AECK/ WG

**RÉPUBLIQUE DU BÉNIN**

Fraternité-Justice-Travail

---

PRÉSIDENCE DE LA RÉPUBLIQUE

---

**DÉCRET N° 2023** – 060 DU 22 FEVRIER 2023
portant approbation des règles de politique de protection des infrastructures d'information critiques en République du Bénin.

**LE PRÉSIDENT DE LA RÉPUBLIQUE,**

**CHEF DE L'ÉTAT,**

**CHEF DU GOUVERNEMENT,**

**Vu** la loi n° 90-32 du 11 décembre 1990 portant Constitution de la République du Bénin, telle que modifiée par la loi n° 2019-40 du 07 novembre 2019 ;

**vu** la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, telle que modifiée par la loi n° 2020-35 du 06 janvier 2021 ;

**vu** la décision portant proclamation, le 21 avril 2021 par la Cour constitutionnelle, des résultats définitifs de l'élection présidentielle du 11 avril 2021 ;

**vu** le décret n° 2021-257 du 25 mai 2021 portant composition du Gouvernement ;

**vu** le décret n° 2021-401 du 28 juillet 2021 fixant la structure-type des ministères, tel que modifié par le décret n° 2022-476 du 03 août 2022 ;

**vu** le décret n° 2021-307 du 09 juin 2021 portant attributions, organisation et fonctionnement du Ministère de l'Economie et des Finances ;

**vu** le décret n° 2021-308 du 09 juin 2021 portant attributions, organisation et fonctionnement du Ministère du Numérique et de la Digitalisation ;

**vu** le décret n° 2022-324 du 1er juin 2022 portant création de l'Agence des Systèmes d'Information et du Numérique, par la fusion de l'Agence du Développement du Numérique, de l'Agence des Services et Systèmes d'Information, de l'Agence nationale de la Sécurité des Systèmes d'Information et de l'Agence béninoise du Service universel des Communications électroniques et de la Poste et approbation de ses statuts ;

**vu** proposition du Ministre du Numérique et de la Digitalisation,

**le** Conseil des Ministres entendu en sa séance du 22 février 2023,

**DÉCRÈTE**

**Article premier**

Sont approuvées, telles qu'annexées au présent décret, les règles de politique de protection des infrastructures d'information critiques en République du Bénin.

**Article 2**

Les règles de politique de protection des infrastructures d'information critiques s'appliquent :

- aux opérateurs d'infrastructures d'information critiques ;
- aux institutions chargées d'assurer les responsabilités de l'Etat pour la protection des opérateurs d'infrastructures d'information critiques face aux cybermenaces ;
- à toutes les parties ayant une part de responsabilité dans l'exploitation et la protection des infrastructures d'information critiques.

**Article 3**

L'Agence des Systèmes d'Information et du Numérique reçoit une dotation spécifique annuelle représentant l'appui de l'Etat pour la protection des infrastructures d'information critiques. Elle met en œuvre toutes les activités entrant dans le cadre de la politique de protection des infrastructures d'information critiques et en rend compte au ministre chargé du Numérique.

**Article 4**

La violation de toute règle de politique de protection des infrastructures d'information critiques expose le contrevenant à des sanctions administratives et financières.

Les sanctions sont prononcées si, trois (03) mois après une mise en demeure, aucune mesure corrective n'est prise par l'opérateur concerné.

Toute attaque de toute nature sur une infrastructure d'information critique est sanctionnée conformément aux textes en vigueur.

**Article 5**

Les opérateurs d'infrastructures d'information critiques disposent d'un délai de six (06) mois, à compter de la date d'entrée en vigueur du présent décret, pour définir et soumettre à l'Agence des Systèmes d'Information et du Numérique, un plan d'actions de mise en œuvre de la politique de protection des infrastructures d'information critiques.

Ils disposent d'un délai de vingt-quatre (24) mois à compter de la date d'entrée en vigueur du présent décret, pour se conformer aux règles de politique de protection des infrastructures d'information critiques.

**Article 6**

Sans préjudice des poursuites prévues par les dispositions légales et réglementaires en vigueur :

Est puni de dix millions (10 000 000) de francs CFA d'amende, tout opérateur d'infrastructures d'information critiques qui ne satisfait pas à l'obligation de déclaration d'incident prescrit par les règles de politique de protection des infrastructures d'information critiques.

Est puni de quinze millions (15 000 000) de francs CFA d'amende, tout opérateur d'infrastructures d'information critiques, qui fait obstacle aux opérations de contrôle et d'audit de conformité prescrites par les règles de politique de protection des infrastructures d'information critiques.

Est puni de vingt-cinq millions (25 000 000) à cinquante millions (50 000 000) de francs CFA d'amende, tout opérateur d'infrastructures d'information critiques, qui reçoit un avis de non-conformité aux exigences critiques de sécurité, par suite d'un audit diligenté par l'Agence des Systèmes d'Information et du Numérique.

**Article 7**

Le Ministre du Numérique et de la Digitalisation, le Ministre de l'Intérieur et de la Sécurité Publique, le Garde des Sceaux, Ministre de la Justice et de la Législation sont chargés, chacun en ce qui le concerne, de l'application du présent décret.

