Sommaire

INTRODUCTION

L'accomplissement de la mission des services publics et la recherche d'une meilleure efficacité passent nécessairement par la mise en œuvre de moyens qui utilisent de plus en plus les Technologies de l'Information et de la Communication (TIC).

Ce recours très large à ces nouvelles technologies, rendu nécessaire par le volume croissant des informations à traiter et par l'extension du besoin de communication, a l'inconvénient de rendre ces services dépendants de leurs systèmes d'information ; ainsi, ils sont vulnérables aux multiples menaces et attaques qui pèsent sur eux, notamment dans le domaine de la cybercriminalité qui constitue les actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Ces risques, sans cesse croissants qu'implique l'utilisation des systèmes d'information, peuvent mettre en cause l'action des services de l'Etat. C'est pourquoi, protéger l'information doit être un souci général, et sécuriser les systèmes d'information de l'Etat du Sénégal une obligation majeure, et par conséquent, un enjeu de souveraineté nationale.

En effet, la sécurité des systèmes d'information est un véritable défi à la fois technologique et économique. Elle vise généralement à assurer la confidentialité de l'information, la disponibilité et l'intégrité de l'information et du système d'information. Afin d'atteindre ces objectifs de sécurité, il est nécessaire de mettre en œuvre une politique de sécurité applicable à l'ensemble des entités, aussi bien publiques que privées, à l'intérieur d'un domaine géographique ou fonctionnel, qui explicitera l'ensemble des règles et des recommandations destinées à protéger les ressources et les informations contre tout préjudice, et également de prévoir le cas de la faillite de la protection.

C'est pourquoi, la présente instruction, qui constitue l'une des bases fondamentales de la stratégie nationale en matière de cybersécurité, est prise pour fixer les principes et les règles à mettre en application pour assurer un niveau de sécurité optimal des systèmes d'information de l'Etat dans le respect des lois et règlements en vigueur.

Elle précise également l'organisation à mettre en place pour sa mise en œuvre. Elle définit la sécurité du personnel et répartit les responsabilités entre les différents intervenants dans ce domaine. En outre, elle fixe les objectifs et les règles relatives notamment à la sécurité physique, la sécurité logique et la sécurité de l'exploitation des systèmes d'information. Enfin, elle insiste sur le plan de secours à mettre en place pour la gestion des incidents ainsi que sur la conformité et les aspects juridiques de la sécurité des systèmes d'information.

Pas de texte

Article 1 : Objet de l'instruction (PSSI-ES)

La présente instruction fixe les conditions de mise en œuvre de la Politique de Sécurité des Systèmes d'Information de l'Etat du Sénégal (PSSI-ES).

Bases de la Politique de Sécurité des Systèmes d'Information de l'Etat

Les principes et les règles contenus dans la Politique de Sécurité des Systèmes d'Information de l'Etat du Sénégal (PSSI-ES) s'appuient sur les textes ci-après :

I. Au niveau national

1. Le Code pénal ;
2. La loi n° 70-23 du 06 juin 1970 portant organisation générale de la Défense nationale, modifiée ;
3. La loi n° 2008-08 du 25 janvier 2008 portant sur les transactions électroniques ;
4. La loi n° 2008-11 du 25 janvier 2008 portant sur la cybercriminalité ;
5. La loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel ;
6. La loi n° 2008-41 du 20 août 2008 portant sur la cryptologie ;
7. La loi n° 2011-01 du 24 février 2011 portant Code des Télécommunications ;
8. Le décret n° 2003-512 du 02 juillet 2003 relatif à l'organisation de la Protection des secrets et des Informations concernant la Défense nationale et la sécurité de l'Etat ;
9. Le décret n° 2008-718 du 30 juin 2008 relatif au commerce électronique pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques ;
10. Le décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, notamment en son article 28 ;
11. Le décret n° 2008-720 du 30 juin 2008 relatif à la certification électronique pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques ;
12. Le décret n° 2013-1152 du 20 août 2013 relatif au Conseil national de Sécurité ;
13. Le décret n° 2014-940 du 31 juillet 2014 portant création et organisation de la Délégation générale au Renseignement national ;
14. L'arrêté n° 02435 du 06 février 2012 fixant les attributions et l'organisation du Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information ;
15. L'Instruction présidentielle n° 0303 PR du 16 juillet 2003 sur la protection du secret ;
16. L'Instruction générale interministérielle n° 54 /PM/SGPR/STCC du 06 juillet 1979 sur la sécurité des communications ;
17. Le Guide pratique n° 0023 PR/SG du 23 janvier 2003 sur la protection du secret à l'usage des personnels des secrétariats et des bureaux du courrier ;
18. La circulaire n° 0288 du 08 avril 2016 relative à la messagerie électronique ;
19. La circulaire n° 0328 du 12 mai 2016 relative à la sécurité des systèmes d'information et à la cybersécurité.

