PRESIDENCE DE LA REPUBLIQUE

REPUBLIQUE DE COTE D'IVOIRE
Union – Discipline – Travail

ANNEXE II AU DECRET N° 2021-916 DU 22 DECEMBRE 2021 PORTANT ADOPTION DU REFERENTIEL GENERAL DE SECURITE DES SYSTEMES D'INFORMATION ET DU PLAN DE PROTECTION DES INFRASTRUCTURES CRITIQUES

№ 2101059

RÉPUBLIQUE DE COTE D'IVOIRE

Union – Discipline – Travail

PLAN DE PROTECTION DES INFRASTRUCTURES D'INFORMATION CRITIQUES

TABLE DES MATIERES

PREAMBULE

Dans le contexte socio-économique et sociétal actuel, la survie d'une nation dépend grandement de sa capacité à fournir des services, produits et prestations les plus critiques aux populations. Garantir un fonctionnement continu des infrastructures critiques qui sous-tendent la fourniture de services ou le maintien des fonctions vitales pour la nation est un enjeu crucial qui s'inscrit indéniablement au premier rang des missions régaliennes de l'Etat.

Le boom technologique de ces dernières années a entraîné, en Côte d'Ivoire, une migration progressive des services critiques et fonctions vitales de l'Etat vers les technologies dites du « numérique». En effet, à l'instar de bien de pays en développement, la Côte d'Ivoire affiche un appétit croissant et une dépendance grandissante aux Technologies de l'Information et de la Communication. Ces technologies sont bien plus qu'un outil confiné à un secteur particulier, car elles interpénètrent l'ensemble des secteurs de l'économie et quasiment tous les domaines de la vie des populations. Une défaillance, un arrêt de fonctionnement ou une destruction de ces infrastructures critiques aura sans nul doute des conséquences extrêmement dommageables sur l'économie, la stabilité socio-politique, la sécurité, la santé des populations, etc.

Si la protection des infrastructures critiques traditionnelles (routes, autoroutes, ponts, aéroports, barrages hydroélectriques, etc.) est un exercice « classique » pratiqué par l'Etat depuis de nombreuses années, force est de constater que l'apparition des technologies de l'information et de la communication a entraîné de profonds changements dans la manière de concevoir cette activité. En effet, les menaces sont protéiformes, distribuées avec un spectre largement plus important, partant des risques d'attaques physiques (destructions physiques d'infrastructures) aux attaques logiques (destructions des systèmes d'information, vol de données, compromission du fonctionnement des logiciels, etc.). De plus, il est évident que la majeure partie des infrastructures d'informations critiques au sein de notre société sont soit détenues, soit gérées au quotidien par des opérateurs privés. Ceci dit, le secteur privé joue un rôle primordial dans cette dynamique de protection des intérêts et de la stabilité du pays.

Il apparaît donc très clair que la protection des infrastructures d'information critiques dans le domaine du numérique requiert une redéfinition des règles du jeu et un renforcement du partenariat public-privé, afin de mettre en œuvre des actions cohérentes et coordonnées sur le plan national.

Fort des missions de sécurisation des réseaux et systèmes d'information à elle confiées par la loi **N°2013-546 du 30 juillet 2013 relative aux transactions électroniques,** l'Etat ivoirien a chargé l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) de la mise en œuvre d'un plan de protection des infrastructures d'information critiques de télécommunications/TIC nationales, dans sa stratégie nationale de cybersécurité. Le présent plan de protection des infrastructures d'information critiques a pour vocation de servir de cadre de référence dans le domaine de la protection des infrastructures critiques. Il définit le champ d'application et les concepts clés pour une compréhension harmonisée dudit plan.

I. CHAMP D'APPLICATION ET DÉFINITION DES CONCEPTS

1) CHAMP D'APPLICATION

Le présent plan de protection des infrastructures d'information critiques s'applique à l'ensemble des [organisations/entités] installées sur le territoire national qui détiennent ou exploitent une infrastructure critique.

