrastructures et services figurant dans le tableau ci-dessous :

Secteurs	Infrastructures et services
1. Activités de l'État	- Sécurité publique - Sécurité intérieure - Services judiciaires - Défense nationale - Finances publiques - Parlement - Processus électoraux - Administration électronique, notamment certains services publics en ligne
2. Énergie	- Production, transport et distribution électrique - Production, transport, raffinage, stockage et distribution de produits pétroliers - Production, transport, traitement, stockage et distribution de gaz - Installations nucléaires
3. Transport	- Transport aérien, routier, ferroviaire, maritime et fluvial - Contrôle de circulation aérienne - Gestion de plate-forme aéroportuaire et portuaire (y compris les systèmes de sécurité) - Gestion d'infrastructure routière et ferroviaire
4. Logistique	- Gestion des plateformes logistiques
5. Finances	- Distribution de minima sociaux (intervention de sécurité/aides financières/incitations sociales) - Gestion du recouvrement et de la trésorerie des organismes sociaux - Transactions bancaires - Services financiers et compensation de crédit - Infrastructures de marchés financiers
6. Santé	- Capacités ou procédures de soins de santé uniques (dans des établissements ou par télémédecine) - Distribution pharmaceutique - Laboratoires de recherche - Bases de données de dossiers médicaux
7. Eau et assainissement	- Production, transport, stockage et distribution d'eau potable (par canalisation ou en bouteille) - Systèmes de collecte et de gestion des eaux usées
8. Communications électroniques	- Réseau Internet national et interconnexion à l'Internet régional et mondial (câbles sous-marins et terrestres, points d'atterrage de câbles, points d'échange Internet, etc.) - Gestion de noms de domaine Internet (DNS) - Fourniture d'accès à Internet - Services de télécommunication (téléphonie, etc.) - Data centers y compris les Data centers nationaux
9. Information	- Stations radio et télévision

10. Alimentation	- Approvisionnement, stockage et distribution des principales denrées alimentaires
11. Industrie	- Industries essentielles pour le pays
12. Divers	- Infrastructures susceptibles de causer des dommages graves à la population en cas de destruction accidentelle ou malveillante (barrage par exemple)

ANNEXE II :

CRITÈRES D'IDENTIFICATION DES OPÉRATEURS

D'INFRASTRUCTURES CRITIQUES ET DE SERVICES ESSENTIELS

La démarche d'identification des opérateurs de services essentiels et d'infrastructures critiques peut utiliser tout ou partie des critères indiqués dans la liste non limitative suivante :

1. Le niveau de gravité, la durée et l'étendue de l'impact qu'aurait une interruption du service ou un incident sur le fonctionnement de l'État, sur l'économie ou sur la santé, la sûreté, la sécurité et le bien-être de la population ;
2. La dimension de la zone ou de la population susceptible d'être touchée par un incident ;
3. Le nombre d'utilisateurs dépendant du service (exprimé en pourcentage de la population par exemple) ;
4. La part de marché de l'opérateur ;
5. La dépendance d'autres infrastructures critiques ou services essentiels à ce service (cas des services de distribution électrique et de communications électroniques par exemple) ;
6. L'importance que revêt l'opérateur pour assurer un niveau de service suffisant, compte tenu de la disponibilité de moyens alternatifs pour la fourniture du service ;
7. Le cas échéant, des facteurs sectoriels.

ANNEXE III :

MESURES POUVANT ETRE IMPOSEES

AUX OPERATEURS D'INFRASTRUCTURES CRITIQUES ET DE SERVICES ESSENTIELS

La liste non limitative suivante fournit des mesures pouvant être imposées aux opérateurs d'infrastructures critiques et de services essentiels.

