PREMIER MINISTERE

SECRETARIAT GENERAL

AGENCE NATIONALE DE SECURITE DES SYSTEMES D'INFORMATION

BURKINA FASO

Unité-Progrès-Justice

GUIDE D'ELABORATION DE POLITITIQUE DE SECURITE DES SYSTEMES D'INFORMATION

Version 1.0

Date: 06/05/2019

Mai 2019

Table des matières

Avant-propos 3

I. Introduction 4

II. Rappel du cadre règlementaire et normatif 4

1. Sur le plan international 4
2. Sur le plan national 5
3. Normes et standards 6

III. Place de la politique de sécurité des systèmes d'information 7

IV. Démarche d'élaboration de la PSSI 8

1. Étude de contexte 8
2. Rédaction 9

V. La mise œuvre en œuvre de la PSSI 12

1. Évaluation et révision 13

Avant-propos

Ce guide pratique vise à apporter un éclairage sur les enjeux de la sécurité des systèmes d'information des ministère et institutions gouvernementales, des Opérateurs de télécommunications et Fournisseurs d'accès Internet, des institutions financières, des organes œuvrant dans le domaine de la sécurité, des Organes dont le rôle est lié à la gouvernance, à la régulation et à la souveraineté de l'Etat. Aussi il vise à exposer aux décideurs et aux responsables des systèmes d'informations de ces établissements les bases de la mise en place d'une démarche de sécurité.

Ce document élaboré par l'Agence Nationale de Sécurité des Systèmes d'information est un guide, il n'a pas de caractère obligatoire. Il s'appuie sur des documents législatifs ou normatifs ainsi que sur l'expérience et le savoir-faire de personnes issues de l'administration publique et d'acteurs venant du secteur privé.

Les références ici citées ont pour objet de servir d'illustration et de souligner le sens qui peut être donné aux principes et aux règles de sécurité des systèmes d'informations d'un organisme.

En ce qui concerne le domaine juridique, le lecteur est averti qu'il doit, dans tous les cas, vérifier la validité, la complétude et la portée des textes législatifs ou réglementaires auxquels il se réfère, dans le cadre des activités spécifiques à son organisme.

I. Introduction

Le présent guide s'inscrit dans la dynamique de mise en œuvre une gouvernance forte, intégrée et co-constructive de la sécurité de l'information numérique sur une échelle nationale.

De plus, ce guide répond à l'obligation de l'entité en charge de la sécurité des systèmes d'information c'est-à-dire ANSSI, d'accompagner les organismes publics et privés et de leur apporter le soutien nécessaire dans la prise en charge des exigences en matière de sécurité de l'information numérique, notamment par l'élaboration et la diffusion de guides, pratiques et outils.

Le document s'adresse de manière générale à toute personne physique ou morale qui s'intéresse à la question de sécurité des systèmes d'information. Plus spécifiquement il a été élaboré pour outiller les acteurs œuvrant dans :

II. Rappel du cadre règlementaire et normatif

Pour garantir l'état de droit dans le cyberspace et réconcilier la nécessité d'un accès efficace aux données à des fins répressives et garantir le respect des exigences en matière de droits de l'homme et de l'état de droit, des initiatives ont été menées sur le plan international que national.

1. Sur le plan international

A l'échelle internationale la question de cyber sécurité préoccupe toutes les nations. Cela s'est matérialisé par des adoptions de résolutions et de conventions :

- **la résolution 58/199** de l'Assemblée Générale de l'Organisations des Nations Unies en 2004 où il est invité les Etats membres de développer des stratégies pour protéger les systèmes d'informations critiques, de partager les bonnes pratiques en matière de cyber sécurité ;

- **la Convention sur la Cybercriminalité du Conseil de l'Europe** ou **la Convention de Budapest** est instrument international cohérent et rassembleur en matière de lutte contre la cybercriminalité et de recueil de la preuve numérique il est un traité international sur les infractions pénales commises via l'Internet ;
- **la Convention de l'Union Africaine sur la Cybersécurité et la protection des données personnelles**, adoptée par les Chefs d'Etat et de gouvernement de l'Union Africaine (UA) qui se sont réunis les 26 et 27 juin 2014 à Malabo en Guinée Equatoriale, pour la 23ème Session Ordinaire du Sommet de l'UA témoigne la prise de consciences des menaces engendrées par le phénomène de la cybercriminalité. La convention vise à renforcer et harmoniser les législations actuelles des Etats membres et des Communautés Economiques Régionales en matière des TIC , dans le respect des libertés fondamentales et des droits de l'Homme et des Peuples. Elle vise aussi la création du cadre normatif approprié correspondant à l'environnement juridique, culturel, économique et social africain.