II. Au niveau international

1. Les lignes directrices de l'Organisation de Coopération et de Développement Economique (OCDE) sur la protection de la vie privée et les flux transfrontières de données à caractère personnel :
   - lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel ;
   - déclaration des flux transfrontières de données ;
   - déclaration des ministres relative à la protection de la vie privée sur les réseaux mondiaux.
2. Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel ;
3. Directive C/DIR/1/0811 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO) ;
4. Acte additionnel A/SA.2/01/10 du 16 février 2010 sur les transactions électroniques ;
5. Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel, adoptée par la 23ème Session Ordinaire du Sommet de l'Union Africaine à Malabo, le 27 juin 2014 ;
6. Les normes techniques de l'Organisation Internationale de Normalisation/ Commission Electrotechnique Internationale (ISO/IEC) :
   - ISO 27001 : Technologies de l'Information - Techniques de Sécurité - Systèmes de management de la sécurité de l'information - Exigences ;
   - ISO 27002 : Technologies de l'Information - Techniques de Sécurité - Code de bonnes pratiques pour le management de la sécurité de l'information.

Article 2 : Principes généraux de la sécurité des systèmes d'information

I. Définitions

1. Information

Elément de connaissance, exprimé sous forme écrite, visuelle, sonore ou numérique susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué.
L'information sensible peut être divisée en deux catégories :

- informations sensibles classifiées : informations affectées de l'une des mentions de classification (**TRES SECRET, SECRET, CONFIDENTIEL**) définies par :
  - le décret n° 2003-512 du 02 juillet 2003 ;
  - l'Instruction présidentielle n° 0303 /PR du 16 juillet 2003.

- informations sensibles non-classifiées : informations sensibles pour lesquelles le non-respect de la confidentialité, la disponibilité ou l'intégrité mettrait en cause la responsabilité du propriétaire ou du dépositaire, ou leur causerait préjudice ou à des tiers. A titre d'exemple, on peut citer les informations qui ne présentent pas un caractère secret, mais qui restent soumises à l'obligation de réserve ou de discrétion professionnelle.

2. Système d'information

Tout moyen dont le fonctionnement fait appel d'une façon ou d'une autre à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.

3. Sécurité des systèmes d'information

C'est l'état de protection, face aux risques identifiés, qui résultent de l'ensemble des mesures générales et particulières, pour assurer la confidentialité de l'information, la disponibilité et l'intégrité de l'information et du système d'information.

- **la confidentialité** : le caractère réservé d'une information dont l'accès est limité aux seules personnes ayant besoin d'en connaître ;
- **la disponibilité** : l'aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performances ;
- **l'intégrité** : la garantie que l'information n'est modifiée que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire à la garantie de son origine et de sa destination.

II. Principes de protection globale

La sécurité des systèmes d'information résulte de mesures générales et particulières :

1. Mesures générales

Mesures administratives et techniques ainsi que de contrôle des systèmes (appréciation et application des principes du besoin d'en connaître et d'utiliser, protection périmétrique des installations où sont traitées les informations sensibles, contrôle d'accès aux locaux, etc.).

2. Mesures particulières

Inclusion, dans les systèmes d'information, de tous les dispositifs de sécurité permettant de protéger les informations en précisant les modalités de leur mise en œuvre et la limitation de l'accès aux informations relatives à ces dispositifs eux-mêmes.

Ces mesures doivent être associées pour assurer la sécurité des systèmes d'information puisqu'aucune d'elles ne permet, isolément, de garantir la disponibilité, l'intégrité et la confidentialité recherchées.