2) DÉFINITION DES CONCEPTS CLÉS

Infrastructures critiques : *Les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique et social des citoyens ou encore sur le fonctionnement continu des services de l'Etat.* ***(Article 1 de la loi N°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité)***

Exploitant d'infrastructures critiques : *Organisation opérant à titre de service public ou privé une infrastructure critique.*

***Criticité* d'une infrastructure** : *Définit le degré d'importance d'une infrastructure dont la défaillance, l'arrêt ou la destruction auraient un impact négatif sur le fonctionnement d'un Etat.*

Plan de protection : *Document cadre définissant la stratégie, les objectifs, règles et principes directeurs, ainsi que les mesures à mettre en œuvre pour atteindre les objectifs de protection sur le plan national.*

Secteurs critiques : *Ensemble de services critiques.*

Services critiques : *Activités ou prestations gratuites ou rémunérées ou fonctions indispensables au bon fonctionnement de l'Etat ou au bien-être économique ou social des citoyens.*

Plan de continuité d'activité : *Document cadre définissant les processus et/ou procédures permettant d'assurer la continuité de l'activité métier.*

Protection des infrastructures d'information critiques : *Ensemble de mesures visant à réduire la probabilité de survenue et/ou l'ampleur des dommages d'un dérangement, d'une défaillance ou d'une destruction d'infrastructures critiques ou qui réduisent le plus possible la durée de non-disponibilité.*

II. LISTE DES SECTEURS, SOUS-SECTEURS ET SERVICES CRITIQUES

Préfixe (abréviation)	Secteurs critiques	Sous-secteurs critiques	Services critiques
SEn	Energie	Electricité	- Production - Transport - Distribution
		Pétrole	- Extraction - Raffinage - Transport - Stockage
		Gaz naturel	- Extraction - Transport - Stockage - Distribution
SIT	Informations et technologies de l'information	Technologie de l'information	- Service web - Data Centre - Service Cloud (XaaS)
		Médias	- Radiotélévision - Presse en ligne
		Communication	- Voix/données - Connectivité Internet
SE	Eau	Eau potable	- Production et traitement - Stockage de l'eau - Distribution d'eau
		Eaux usées	- Collecte et traitement
SSa	Santé		- Service urgence - Service de consultation - Service épidémiologique, contrôle sanitaire, infection - Fourniture pharmaceutique, Vaccin, banque de sang - CMU, CNAM
SFi	Finances	Banque et Assurance	- Services financiers - Transfert d'argent - Paiement en ligne - Paiement mobile - Bourse
SSO	Sureté et Ordre public		- Maintien de l'ordre public et sécurité
STr	Transport	Transport aérien	- Services de navigation aérienne - Opérations aéroportuaires
		Transport terrestre	- Transport public
		Transport maritime	- Opérations portuaires
SAc	Administration civile	Gouvernement et institutions Agences d'Etat Autorités administratives indépendantes	-

III. IDENTIFICATION ET NOTIFICATION DES EXPLOITANTS D'INFRASTRUCTURES D'INFORMATION CRITIQUES

L'identification et la notification des exploitants d'infrastructures d'information critiques sont des activités réalisées par l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI). Ces activités s'appuient sur les outils méthodologiques du cadre global de protection des infrastructures d'information critiques. Le processus d'identification et de notification se subdivise en cinq phases :

a) Identification (ID)

L'identification des exploitants d'infrastructures d'information critiques est réalisée en tenant compte des secteurs et sous-secteurs critiques définis dans le présent plan de protection. Les organisations fournissant un ou plusieurs services critiques sont identifiées et répertoriées.

b) Évaluation (EV)

Les organisations opérant dans un secteur critique et fournissant un ou plusieurs services critiques identifiés dans la phase précédente sont évaluées, afin de déterminer si elles relèvent du champ d'action du plan de protection des infrastructures critiques.

c) Classification (CL)

Les organisations évaluées et définies comme exploitants d'infrastructures d'information critiques sont classifiées par niveau de criticité Les niveaux de criticité tiennent compte de l'indice de criticité déterminé après l'évaluation réalisée dans la phase précédente.