**Article 8**

Le présent décret, qui prend effet pour compter de sa date de signature, abroge toutes dispositions antérieures contraires.

Il sera publié au Journal officiel.

Fait à Cotonou, le 22 février 2023

Par le Président de la République,
Chef de l'État, Chef du Gouvernement,

**Patrice TALON.**

Le Ministre de l'Economie
et des Finances,

**Romuald WADAGNI**
Ministre d'Etat

Le Ministre du Numérique
et de la Digitalisation,

**Aurelie I. ADAM SOULE ZOUMAROU**

Le Garde des Sceaux, Ministre de
la Justice et de la Législation,

**Séverin Maxime QUENUM**

Le Ministre de l'Intérieur
et de la Sécurité Publique,

**Alassane SEIDOU**

**AMPLIATIONS** : PR : 6 ; AN : 4 ; CC : 2 ; CS : 2 ; C. COM : 2 ; CES : 2 ; HAAC : 2 ; HCJ : 2 ; MEF : 2 ; MJL : 2 ; MISP : 2 ; MND : 2 ; AUTRES MINISTERES : 19 ; SGG : 4 ; JORB : 1.

# Règles de politique de protection des infrastructures d'information critiques en République du Bénin

## Sommaire

## i. Définitions

Au sens du présent document, les termes ci-après se définissent comme suit :

**cybersécurité** : ensemble des mesures et des actions destinées à protéger les moyens numériques et à prévenir les dommages face aux cybermenaces. 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.

**infrastructure sensible ou critique :** point, système ou partie de celui-ci, situé sur le territoire de la République du Bénin et qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, comme les centrales électriques, les réseaux de transport et les réseaux publics, et dont l'arrêt ou la destruction aurait un impact significatif sur la République du Bénin du fait de la défaillance de ces fonctions.

**infrastructure d'information critique** : systèmes et réseaux d'information interconnectés, dont la perturbation ou la destruction aurait un sérieux impact sur la santé, la sécurité, la sûreté ou le bien-être économique des citoyens ou sur le fonctionnement efficace du Gouvernement ou de l'économie.

**opérateur d'infrastructure d'information critique :** opérateur public ou privé qui gère une infrastructure d'information critique.

**politique de protection des infrastructures d'information critiques :** organisation et mesures mises en place par l'État pour assurer la protection des infrastructures d'information critiques.

**service critique** : tout service fourni par un opérateur d'infrastructure d'information critique et 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 comme "critique" le service considéré.

**système d'information** : ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un environnement donné.

**réseaux** : ensemble connecté de systèmes informatiques, quel que soit leur mode de connexion. Les connexions peuvent être reliées à la terre, sans fil ou les deux. Un réseau peut être géographiquement limité à une zone peu étendue ou couvrir une zone étendue et de tels réseaux peuvent eux-mêmes être interconnectés.

### ii. Glossaire

**ASIN :** Agence des Systèmes d'Information et du Numérique

**bjCSIRT** : Equipe nationale de réponse aux incidents de sécurité informatique

**CCII :** Cadre de Classification des Infrastructures d'Information

**CEDEAO :** Communauté Economique des Etats de l'Afrique de l'Ouest

**FSSNQ** : Fournisseurs de Services de Sécurité Numérique Qualifiés

**IIC** : Infrastructures d' Information Critiques

**OCWAR-C:** West African Response On Cybersecurity And Fight Against Cybercrime

**OIIC :** Opérateur d'Infrastructure d'Information Critique

**PPIIC** : Politique de Protection des Infrastructures d'Information Critiques

**PSSIE** : Politique de Sécurité des Systèmes d'Information de l'Etat

**SNSN :** Stratégie Nationale de Sécurité Numérique

## 1 Introduction

Les nombreux investissements consentis dans le cadre des grands projets numériques du Programme d'Actions du Gouvernement (PAG) au Bénin ont entraîné la création et l'émergence d'acteurs privés et publics dont l'importance des services qu'ils offrent devient vitale pour l'Etat. La faillite de ces opérateurs, l'indisponibilité même temporaire de leurs services ou la compromission des données qu'ils traitent deviennent un enjeu central pour le maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens.

Il est donc d'une importance capitale de garantir la résilience et la sécurité de ces infrastructures critiques, notamment sur leur composante numérique, face à tous les risques et menaces cybernétiques qui pourraient en affecter la disponibilité, la confidentialité ou l'intégrité. Ces risques et menaces peuvent être de natures très diverses. La protection de chaque infrastructure d'information critique doit donc prendre en compte l'ensemble des risques et menaces auxquels elle peut être exposée.

Face à ces défis, une première étape dans la sécurisation de ces infrastructures a été l'élaboration d'un cadre de classification des infrastructures d'information dont l'objectif est d'identifier formellement dans tous les secteurs critiques, les opérateurs dont l'importance serait vitale pour le pays.

La protection des infrastructures d'information critiques nécessite la mise en place de tout un ensemble de mesures de natures variées, notamment techniques, organisationnelles et juridiques. De ce fait, sa mise en œuvre représente une lourde charge pour les opérateurs. Il convient donc d'assurer une protection renforcée mais adaptée et proportionnée au contexte d'évolution des menaces.

