AECK/WG

RÉPUBLIQUE DU BÉNIN

Fraternité-Justice-Travail

PRÉSIDENCE DE LA RÉPUBLIQUE

DÉCRET N° 2021 – 550 DU 27 OCTOBRE 2021
portant approbation des règles de Politique de Sécurité des Systèmes d'Information de l'État 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 ;

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° 2018-529 du 14 novembre 2018 portant approbation des statuts de l'Agence nationale de la Sécurité des Systèmes d'Information ;

sur proposition du Ministre du Numérique et de la Digitalisation,

le Conseil des Ministres entendu en sa séance du 27 octobre 2021,

DÉCRÈTE

Article premier

Sont approuvés, comme ci-joint en annexe au présent décret, les règles de politique de sécurité des systèmes d'information de l'État.

Article 2

Les règles de politique de sécurité des systèmes d'information de l'État s'appliquent :

- à tous les systèmes d'information des administrations publiques y compris les établissements publics et les sociétés d'État ;
- au personnel ou organismes tiers ayant une responsabilité dans les systèmes d'information des institutions et structures ci-dessus indiquées ;

- aux utilisateurs des systèmes d'information de l'État, aux personnes chargées de leur gestion et aux personnes chargées de leur sécurité.

Article 3

Sont exclus du champ d'application des règles de politique de sécurité des systèmes d'information de l'Etat :

- les systèmes d'information soumis au régime de la loi relative au secret de la défense nationale et,
- les organismes privés mettant en œuvre leurs propres systèmes d'information.

Article 4

Les institutions et structures de l'État indiquées à l'article 2 du présent décret disposent d'un délai d'un (01) an à compter de la date d'entrée en vigueur du présent décret pour définir un plan d'actions pour la mise en œuvre de la politique.

Elles devront être en conformité totale avec les règles de politique de sécurité des systèmes d'information de l'État dans les trois (03) années suivant son adoption.

L'Agence nationale de la Sécurité des Systèmes d'Information évalue chaque année, la mise en œuvre de la Politique de Sécurité des Systèmes d'Information et en rend compte au ministre chargé du Numérique.

Article 5

Le Ministre du Numérique et de la Digitalisation et le Ministre de l'Économie et des Finances sont chargés, chacun en ce qui le concerne, de l'application du présent décret.

Article 6

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 27 octobre 2021

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

Patrice TALON

Le Ministre de l'Économie
et des Finances,

Romuald WADAGNI
Ministre d'État

La Ministre du Numérique
et de la Digitalisation,

Aurelie I. ADAM SOULE ZOUMAROU

AMPLIATIONS : PR 6 ; AN 4 ; CC 2 ; CS 2 ; CES 2 ; HAAC 2 ; HCJ 2 ; MEF 2 ; MND 2 ; AUTRES MINISTÈRES 21 ; SGG 1 ; JORB 1.

ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DE L'ETAT (PSSIE)

Version finale
Date de révision : 01.07.2021

TABLE DES MATIERES

1. PRÉAMBULE

1.1. Contexte

L'ambition du Gouvernement du Bénin est de positionner le pays comme la référence en Afrique de l'Ouest en matière de plateformes de services numériques à l'horizon 2021, et de faire des technologies de l'information et de la communication l'un des principaux leviers de son développement socio-économique.
Pour soutenir cette ambition, le Bénin a adopté sa Stratégie Nationale de Sécurité Numérique (SNSN) qui confirme sa volonté de garantir un cyberespace sécurisé pour une économie numérique florissante.

Cette stratégie qui se veut ambitieuse a inscrit la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) comme un pilier de la protection des infrastructures et systèmes d'information de l'Etat. La PSSIE définit les bases de la confiance des utilisateurs dans les usages qu'ils font des systèmes d'information de l'Etat. Elle constitue le socle de base des mesures techniques, organisationnelles, physiques et règlementaires à mettre en œuvre par les entités étatiques pour protéger les systèmes d'information qu'ils déploient dans leur secteur d'activité.

1.2. Enjeux

Les enjeux de la PSSIE résident dans l'engagement de l'Etat à protéger les ressources informationnelles des entités concernées par les dispositions et règles de la présente politique. Ainsi, il s'agit pour l'Etat de positionner la PSSIE au rang des axes stratégiques en matière de sécurité et de protection des systèmes d'information. Dans ce sens, la PSSIE vise sur le plan national et de manière directe à :

- contribuer à la promotion des bonnes pratiques de sécurité au sein des entités de l'Etat ;
- harmoniser la protection des infrastructures des systèmes d'information à l'échelle de l'Etat;
- favoriser la confiance des utilisateurs dans les systèmes d'information de l'Etat ;
- définir le cadre relationnel entre l'ANSSI et les entités de l'Etat ;
- contribuer à l'économie numérique au Bénin en favorisant la consommation des services et produits de confiance numérique.

La PSSIE contribue aussi à promouvoir l'image du Bénin à l'international et à le démarquer dans la sous-région ouest africaine.

1.3. Risques

Le développement de l'économie numérique s'appuyant en grande partie sur les technologies de l'information et de la communication, il n'en demeure pas moins que ce développement est source de cybermenaces. Au Bénin, les cybermenaces les plus importantes identifiées au niveau du cyberespace et qui touchent particulièrement les systèmes d'information des entités de l'Etat sont répertoriées comme suit :

- les cyber-attaques : attaques contre les sites web des institutions de l'Etat, les infections virales, la prise de contrôle à distance des systèmes d'information et leur usage illégitimes par des réseaux criminels nationaux ou étrangers ;
- le vol de données sensibles détenues par les entités de l'Etat ;
- les attaques contre les infrastructures critiques pouvant entraîner une atteinte à la sécurité nationale ;
- le faible niveau de sensibilisation des utilisateurs des systèmes d'information constituant les relais à partir desquels les cybercriminels réussissent souvent leurs attaques.

1.4. Objectifs de la PSSIE

Il s'avère nécessaire de définir et de mettre en œuvre les actions permettant d'apporter une réponse commune et harmonisée aux risques pesant sur les systèmes d'information de l'Etat.
Les principes directeurs et règles de la PSSIE visent donc à encadrer et à orienter l'ensemble des actions permettant de garantir pour les systèmes d'information de l'Etat :

- la disponibilité, qui se définit comme étant la propriété pour un système d'information à être accessible et utilisable à la demande par les utilisateurs autorisés ;
- l'intégrité, qui se définit comme étant la propriété d'un système d'information de ne permettre que les modifications autorisées ;
- la confidentialité, qui se définit comme la propriété pour un système d'information d'être accessible seulement à des utilisateurs ou autres systèmes d'information autorisés ;
- la traçabilité qui est la propriété pour un système d'information de permettre la vérification d'une action ou d'un événement à des fins d'analyse et d'en retrouver l'auteur.

La PSSIE vise donc à offrir des mesures de base pour gérer les risques inhérents aux usages qui sont faits des systèmes d'information de l'Etat. Son adoption par les entités de l'Etat permettra d'améliorer leur niveau de maturité en matière de sécurité de l'information.

1.5. Démarche d'élaboration

Pour établir les règles de la PSSIE, l'ANSSI s'est inspirée de la norme ISO/CEI 27001 : 2013 ainsi que la norme ISO/CEI 27005 de management des risques et s'est basée sur les résultats des différents ateliers organisés au profit des parties prenantes identifiées. Ces ateliers se sont déroulés courant le mois d'octobre 2020. Les activités qui ont été réalisées pour parvenir à la présente version comprennent :

- analyse du contexte législatif et réglementaire en République du Bénin portant sur la sécurité des systèmes d'information ;
- compréhension du fonctionnement des systèmes d'information de l'Etat et des administrations béninoises et détermination du domaine d'application de la PSSIE ;
- analyse sommaire des risques auxquels sont exposés les systèmes d'information de l'Etat ;
- benchmark international sur les approches régaliennes d'autres pays en matière de sécurité des systèmes d'information ;
- formalisation des objectifs et des règles de sécurité applicables ;
- organisations de plusieurs sessions du Comité de Pilotage du projet.