La classification est assurée par l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI).

d) Notification (NO)

Les exploitants d'infrastructures d'information critiques sont notifiés par l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI). Toutes les informations relatives à la liste aux actifs et autres informations d'un exploitant d'infrastructures critiques sont strictement confidentielles et contiennent des informations dont la révélation est réprimée par les dispositions du code pénal. Ils sont, le cas échéant, couverts par le secret de la défense nationale. Par conséquent, elles ne peuvent être ni publiées, ni divulguées au grand public.

Les courriers de notification sont adressés exclusivement aux destinataires identifiés et désignés comme exploitant d'infrastructures critiques.

e) Mise en œuvre des mesures de protection (MP)

Les organisations désignées comme exploitant d'infrastructures d'information critiques mettent en œuvre les directives de protection en coordination avec l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI).

IV. PRINCIPES DE PROTECTION DES INFRASTRUCTURES D'INFORMATION CRITIQUES

La protection des infrastructures d'information critiques décrite dans le présent plan est basée sur trois (03) principes fondateurs, à savoir : 1) approche globale de gestion des risques, 2) régulation à responsabilité partagée des acteurs, 3) partenariat public-privé.

1) APPROCHE GLOBALE DE GESTION DES RISQUES

L'approche fondée sur la gestion des risques décrite dans le cadre de ce plan peut être appliquée à tous types de menaces et dangers, y compris les incidents de sécurité informatique, les catastrophes naturelles, les menaces d'origine humaine et les actes terroristes, bien que différentes informations et méthodologies puissent être utilisées pour comprendre chacune d'elles. (cf. annexe A)

Le cadre de gestion des risques liés aux infrastructures critiques n'est pas destiné à remplacer les modèles ou processus déjà utilisés. Il préconise plutôt une approche commune pour la gestion des risques, que tous les partenaires d'infrastructures essentielles doivent utiliser, mettre en relation et harmoniser avec leurs propres modèles et activités de gestion des risques. Par ailleurs, il peut être adapté et appliqué à un actif, à un système, à un réseau ou à une base fonctionnelle, en fonction des caractéristiques fondamentales des décisions à prendre en charge et de la nature de l'infrastructure associée.

Les activités à réaliser dans cette approche de gestion des risques sont :

- **Faire un état des lieux** : Identifiez les actifs, les systèmes et les réseaux qui contribuent aux fonctionnalités critiques et collectez des informations pertinentes pour la gestion des risques, y compris l'analyse des dépendances et des interdépendances ;
- **Fixer des buts et objectifs** : Définir des résultats, conditions, points finaux ou objectifs, indicateurs de performance spécifiques décrivant collectivement une posture de gestion des risques efficace et souhaitée ;
- **Évaluer et analyser les risques** : Évaluer le risque en tenant compte des conséquences directes et indirectes potentielles d'un incident, des vulnérabilités connues de diverses menaces ou dangers potentiels et de l'information générale ou spécifique sur la menace ;
- **Mettre en œuvre des activités de traitement des risques** : Prendre des décisions et mettre en œuvre des approches de gestion des risques pour contrôler, accepter, transférer ou éviter les risques. Les approches peuvent inclure des activités de prévention, de protection, d'atténuation, d'intervention et de rétablissement ;
- **Mesurer l'efficacité** : Utiliser des paramètres et d'autres procédures d'évaluation pour mesurer les progrès et évaluer l'efficacité des efforts déployés pour sécuriser et renforcer la résilience des infrastructures critiques.