Ces différents enjeux sont traduits dans ce document de règles de politique de protection des infrastructures d'information critiques qui est l'expression de l'engagement de l'Etat en la matière. Cette vision transparaît déjà dans la loi n°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin[1] et dans les orientations de la Stratégie nationale de Sécurité numérique, notamment le premier axe qui traite de la protection des systèmes d'information et des infrastructures.

Les cybermenaces sont transfrontalières et la protection des infrastructures d'information critiques implique souvent des actions de coopération entre Etats. C'est pourquoi, les règles de politique de protection des infrastructures d'information critiques s'inspirent largement de la politique régionale de protection des infrastructures critiques adoptée par les États membres de la CEDEAO en novembre 2020.

[1] Telle que modifiée par la loi N°2020-35 du 6 janvier 2021 en République du Bénin dans toutes ses dispositions qui ne sont pas contraires au Livre Cinquième du code du numérique qui traite de la protection des données à caractère personnel

## 2 Objectifs

L'objectif principal des règles de politique de protection des infrastructures d'information critiques est de fixer les responsabilités, l'organisation et les principes de mise en œuvre de la stratégie de l'Etat destinée à assurer la sécurité et la résilience des infrastructures d'information critiques du Bénin face aux divers risques et menaces qui pourraient en affecter la disponibilité, l'intégrité ou le bon fonctionnement. Elles définissent le cadre permettant d'apporter une réponse coordonnée et harmonisée aux risques pesant sur les infrastructures d'information critiques au plan national. A cette fin, les présentes règles de politique visent à :

- définir l'organisation et les mesures mises en place par l'État pour assurer la protection des infrastructures d'information critiques ;
- établir le processus de désignation des opérateurs d'infrastructures d'information critiques ;
- renforcer la gestion des infrastructures d'information critiques par l'Etat ;
- élever le niveau de maturité des opérateurs d'infrastructures d'information critiques en matière de sécurité numérique ;
- renforcer la résilience des infrastructures d'information critiques en réduisant l'impact des incidents grâce à une planification préalable ;
- favoriser le partage d'informations pertinentes dans la communauté des opérateurs d'infrastructures d'information critiques afin de se prémunir contre les menaces ;
- améliorer la culture de la cybersécurité chez les opérateurs d'infrastructures d'information critiques et accroître l'intégration de la cybersécurité dans leurs plans d'actions ;
- renforcer la coopération internationale sur la sécurité des infrastructures d'information critiques transnationales.

## 3 Champ d'application des règles de politique de protection des infrastructures d'Information critiques

Les règles de politique de protection des infrastructures d'information critiques s'appliquent à toutes les parties ayant une part de responsabilité dans l'exploitation et la protection des infrastructures d'information critiques. Il s'agit des opérateurs d'infrastructures d'information critiques résultant de l'application du cadre de classification des infrastructures d'information et dont la liste est validée par le Conseil des Ministres, des institutions chargées d'assurer les responsabilités de l'Etat et des organismes assurant la contribution de l'Etat pour la protection physique des sites des opérateurs d'infrastructures d'information critiques face aux menaces. Ces institutions et organismes sont listés dans le cadre institutionnel de la politique de protection des infrastructures d'information critiques.

## 4 Relation entre la politique de protection des infrastructures d'information critiques et la politique de sécurité des systèmes d'information de l'Etat

La politique de sécurité des systèmes d'information de l'Etat adoptée le 20 octobre 2021 par le Conseil des Ministres, définit les règles d'usage pour assurer la protection des systèmes

d'information des administrations publiques, établissements publics et sociétés d'Etat. A cet effet, elle s'applique essentiellement à ces entités, ainsi qu'à toute personne ou tiers ayant une part de responsabilité dans la mise en œuvre ou l'exploitation des systèmes d'information de l'Etat. Ainsi les entités de l'état désignées comme opérateur d'infrastructures d'information critiques devront respecter les exigences de la politique de sécurité des systèmes d'information de l'Etat.

Les règles de politique de protection des infrastructures d'information critiques, quant à elles, s'adressent aux structures des secteurs publics et privés désignées comme opérateurs d'infrastructures d'information critiques, aux institutions chargées d'assurer les responsabilités de l'Etat dans la protection des infrastructures d'information critiques ainsi qu'aux organismes assurant la contribution de l'Etat pour la protection physique des sites des opérateurs d'infrastructures d'information critiques.

## 5 Evolution des règles de politique de protection des infrastructures d'information critiques

La mise à jour des règles de politique de protection des infrastructures d'information critiques est initiée par l'Agence des Systèmes d'Information et du Numérique et validée par le ministre chargé du Numérique. La mise à jour est approuvée par décret pris en Conseil des Ministres.

Les règles de politique de protection des infrastructures d'information critiques font l'objet de mise à jour en fonction :

- des évolutions des contextes organisationnel, juridique, réglementaire et technologique ;
- du poids ou du niveau de maturité numérique des secteurs d'activités au plan national ;
- des résultats des missions de contrôle de conformité et de sécurité auprès des opérateurs d'infrastructures d'information critiques ;
- de l'évolution des menaces et des retours d'expériences relatives aux traitements d'incidents ;
- des difficultés de mise en œuvre de la présente version ou ses insuffisances.