3. DISPOSITIONS GÉNÉRALES

3.1. Définitions

ANSSI Agence Nationale de la Sécurité des Systèmes d'Information

ASSI Agence des Services et Systèmes d'Information

APDP Autorité de Protection des Données à caractère Personnel

bjCSIRT Equipe nationale de réponse aux incidents de sécurité informatique

FSSN Fournisseur de Services de Sécurité Numérique

FSSNQ Fournisseur de Services de Sécurité Numérique Qualifié

Information Tous signes, tous signaux, tous écrits, toutes images, tous sons ou tous enregistrements de toutes natures pouvant être véhiculés par des procédés de communications électroniques

Information sensible Toutes les données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, à la génétique, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives

PKI Public Key Infrastructure (Infrastructure à clé publique)

Politique Intentions et orientations globales telles qu'exprimées formellement par l'Etat

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

RSSI Responsable de la Sécurité du Système d'Information

Sécurité du système d'information Ensemble des mesures techniques et non techniques (organisationnelles et humaines) de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises

Système d'Information (SI) 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

TSA Timestamp Authority (Autorité de certification des temps)

3.2. Champ d'application

La **PSSIE** s'applique :

- à tous les systèmes d'information sans exception des administrations publiques (Présidence de la République, Ministères, Institutions de la République, Agences ou structures sous tutelles) y compris les établissements publics et les sociétés d'Etat. Ces administrations sont dénommées « entités » dans le reste du document ;
- au personnel ou aux organismes tiers (prestataires ou sous-traitants) ayant une responsabilité dans le système d'information desdites entités ;
- aux utilisateurs des systèmes d'information de l'Etat, aux personnes chargées de leur gestion et aux personnes chargées de leur sécurité.

La **PSSIE** ne s'applique pas :

- aux systèmes d'information pris en compte par la Loi n° 2019-05 portant organisation du secret de la défense nationale en République du Bénin. Il appartient aux responsables des entités concernées d'assurer une cohérence entre les dispositions de la présente PSSIE et la réglementation relative à la protection des informations classifiées de défense. ;
- aux organismes privés mettant en oeuvre leurs propres systèmes d'information (banques, opérateurs télécoms, ...). La PSSIE peut toutefois servir de source d'inspiration pour ces organismes qui sont libres de l'adopter ou non.

3.3. Cadre réglementaire

La PSSIE est en conformité avec les dispositions légales et réglementaires applicables au Bénin. En conséquence, les règles qui y sont inscrites tiennent compte de la Loi n°2017-20 du 20 Avril 2018 portant code du numérique en République du Bénin et de la loi n°2009-09 portant protection des données à caractère personnel 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.

3.4. Principes de base

La PSSIE s'appuie sur des principes directeurs ci-dessous, qui sont en phase avec la Stratégie Nationale de Sécurité Numérique.

	Clauses	Exigence
P1	Respect des exigences légales, réglementaires et contractuelles	L'entité établit un registre des textes juridiques qui sont applicables à ses systèmes d'information et met en oeuvre des procédures de conformitéa à ces textes.
P2	Structure organisationnelle	L'entité met en place une structure organisationnelle dédiée à la sécurité du SI impliquant à minima les acteurs clés de la mise en oeuvre de la PSSIE.
P3	Gestion des risques de Sécurité des SI	L'entité met en place un dispositif de gestion des risques liés à la sécurité des SI en s'appuyant sur un processus régulier d'identification, d'appréciation et de traitement des risques.
P4	Politique de sécurité spécifique	L'entité complète la présente PSSIE en adoptant suivant les résultats de son appréciation des risques, des politiques de sécurité spécifiques adaptées à son contexte (infrastructure d'importance vitale, externalisation des SI, interconnexions avec d'autres SI, ...). L'entité pourra s'inspirer des guides et publications de l'ANSSI.
P5	Plan d'actions sécurité	Pour la mise en oeuvre de la PSSIE, l'entité définit un plan d'actions comprenant des mesures à la fois organisationnelles et techniques et qui tiennent compte des impacts sur les activités ainsai que des moyens financiers et humains à mettre en oeuvre.
P6	Budgétisation de la sécurité	L'entité quantifie et planifie le budget nécessaire à la mise en conformité avec la PSSIE.
P7	Formation et sensibilisation	L'entité définit et déploie un programme de formation et de sensibilisation en matière de sécurité des systèmes d'information au profit du personnel, notamment les administrateurs informatiques et les utilisateurs des systèmes d'information.

3.5. Interactions entre les entités, l'ANSSI et le Ministère en charge de la Digitalisation dans le cadre de la mise en œuvre de la PSSIE

Dans le cadre de la mise en œuvre de la PSSIE et sous la supervision technique du Ministère en charge du Numérique et de la Digitalisation, l'ANSSI:

- apporte son concours aux entités dans l'assimilation des règles de la présente politique ;
- diffuse aux entités des informations de veille sécurité leur permettant d'évaluer les risques ;
- effectue un contrôle général de la mise en oeuvre de la présente politique et en rend compte au Ministre du Numérique et de la Digitalisation ;
- élabore des normes et guides afin de faciliter la mise en oeuvre de la présente politique par les entités ;
- évalue la mise en oeuvre de la PSSIE et propose les évolutions de celle-ci ;
- appuie les entités dans le cadre de l'élaboration de leur PSSI spécifique ;
- co-organise la conférence des DSI avec l'ASSI en faisant participer les RSSI des administrations et structures publiques.

Les entités :

- organisent et coordonnent l'application de la PSSIE au sein de leurs structures;
- élaborent leur PSSI spécifique basée sur la PSSIE ;
- créent et mettent en place la fonction RSSI au sein de leur organisation ;
- opérationnalisent la fonction RSSI et allouent le budget approprié pour l'exécution de son plan d'actions ;
- sollicitent l'ANSSI en cas de nécessité eu égard aux termes de la PSSIE ;
- diligentent des contrôles internes pour s'assurer de la mise en œuvre des règles de la PSSIE et rendent compte à l'ANSSI ;
- remontent les incidents significatifs de sécurité à l'ANSSI ;
- se prêtent aux missions d'audit organisées par l'ANSSI.

3.6. Mise en application de la PSSIE

La PSSIE définit les règles qui sont des exigences minimales obligatoires et des recommandations (formulées en caractère italique) visant à aider les entités à implémenter les règles. L'application des recommandations est libre. Afin d'aider les entités à prioriser les actions à mettre en oeuvre, à chaque règle est associé un poids marqué par un code couleur de la mesure correspondante :

- en **bleu gras** les règles de sécurité de poids critique identifiables par la lettre (**C**)
- en **noir gras** les règles de sécurité de poids normal identifiables par la lettre (**N**)

Il peut être nécessaire, dans certains cas spécifiques, de déroger à des règles énoncées par la PSSIE. Il appartient alors au Management de l'entité concernée de les substituer formellement par des règles particulières. Pour chacune de ces règles, la dérogation, motivée, justifiée et documentée, doit être expressément accordée par le Management de l'entité concernée. La décision de dérogation accompagnée de la justification est tenue à la

3.7. Date d'entrée en vigueur

La PSSIE entre en vigueur à partir de la date de son adoption par le Conseil des Ministres. L'ANSSI organisera des ateliers dédiés aux différents acteurs en vue de la vulgarisation et de la sensibilisation à la PSSIE.

3.8. Dispositions transitoires

Les entités disposent d'un délai d'un (01) an à compter de la date d'entrée en vigueur de la PSSIE pour définir un plan d'actions de mise en oeuvre de ladite politique.
Les entités devront être en conformité totale avec la PSSIE dans les trois (03) années suivant son adoption et sa publication.

3.9. Evolution de la PSSIE

L'ANSSI élabore les évolutions de la PSSIE, en liaison avec l'ASSI et les entités, en prenant en compte :

- des évolutions des contextes organisationnel, juridique, réglementaire et technologique ;
- des résultats des missions de contrôle de sécurité des entités ;
- de l'évolution des menaces et les retours d'expérience des traitements d'incidents ;
- des demandes de dérogation centralisées par l'ANSSI et émanant des entités.

4. OBJECTIFS ET RÈGLES DE SÉCURITÉ

4.1. Organisation de la sécurité des systèmes d'information

Objectif n°1
Etablir un cadre de gestion pour engager, puis vérifier la mise en oeuvre et le fonctionnement de la sécurité des systèmes d'information au sein de l'entité.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ORG-01	Fonction sécurité	**Règle :** Chaque entité est tenue de désigner un RSSI dont les tâches sont détaillées dans une fiche de poste. Le RSSI fait valider les mesures d'application de la PSSIE par son Management et veille à leur application au sein de l'entité. **Recommandation :** Eu égard à la nature de sa mission, et afin de le doter des pouvoirs et moyens requis, il est recommandé de rattacher le RSSI à un responsable de niveau direction. L'entité peut au besoin recourir aux services d'un FSSNQ pour jouer le rôle de RSSI.	C
ORG-02	Coordination de la sécurité	**Règle :** L'entité crée un comité sécurité des systèmes d'information ou toute autre structure organisationnelle constituée de responsables seniors. Ce comité pilote et coordonne le déploiement de la PSSIE au niveau de l'entité. Ses missions, sa composition et son mode de fonctionnement doivent être détaillés dans une note de service. **Recommandation :** Afin que ce comité soit le plus représentatif possible, il est recommandé qu'il soit élargi aux fonctions de direction en charge des ressources humaines, des ressources financières, des services généraux et des services juridiques.	N
ORG-03	Séparation des tâches	**Règle :** L'administration des différents composants du système d'information (systèmes d'exploitation, bases des données, équipements réseau, ...) doit être cloisonnée et les accès des administrateurs informatiques doivent respecter ce cloisonnement, chacun étant dans l'impossibilité d'accéder à un domaine qui n'est pas le sien. **Recommandation :** Pour garantir la séparation des tâches au sein des fonctions en charge de l'administration des systèmes d'information, il est recommandé de définir et de maintenir une matrice des fonctions incompatibles et une procédure de contrôle compensatoire des activités des administrateurs lorsqu'il est impossible de séparer certaines tâches.	C