Article 3 : Champ d'application de la PSSI-ES

1. La PSSI-ES s'applique à tous les systèmes d'information sans exception des entités de l'Etat, tenant compte des principes définis à l'article 2, et qui sont gérés aussi bien par l'Administration, les Institutions, les Organismes nationaux et le Gouvernement (Ministères, Directions générales, Services déconcentrés et les Autorités administratives). Les mesures qui y sont contenues doivent être strictement appliquées à tous les niveaux de responsabilité, que ce soit au niveau de l'Etat et même au-delà de ses structures.
2. La PSSI-ES concerne l'ensemble des personnes physiques ou morales intervenant dans ces systèmes d'information, qu'il s'agisse des administrations de l'Etat, de leurs agents ou bien de tiers et de leurs employés.
3. La PSSI-ES ne s'impose pas aux systèmes aptes à traiter des informations classifiées de défense, soumis à un corpus règlementaire spécifique, plus contraignant. Il appartient aux responsables des entités concernées d'assurer une cohérence entre les dispositions de la présente PSSI-ES et la règlementation relative à la protection des informations classifiées de défense.
4. La plupart des règles de sécurité de la PSSI-ES constituent des règles de base qui doivent être appliquées plus largement, au-delà des administrations de l'Etat.

Article 4 : Organisation de l'Etat pour la mise en application de la PSSI-ES

Pour la gestion des différentes composantes de la sécurité et de leur évolution, **une structure de sécurité** doit être mise en place dans les différentes entités dans les conditions ci-dessous, avec une bonne répartition des responsabilités entre les différents niveaux hiérarchiques suivants :

- niveau décisionnel ;
- niveau pilotage ;
- niveau opérationnel.

I. Au niveau décisionnel

La sécurité des systèmes d'information dans les entités est assurée sous l'autorité du Ministre qui en contrôle l'application. Il peut déléguer cette responsabilité au Haut Fonctionnaire de Défense-HFD (Secrétaire général, Directeur de cabinet, Attachés de défense). La mission de ce HFD s'étend à tous les organismes qui relèvent du département ministériel, y compris les organismes sous tutelle au sein desquels l'intérêt national rend impératif la sécurisation de l'information.

II. Au niveau pilotage

Le Haut Fonctionnaire de Défense est assisté dans sa mission par un **Comité de sécurité** dont les membres nommément désignés par le Chef de département agissent en tant qu' « **Autorités Qualifiées pour la Sécurité des Systèmes d'Information (AQSSI)** ».

A ce niveau, il s'agit notamment des conseillers, des Directeurs généraux, des Directeurs et Chefs de service, des chargés de mission et des fonctionnaires chargés de la sécurité des systèmes d'information qui sont personnellement responsables de l'application des mesures destinées à assurer la sécurité des systèmes d'information du département.

1. Mission du Comité de sécurité

Veiller à la mise en œuvre de la politique de sécurité des systèmes d'information de l'Etat du Sénégal et vérifier la cohérence des règles de sécurité.

2. Missions des AQSSI

- s'assurer que les dispositions réglementaires sur la sécurité des systèmes d'information sont appliquées à tous les niveaux dans les systèmes d'information de l'Administration ;
- développer à tous les échelons le souci de sécurité ;
- apprécier en permanence le niveau de sécurité des installations ;
- recenser les besoins en matière de protection des systèmes d'information et veiller à ce qu'ils soient satisfaits ;
- s'assurer de la mise en œuvre des procédures prescrites pour la protection et le contrôle des personnes ;
- s'assurer que les contrôles internes de sécurité sont régulièrement effectués ;
- organiser la sensibilisation et la formation du personnel aux questions de sécurité de l'information.

III. Au niveau opérationnel

A ce niveau, les **Autorités Qualifiées pour la Sécurité des Systèmes d'Information (AQSSI)** sont assistées par **un ou plusieurs Agents de Sécurité des Systèmes d'Information (ASSI),** chargés de la gestion et du suivi des moyens de sécurité des systèmes d'information se trouvant sur le(s) site(s) où s'exercent leurs responsabilités.

Missions des ASSI

1. Au plan de la protection des personnes

- tenir à jour la liste des agents affectés au traitement des informations ;

- faire surveiller en permanence les activités du personnel extérieur, comme le personnel de maintenance, les visiteurs temporaires ou le personnel de nettoyage, appelé à effectuer des travaux temporaires ;
- s'assurer de l'application, par les agents de l'entité, des règles de sécurité prescrites.

2. **Au plan de la protection des informations**
   - veiller à la mise en œuvre des mesures prescrites ;
   - tenir une comptabilité d'entrée et de sortie des supports d'information ayant reçu une mention de sensibilité, et en assurer périodiquement l'inventaire ;
   - faire appliquer les consignes de sécurité relatives à la conservation et au stockage des supports des informations sensibles classifiées ;
   - contrôler la destruction des informations qui ont une mention de sensibilité et qui doivent être expurgées du système.