## 6 Sanctions

La violation de toute règle de politique de protection des infrastructures d'information critiques expose le contrevenant à des sanctions administratives et financières.

Toute attaque de toute nature sur une infrastructure d'information critique est sanctionnée conformément aux textes en vigueur.

Le décret portant adoption des règles de politique de protection des infrastructures d'information critiques fixe les sanctions sur les aspects suivant :

- les manquements dans la mise en œuvre des exigences minimales de sécurité énoncées dans la présente politique de protection des infrastructures d'information critiques ;
- tout obstacle aux opérations d'audit et de contrôle ;
- la non déclaration d'incident de sécurité aux autorités compétentes.

Les sanctions sont prononcées si, trois (03) mois après une mise en demeure, aucune mesure corrective n'est prise par l'opérateur concerné.

## 7 Entrée en vigueur et dispositions transitoires

Les règles de politique de protection des infrastructures d'information critiques entrent en vigueur à partir de la date de son adoption par le Conseil des Ministres.

Les opérateurs d'infrastructures d'information critiques disposent d'un délai de six (06) mois à compter de la date d'entrée en vigueur du présent décret, pour définir et soumettre à l'Agence des Systèmes d'Information et du Numérique, un plan d'actions de mise en œuvre de la politique de protection des infrastructures d'information critiques.

Ils disposent d'un délai de vingt-quatre (24) mois à compter de la date d'entrée en vigueur du présent décret, pour se conformer aux règles de politique de protection des infrastructures d'information critiques.

## 8 Cadre institutionnel de mise en œuvre des règles de politique de protection des infrastructures d'information critiques

La mise en œuvre efficace des règles de politique de protection des infrastructures d'information critique implique une gouvernance concertée où plusieurs acteurs doivent coopérer. Les responsabilités pour une protection efficace des IIC sont donc partagées entre le ministère en charge du numérique, le ministère en charge de la Sécurité publique, l'Agence des Systèmes d'Information et du Numérique et les autorités des entités sectorielles.

### 8.1 Le ministère en charge du Numérique

Dans le cadre de la mise en œuvre des règles de politique de protection des infrastructures d'information critiques, le ministre chargé du Numérique assure la supervision des actions de l'Etat pour la protection des infrastructures d'information critiques. A ce titre, il est chargé de :

- définir et faire adopter par le Conseil des Ministres, les orientations nationales pour la protection des infrastructures d'information critiques ;
- faire approuver par le Conseil des Ministres la liste des opérateurs d'infrastructures d'information critiques et des infrastructures d'information critiques issue de l'application du cadre de classification des infrastructures d'information ;
- rendre compte périodiquement au Conseil des Ministres de la mise en œuvre des règles de politique de protection des infrastructures d'information critiques ;

- valider les mesures spécifiques proposées par l'Agence des Systèmes d'Information et du Numérique.

### 8.2 L'Agence des Systèmes d'Information et du Numérique

Dans le cadre de la présente politique, l'Agence des Systèmes d'Information et du Numérique assure la coordination technique de sa mise en œuvre. Ainsi, de façon générale, elle est chargée de :

- s'assurer de la mise en œuvre des activités techniques issues de la présente politique ;
- assister les sectoriels dans l'élaboration de leur budget pour la protection des infrastructures d'information critiques relevant de leur secteur ;
- proposer et exécuter le budget commun de l'Etat pour la protection des infrastructures d'information critiques ;
- proposer des mises à jour des règles de politique de protection des infrastructures d'information critiques.

**Sur le plan organisationnel**

- organiser avec les autorités sectorielles l'identification des opérateurs d'infrastructures d'information critiques sous la supervision du ministre chargé du Numérique ;
- veiller à l'application des orientations stratégiques nationales et au suivi de la mise en œuvre des exigences de la politique de protection des infrastructures d'information critiques ;
- veiller à la coordination technique de l'action des autorités publiques qui doivent concourir à la protection des infrastructures d'information critiques;
- participer à la gestion de crise en cas d'incident grave affectant une infrastructure d'information critique ;
- assister et conseiller les opérateurs d'infrastructures d'information critiques pour le renforcement de la sécurité de leurs systèmes d'information ;
- soutenir les activités de recherches scientifiques et techniques dans le domaine de la cybersécurité des secteurs critiques identifiés ;
- mettre en place un canal pour les échanges avec les points focaux désignés par les opérateurs d'infrastructures d'information critiques ;
- contribuer à la coopération internationale en matière de protection des infrastructures d'information critiques transnationales.

### 8.3 Le ministère en charge de la Sécurité publique

Au terme de la présente politique, il est chargé d'organiser l'intervention de l'Etat pour la protection physique des sites des opérateurs d'infrastructures d'information critiques face aux menaces. Cette responsabilité peut sans s'y limiter, prendre la forme d'appui des forces de sécurité publique à la protection de certains sites, de partages d'informations sur certaines menaces.