ORG-04	Responsabilités des administrateurs informatiques	**Règle :** L'entité doit encadrer, d'un point de vue sécurité, l'activité des administrateurs informatiques en établissant une charte administrateur indiquant les responsabilités et les limites de la fonction « administrateur » en matière de sécurité SI.	**C**
ORG-05	Relations avec les autorités compétentes en sécurité SI	**Règle :** L'entité doit entretenir des relations étroites avec l'ANSSI, autorité compétente en matière de sécurité des SI au plan national. Elle fournit à l'ANSSI les coordonnées du RSSI en vue des échanges d'informations autour de la sécurité (veille, incidents de sécurité, aspects liés au contrôle, ...).	**N**
ORG-06	Relations avec les groupes de spécialistes en sécurité SI	**Règle :** L'entité doit définir une procédure de veille permettant au personnel en charge de la sécurité du SI d'entretenir des contacts particuliers avec un cercle professionnel élargi pouvant comprendre les services spécialisés en veille sécurité, les cabinets de conseils, les éditeurs de solutions de sécurité, les associations professionnels, ...	**C**

4.2. Sécurité des ressources humaines

Objectif n°2
Faire des ressources humaines, un maillon fort de la sécurité des systèmes d'information.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
RH-01	Sélection des candidats	**Règle :** Le recrutement des rôles de confiance (administrateurs bases de données, systèmes, réseau, consultants, auditeurs, ...) devra faire l'objet de vérifications sécuritaires approfondies, dans le strict respect du cadre juridique applicable au Bénin, afin de garantir la probité des postulants. **Recommandation :** L'entité peut procéder à des vérifications portant sur le casier judiciaire, les contrôles de référence, l'authenticité des diplômes et certifications professionnelles, les réseaux sociaux, ...	C
RH-02	Engagement sécurité	**Règle :** Tout personnel embauché (interne, partenaire ou tiers) destiné à manipuler un composant du système d'information, reçoit et signe une charte, opposable juridiquement, récapitulant les mesures pratiques d'utilisation du SI. Il doit signer un « accord de non-divulgation » dès son entrée en fonction. **Recommandation :** Lorsque cela est administrativement faisable, il est recommandé de faire modifier le règlement intérieur de l'organisme pour inclure les dispositions applicables en matière de sécurité du SI (PSSI spécifique, respect des textes règlementaires applicables, sanctions en cas de violation des règles de sécurité, ...).	C
RH-03	Intégration des nouvelles recrues	**Règle :** Le circuit d'intégration des nouvelles recrues au sein de la structure d'accueil de l'entité doit prévoir une étape de formation aux outils de travail, aux procédures et pratiques de sécurité en vigueur.	N
RH-04	Sensibilisation du personnel	**Règle :** L'entité doit dispenser régulièrement et au moins deux fois l'an, au profit du personnel, des formations de sensibilisation sur les règles d'hygiène pour une sécurité numérique améliorée dont le contenu sera adapté au profil des utilisateurs (utilisateurs sédentaires, itinérants, administrateurs, fournisseurs, ...). Ces formations doivent faire l'objet d'évaluation des acquis par les utilisateurs.	C

RH-05	Mouvement du personnel	**Règle :** Une procédure permettant de gérer les mobilités et les départs des collaborateurs doit être formalisée et appliquée strictement. Cette procédure doit couvrir au minimum l'adaptation ou la suspension des accès logiques et physiques, le retrait des actifs SI, la passation des consignes et affaires en cours, ... **Recommandation :** Il est fortement recommandé que les procédures de gestion de la mobilité et des départs prescrivent les délais de retrait des accès et des actifs suivant la nature du mouvement (changement d'entité, départ à l'initiative de l'employé, à l'initiative de l'employeur, ...).	**N**
RH-06	Mesures disciplinaires	**Règle :** L'entité doit prévoir les sanctions applicables en cas de violation de la politique de sécurité du système d'information en vigueur. Les utilisateurs sont informés de ces sanctions de manière formelle.	**N**

4.3. Gestion des actifs du système d'information

Objectif n°3

Identifier les actifs du système d'information de l'entité et s'assurer que les responsabilités sont définies pour la protection des actifs.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ACT-01	Inventaire des actifs SI	**Règle :** Chaque entité établit et maintient à jour un inventaire des actifs du système d'information (matériels, logiciels, réseaux, locaux informatiques...) sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire doit être certifié sur une base annuelle à minima.	C
ACT-02	Responsabilités sur les actifs	**Règle :** A chaque actif SI identifié, l'entité doit s'assurer qu'un responsable est désigné pour en assurer la sécurité.	C
ACT-03	Usage correct des actifs SI	**Règle :** L'entité doit rédiger et diffuser une charte d'utilisation des systèmes d'information à tous les utilisateurs des actifs du SI. L'entité doit s'assurer que les termes de ladite charte sont compris par les utilisateurs.	N

Objectif n°4

Identifier la sensibilité des actifs du système d'information pour permettre aux utilisateurs d'en faire un bon usage.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ACT-04	Sensibilité des actifs SI	**Règle :** La sensibilité de tout actif SI identifié doit être évaluée suivant une grille de classification qui fixe les niveaux de sensibilité en considérant les critères de disponibilité, d'intégrité et de confidentialité. Cette sensibilité est réévaluée au moins une fois sur un cycle de trois ans à l'échelle de l'entité. **Recommandation :** Il convient de s'appuyer sur le cadre de classification des SI de l'ANSSI au cas où l'entité se trouve être un opérateur d'infrastructure d'information critique.	C
ACT-05	Marquage des actifs SI sensibles	**Règle :** L'entité doit procéder au marquage physique des actifs SI matériels stockant des données sensibles ou vitales afin d'attirer l'attention des utilisateurs sur la sensibilité desdits actifs.	C

Objectif n°5

Maîtriser la sécurité du cycle de vie des actifs S.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ACT-06	Cycle de vie des actifs SI	**Règle :** L'entité définit des procédures encadrant le cycle de vie sécurisé des actifs SI depuis leur acquisition jusqu'à leur mise au rebut en passant par leur utilisation et leur maintenance.	**C**

Objectif n°6

Sécuriser les informations qui sont stockées sur les supports numériques.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ACT-07	Chiffrement des supports numériques	**Règle :** Les supports numériques stockant des données sensibles doivent être chiffrés. **Recommandation :** Il est recommandé de recourir aux outils de chiffrements agréés par l'ANSSI.	**C**
ACT-08	Supports physiques en transit	**Règle :** L'entité doit élaborer et appliquer une procédure permettant de gérer les mouvements de supports stockant des données. Cette procédure doit garantir la traçabilité du mouvement des supports et leur protection durant le transit.	**C**
ACT-9	Réforme (cession ou vente) des passifs du SI / Mise au rebut	**Règle :** L'entité doit s'assurer que les matériels et équipements informatiques éligibles aux réformes sont proprement décommissionnés. La mise au rebut des supports physiques numériques (CD, DVD, disque dur, etc.) ne pourra se faire qu'une fois les données qui y sont stockées sont détruites de manière sécurisée. Une procédure d'effacement sécurisée des données doit être mise en place.	**N**

4.4. Contrôle d'accès logique au système d'information

Objectif n°7
Limiter l'accès aux systèmes d'information aux seules personnes autorisées.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
CAL-01	Politique de contrôle d'accès	**Règle :** Un document de politique de contrôle d'accès logique doit être établi au sein de l'entité en prenant en compte, à minima, la définition des identités, la standardisation des profils d'habilitation, la normalisation des identifiants, la gestion des autorisations, les conditions d'accès au SI, délais de validité des comptes, des sessions, ...	C
CAL-02	Identifiant utilisateur	**Règle :** Chaque utilisateur interne ou externe à l'entité, permanent ou temporaire, accédant au système d'information doit être reconnu par une identité unique et normée. L'utilisation par plusieurs personnes d'un même identifiant individuel est strictement interdite.	C
CAL-03	Identifiant administrateur	**Règle :** Les identifiants « administrateurs » donnant accès aux composants techniques ou logiques des systèmes d'information (serveurs, équipements de communication, paramètres techniques ou de sécurité) doivent être distincts des identifiants « utilisateurs » attribués au personnel assurant l'administration desdits systèmes.	C
CAL-04	Authentifiant utilisateur	**Règle :** Chaque utilisateur accédant au système d'information doit prouver son identité à l'aide d'un authentifiant basé sur ce qu'il connaît (code secret). La procédure de fourniture d'un authentifiant à un utilisateur (première attribution, modification, remplacement après oubli ou perte, ...) doit en garantir la **confidentialité** (vérification systématique de l'identité du demandeur et du destinataire à partir d'éléments personnels, fiables et précis).	C
CAL-05	Authentifiant administrateur	**Règle :** Les identifiants permettant l'administration des SI (serveurs, bases de données, équipements réseaux, ...) doivent être placés sous séquestre dans un endroit sécurisé à l'instar d'un coffre-fort. L'entité définira une procédure de gestion des accès de ces identifiants.).	C