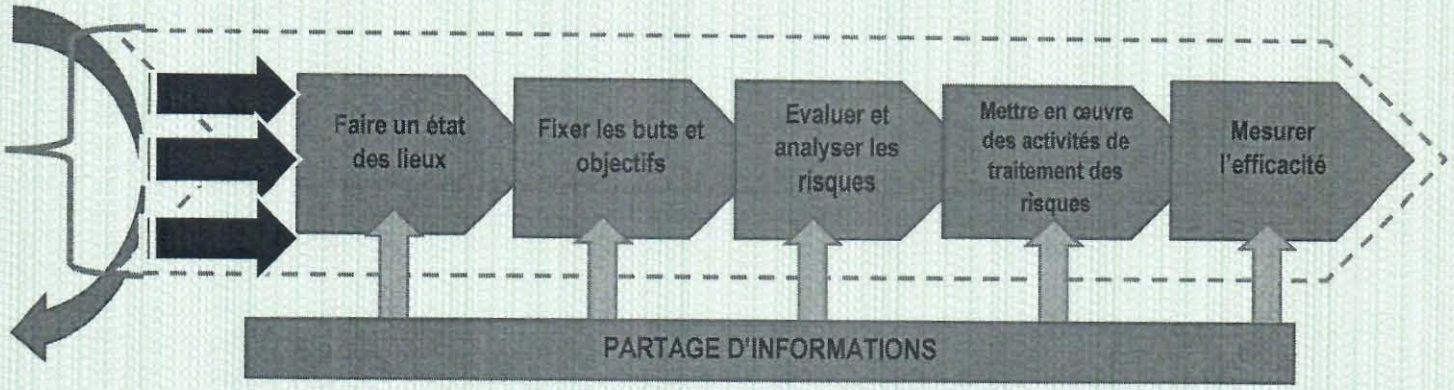

Schéma 1 : Approche de gestion des risques pour la protection des infrastructures d'information critiques

2) REGULATION A RESPONSABILITE PARTAGEE DES ACTEURS

Le mode régulation de la protection des infrastructures d'information critiques adopté dans le présent plan est basé sur la posture centriste du continuum de régulation[1]. Ladite posture correspond à la délégation de la protection des infrastructures critiques à une agence ou une autorité nationale tout en privilégiant l'adhésion volontariste du secteur privé à travers la négociation et la coopération participative à la définition des règles et principes de protection. En effet, l'Etat, à travers l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI), initie les réflexions et travaux relatifs à la protection des infrastructures critiques, mène des consultations, voire même des négociations avec des entités réglementées du secteur privé. Cette approche présente l'avantage de mettre au cœur de l'action les acteurs du secteur privé, afin de favoriser un partage des compétences pour le développement continuel du marché et de l'économie. De plus, elle implique un plus grand engagement et une meilleure prise en compte des spécificités des acteurs opérationnels, afin de proposer des mesures et dispositions les plus adaptées.

En somme, l'Etat conserve son pouvoir discrétionnaire et exerce ses missions régaliennes de protection en recherchant la plus grande acceptation et donc la conformité du marché.

3) PARTENARIAT PUBLIC-PRIVE

La protection des infrastructures d'information critiques en Côte d'Ivoire implique absolument une collaboration accrue entre tous les acteurs concernés, que ce soit ceux du secteur public, du gouvernement, de l'administration ou ceux du secteur privé. Les mesures de protection sont dans la mesure du possible élaborées, appliquées, voire financées en commun en tenant compte des spécificités de chaque acteur. Les conventions et entente de coopération entre le public et le privé doivent être établies dans tous les domaines de la protection des infrastructures critiques, singulièrement quand il s'agit de projet de construction de nouvelles infrastructures physiques critiques, de modification des

[1] Models of critical information infrastructure protection. Dan Assaf
University of Toronto, Faculty of Law, 84 Queen's Park, Toronto, ON M5S 2C5, Canada

conditions de fourniture de services critiques, de renforcement des capacités, de partage d'information, et d'élaboration des directives et des normes de protection.