### 8.4 Les autorités sectorielles

Les autorités des entités sectorielles sont les ministères en charge des secteurs dont relèvent les infrastructures critiques identifiées par le cadre de classification des infrastructures d'information. Dans le cadre de la présente politique de protection des infrastructures d'information critiques, elles :

- contribuent à l'identification des opérateurs d'infrastructures d'information critiques dans leurs secteurs ;
- facilitent les échanges avec les opérateurs d'infrastructures d'information critiques de leurs secteurs, le ministère en charge du Numérique et l'Agence des Systèmes d'Information et du Numérique ;
- facilitent la coopération internationale sur les infrastructures d'information critiques transnationales issues de leurs secteurs ;
- veillent à la mise en application de la politique de protection des infrastructures d'information critiques par les opérateurs d'infrastructures d'information critiques de leurs secteurs respectifs ;
- s'assurent de la disponibilité du budget sectoriel consacré à la protection des infrastructures d'information critiques.

## 9 Obligations des OIIC

Les OIIC sont les premiers responsables de la sécurité de leurs infrastructures d'information. A ce titre, ils ont l'obligation de :

- respecter les mesures qui leur sont prescrites pour renforcer la sécurité physique et la cybersécurité de leurs installations ;
- déclarer rapidement à l' Agence des Systèmes d'Information et du Numérique tout incident pouvant avoir un impact grave sur son système d'information ;
- collaborer avec l'Agence des Systèmes d'Information et du Numérique en cas de nécessité ;
- mettre en place au niveau de leur direction, une organisation destinée à organiser et à prendre en compte la protection de leurs systèmes d'information critiques ;
- mettre en place les ressources nécessaires pour la mise en conformité de leurs structures et systèmes d'information critiques avec les règles de politique de protection des infrastructures d'information critiques ;
- faciliter les missions d'audits de sécurité et de conformité.

Tout opérateur d'infrastructures d'information critiques doit décrire les mesures qu'il met en place en application des mesures de protection qui lui sont imposées dans les documents ci-après, qu'il soumet à l'Agence des Systèmes d'Information et du Numérique :

- une cartographie de son infrastructure d'information critique ;
- une politique de sécurité des systèmes d'information mettant l'accent sur les systèmes d'information et infrastructures critiques pour les services importants qu'il assure ;
- un plan d'actions pour un alignement aux mesures prescrites par les règles de politique de protection des infrastructures d'information critiques.

## 10 Identification des infrastructures d'information critiques et désignation des opérateurs d'infrastructures d'information critiques

### 10.1 Cadre de classification des infrastructures d'information

Il a été élaboré un cadre de classification des infrastructures d'information, développé sous forme d'une méthodologie d'analyse de risques dont l'objectif ultime est d'établir un processus rigoureux pour l'identification des infrastructures d'information critiques. Ledit cadre définit cinq (05) étapes nécessaires pour y parvenir à savoir :

1. identification des secteurs critiques ;
2. identification des sous-secteurs critiques ;
3. identification des interdépendances entre les sous-secteurs ;
4. identification des infrastructures d'information importantes ;
5. identification des infrastructures d'information critiques.

Ces étapes sont validées à la lumière de critères listées en **annexe III**.

### 10.2 Identification des opérateurs d'infrastructures d'information critiques

De manière périodique ou sur la base de la maturité et de l'émergence de nouveaux secteurs d'activités critiques, le ministre chargé du Numérique peut déclencher la démarche de mise à jour par un comité ad hoc, de la liste des opérateurs d'infrastructures d'information critiques et l'introduction en Conseil des Ministres. Ledit comité est composé des représentants du ministère en charge du Numérique, du ministère en charge de la Sécurité publique et de l'Agence des Systèmes d'Information et du Numérique.

Cette liste est déterminée par l'application du cadre de classification des infrastructures d'information. En tout état de cause, elle est revue tous les trois (03) ans.

### 10.3 Désignation des opérateurs d'infrastructures d'information critiques

A l'issue du travail en comité, les opérateurs d'infrastructures d'information critiques concernés reçoivent une première notification de leur statut. Ils disposent d'un délai de trente (30) jours ouvrés à compter de la date de notification pour transmettre leurs observations au ministre chargé du Numérique.

Sur demande du ministre, l'Agence des Systèmes d'Information et du Numérique collecte, évalue les observations, statue techniquement sur les éventuels recours. Elle élabore un rapport technique qu'elle soumet à l'appréciation du ministre chargé du Numérique.

La liste finale est introduite en Conseil des Ministres pour adoption.

## 11 Exigences minimales de sécurité

Certaines exigences de sécurité sont communes et s'imposent à tous les opérateurs d'infrastructures d'information critiques. Ces exigences de sécurité sont listées en annexe I.

Toutefois, en tenant compte du contexte environnemental de chaque opérateur d'infrastructures d'information critiques et sur la base d'une analyse de risque approfondie,

l'Agence des Systèmes d'Information et du Numérique élabore des mesures de protection spécifiques pour chaque opérateur d'infrastructures d'information critiques.