CAL-06	Enregistrement et désinscription des utilisateurs	**Règle :** Une procédure formelle de création et de suspension des identifiants doit être définie et appliquée au sein de l'entité. Ladite procédure devra inclure, à minima, les actions suivantes : création d'identifiants uniques, détection et suppression périodique des identifiants redondants, suppression ou blocage immédiat des droits d'accès des utilisateurs qui ont changé de rôle ou de fonction ou qui ont quitté l'entité.	C
CAL-07	Maîtrise des accès utilisateurs	**Règle :** Une procédure formelle de création, de revue et de suspension des droits d'accès aux SI doit être définie et appliquée au sein de l'entité. Ladite procédure devra inclure, à minima, les actions suivantes : demande de droits d'accès d'un utilisateur, chaine de validation de la demande ; octroi, engagement de l'utilisateur, mise en service des droits d'accès, revue périodique de l'utilisation des droits, suspension, ...	C
CAL-08	Politique de mot de passe	**Règle :** L'entité doit définir et implémenter au sein de ses systèmes d'information une politique de gestion des mots de passe utilisateur (complexité, durée de vie minimale et maximale des mots de passe, antériorité des mots de passe, ...).	C

4.5. Sécurité physique des locaux abritant les actifs SI

Objectif n°8

Empêcher tout accès physique non autorisé, tout dommage ou toute intrusion dans les environnements des SI.

Code	Exigences spécifiques	Règles / Recommandations	**Criticité** C = Critique N= Normal
PHY-01	Périmètre de sécurité	**Règle :** Tous les équipements qui sont répertoriés comme importants ou vitaux pour l'entité doivent être installés dans des locaux sûrs. Ces locaux doivent être protégés contre l'accès de personnes non autorisées et donc a fortiori aux personnes étrangères.	C
PHY-02	Contrôle physique des accès du personnel	**Règle :** Seules les personnes autorisées à pénétrer dans les locaux abritant les SI de l'entité doivent disposer de droits d'accès physiques permanents. L'entité définira à cet effet une procédure de gestion des habilitations physiques encadrant l'octroi, la revue et la suspension desdites habilitations.	C
PHY-03	Locaux sensibles	**Règle** : L'entité doit implémenter un système de contrôle d'accès individualisé aux locaux sensibles permettant de garantir la précision de la traçabilité des accès (date, heure, ...).	C
PHY-04	Accès des visiteurs	**Règle :** L'entité doit définir une procédure formelle d'encadrement des visites aux locaux abritant les actifs SI (identification du visiteur, contrôle d'identité, traçabilité de l'accès, ...).	C
PHY-05	Protection des ports physiques d'accès au réseau	**Règle :** Tout accès réseau installé dans une zone d'accueil du public (ou à usage public) doit être filtré ou isolé du réseau informatique privé de l'entité.	C
PHY-06	Gestion des clés physiques des locaux	**Règle :** Pour des raisons de continuité de service, l'usage des clés est autorisé pour l'accès aux locaux abritant les actifs SI. Une procédure devra être formalisée pour la protection et l'utilisation sécurisée des clés d'accès aux locaux abritant les	C
PHY-07	Travail dans les locaux abritant les actifs SI	**Règle :** L'entité doit rédiger et afficher dans tous les locaux abritant les actifs SI des consignes de sécurité destineés au personnel qui exploite ces locaux.	C

4.6. Protection du matériel

Objectif n°9
Empêcher la perte, l'endommagement, le vol ou la compromission des actifs

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
PHY-08	Emplacement du matériel	**Règle :** Les matériels sensibles sont installés dans des locaux dédiés munis de système de vidéosurveillance, protégés contre l'accès non autorisé, l'incendie et les infiltrations d'eau (par des mécanismes de contrôles et de détection tels que verrous, alarmes) et munies des servitudes nécessaires (alimentation convenablement secourue, climatisation). **Recommandation :** Il est vivement recommandé de stocker les matières dangereuses ou combustibles à une distance suffisante des locaux sensibles ainsi que le matériel de secours et les supports de sauvegarde pour éviter les effets dominos.	C
PHY-09	Services généraux	**Règle :** L'ensemble des matériels sensibles doit être protégé contre les coupures de courant par un onduleur ou un groupe électrogène.	C
PHY-10	Sécurité du câblage réseau	**Règle :** L'ensemble des câbles réseaux doit être correctement étiqueté, c'est-à-dire aux deux extrémités. L'entité doit documenter le plan de câblage du réseau informatique et s'assurer que le câblage réseau est à l'abri des endommagements (travaux de voierie, ...).	C
PHY-11	Maintenance du matériel	**Règle :** Pour les actifs SI vitaux, un contrat de maintenance doit être conclu avec un délai d'intervention ou de remplacement garanti, compatible avec les besoins de disponibilité et d'intégrité de ces actifs.	C
PHY-12	Sortie du matériel	**Règle :** Aucun matériel contenant des données de l'entité ne doit sortir hors de ses locaux sans autorisation préalable dûment signée par les responsables habilités. L'entité encadre cette mesure par une procédure formelle garantissant la traçabilité des sorties de matériel.	C

4.7. Sécurité des réseaux informatiques

Objectif n°10
Garantir la protection de l'information sur les réseaux informatiques de l'entité.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
RESX-01	Architecture réseau	**Règle :** L'architecture réseau du système d'information doit être décrite et formalisée à travers des schémas d'architecture, et des configurations, mis à jour au fil des évolutions apportées au SI. **Recommandation :** Il est recommandé de conserver les schémas d'architecture et les fichiers de configuration dans des répertoires sécurisés.	C
RESX-02	Cloisonnement réseau	**Règle :** Afin de réduire les risques d'interception de données, de compromission virale et d'augmenter les performances, les différents réseaux informatiques de l'entité devront être cloisonnés en fonction des besoins métiers et en différentes zones réseaux (zone de confiance dont la sécurité est réputée adéquate, zone d'administration, zone utilisateur, ...).	C
RESX-03	Contrôle sur les réseaux	**Règle :** L'ensemble des flux entrants et sortants d'une zone réseau à une autre, doit être contrôlé et analysé afin de protéger les ressources hébergées contre les tentatives d'attaque et les codes malveillants.	C
RESX-04	Maîtrise des flux	**Règle :** L'entité doit établir et maintenir à jour les matrices de flux au niveau de chaque équipement de filtrage (pare-feu, routeur, ...). Aucun flux ne peut être implémenté en dehors des matrices de flux dûment validées. Les flux doivent être régulièrement revus dans le cadre d'une procédure formelle établie par l'entité.	C
RESX-05	Configuration des équipements réseaux	**Règle :** Les configurations opérationnelles des équipements de communication et filtrage doivent être durcies notamment par rapport aux versions natives des fournisseurs par le changement des mots de passe et certificats, et la fermeture des services et des ports non nécessaires.	C

RESX-06	Accès distants	**Règle :** L'accès d'utilisateurs distants ne doit être réalisable que par des personnes autorisées et bien définies par l'entité. Des mesures d'authentification fortes par l'usage de protocoles sécurisés pour ce type de connexions sont nécessaires lors d'échanges sensibles.	C
RESX-07	Services généraux	**Règle :** Le déploiement du réseau sans fil doit être limité et doit faire l'objet d'une étude de sécurité spécifique. **Recommandation :** Il est fortement conseillé de cloisonner le réseau sans fil du reste du réseau : une passerelle maîtrisée doit être mise en place permettant de tracer les accès et de restreindre les échanges aux seuls flux nécessaires.	C
RESX-08	Interconnexion avec les réseaux externes	**Règle :** Un inventaire exact de l'ensemble des interconnexions avec les réseaux externes doit être tenu à jour. Une zone d'échange permettant de relayer les flux et éviter des communications directes entre les réseaux externes et le réseau interne de l'entité doit être définie (proxy, antivirus, ...). Les interconnexions entre **administ**rations, systèmes et autres structures de l'Etat doivent se faire via le bus d'interopérabilité X-ROAD.bj.	C
RESX-09	Connexion des équipements au réseau	**Règle :** Seuls les équipements maîtrisés (configurés par l'entité ou respectant sa politique de sécurité) peuvent être connectés au SI de l'entité.	C