2. Sur le plan national

Le Burkina Faso à l'instar de nombreux pays d'Afrique s'est lancé dans la protection de son cyberespace. En se basant sur des références internationales et nationales des actions remarquables ont été menées par l'Etat burkinabé dans le domaine de cybersécurité :

- des projets de loi et de décret portant sécurité des systèmes d'information sont en cours d'examen par le gouvernement et l'assemblée nationale ;
- le Code pénal Burkinabé a été révisé pour prendre en compte les questions de cybercriminalité ;
- la loi n° 061-2008/an portant règlementation générale des réseaux et services de communications électroniques au Burkina Faso ;

- la loi n°010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel est la Loi qui encadre toutes les formes d'utilisations ou manipulation des données personnelles au Burkina ;
- la loi n°045-2009/AN du 10 novembre 2009 portant réglementation des services et des transactions électroniques au Burkina Faso ;
- le décret n° 2012-64/PRES/PM/MTPEN/MJ/MEF/MFPTSS/MICA du 13 décembre 2012 portant sur les échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives elles-mêmes.

3. Normes et standards

Dans l'objectif de disposer d'un référentiel commun et documenté destiné à harmoniser l'activité d'un secteur, plusieurs normes ou standards, de référentiels de bonnes pratiques en matière de sécurité des systèmes d'information sont été proposés par des organismes spécialisés. Ces normes constituent des guides méthodologiques ainsi que le moyen de fournir l'assurance d'une démarche de sécurité cohérente. Dans le présent guide nous allons évoquer deux normes qui traitent de la politique de sécurité des systèmes informations :

- ISO 27002 : cette norme est un code de bonne pratique pour le management de la sécurité des systèmes d'informations. Elle recommande des mesures de sécurité de l'information portant sur les objectifs de contrôle de sécurité de l'information résultant des risques pour la confidentialité, l'intégrité et la disponibilité des informations.
- NIST 800 : La National Institute of Standards and Technology (NIST) est la structure des Etats Unis d'Amérique qui élabore et publie des normes, directives et autres publications pour aider les agences sœurs à mettre en œuvre la loi fédérale sur la gestion de la sécurité de l'information, la (FISMA) Federal Information Security Management Act. La NIST accompagne également les agences des Etats fédéraux dans la mise en œuvre des programmes de protection de l'information et des systèmes d'information. C'est dans ce dans ce qu'elle elabora la

Specification Publication(SP) 800-53 qui se veut être le fournisseur de catalogue de contrôles de sécurité pour tous les systèmes d'information des Etats fédéraux américains.