V. DIRECTIVES DE PROTECTION

L'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) joue le rôle de coordinateur principal du plan de protection des infrastructures critiques, en étroite collaboration avec les instances compétentes, notamment les comités stratégiques sur la cybersécurité, groupes de travail, etc. Le rôle de l'ARTCI consiste essentiellement à définir en collaboration avec l'ensemble des acteurs impliqués, les lignes directrices et les principes de gestion du plan de protection des infrastructures critiques.

Cependant, il appartient à chaque responsable de département ministériel ou secteur critique, de traduire en exigences sectorielles, les lignes directrices du plan de protection des infrastructures d'information critiques. Aussi dans une approche d'adhésion et de participation volontariste, tous les acteurs opérationnels (propriétaires ou gestionnaires d'infrastructures critiques) s'engagent-ils à mettre en œuvre les exigences de protection, afin d'atteindre les objectifs fixés. Les présentes lignes directrices tiennent compte des objectifs de sécurité définis à la section « objectifs ».

- **Objectif Stratégique 1 : DEVELOPPER LES CAPACITES DE RESILIENCE**

1.1. IDENTIFICATION DES INFRASTRUCTURES D'INFORMATION CRITIQUES ET FIXATION DES PRIORITES DE PROTECTION

But

La mise en œuvre de toutes mesures proactives ou réactives implique nécessairement une bonne connaissance des infrastructures les plus essentiels pour la fourniture des services critiques. Cet effort de connaissance détaillée des infrastructures clés permet également d'améliorer la rationalisation des ressources allouées en fonction de leur sensibilité et de leur criticité.

Résultats attendus

Les infrastructures critiques nationales sont identifiées et classifiées ;

Les priorités de traitement de l'information relative à la gestion administrative et opérationnelle de ces infrastructures critiques sont fixées ;

1.1.1. Etablir un inventaire des infrastructures (réseaux, installations physiques, technologies, actifs, services, applications, ressources humaines, etc.) indispensable à la fourniture de services critiques

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures d'information critiques établit un registre tenu à jour et revu selon une périodicité de six (6) mois, de toutes ses infrastructures critiques. Le registre liste l'ensemble des infrastructures critiques et définit les priorités et objectifs de sécurité (confidentialité, intégrité, disponibilité) à mettre en œuvre.

Le registre des infrastructures critiques est communiqué au responsable sectoriel de la protection des infrastructures critiques et à l'ARTCI, dans les conditions de sécurité et de confidentialités prévues dans le cadre du présent plan de protection.

1.2. ANALYSE DES RISQUES ET CONNAISSANCE DES MENACES ET VULNERABILITES PESANT SUR LES INFRASTRUCTURES CRITIQUES

But

Les mesures à prendre doivent être en cohérence avec la nature des menaces, risques et vulnérabilités auxquelles les infrastructures critiques sont soumises. A cet effet, il est capital d'effectuer une analyse des risques globale du point des vues du contexte interne et de l'état des connaissances des vulnérabilités et risques intra sectorielles. Une bonne analyse des risques est l'élément clé pour la mise en œuvre de mesures de protection adaptées à la menace et une définition précise des priorités.

Résultats attendus

Les risques pesant sur les infrastructures critiques sont connus et les priorités sont définies
Les mesures de traitement des risques (réduction, maintien, refus, transfert) sont clairement définies pour chaque infrastructure critique.

1.2.1. Effectuer une analyse des risques complète

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures critique effectue une étude des risques complète sur tout le périmètre couvrant ses infrastructures critiques. L'analyse des risques est renouvelée au moins tous les six (06) mois et les rapports mis à jour.

1.3. TRAITEMENTS DES INCIDENTS DE SECURITE

But

Les incidents de sécurité doivent être traités avec la plus grande célérité en fonctions du niveau de sévérité et des impacts directs et directs sur la qualité, la disponibilité du service critique fourni. Les capacités de réponses doivent absolument être disponibles et opérationnelles, afin de limiter l'impact des incidents quand ils sont déclarés.