3. **Au plan de la sécurité des systèmes et réseaux**
   - vérifier périodiquement le bon fonctionnement des dispositifs de sécurité ;
   - veiller au respect des procédures opérationnelles de sécurité propres au système de traitement utilisé ;
   - s'assurer de l'installation correcte, au plan technique, des différents matériels utilisés ;
   - établir et diffuser aux utilisateurs les éléments d'authentification pour les applications ayant reçu une mention de sensibilité ;
   - surveiller les opérations de maintenance ;
   - rendre compte de toute anomalie constatée.

Pour l'exercice de ses attributions, l'ASSI peut disposer **d'une équipe restreinte de sécurité.** La liste des ASSI et des équipes de sécurité doit être transmise au Président du Comité de sécurité. Les ASSI assistent aux réunions du Comité de sécurité.

IV. Autres Institutions, Organisations et entités privés

Les autres Institutions, Organisations et entités privées doivent s'inspirer de ce modèle d'organisation pour assurer la sécurité des systèmes d'information.

Article 5 : Contrôle et suivi de l'application de la PSSI-ES

La sécurité des systèmes d'information dans les départements ministériels fait partie des responsabilités propres à chaque ministre qui assure le contrôle et le suivi de l'application de la PSSI-ES. Chaque ministre doit prendre des dispositions en vue de faire:

- développer, à tous les niveaux, la culture de la sécurité ;
- appliquer les prescriptions réglementaires ;
- recenser les besoins en matière de sécurité des systèmes d'information et dégager les ressources nécessaires à ce sujet ;
- apprécier en permanence le niveau de sécurité des systèmes d'information.

Article 6 : Gestion des crises

Un centre d'alerte et de réaction aux attaques informatiques, dont l'objectif principal est d'élaborer une stratégie de traitement des incidents et de gestion des crises, doit être mis en place afin de rétablir le fonctionnement normal des systèmes d'information de l'Etat, notamment en cas d'attaques informatiques de grande ampleur.

Toutes les structures de sécurité précitées doivent remonter tout événement pouvant affecter la sécurité des systèmes d'information et qui doit être signalé aux organismes compétents notamment, l'Agence De l'Informatique de l'Etat (ADIE), l'Autorité de Régulation des Télécommunications et des Postes (ARTP), le Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information (STCC-SSI) et tout autre organisme de l'Etat intéressé par la sécurité des systèmes d'information. Les actions à mener doivent être coordonnées afin d'atteindre l'objectif recherché.

Article 7 : Mise en œuvre

Les objectifs à atteindre et les règles à mettre en application pour assurer la sécurité des systèmes d'information de l'Etat figurent à l'annexe, ci-jointe, qui fait partie intégrante de la présente instruction.

Article 8 : Date d'entrée en vigueur

La présente instruction entre en vigueur pour compter de sa date de signature.

Dakar, le

Macky SALL

Pas de texte

ANNEXE

MODALITES DE MISE EN ŒUVRE DES OBJECTIFS A ATTEINDRE ET DES REGLES A METTRE EN APPLICATION POUR ASSURER LA SECURITE DES SYSTEMES D'INFORMATION DE L'ETAT DU SENEGAL

Pas de texte

I. POLITIQUE D'ORGANISATION DE LA SECURITE DES SYSTEMES D'INFORMATION DE L'ETAT DU SENEGAL

Objectif 1 : *Mettre en place une organisation appropriée pour engager, puis contrôler la mise en œuvre et le fonctionnement de la sécurité des systèmes d'information.*

Règles

Il importe de faire du personnel un maillon fort de la sécurité des systèmes d'information de l'Etat. En effet, il faut faire face aux comportements et aux agissements du personnel, aussi bien permanent que contractuel, qui peuvent avoir une incidence sur la préservation des intérêts de l'Etat, notamment en matière de sécurité des systèmes d'information. Chacun des intervenants est informé de ses droits et obligations relatifs à la sécurité des systèmes d'information.

REG 1-1 : Au niveau pilotage, les membres du Comité de sécurité qui agissent en tant qu'Autorités Qualifiées pour la Sécurité des Systèmes d'Information (AQSSI) doivent au préalable subir une sensibilisation et une formation en matière de sécurité des systèmes d'information, en vue d'accomplir avec efficience les missions qui leur sont confiées.