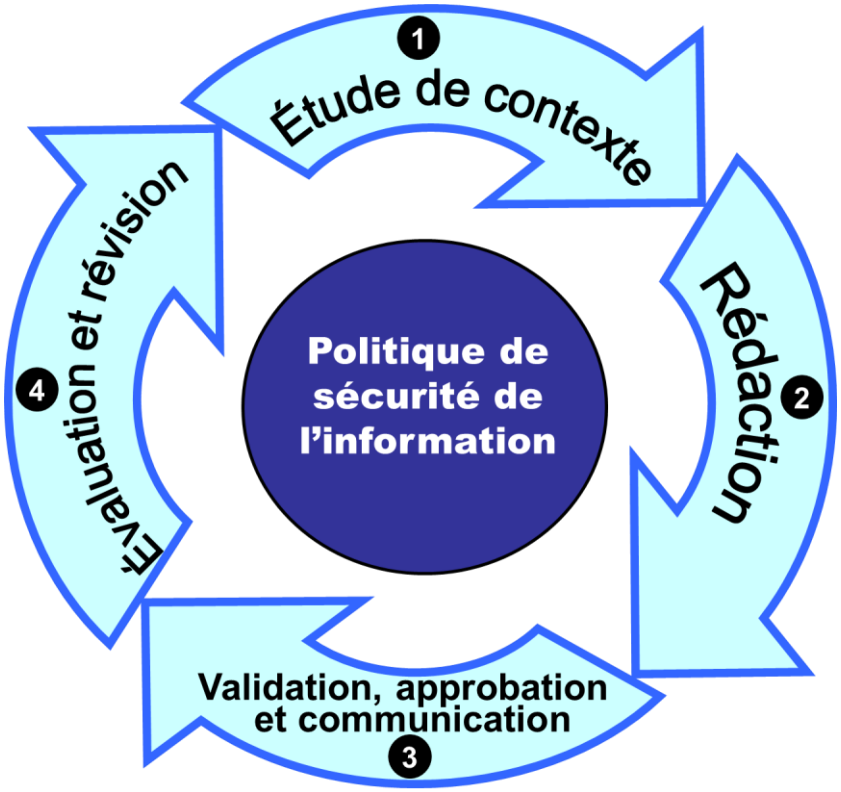
III. Place de la politique de sécurité des systèmes d'information

La politique de sécurité des systèmes d'information occupe une place prépondérante dans le secteur de l'information. Elle se repose sur un cadre légal. Le cadre légal est constitué de lois nationales et internationales, générales ou propres à un organisme public ou privé, et de règlements dont les dispositions touchent spécialement la sécurité de l'information et la protection des données personnelles.

IV. Démarche d'élaboration de la PSSI

La figure présentée ci-dessous décrit la démarche recommandée pour la réalisation d'une politique de sécurité de l'information. Elle s'inscrit dans une logique de perfectionnement continue.

Étapes de réalisation d'une politique de sécurité



1. Étude de contexte

La mise en œuvre de la PSSI est soumise à des obligations relevant de nombreux textes d'ordre législatif et réglementaire qui accordent un enjeu juridique important à cette activité.

La détermination des composantes d'une politique de sécurité de l'information prend appui sur :

- ✓ le cadre légal et le cadre réglementaire, gouvernemental et sectoriel;
- ✓ les normes et standards de l'industrie;
- ✓ la mission de l'organisation et les risques auxquels elle est exposée;
- ✓ les priorités d'actions gouvernementales;
- ✓ tout autre document pertinent.

2. Rédaction

Les principales composantes à examiner dans le cadre de la rédaction de la PSSI sont :

- ✓ le contexte d'adoption, qui expliquera l'importance de consolider la politique de la sécurité de l'information de l'organisation, en implantant les obligations visant à préserver proprement la confidentialité, à garantir l'intégrité et à prendre en charge la disponibilité effective de l'information;
- ✓ la termes et les acronymes utilisés;
- ✓ les lois, les règlements, les directives, les normes et les standards applicables sur lesquels la politique prendra appui;
- ✓ l'objectif visé, notamment l'engagement officiel de la haute direction à soutenir la prise en charge des exigences de sécurité de l'information et à promouvoir au sein de l'entreprise les moyens nécessaires à leur accomplissement;
- ✓ le champ d'usage de la politique, notamment toute personne, physique ou morale, ayant accès, sur place ou à l'extérieur des locaux de l'organisation, aux informations desquelles un organisme public ou un organisme privé a la responsabilité d'assurer la sécurité;

- ✓ la rédaction de principes généraux, notamment l'accord d'un organisme public ou privé aux objectifs stratégiques gouvernementaux et son engagement à ce que les solutions retenues vont avec les actions exemplaires en matière de sécurité de l'information, tant sur le plan national que sur le plan international;
- ✓ les devoirs des acteurs clés en matière de sécurité de l'information, comme le dirigeant d'organisme, et celles des utilisateurs des informations de l'organisation, qu'il s'agisse d'un gestionnaire, d'un employé, d'un partenaire d'affaires, d'un fournisseur ou d'un mandataire agissant pour le compte d'un organisme public ou privé;
- ✓ les sanctions ou représailles auxquelles s'expose tout utilisateur dérogeant aux mesures de la politique ou à ses instructions. Des condamnations devront être en accord aux dispositions des conventions collectives, des ententes et des contrats. Elles peuvent inclure la suspension de privilège, la réprimande, etc.;
- ✓ les dispositions finales, notamment son approbation par le dirigeant de l'organisme public et sa mise en œuvre, sa date d'entrée en vigueur et ses modalités de révision.