4.8. Sécurité du poste de travail utilisateur

Objectif n°11

Fournir aux utilisateurs, des postes de travail sécurisés pour leurs activités professionnelles.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
PDT-01	Attribution, usage et restitution	**Règle :** Le processus d'attribution des postes de travail doit être formalisé et contrôlé. Ce processus devra prendre en compte la demande, l'affectation et une décharge de l'utilisateur.	C
PDT-02	Privilèges sur les postes	Les utilisateurs ne doivent pas avoir, par défaut, les droits administrateurs sur leur poste de travail. Chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission. Un contrôle automatisé doit être régulièrement réalisé sur les postes de travail en utilisant les outils de gestion de parc afin de vérifier qu'un utilisateur n'ait pas de permissions auxquelles il n'aurait pas droit.	C
PDT-03	Configuration des postes de travail	**Règle :** Les postes de travail sont déployés conformément à des paramétrages standardisés et sécurisés, définis par l'entité (changement de mot de passe par défaut, désactivation des services inutiles, configuration BIOS protégé par mot de passe, protection antivirale, programmation des mises à jour, verrouillage des sessions, ...). L'utilisateur ne doit pas être en mesure de modifier les paramètres de sécurité du poste de travail. **Recommandation :** L'entité peut centraliser la gestion des paramètres de sécurité et faire recours aux guides de durcissement préconisés par l'ANSSI.	C
PDT-04	Installation des composants logiciels et matériels	**Règle :** Seuls les composants logiciels ou matériels validés peuvent être installés sur les postes de travail de l'entité. L'entité doit veiller à ce que tout composant logiciel ou matériel à installer fasse l'objet d'une acquisition de licences d'utilisation s'il y est soumis.	C
PDT-05	Partage des fichiers	**Règle :** Le partage de répertoires ou de données hébergées localement sur les postes de travail n'est pas autorisé. **Recommandation :** Il est recommandé de réaliser le partage de fichiers entre les utilisateurs par l'intermédiaire des espaces partagés mis à disposition par les administrateurs.	C

PDT-06	Sauvegarde des données	**Règle :** Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs. Les disques de stockage en local doivent être chiffrés avec des outils de confiance.	**N**
PDT-07	Réaffectation d'un poste de travail déjà utilisé	**Règle :** L'entité définit une procédure concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.	**N**
PDT-08	Utilisation des équipements personnels (BYOD)	**Règle** : L'entité définit une politique d'utilisation des appareils mobiles personnels dans le cadre d'activités professionnelles. Ces appareils doivent être soumis aux règles de sécurité édictées au sein de l'entité.	**N**
PDT-09	Chiffrement des postes de travail	**Règle :** Les unités de stockages des postes de travail doivent être systématiquement chiffrées de sorte que les données soient illisibles ou inaccessibles tant que le système d'exploitation n'est pas démarré.	**N**

4.9. Sécurité des équipements itinérants

Objectif n°12
Protéger l'information stockée sur des équipements nomades.

Code	Exigences spécifiques	Règles / Recommandations	**Criticité** C = Critique N= Normal
ITIN-01	Stockage des données sensibles	**Règle :** Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement agréé par l'ANSSI.	C
ITIN-02	Filtre de confidentialité	Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité doit être fourni et être positionné sur l'écran dès lors que le poste est utilisé en dehors de l'entité.	N
ITIN-03	Pare-feu local	**Règle :** Un pare-feu local conforme aux recommandations de l'ANSSI doit être installé sur les postes nomades.	N
ITIN-04	Protection physique	**Règle :** Un câble physique de sécurité doit être fourni avec chaque poste portable.	N
ITIN-05	Incident de perte/vol	**Règle :** L'entité doit définir une procédure de réaction d'urgence en cas d'incident de vol ou de perte des équipements itinérants.	N

4.10. Sécurité liée à l'exploitation des SI

Objectif n°13
Assurer l'exploitation correcte et sécurisée des SI et gérer les actions d'administration du SI.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
EXP-01	Procédures d'exploitation	**Règle :** Chaque entité doit documenter les procédures d'exploitation des SI, les rendre disponibles, les expliquer à toute personne ayant besoin d'en connaître et les maintenir à jour. Ces procédures incluent à minima : l'administration et la sécurisation des actifs SI, les sauvegardes des fichiers de configuration, les mises à jour et application des correctifs de sécurité, l'exploitation des locaux techniques.	C
EXP-02	Accès aux outils et interfaces d'administration	**Règle :** L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès.	C
EXP-03	Administration à distance	**Règle :** Les actions d'administration à distance sur les composants locaux du SI doivent s'appuyer sur des protocoles d'administration sécurisés.	C
EXP-04	Configuration système	**Règle :** Les systèmes d'exploitation et les logiciels doivent être configurés et mis à jour selon des procédures formalisées (tests de non-régression, compatibilité avec les logiciels métiers, etc.).	N
EXP-05	Dimensionnement	**Règle :** Des analyses régulières du bon dimensionnement des systèmes et des réseaux (capacité mémoire, bande passante, temps de réponse, ...) doivent être réalisées dans le but de mener les actions de redimensionnement améliorant la disponibilité du SI.	N

EXP-06	Protection contre les codes malveillants	**Règle :** L'entité doit formaliser et mettre en œuvre une politique de lutte antivirale qui stipule les mesures de prévention, de détection et de réaction en cas d'infections virales. En règle générale, une solution antivirus ou Endpoint Detection and Response doit être installée sur chaque composant du SI (postes de travail, portables, serveurs, passerelles, ...). **Recommandation :** Il est recommandé l'utilisation de solutions centralisées pour la gestion antivirale.	C
EXP-07	Utilisation de la messagerie personnelle et professionnelle	Le système de messagerie professionnelle mis en place par l'entité est le seul autorisé dans le cadre des activités professionnelles. L'utilisation des courriels personnels (Gmail, Yahoo, Hotmail...) est interdite.	C
EXP-08	Sauvegarde des données	**Règle :** Chaque entité doit mettre en place des procédures de sauvegarde qui précisent pour chaque système d'information la nature des sauvegardes, la fréquence, le type de support, le calendrier des tests de restauration. Les supports de sauvegarde doivent être protégés physiquement (coffre-fort).	C
EXP-09	Journalisation des évènements sécurité	**Règle :** Des mécanismes permettant de surveiller l'utilisation des SI et de réexaminer périodiquement les résultats des activités de surveillance doivent être implémentés. Le niveau de surveillance requis pour chaque système est déterminé par le biais d'une appréciation du risque. Par ailleurs, toutes les activités de surveillance devront être réalisées dans le respect des exigences légales applicables.	C
EXP-10	Synchronisation des horloges	**Règle :** Les serveurs et équipements réseaux doivent être synchronisés sur la même base de temps. **Recommandation :** Il est recommandé d'utiliser le service TSA de la PKI nationale.	C

EXP-11	Mesures relatives aux vulnérabilités techniques	**Règle :** Des études de vulnérabilités système et applicative (scans des systèmes et des réseaux, tests d'intrusion) doivent être périodiquement menées. Cela nécessite une attention permanente sur les bulletins publiés par l'ANSSI. **Recommandation :** L'entité peut recourir aux services des Fournisseurs de Services de Sécurité Numérique Qualifiés (FSSNQ) dont la liste est publiée par l'ANSSI.	C
EXP-12	Surveillance des évènements de sécurité	Règle : Les actifs critiques (serveurs, routeurs de tête, pares-feux etc..) doivent être constamment supervisés. Pour certains SI et sous le contrôle de l'ANSSI, des sondes de supervision doivent être posées à des endroits clés du système d'information de l'entité et les événements y relatifs remontés à un centre d'expertise.	C

4.11. Sécurité dans l'acquisition, le développement et la maintenance des SI

Objectif n° 14
Intégrer la sécurité dans le cycle de vie des systèmes d'information qu'ils soient acquis ou développés par l'entité.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ADM-01	Sécurité dans les projets	**Règle :** La sécurité doit être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette. L'entité doit formaliser une procédure dans ce sens. **Recommandation :** Il est recommandé d'intégrer systématiquement le RSSI dans tout projet portant sur les systèmes d'information de l'entité et de modifier les Framework de gestion de projet pour intégrer les exigences de sécurité à toutes les étapes d'un projet.	C
ADM-02	Spécifications sécurité	**Règle :** Les cahiers de charges en vue de l'acquisition, du développement ou de la maintenance des SI devront indiquer systématiquement les exigences en matière de sécurité pour le SI.	C
ADM-03	Choix des produits	**Règle :** Les progiciels et produits achetés sont soit certifiés soit évalués en interne pour vérifier l'adéquation avec les mesures et dans le cas contraire, une analyse des risques est conduite pour définir les mesures associées avant d'acheter ou de rejeter le produit concerné.	N
ADM-04	Développement des applications	**Règle :** Les applications développées par l'entité ne doivent pas comporter des faiblesses qui pourraient compromettre la sécurité de l'application elle-même ou d'autres systèmes en production. **Recommandation :** Il est vivement recommandé de faire recours aux standards internationaux de développements sécurisés comme OWASP, guide de l'ANSSI, ...	N