Résultats attendus

Les capacités de réponses aux incidents sont définies, disponibles et opérationnelles
Les mesures de prévention, de détection et de traitement des incidents sont définies et mises en œuvre

1.3.1. Etablir un accord formel de partenariat avec le CERT national (CI-CERT)

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures critiques établit un accord formel de collaboration avec le CI-CERT dans le cadre de la gestion des incidents. Cet accord définit les domaines clés de la collaboration entre le CI-CERT et les équipes opérationnelles de sécurité, à savoir au minimum et sans s'y limiter :

- Définition et établissement d'un canal de communication sécurisé pour le partage d'informations sensibles
- Partage d'informations spécifiques sur les vulnérabilités et failles de sécurité
- Mutualisation des ressources de formation et de renforcement des capacités
- Traitement des alertes d'incidents

1.3.2. Désigner un référent cybersécurité

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures d'information critiques désigne un référent cybersécurité, qui joue le rôle de point de contact entre l'organisation et les autorités compétentes (ARTCI, Responsable sectoriel à la cybersécurité, CI-CERT, etc.). Le référent cybersécurité est désigné pour ses connaissances en matière de cybersécurité et son aptitude à traiter les informations en considération de leur haut niveau de confidentialité et de sensibilité. La sélection du référent cybersécurité fait l'objet d'une attention toute particulière de la part de l'organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructure critique.

1.3.3. Mettre en œuvre des mesures techniques dédiées au traitement des incidents

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures d'information critiques met en place un système d'information spécifique pour traiter les incidents, notamment pour stocker les relevés techniques relatifs aux analyses des incidents.
Les relevés techniques relatifs aux analyses des incidents sont transmis, sans délai, à l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) et conservés pendant une durée d'au moins six (06) mois.

Les relevés techniques sont des documents strictement confidentiels susceptibles de contenir des informations dont la révélation est réprimée par les dispositions du code pénal. Ils sont, le cas échéant, couverts par le secret de la défense nationale.
Les incidents de sécurité affectant leurs systèmes d'information sont communiqués sans délais dès qu'ils en ont eu connaissance.

1.3.4. Mettre en œuvre des mesures techniques de détection des incidents de sécurité

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures critiques met en œuvre, un système de détection d'incidents de sécurité.
Le traitement des alertes enregistrées par ses propres systèmes de détection ou transmises par le CI-CERT, font l'objet d'une procédure formelle clairement définie et mise en œuvre en cas d'alerte. Le référent cybersécurité est garant de la mise en œuvre de la procédure de traitement des alertes.
Les alertes enregistrées par ses propres systèmes sont immédiatement communiquées à l'ARTCI quand celles-ci présentent une menace pour un ou plusieurs autres secteurs critiques.

1.4. EVALUATION DE LA SECURITE DU SYSTEME D'INFORMATION

1.4.1. Réaliser un audit annuel de la sécurité des systèmes d'information

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures critiques commandite chaque année, au moins un audit de sécurité du système d'information réalisé par un prestataire d'audit de sécurité des systèmes d'information agréé par l'ARTCI.
Conformément aux dispositions réglementaires, les rapports d'audit sont transmis à l'ARTCI et conservés dans des conditions de sécurité adéquates.

1.4.2. Certifier son système d'information conformément aux exigences de l'ARTCI

Le processus de certification du système d'information est défini par l'ARTCI. Il présente une démarche d'évaluation complète de la sécurité du système d'information et de la conformité avec les exigences du Référentiel Général de Sécurité des Systèmes d'Information.