## ANNEXE I : Exigences minimales de sécurité

### 11.1 Gouvernance de la protection

| Code | Exigences de sécurité | Criticité C= Critique N= Normal |
|---|---|---|
| **Gouv-01** | Désigner un point focal au sein de l'opérateur d'infrastructures d'information critiques servant de point de contact entre sa direction et les autorités publiques sur toutes les questions de sécurité numérique. | **C** |
| **Gouv-02** | Mettre en place les ressources nécessaires pour la mise en conformité de leurs structures et systèmes avec les règles de politique de protection des infrastructures d'information critiques. | **C** |
| **Gouv-03** | Définir un modèle d'organisation et mettre en place une organisation pour assurer la protection physique et la cybersécurité des infrastructures d'information critiques de l'opérateur d'infrastructures d'information critiques. Cette organisation transparaît dans les documents ci-après à soumettre à l'Agence des Systèmes d'Information et du Numérique :<br>• une cartographie de son infrastructure d'information critique ;<br>• une politique de sécurité des systèmes d'information mettant l'accent sur les systèmes d'information et infrastructures critiques pour les services importants qu'il assure ;<br>• un plan d'actions pour une mise en conformité avec les règles de politique de protection des infrastructures d'information critiques. | **N** |
| **Gouv-04** | Adresser annuellement à l'Agence des Systèmes d'Information et du Numérique, un rapport sur les incidents, les risques, les menaces, les vulnérabilités identifiés et les principales mesures prises en conséquence. | **C** |

## 11.2 Sécurité physique

| Code | Exigences de sécurité | Criticité C= Critique N= Normal |
|---|---|---|
| **Phys-01** | Sensibiliser et former le personnel de l'opérateur des infrastructures d'information critiques sur les thématiques relatives à la sécurité numérique. | **C** |
| **Phys-02** | Assurer la sécurité des accès aux systèmes d'information critiques : gestion des identités et des droits d'accès ; déployer des dispositifs visant à interdire ou à limiter les accès non autorisés aux systèmes critiques et des dispositifs de détection d'intrusion. | **N** |
| **Phys-03** | Assurer la sécurité face aux risques naturels ou accidentels : dispositifs de prévention et de lutte contre l'incendie ; prévention des inondations, prévention des accidents. | **C** |
| **Phys-04** | Mettre en place des redondances pour les installations ou les systèmes d'alimentation critique. | **C** |
| **Phys-05** | Établir et mettre en œuvre un plan de sécurité de l'opérateur. | **N** |
| **Phys-06** | Faire réaliser un audit périodique de sécurité physique par un fournisseur de services de sécurité numérique qualifié, au moins une fois tous les cinq (5) ans et transmettre la copie du rapport à l'Agence des Systèmes d'Information et du Numérique et au ministère en charge du Numérique. | **C** |

### 11.3 Cybersécurité

| Code | Exigences de sécurité | Criticité C= Critique N= Normal |
|---|---|---|
| **Cy-01** | Mettre en œuvre une démarche d'analyse de risques pour identifier et corriger les principales vulnérabilités pouvant avoir un impact grave sur l'infrastructure critique. | **N** |
| **Cy-02** | Transmettre à l'Agence des Systèmes d'Information et du Numérique une cartographie des réseaux et systèmes d'information critiques et la mettre à jour à chaque changement important. | **C** |
| **Cy-03** | Sensibiliser et former le personnel sur les thématiques liées à la cybersécurité et adapter le message à chaque groupe cible. | **N** |
| **Cy-04** | Appliquer les règles d'hygiène informatique édictées par l'Agence des Systèmes d'Information et du Numérique et publiées sur son site internet. | **C** |
| **Cy-05** | Cartographier la chaîne d'approvisionnement et veiller à sa cyber-hygiène. | **C** |
| **Cy-06** | Traiter les alertes données par le bjCSIRT. | **C** |
| **Cy-07** | Assurer la sécurité des réseaux et des systèmes : règles sur les configurations, le cloisonnement, les accès distants, le filtrage. | **C** |
| **Cy-08** | Assurer la sécurité de l'administration des réseaux et des systèmes : règles sur les comptes et les systèmes d'administration. | **N** |
| **Cy-09** | Assurer la sécurité des données : règles de sauvegarde périodique, mise en place de redondances et de réplication, chiffrement des dispositifs de stockage et des canaux de communication. | **C** |
| **Cy-10** | Assurer la gestion des identités et des accès : règles sur l'identification, l'authentification et les droits d'accès. | **C** |
| **Cy-11** | Assurer la défense des réseaux et des systèmes : règles de détection des incidents de sécurité, journalisation des événements, corrélation et analyse des journaux. | **C** |

| Code | Exigences de sécurité | **Criticité**<br>C= Critique<br>N= Normal |
|---|---|---|
| **Cy-12** | Mettre en place des redondances pour les installations ou les systèmes d'alimentation critique. | **N** |
| **Cy-13** | Établir et mettre en œuvre une politique de sécurité des systèmes d'information et en tenir copie à l'Agence des Systèmes d'Information et du Numérique pour avis. | **N** |
| **Cy-14** | Faire réaliser un audit de sécurité des systèmes d'information par un fournisseur de service de sécurité numérique qualifié au moins une fois tous les trois (03) ans et après chaque incident ou évolution majeure des systèmes d'information. Tenir copie du rapport d'audit à l'Agence des Systèmes d'Information et du Numérique et au ministère en charge du Numérique. | **C** |
| **Cy-15** | Élaborer des plans de continuité et de reprise des activités et les tester régulièrement sur une base annuelle de préférence ou à chaque évolution significative du système d'information. | **C** |
| **Cy-16** | Participer aux sessions d'entraînement et exercices pratiques sur la prise en charge d'incidents de cybersécurité organisés par l'Agence des Systèmes d'Information et du Numérique. | **N** |