A partir des éléments cités ci-haut et afin de s'octroyer une politique de sécurité solide, nous proposons une méthodologie pour l'élaboration d'une politique de sécurité des systèmes d'information (PSSI) ont été identifiés.

Cette méthodologie aborde les différents domaines de la sécurité généralement couverts par une PSSI . Ces principes couvrent 21 domaines de la sécurité des systèmes d'information.

Principes organisationnels

1. Politique de sécurité :
2. Organisation de la sécurité
3. Garantir la maitrise du risque
4. Audits de sécurité
5. Gestion des risques SSI
6. Sécurité et cycle de vie
7. Mesures de protection des SI
8. Assurance et certification

Principes de mise en œuvre

9. Aspects humains
10. Planification de la continuité des activités
11. Gestion des incidents
12. Sensibilisation et formation
13. Exploitation
14. Aspects physiques et environnementaux

Principes techniques

15. Identification / authentification
16. Protocoles de sécurité
17. Contrôle d'accès logique
18. Journalisation
19. Cryptographie et Sténographie
20. Infrastructures de gestion des clés cryptographiques
21. Signaux compromettants

Chacun des principes pourrait être décliné en règles d'application pour rédiger une PSSI. Il s'agit d'une proposition que nous pouvons prendre en compte dans notre PSSI.

V. La mise œuvre en œuvre de la PSSI

L'approbation de la politique de sécurité nécessite la contribution des entités administratives de l'organisation et de l'équipe chargée de la sécurité de l'information. La politique de sécurité est approuvée par le dirigeant d'organisme.

La PSSI doit être connue de l'ensemble des personnels, ainsi que, le cas échéant, de l'ensemble des personnes accédant au système d'information de l'organisme (sous-traitants, prestataires, stagiaires…) ;

Cependant, elle peut contenir des informations confidentielles et les personnels de l'organisme peuvent être concernés de façon différenciée en fonction de leur rôle. De ce fait, il est recommandé, le cas échéant, d'élaborer et de diffuser des synthèses, incluant des extraits plus détaillés pour les informations pertinentes en fonction des lecteurs. Le but de ces synthèses est de permettre à chacun de connaître les enjeux et les règles de sécurité en fonction de ses besoins

Une fois approuvée, la politique est diffusée, auprès de l'ensemble du personnel de l'organisation, en utilisant les moyens appropriés dont :

- ✓ les sites Web (intranet ou extranet);
- ✓ les trousses de sensibilisation à la sécurité de l'information;
- ✓ les bannières publicitaires sur le site intranet ou extranet;
- ✓ les articles dans les journaux internes;

 etc.

Il convient également d'organiser, à l'intention de l'ensemble du personnel, des séances de formation et de sensibilisation, afin de s'assurer d'une bonne compréhension des énoncés de la politique.

1. Évaluation et révision

Un organisme peut changer au cours du temps (organisation, missions, périmètre, axes stratégiques, valeurs). Son système d'information est donc l'objet de modifications fréquentes, tout comme les menaces et vulnérabilités qui s'y appliquent. Il convient alors de prévoir un réexamen de la PSSI :

- lors de toute évolution majeure du contexte ou du SI ;
- dans le cas d'une évolution de la menace ;
- dans le cas d'une évolution des besoins de sécurité ;
- à la suite d'un audit ;
- à la suite d'un incident de sécurité ;
- systématiquement à intervalle défini ;
- sur demande d'une autorité (responsable de la sécurité, direction…) dans le cadre d'une procédure à définir dans la PSSI. Une fois l'étape d'évaluation terminée, la politique pourra faire l'objet d'une révision qui assurera l'adéquation de ses énoncés aux besoins de l'organisation en matière de sécurité de l'information