1.5. GESTION DES CRISES

But

Les nombreux exemples de graves crises vécues par des organisations de tout type et de toute taille, montrent que celles qui ont mis en œuvre une démarche visant à garantir la continuité de leur activité sont les plus résilientes face aux événements déstabilisants. Dans le cadre de la protection des infrastructures critiques, la mise en œuvre d'une telle démarche est un gage incontestable de la confiance des citoyens en général, de la stabilité socio-économique et du fonctionnement continu des services de l'Etat. Les capacités de gestion de crise sont un bon socle pour construire la résilience de l'organisation des infrastructures critiques nationales.

Résultats attendus

Les moyens et procédures de gestion de crise sont définis et évaluées

Des mesures sont prises pour garantir la continuité des activités, de fonctionnement des infrastructures critiques même en cas de graves crises.

1.5.1. Définir une procédure et une cellule de gestion de crise

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures d'information critiques met en place une cellule de gestion des crises. La cellule de gestion des crises a pour rôle de contribuer à maîtriser l'incertitude durant la survenance d'une crise, afin de favoriser la prise de décision les plus rationnels et adaptés à l'ampleur de l'incident. Elle comprend notamment les fonctions, rôles et responsabilités suivantes :

- suivi et analyse de la situation,
- anticipation,
- cellules techniques (ou processus) capables d'analyser les conséquences sur les métiers et activités,
- cellule d'aide à la décision (capable de simuler différentes réponses possibles, à différents paliers de la crise, et de proposer la meilleure solution, dans un contexte d'incertitude),
- cellule de décision,
- cellule de coordination et suivi des actions,
- cellule de relation avec les parties prenantes (dont l'État et les partenaires),
- cellule de communication avec les médias
- cellule de relation avec les parties prenantes.

Une procédure de gestion des crises décrivant les moyens de communication, les rôles et responsabilité, l'annuaire de crise (contacts de personnes jouant un rôle dans le processus de gestion de crise) est également défini.

1.5.2. Définir un Plan de Continuité d'Activités (PCA)

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures critiques définit un plan de continuité d'activité (PCA) qui vise à décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir la reprise et la continuité de ses activités critiques à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal.
Le PCA est tenu à la disposition de l'ARTCI et du responsable sectoriel de la cybersécurité.

➢ Objectif Stratégique 2 : MAINTENIR LA SECURITE ECONOMIQUE ET LA STABILITE SOCIO-POLITIQUE

2.1. RENFORCEMENT DES CAPACITES DES RESSOURCES HUMAINES

But

Les compétences des personnels affectés à l'administration, la gestion technique et opérationnelles des infrastructures critiques doivent être continuellement mises à niveau, à mesure que les technologies, les techniques d'attaques, les menaces, les besoins de qualité de service évoluent. Si le facteur humain est d'une manière générale le maillon faible de la sécurité, il est indispensable de mettre un accent particulier sur la formation et la sensibilisation des ressources humaines, surtout celles ayant un rôle direct dans la gestion des infrastructures critiques.

Résultats attendus

Des moyens et planning de renforcement des capacités des personnels affectés à la gestion opérationnelle des infrastructures critiques sont définis et disponibles

Les ressources humaines affectées à la gestion opérationnelle des infrastructures critiques sont allouées de manière rationnelle et cohérente avec les charges de travail

2.1.1. Etablir un plan de formation annuel spécifique pour les personnels affectés à la gestion opérationnelle des infrastructures d'information critiques

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures critiques définit et met en œuvre un plan de formation annuel spécifique pour les personnels affectés à la gestion opérationnelle des infrastructures critiques. Ceci passe tout d'abord par l'identification et la catégorisation de ces personnels et par la définition de cycles de formation métier.

2.1.2. Réaliser des sessions de sensibilisation internes sur la sécurité de l'information

Les sessions de formation et de sensibilisation en sécurité de l'information sont à privilégier pour l'ensemble des personnels, quel qu'en soit la fonction et le domaine d'activités. Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures critiques d'information réalise des sessions de sensibilisation à la sécurité de l'information à l'attention de tous les personnels techniques, administratifs ou de support.