ADM-05	Externalisation du développement applicatif	**Règle :** Les fournisseurs externes de logiciels doivent garantir l'intégrité de leur code et l'absence de "portes dérobées" ou de vulnérabilités. Lorsque le logiciel est utilisé pour une activité métier en production, et que la pérennité du fournisseur n'est pas garantie, celui-ci doit soit fournir le code source sous licence, soit le placer sous séquestre chez un tiers.	**N**
ADM-06	Recette sécurité (homologation)	**Règle :** Par défaut, avant la mise en production de tout système développé ou acquis, des recettes sécurité doivent être effectuées et les vulnérabilités identifiées doivent être corrigées après acceptation des risques résiduels par le sponsor ou le propriétaire du système d'information. **Recommandation :** L'entité peut faire appel à des jeux d'exercice de tests d'intrusion, d'audit de configuration, d'architecture, de revue de code source, ... ou faire effectuer la recette sécurité par un FSSNQ.	**C**
ADM-07	Données de test	**Règle :** En règle générale, les données utilisées comme jeu d'essais pour les applications ne peuvent être des données réelles. En cas de sélection de données réelles comme données d'essai, l'entité doit définir des dispositions empêchant la divulgation de ces données et garantissant leur destruction dans les environnements de test une fois les tests achevés. **Recommandation :** Il est recommandé de procéder si techniquement faisable à l'anonymisation des données réelles dans les environnements de test.	**N**
ADM-08	Collecte et traitement des données à caractère personnel	**Règle :** Les entités doivent se référer à l'APDP dans le cadre de toute activité nécessitant la collecte et le traitement des données à caractère personnel.	**N**

4.12. Sécurité des e-services

Objectif n°15

Sécuriser les informations impliquées dans les applications de e-services.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
ESV-01	Sécurité des services d'application en ligne	**Règle :** Toute plateforme de e-services doit employer des méthodes d'authentification sécurisée pour réduire les risques grâce à la cryptographie à clef publique et aux signatures numériques offertes par la PKI nationale. Des services de tiers de confiance doivent être utilisés. **Recommandation:** Les systèmes d'authentification de la PKI nationale ou du Portail National des Services Publics (PNSP) peuvent être utilisés.	C
ESV-02	Filtrage applicatif	**Règle :** L'entité qui met en oeuvre une plateforme de e-services doit faire usage d'une solution tierce de filtrage applicatif.	C

4.13. Sécurité des applications Web

Objectif n°16

Sécuriser les applications exposées sur Internet.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
SAW-01	Evaluation des risques spécifiques	**Règle :** L'entité doit identifier et documenter les risques auxquels l'application Web pourrait être confrontée, que ce soit sur les biens (infrastructures informatiques, données, etc.) ou sur les fonctions importantes fournies par cette application.	C
SAW-02	Exigences de sécurité spécifiques	**Règle :** Les exigences de sécurité doivent être élaborées en fonction des spécifications de l'application Web à développer. En règle générale, doivent être considérées dans tout projet de développement d'une application Web, les aspects suivants : ☑ Gestion des entrées et sorties ☑ Gestion des sessions ☑ Authentification ☑ Contrôle d'accès ☑ Gestion des erreurs ☑ Connexions aux systèmes externes ☑ Journalisation ☑ Chiffrement	C

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
SAW-03	Utilisation des outils de développement des applications et sites web	**Règle :** L'entité doit veiller à la prise en compte des exigences minimales ci-dessous dans le développement de ses applications et sites web. ☑ Utiliser les gestionnaires de contenu (CMS) de façon sécurisée en suivant le guide publié par l'ANSSI ; ☑ Privilégier l'utilisation de référentiels (frameworks) recommandés par l'ANSSI ou l'ASSI ; ☑ Eviter au maximum l'utilisation de plugins externes ; ☑ Toujours utiliser la dernière version des outils de développement.	**N**
SAW-04	Données en transit	**Règle :** Le protocole SSL doit être utilisé à tous les niveaux de l'application. En cas de contraintes ou de limitation d'utilisation de ce protocole, il doit être appliqué à toutes les pages d'authentification ainsi que toutes les pages une fois que l'utilisateur est authentifié.	**C**
SAW-05	Certificats SSL	**Règle :** L'entité doit avoir recours à des certificats SSL validés par une autorité de certification reconnue par l'ANSSI. Le nom sur le certificat doit correspondre au nom complet du domaine du site et la date d'expiration du certificat doit être encore valide. En fonction du type d'usage, un certificat de validation de domaine de validation d'organisation ou de validation étendue peut être requis.	**C**
SAW-06	Pages d'erreur	**Règle :** Toutes les pages d'erreurs doivent être personnalisées de façon à ne divulguer aucune information qui puisse aider un hacker.	**C**
SAW-07	Infrastructure d'hébergement	**Règle :** L'infrastructure prévue pour héberger l'application Web doit être durcie (serveur Web dédié, services inutiles désactivés, comptes par défaut bannis, contrôle d'accès aux répertoires, durcissement des systèmes d'exploitation, mises à jour régulières des systèmes d'exploitation...).	**C**

4.14. Mesures cryptographiques

Objectif n°17
Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
CRY-01	Politique cryptographique	**Règle :** Lorsqu'elle met en oeuvre des fonctions de sécurité (authentification, signature électronique, chiffrement, horodatage) utilisant des mécanismes cryptographiques sur des systèmes d'information, l'entité doit rédiger une politique de certification pour chaque fonction de sécurité mise en oeuvre. Elle doit se conformer aux exigences définies par la Commission de Cryptologie de l'ANSSI. **Recommandation :** Il est recommandé de s'inspirer des politiques de certifications types pour l'élaboration des politiques de certification des fonctions de sécurité.	**N**
CRY-02	Usage des certificats électroniques	**Règle :** Lorsque l'entité recourt à des certificats électroniques, le niveau de sécurité de ces derniers doit être proportionné à la sensibilité des systèmes d'information mis en oeuvre. Tout système d'information mettant en jeu des données sensibles doit recourir à des certificats électroniques d'un niveau de sécurité élevé c'est-à-dire empêchant toute usurpation d'identité. **Recommandation :** Il est recommandé de s'inspirer des politiques de sécurité des certificats électroniques disponibles.	**C**
CRY-03	Exigences de sécurité spécifiques	Règle : L'entité doit documenter les procédures pour protéger la confidentialité des clés cryptographiques. Ceci inclut : ☑ Génération des clés ☑ Stockage sécurisé des clés ☑ Distribution sécurisée des clés ☑ Activation des clés ☑ Changement des clés ☑ Recouvrement d'une clé (en cas de perte, ...) ☑ Destruction des clés	**C**

4.15. Relations avec les fournisseurs

Objectif n° 18
Garantir la protection des actifs de l'organisation accessibles aux fournisseurs.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
FRN-01	Accord de non-divulgation	**Règle :** Tout contrat commercial entre l'entité et un tiers doit faire l'objet d'une signature systématique d'un accord de non-divulgation lorsque des informations de l'entité sont susceptibles d'être communiquées au tiers.	C
FRN-02	Contractualisation des exigences de sécurité	**Règle :** Toute fourniture de biens et/ou services dans le domaine des SI doit être encadrée par des clauses contractuelles entre l'entité et les tiers. Le contrat signé entre l'entité et ces tiers doit refléter les exigences de sécurité à la hauteur des risques induits par la relation entre l'entité et ces tiers. Les clauses de sécurité minimales à aborder incluent : la responsabilité du tiers, la prise en compte de la PSSI spécifique, les procédures d'échanges des données, l'auditabilité, la réversibilité, la confidentialité, ...	C
FRN-03	Contrôle des accès des intervenants tiers	**Règle :** Un inventaire des accès physiques et/ou logiques à attribuer aux intervenants du tiers doit être établi et mis à la disposition du RSSI pour les besoins de contrôle de conformité avec la PSSI spécifique. Ces derniers doivent disposer des accès spécifiques sur la base des procédures en place au sein de l'entité.	C
FRN-04	Engagement sécurité des intervenants tiers	**Règle :** Tout intervenant d'un tiers amené à interférer avec le système d'information de l'entité ou l'un des composants de ce dernier signe une charte de sécurité dite « Charte Prestataire » qui l'engage individuellement vis-à-vis de l'entité.	C
FRN-05	Surveillance de la sécurité liée aux prestations	**Règle :** Durant la prestation, les différentes mesures de sécurité activées doivent faire l'objet d'une journalisation à des fins d'audit de conformité avec la politique de sécurité. Les points à surveiller incluent à minima : usage des accès physiques et logiques octroyés, respect des consignes de sécurité, niveaux de service, coopération du tiers en matière de sécurité, ...	C
FRN-06	Cessation de la relation	**Règle :** Tous les actifs SI confiés au tiers dans le cadre des prestations réalisées doivent être restitués à la cessation de la relation. Les droits d'accès des intervenants tiers aux SI de l'entité doivent être retirés dans les plus brefs délais après la cessation des activités liées à la prestation.	C

4.16. Sécurité du cloud computing

Objectif n° 19
Assurer la sécurité des informations hébergées dans une infrastructure cloud.