Mesures préventives

- Gouvernance de la protection :
    1. Désigner une autorité de l'opérateur assurant la responsabilité devant les autorités publiques de toutes les questions de sécurité ;
    2. Mettre en place une organisation pour assurer la protection physique et la cybersécurité des infrastructures de l'opérateur ;
    3. Adresser aux autorités publiques, à une périodicité à fixer par chaque État, un rapport sur les risques, les menaces, les vulnérabilités identifiés et les principales mesures prises en conséquence ;
- Sécurité physique :
    1. Mettre en œuvre une démarche d'analyse de risque pour identifier et corriger les principales vulnérabilités pouvant aboutir à un impact grave sur la Nation ;
    2. Sensibiliser et former le personnel ;
    3. Assurer la sécurité des accès : gestion des identités et des droits d'accès, dispositifs visant à interdire ou à retarder les pénétrations non autorisées, dispositifs de détection d'intrusion ;
    4. Assurer la sécurité face aux risques naturels ou accidentels : dispositifs de prévention et de lutte contre l'incendie, prévention des submersions, prévention des accidents ;
    5. Mettre en place des redondances pour les installations ou les alimentations les plus critiques:
    6. Établir et mettre en œuvre un plan de sécurité de l'opérateur (PSO) ;
    7. Faire réaliser un audit périodique de sécurité physique par un service de l'État ou par un prestataire agréé par l'État, au moins tous les 5 ans ;
    8. Établir des plans de continuité et de reprise des activités ;
    9. Participer à des entrainements et exercices, à une périodicité à fixer par chaque État ;
- Cybersécurité :
    1. Mettre en œuvre une démarche d'analyse de risque pour identifier et corriger les principales vulnérabilités pouvant aboutir à un impact grave sur la Nation ;
    2. Transmettre aux autorités une cartographie des réseaux et systèmes d'information critiques, et la mettre à jour à chaque changement important ;
    3. Sensibiliser et former le personnel ;
    4. Appliquer les règles d'hygiène informatique ;
    5. Maintenir en condition de sécurité les systèmes et applications ;
    6. Cartographier la chaîne d'approvisionnement et veiller à sa cyber-hygiène ;
    7. Traiter les alertes données par le CSIRT de rattachement ;
    8. Assurer la sécurité des réseaux et des systèmes : règles sur les configurations, le cloisonnement, les accès distants, le filtrage ;
    9. Assurer la sécurité de l'administration des réseaux et des systèmes : règles sur les comptes et les systèmes d'administration ;
    10. Assurer la sécurité des données : sauvegarde périodique, mise en place de redondances et de réplication, chiffrement des dispositifs de stockage et des canaux de communication, etc. ;

11. Assurer la gestion des identités et des accès : règles sur l'identification, l'authentification, les droits d'accès ;
12. Assurer la défense des réseaux et des systèmes : détection des incidents de sécurité, journalisation des évènements, corrélation et analyse des journaux ;
13. Mettre en place des redondances pour les installations ou les alimentations les plus critiques ;
14. Établir et mettre en œuvre une politique de sécurité des systèmes d'information (PSSI) ;
15. Effectuer l'homologation de sécurité des systèmes d'information critiques ;
16. Faire réaliser un audit de sécurité des systèmes d'information par un service de l'État ou par un prestataire agréé par l'État, au moins tous les 3 ans et après chaque incident et évolution des systèmes d'information ;
17. Établir des plans de continuité et de reprise des activités ;
18. Participer à des entrainements et exercices, à une périodicité à fixer par chaque État ;

Mesures réactives

1. Notifier sans délai aux autorités publiques tout incident pouvant provoquer un impact grave ;
2. Activer des mécanismes et des systèmes pour recueillir et diffuser les informations pertinentes en temps voulu ;
3. Activer l'organisation interne de gestion de crise se tenant en liaison avec les autorités publiques (responsables identifiés et joignables, locaux, liaisons, annuaires, etc.) ;
4. Activer les plans de continuité et de reprise des activités.

Mesures proactives

1. Après la reprise des opérations, analyser la cause de l'incident ;
2. Transmettre les résultats de l'analyse aux autorités nationales compétentes (y compris à l'autorité nationale de cybersécurité ou au CSIRT national si l'incident a été provoqué par une cyberattaque) afin que l'incident et ses causes soient intégrés dans une base de données centrale ;
3. Intégrer dans les mesures préventives les mesures de protection et de détection découlant de l'analyse de l'opérateur ou des recommandations transmises par les autorités nationales compétentes.