**ANNEXE II : Liste des secteurs et sous-secteurs critiques**

| Secteurs | Sous-secteurs |
|---|---|
| 1. Technologies de l'information et de la communication | • la télécommunication<br>• la télédiffusion<br>• l'internet<br>• l'informatique |
| 2. Finances | • le sous-secteur bancaire<br>• le sous-secteur d'assurances<br>• le sous-secteur boursier |
| 3. Energie | • l'énergie électrique (les infrastructures et les installations de transport d'électricité)<br>• le gaz (production, raffinage, traitement, stockage et transmission par pipeline)<br>• le pétrole (production, raffinage, traitement, stockage et transmission par pipeline)<br>• l'énergie renouvelable |
| 4. Eau | • la chaîne de production et de distribution de l'eau<br>• les barrages |
| 5. Services publics | • les activités civiles de l'Etat<br>• les activités fiscales de l'Etat et les finances publiques<br>• les activités de justice<br>• les réseaux E-gouv<br>• les services de la sécurité nationale |
| 6. Transport | • les routes<br>• les chemins de fer<br>• le transport aérien<br>• le transport maritime et fluvial<br>• le transport urbain civil |
| 7. Santé | • la pharmaceutique<br>• l'hospitalisation |
| 8. Le secteur des médias | • la presse écrite et en ligne<br>• la radio diffusion |

## ANNEXE III : Critères de classification des infrastructures d'information

La classification des infrastructures d'information nécessite une vision holistique qui prend en considération tous les effets et tous les potentiels impacts générés lors d'une attaque qui pourrait cibler le cyberespace du Bénin et ses services vitaux. Les impacts politiques et sociaux peuvent être ressentis d'une manière indirecte suite à des incidents touchant l'économie ou la sécurité nationale. Lors d'une cyberattaque sophistiquée, les dégâts directs peuvent être économiques, environnementaux et humains et peuvent engendrer des effets indirects à l'échelle politique et sociale. Cependant, l'identification de la criticité ne dépend pas seulement des effets directs mais aussi des effets indirects.

La démarche d'identification des opérateurs d'infrastructures d'information critiques repose sur les critères pertinents indiqués dans la liste ci-après et tels que spécifiés dans le cadre de classification des infrastructures d'information :

1. public touché (taille de la population touchée) ;
2. impact sur la sécurité nationale ;
3. impact politique ;
4. impact social ;
5. impact sur l'économie ;
6. impact sur les vies humaines ;
7. impact sur la santé publique ;
8. impact environnemental ;
9. contribution à l'économie ;
10. dépendance technologique ;
11. dépendance avec des services critiques.

## ANNEXE IV : Types d'incidents à remonter à l'ASIN

Les incidents de sécurité informatique relatifs à la confidentialité, à l'intégrité ou à la disponibilité des infrastructures d'information critiques sont notifiés à l'Agence des Systèmes d'Information et du Numérique dans un délai de quarante-huit (48) heures après leur détection. Cette obligation concerne aussi les utilisations frauduleuses des systèmes d'information critiques par des acteurs internes ou externes. Toutefois, les incidents de sécurité de poids critiques sont remontés sans délai et dès leur découverte à l'Agence des Systèmes d'Information et du Numérique.

La notification est faite en ligne sur le site internet du bjCSIRT (https://csirt.gouv.bj/), contact : +229 21 36 87 23. La notification précise à minima la nature de l'incident, les détails techniques à disposition, les systèmes et services impactés ainsi que les mesures prises pour contenir l'impact de l'incident et y remédier.

A titre informatif, le bjCSIRT catégorise les incidents (Critique ou Normal) comme décrit dans le tableau ci-dessous et cette répartition sera utilisée pour déterminer les incidents qui seront notifiés par les opérateurs d'infrastructures d'information critiques à l'Agence des Systèmes d'Information et du Numérique et pour lesquels le bjCSIRT apporterait sa contribution à la résolution.