SCC-01	Externalisation dans un cloud	**Règle :** Les processus métiers et les services à externaliser dans une infrastructure cloud doivent être identifiés. Pour chaque processus ou service identifié, une analyse de risques doit être conduite pour évaluer l'impact lié à la perte de confidentialité, d'intégrité et de disponibilité des informations impliquées. Cette analyse est conduite en liaison avec l'ASSI et l'ANSSI.	C
SCC-02	Sélection d'un fournisseur cloud national	**Règle :** L'entité doit donner priorité aux Datacenters se trouvant sur le territoire national pour ses besoins d'externalisation.	C
SCC-03	Sélection d'un fournisseur cloud non national	**Règle :** L'entité doit veiller à souscrire à des services cloud auprès de fournisseurs démontrant des garanties de sécurité (transparence des traitements, protection des données personnelles, isolement des données, auditabilité, conformité avec les normes de sécurité reconnues, niveaux de services, haute disponibilité, coopération lors des **audits** et des investigations, loi sur la protection des données à caractère personnel ...). **Recommandation :** Il est recommandé de procéder à une évaluation du fournisseur au moyen d'un questionnaire de sécurité permettant d'examiner la posture sécurité du fournisseur.	C
SCC-04	Aspects contractuels	**Règle :** Un accord de non-divulgation doit être signé entre l'entité et le fournisseur de services cloud avant toute fourniture de service. Le contrat passé entre l'entité et le fournisseur de services cloud doit stipuler à minima des clauses garantissant : ☑ Un contrôle total de l'entité sur ses données, ☑ La protection des données à caractère personnel suivant la législation du Bénin, ☑ La destruction des données de l'entité, ☑ La coopération notamment en matière d'audit de sécurité et d'investigation ☑ La conformité avec la PSSI spécifique de l'entité	C

SCC-05	Protection des	**Règle :** L'entité doit veiller à implémenter des mécanismes de chiffrement de bout en bout des données en transit et au repos dans une infrastructure cloud. L'entité doit s'assurer contractuellement qu'elle dispose des clés de chiffrement. Le contrat d'hébergement devra prendre en compte la réversibilité et l'obligation de destruction sous contrôle des données, applicables lors de l'extinction du contrat de services Cloud.	**C**

4.17. Gestion des incidents de sécurité

Objectif n° 20

Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité du SI, incluant la communication des événements et des failles liés à la sécurité.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
INC-01	Signalement des incidents sécurité SI	**Règle :** Une procédure de signalement d'incidents liés à la sécurité du SI doit être formalisée et connue des utilisateurs et administrateurs informatiques. La procédure devra prévoir la remontée d'incidents significatifs à l'ANSSI.	**C**
INC-02	Réponse aux incidents sécurité SI	**Règle :** Les procédures de réponse aux incidents liés à la sécurité du SI doivent être formalisées et couvrir les différents types d'incidents de sécurité (malveillances, dénis de service, infections virales, intrusion, vol/perte d'équipements, perte de données, etc.).	**C**
INC-03	Répertoire des incidents sécurité SI	**Règle :** La typologie et la description des incidents liés à la sécurité SI doivent être localement enregistrées dans une base de données permettant un enrichissement progressif ainsi qu'un accès sélectif facile pour effectuer le traitement et le suivi des divers incidents futurs.	**N**
INC-04	Collecte des traces	**Règle :** L'entité doit mettre en place une procédure garantissant la sécurité des preuves numériques depuis leur collecte jusqu'à leur présentation éventuelle à un tribunal en cas d'incidents conduisant à une procédure pénale. **Recommandation :** L'entité peut recourir au bjCSIRT (Equipe gouvernementale de réponse aux incidents de sécurité informatique) afin de porter une assistance technique dans le cadre d'une investigation numérique.	**N**

4.18. Gestion de la continuité de la sécurité du SI

Objectif n° 21
Faire en sorte que la sécurité des systèmes d'information fasse partie intégrante du processus de continuité d'activité de l'entité.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
CONT-01	Plan de continuité de la sécurité SI	**Règle :** Chaque entité doit développer un plan de continuité des mesures de sécurité afin de faire face aux évènements pouvant causer leur arrêt (panne, sinistre, pandémie, déni de service, ...). Ce plan doit être testé au moins une fois par an.	C
CONT-02	Intégration de la sécurité dans les plans de continuité/reprise d'activité informatique	**Règle :** Les dispositifs de sécurité des systèmes d'information doivent être intégrés aux composants d'infrastructure éligibles au plan de continuité ou de reprise d'activité informatique de l'entité.	C
CONT-03	Redondance	**Règle :** Les architectures SI doivent être dépourvues de SPOF (Single Point Of Failure) par des mécanismes de redondance.	N
CONT-04	Tests du plan de continuité de la sécurité SI	**Règle :** Le plan de continuité de la sécurité du SI doit inclure la planification annuelle de tests afin de s'assurer que chacun des dispositifs de sécurité identifiés critiques est correctement couvert par ce plan.	N

4.19. Conformité, audit et contrôles de sécurité

Objectif n° 22
Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
CONF-01	Droits de propriété intellectuelle	**Règle :** L'entité doit se soumettre au texte du code du numérique se rapportant à la protection de la propriété intellectuelle et des droits d'auteurs. En règle générale tout logiciel (payant, gratuit et open source) utilisé par l'entité doit être accompagné d'une licence.	C
CONF-02	Données à caractère personnel	**Règle :** Les entités doivent se référer à l'APDP dans le cadre de toute activité nécessitant la collecte et le traitement des données à caractère personnel.	N
CONF-03	Mesures cryptographiques	**Règle :** L'entité doit se conformer aux dispositions du code du numérique se rapportant à la cryptologie et aux recommandations de la Commission Cryptologie.	N

Objectif n° 23

Effectuer des contrôles et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

Code	Exigences spécifiques	Règles / Recommandations	Criticité C = Critique N= Normal
CONF-04	Contrôles locaux	**Règle :** La conformité à la PSSIE et à la PSSI spécifique est vérifiée par des contrôles réguliers. Le RSSI de chaque entité conduit des actions locales d'évaluation de la conformité à la PSSIE et contribue à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en oeuvre.	C
CONF-05	Audits de sécurité	**Règle :** Des audits de sécurité approfondis du SI doivent être réalisés dans le cadre d'un programme de tests de sécurité. Ces audits doivent être confiés à des FSSNQ.	C
CONF-06	Encadrement des audits effectués par les tierces parties	**Règle :** Les audits de sécurité réalisés sur les systèmes d'information de l'entité par des tiers doivent faire l'objet d'une charte d'audit signée entre le prestataire externe d'audit et l'entité, laquelle charte précisera le périmètre et les limites de l'audit, les plages horaires pour les activités d'audit, les méthodes utilisées, les outils de tests, les engagements de bonne conduite des auditeurs, les accès à accorder, la restitution/destruction des données collectées par les auditeurs, ...	C

5. GLOSSAIRE

- Analyse des risques :
  Utilisation systématique d'informations pour identifier les sources et pour estimer le risque.

- Audit :
  Activité périodique (ou ponctuelle) permettant d'évaluer la sécurité d'un système ou de détecter les traces d'une activité malveillante.

- Cloisonnement du réseau :
  Technique ayant pour objectif de diviser un réseau informatique en plusieurs sous-réseaux. Le cloisonnement est principalement utilisé afin d'augmenter les performances globales du réseau et améliorer sa sécurité ; découpage en domaines ou périmètres de sécurité, facilite le contrôle d'accès, mieux se protéger contre les intrusions, et empêcher la fuite d'information.

- Confidentialité :
  Objectif de sécurité permettant de s'assurer que les informations transmises ou stockeés ne sont accessibles qu'aux personnes autorisées à en prendre connaissance.