2.2. GOUVERNANCE DE LA PROTECTION DES INFRASTRUCTURES D'INFORMATION CRITIQUES

But

Pour être efficace, toute stratégie doit être clairement définie dans ses objectifs, les rôles et responsabilités définis et attribués, les ressources clairement définies et mise à disposition.

Résultats attendus

Un cadre formel de protection des infrastructures d'information critiques est élaboré

Les rôles et responsabilités sont clairement définis et communiqués aux acteurs

Les mécanismes d'évaluation sont définis.

Elaborer un Plan Annuel de Sécurisation (PAS)

Le plan annuel de sécurisation constitue le document cadre de la stratégie de l'organisation pour la sécurisation de ses infrastructures critiques d'information. A cet effet, chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures critiques définit en début de chaque année d'exercice, un plan annuel de sécurisation qui comprend l'ensemble des exigences, actions et lignes directrices contenus dans le présent plan de protection.
Le plan comporte également un plan d'action qui définit les actions prévues pour atteindre les objectifs de protection établis sur les différentes infrastructures critiques d'information, ainsi que les moyens prévus à cet effet et les responsabilités attribuées à chacun des acteurs dans le cadre de la mise en œuvre du plan.

- **Objectif Stratégique 3 : RENFORCER LA CONFIANCE DES CONSOMMATEURS DANS LA FIABILITE DE LA CHAINE DE FOURNITURE ET D'APPROVISIONNEMENT DES SERVICES CRITIQUES**

3.1. COLLABORATION ET PARTAGE D'INFORMATION INTERSECTORIELLE / INTRA SECTORIELLE

But

Une collaboration et un cadre d'échange permanent sur les risques et les meilleures techniques et mesures de protection possibles est très important entre les différents secteurs et opérateurs d'infrastructures critiques. La collaboration et la communication entre les exploitants, gestionnaire ou propriétaires d'infrastructures critiques et les entités étatiques compétentes est un enjeu majeur de la protection des infrastructures critiques. Cette dernière doit être renforcée.

Résultats attendus

Des moyens, procédures de communication, de partages d'information entre les exploitants d'infrastructures critiques et les entités étatiques compétentes sont définis et mis en œuvre

La coopération internationale est renforcée

3.1.1. Créer des groupes de travail sectoriels

L'Autorité de Régulation des télécommunications/TIC de Côte d'Ivoire et les responsables sectoriels à la protection des infrastructures d'information critiques, mettent en place et animent des groupes de travail et des cadres d'échange permanents entre les différents exploitants d'infrastructures critiques d'information.

3.1.2. Etablir des liens formels de coopération avec les groupes ou organisations spécialisées en matière de cybersécurité/sécurité de l'information, tels que les CIRT, FIRST, CSIRT, CERT, Groupe de travail, organisations internationales, etc.

Chaque organisation désignée et notifiée comme opérateur ou gestionnaire d'infrastructures d'information critiques établit des conventions formelles de coopération avec les organisations spécialisées en matière de cybersécurité ou sécurité de l'information, afin de renforcer la coopération internationale et le développement des capacités des personnels opérationnels.

VI. CONTROLE ET REVISION DU PPICI

Le contrôle du plan de protection des infrastructures d'information critiques est assuré par l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI).

Le plan de protection des infrastructures critiques est mis à jour par l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) conformément aux dispositions du référentiel général de sécurité des systèmes d'information (RGSSI).

Fait à Abidjan, le 22 décembre 2021

Copie certifiée conforme à l'original
Le Secrétaire Général du Gouvernement

Alassane OUATTARA

RÉPUBLIQUE DE CÔTE D'IVOIRE ★ SECRÉTARIAT GÉNÉRAL DU GOUVERNEMENT ★

Eliane Atté BIMANAGBO
Préfet

№ 2101059