| Classification des incidents | Exemples d'incidents | Description / Explication | Criticité C= Critique N= Normal |
|---|---|---|---|
| Contenus abusifs | Spam | Le spam est un type de communication numérique non désirée et non sollicitée qui est envoyée en masse. Le spam est souvent envoyé par courrier électronique, mais il peut aussi être distribué par des messages texte, des appels téléphoniques ou des médias sociaux. | N |
| | Discours de haine ou préjudiciable | Discrédit ou discrimination à l'égard de quelqu'un (par exemple, cyber-harcèlement, racisme et menaces à l'encontre d'une ou plusieurs personnes). | N |
| | Pédo-pornographie/ Violence sexuelle/... | Pornographie enfantine, apologie de la violence, ... | N |
| Code malveillant | Virus/ransomware | Logiciel ou bout de code inclus ou inséré intentionnellement dans un système dans un but nuisible ou malveillant. Il se réplique automatiquement et s'infiltre subrepticement dans votre appareil sans votre autorisation à la suite d'une action de la part de l'utilisateur. | C |
| | Ver | | C |
| | Cheval de Troie | | C |
| | Logiciel espion | | C |
| | Rootkit | | C |

| Classification des incidents | Exemples d'incidents | Description / Explication | Criticité C= Critique N= Normal |
|---|---|---|---|
| Collecte d'informations | Scanning | Attaques qui envoient des requêtes à un système pour découvrir ses points faibles ou vulnérables. Il s'agit également d'un certain type de processus de test visant à recueillir des informations sur les hôtes, les services et les comptes.<br>Exemples : Interrogation du DNS, ICMP, SMTP (EXPN, RCPT...), balayage de ports. | N |
| | Sniffing | Le reniflage est un processus de surveillance et de capture de tous les paquets de données passant par un réseau donné.<br>Les attaquants utilisent les renifleurs pour capturer des paquets de données contenant des informations sensibles telles que des mots de passe, des informations de compte, etc. | C |
| | Social Engineering | Collecte d'informations sensibles auprès d'un individu d'une manière non technique (par exemple, mensonges, ruses, pots-de-vin ou menaces). | N |
| Tentatives d'intrusion | Exploitation de vulnérabilités connues | Tentative de compromettre un système ou de perturber un service en exploitant ses vulnérabilités avec un identifiant standardisé tel qu'un CVE (par exemple, dépassement de tampon, porte dérobée, cross site scripting, etc.). | C |
| | Tentatives de connexion | Tentatives de connexion multiples (deviner / craquer les mots de passe, attaque par force brute). | N |

| Classification des incidents | Exemples d'incidents | Description / Explication | Criticité C= Critique N= Normal |
|---|---|---|---|
| | Attaque basée sur une nouvelle signature | Une tentative utilisant un exploit inconnu. | C |
| Intrusions | Compromission de comptes privilégiés (Administrateurs) | Cette catégorie d'incidents regroupe toute compromission réussie d'un système ou d'une application (service). Cela peut être causé via accès distant par l'exploitation d'une vulnérabilité connue ou nouvelle, mais aussi par un accès local non autorisé. Elle peut être le fait d'un réseau de zombie (botnet). | C |
| | Compromission de comptes non privilégiés | | N |
| | Compromission d'application | | C |
| Disponibilité | DoS | Les incidents sur la disponibilité d'un système regroupent les attaques par lesquelles un système est inondé de tant de requêtes que les opérations légitimes sont retardées ou que le système tombe en panne.<br>Les exemples de DoS sont les inondations de paquets de types ICMP et SYN, les attaques Teardrop et le mail-bombing.<br>Les attaques DDoS sont souvent basées sur des attaques DoS provenant de réseau de zombies (botnets), mais il existe aussi d'autres scénarios comme les attaques par amplification DNS. | C |
| | DDoS | | C |
| | Sabotage | | C |
| | Panne (pas de malveillance) | | N |

| Classification des incidents | Exemples d'incidents | Description / Explication | Criticité C= Critique N= Normal |
|---|---|---|---|
| | | Cependant, la disponibilité peut également être affectée par des actions locales (destruction, interruption de l'alimentation électrique, etc.) - ou par un cas de force majeure, des défaillances spontanées ou une erreur humaine, sans qu'il y ait malveillance ou négligence grave. | |
| Sécurité du contenu de l'information | Accès non autorisé à l'information | Outre un abus local des données et des systèmes, la sécurité des informations peut être mise en danger par une compromission réussie d'un compte ou d'une application. En outre, des attaques sont possibles pour intercepter et accéder aux informations pendant leur transmission (écoute téléphonique, usurpation d'identité ou détournement). Une erreur humaine/de configuration/de logiciel peut également en être la cause. | C |
| | Modification non autorisée d'information | | C |
| Fraude | Utilisation non autorisée des ressources | L'utilisation des ressources à des fins non autorisées, y compris par les entreprises à but lucratif (par exemple, l'utilisation du courrier électronique pour participer à des chaînes de lettres ou à des systèmes pyramidaux illégaux). | N |
| | Usurpation d'identité | Type d'attaques dans lesquelles une entité prend illégitimement l'identité d'une autre afin d'en tirer profit ou à des fins malveillantes. | N |
| | Hameçonnage | Attaques consistant pour un attaquant à se faire passer pour une autre entité connue de la victime afin de persuader cette dernière à révéler un justificatif d'identité privée ou une information sensible. | N |

| **Classification des incidents** | **Exemples d'incidents** | **Description / Explication** | **Criticité** C= Critique N= Normal |
|---|---|---|---|
| Autres | - | Tous les incidents qui n'entrent pas dans l'une des catégories données énumérées ci-dessus doivent être mis dans cette catégorie. | N |