- Certificat SSL :
  Le certificat se matérialise par un fichier de données liant une clé cryptographique aux informations d'une personne physique ou morale. Le certificat sécurise les échanges de données par chiffrement entre un serveur web et le navigateur d'un visiteur du site Internet.

- Disponibilité :
  Objectif de sécurité qui consiste à assurer un accès permanent à l'information et aux services offerts par le système d'information. C'est une garantie de la continuité de service et de performances des applications, du matériel et de l'environnement organisationnel.

- Filtrage :
  Technique de contrôle de flux sur un réseau qui empêche le passage des informations jugées suspectes.

- Incident de sécurité :
  Un ou plusieurs évènements liés à la sécurité de l'information indésirables ou inattendus d'origine accidentelle ou malveillante, impactant l'un ou plusieurs objectifs de sécurité (Confidentialité, Intégrité, Disponibilité), et présentant une probabilité forte de compromettre les activités de l'organisme et de menacer la sécurité de l'information (Fuites de données, Déni de service, Intrusion informatique ou physique, inondation...).

- Intrusion :
  Accès non autorisé à un système informatique afin de lire ses données internes ou d'utiliser ses ressources.

- Menace :
  Cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'une entité.

- Mesure :
  Moyen de gérer un risque, et pouvant être de nature administrative, technique, gestionnaire ou juridique.
- Normes :
  Document de référence contenant des spécifications techniques précises destiné à être utilisé comme règles ou lignes directrices.
- Network Time Protocol (NTP) :
  Protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure.
- Infrastructure à clé publique (PKI) :
  Ensemble de composants physiques, logiciels, procédures et documents visant à gérer le cycle de vie des clés cryptographiques et leurs certificats.
- Réseau privé virtuel (VPN) :
  Technique d'interconnexion de réseaux locaux permettant de chiffrer les communications pour en conserver la confidentialité.
- e-service :
  Services utilisant les technologies de l'information et de la communication.
- Tiers :
  Personne ou organisme reconnu(e) comme indépendant(e) des parties concernées.
- Vulnérabilité :
  Faille de sécurité dans un programme ou sur un système informatique.
- Cyberespace :
  Espace de communication créé par l'interconnexion mondiale des ordinateurs.
- Cybermenace :
  Activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient.
- Cybersécurité :
  Ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un État, d'une entreprise.

6. ANNEXE : FICHE DE POSTE TYPE D'UN RSSI

Identification de la fonction	
Intitulé de la fonction	Responsable Sécurité Système d'Information
Intitulé de la fonction du supérieur hiérarchique	Selon chaque entité

Missions principales de la fonction

- Définir la politique de sécurité du SI et veiller à sa mise en application
- Assurer le rôle de conseil, d'assistance, d'information, de formation et d'alerte en sécurité du SI.
- Identifier, apprécier les risques et définir les exigences de sécurité des SI
- Assurer la veille technologique et prospective dans le domaine de sécurité des SI.
- Définir le plan de secours informatique, s'assurer de son fonctionnement et de sa mise à jour
- Réaliser des contrôles de premier niveau relatifs aux mesures de sécurité mises en oeuvre
- Rendre compte à sa hiérarchie sur la gestion de la sécurité des SI.

Activités principales de la fonction

Gouvernance & Référentiel de sécurité

- Participe à la définition des objectifs et du niveau de sécurité cible du SI.
- Rédige, met en place et fait vivre la politique de sécurité du système d'information
- Rédige et suit l'application des procédures de sécurité du SI
- Définit la charte d'utilisation des ressources informatiques et la charte des administrateurs IT
- Participe aux Comités DSI ou en rapport avec la technologie
- Anime le système de management de la sécurité des SI.

Gestion des vulnérabilités et appréciation des risques liés à la sécurité des SI

- Définit et fait vivre le cadre de gestion des risques liés à la sécurité des SI.
- Met en place et fait vivre le programme de gestion des vulnérabilités techniques et des correctifs de sécurité SI
- Maintient une cartographie des risques liés à la sécurité des SI
- Suit les chantiers de mise en place des actions de réduction des risques liés à la sécurité SI.

Sensibilisation et formation des utilisateurs en matière de sécurité SI

- Alerte sur les évènements en rapport avec la sécurité et la cyber-sécurité
- Définit et fait vivre le programme de sensibilisation des utilisateurs et des administrateurs IT
- Conseille et assiste les administrateurs de la DSI sur les questions relatives à la sécurité des SI.

Gestion des projets & exploitation sécurité SI

- S'assure de la prise en compte des exigences de sécurité dans le cycle de vie des projets SI (analyse des risques, définition des exigences sécurité dans les cahiers de charges, ...)
- Procède à la recette sécurité des systèmes, applications et architectures à mettre en production
- Pilote les projets de mise en place des solutions et outils de sécurité retenus dans le cadre du traitement des risques
- Assure l'exploitabilité des solutions et outils de sécurité mis en oeuvre (intégration des SI à l'architecture sécurité, fonctionnement des solutions de sécurité, monitoring, ...)
- Participe à la gestion des changements sur les SI (analyse d'impact, validation sécurité, ...).

Gestion des vulnérabilités et appréciation des risques liés à la sécurité des SI

- S'assure de la prise en compte des exigences de sécurité dans le cycle de vie des projets SI (analyse des risques, définition des exigences sécurité dans les cahiers de charges, ...)
- Procède à la recette sécurité des systèmes, applications et architectures à mettre en production
- Pilote les projets de mise en place des solutions et outils de sécurité retenus dans le cadre du traitement des risques
- Assure l'exploitabilité des solutions et outils de sécurité mis en oeuvre (intégration des SI à l'architecture sécurité, fonctionnement des solutions de sécurité, monitoring, ...)
- Participe à la gestion des changements sur les SI (analyse d'impact, validation sécurité, ...).

Gestion du secours informatiques

- Participe au choix des solutions techniques de secours informatique
- Formalise les procédures de reprise informatique et en assure le maintien en condition opérationnelle.

Surveillance & reporting

- Assure le contrôle premier niveau de la sécurité des SI (suivi du respect du référentiel sécurité, de la conformité avec les normes définies, ...)
- Diligente des missions d'audits externes de sécurité SI et suit leur exécution
- Assure la surveillance quotidienne des évènements de sécurité SI
- Produit les tableaux de bord de sécurité SI et les remonte à sa direction.

Veille technologique et prospective

- Suivre les évolutions réglementaires et techniques relevant de la sécurité des SI.
- Proposer les évolutions nécessaires pour garantir la sécurité du SI dans son ensemble.

Relations internes et externes de la fonction

Liaisons fonctionnelles internes

Fonctions interfaces
- Maîtrise d'ouvrage (Chefs de projet DSI)
- Autres directions.

Objet de la relation
- Etude des besoins de sécurité
- Fixation des cahiers de charge sécurité
- Contrôle des procédures sécurité SI
- Sensibilisation et formation.

Partenaires externes

Fonctions interfaces
- Fournisseurs
- Groupe de spécialistes
- Autorités compétentes.

Objet de la relation
- Etude des besoins de sécurité
- Fixation des cahiers de charge sécurité
- Contrôle des procédures sécurité SI
- Sensibilisation et formation.

Résultats attendus de la fonction

Résultats attendus de la fonction
- Pertinence et adéquation de la documentation de gestion de la sécurité SI
- Efficacité du traitement des risques liés à la sécurité des SI
- Effectivité des mesures de sécurité dans les opérations
- Effectivité de l'organisation sécurité interne.

Formation

Bac + 4 ou 5 en informatique, télécoms ou SI / Ingénieur grandes Ecoles en Informatique, télécoms ou SI

Certifications : ISO 27001 LI, ISO 27001 LA, CEH, CISA, CISSP, ITIL, etc... et toutes autres certifications spécifiques relatives à la sécurité des SI et à la cybersésurité.

Expérience/ Connaissances/ Savoir faire

- 5 ans d'expérience minimum dans le domaine
- Normes, procédures et législation sur la sécurité du SI
- Protocole réseaux et Internet
- Connaissance du marché de l'offre sur la sécurité
- Evaluation et maîtrise des risques SI
- Systèmes de management
- Capacité à anticiper les évolutions des techniques informatiques et leur impact sur l'entreprise.

Qualités humaines et aptitudes

- Confidentialité, respect du secret
- Rigueur, sens de la méthode et probité
- Charisme et sens du relationnel
- Facilité et rapidité d'adaptation
- Capacité d'analyse et de synthèse
- Qualités de communicant
- Capacités managériales.

MINISTÈRE DU NUMÉRIQUE
ET DE LA DIGITALISATION
RÉPUBLIQUE DU BÉNIN

ANSSI
AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

numerique.gouv.bj | @numeriquebenin