REG 1-2 : Cette sensibilisation et cette formation doivent être confiées aux organismes compétents, notamment l'Agence De l'Informatique de l'Etat (ADIE), le Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information (STCC-SSI), l'Autorité de Régulation des Télécommunications et des Postes (ARTP) ou tout autre Organisme public ou privé dont les compétences sont avérées. Elles doivent, en outre, tenir compte de l'évolution des menaces et des attaques.

REG 1-3 : Au niveau opérationnel, les Agents de Sécurité des Systèmes d'Information (ASSI) doivent, en permanence, être sensibilisés sur leurs responsabilités et formés au même titre que les Autorités Qualifiées pour la Sécurité des Systèmes d'Information (AQSSI).

REG 1-4 : Une note d'organisation doit fixer la répartition des responsabilités au sein de l'entité ; cette note doit être proposée par le Responsable de la sécurité des systèmes d'information et validée par l'autorité de l'entité.

REG 1-5 : Le Responsable de la sécurité des systèmes d'information planifie les actions de mise en place de la PSSI-ES.

REG 1-6 : Le Responsable de la sécurité des systèmes d'information doit formaliser et tenir à jour les documents validés par le Chef de département (sur son périmètre).

II. SECURITE DU PERSONNEL

II.1 Sélection du personnel

Objectif 2 : *Les services chargés de recruter du personnel doivent s'entourer de toutes les garanties nécessaires pour n'engager que des agents qui ne présentent aucun caractère de vulnérabilité particulière pour la sécurité des systèmes d'information. Ainsi, les agents qui sont amenés, dans le cadre de leurs activités, à connaître des informations sensibles et à avoir accès aux moyens de traitement de l'information, doivent faire, au préalable, l'objet d'enquête de sécurité et de moralité, être habilités et signer une charte de confidentialité, conformément à la réglementation.*

Règles

REG 2-1 : A l'embauche, les agents doivent être informés, au préalable, de leur rôle sur la sécurité de l'information et leurs responsabilités dans l'application effective de la politique de sécurité de l'organisme.

REG 2-2 : Ils doivent s'engager à avoir un comportement responsable et qui ne représente aucun risque pour la sécurité de l'information.

REG 2-3 : Les agents, qui ont accès à l'information sensible et aux systèmes d'information, doivent faire, au préalable, l'objet d'enquêtes de sécurité et de moralité, être habilités et signer une charte de confidentialité et de non-divulgation desdites informations. Il doit en être de même pour les prestataires qui interviennent sur les systèmes d'information.

L'habilitation est la garantie que ces personnes peuvent, sans risque pour elles-mêmes comme pour la collectivité, connaître des informations sensibles.

REG 2-4 : Les agents, qui ont accès à l'information sensible et aux systèmes d'information, doivent être informés de leurs responsabilités en matière de sécurité de l'information et être prévenus des sanctions qui sont prévues en cas de violation de la politique de sécurité de l'organisme (Code pénal : articles 60 à 64 et 363 - loi 61-33 du 15 juin 1961 portant statut général des fonctionnaires : article 14, et tout contrat d'embauche).

REG 2-5 : Tout personnel utilisateur d'un système d'information, qui constate un événement susceptible de dénoter un incident de sécurité informatique, doit le signaler, sans délai, au service compétent.

REG 2-6 : Les données à caractère personnel doivent être protégées et traitées conformément aux dispositions de la loi 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel.

II.2 Affectation du personnel

Objectif 3 : *En cas de mouvement de personnel, des dispositions particulières doivent être prises pour gérer les arrivées, les départs et les mutations dans les systèmes d'information.*

Règle

REG 3-1 : En cas de mouvement, de changement de personnel, ou en cas de rupture de contrat ou de fin de contrat, tous les aspects relatifs à la sécurité de l'information doivent être pris en compte :

- la gestion et la révocation des comptes et des droits d'accès aux systèmes d'information ;
- la gestion du contrôle d'accès aux locaux ;
- la gestion des équipements mobiles ;
- la gestion du principe d'habilitation ainsi que des principes du besoin d'en connaître et d'utiliser.

II.3 Sensibilisation et formation du personnel à la sécurité des systèmes d'information

Objectif 4 : *Tous les agents doivent être sensibilisés et formés à la problématique de la sécurité de l'information lors de sessions de formation régulières. Ces sessions de formation doivent être adaptées aux différentes catégories de personnel. La sensibilisation et la formation doivent aller de pair : la sensibilisation justifiant la formation et la formation permettant de délivrer des messages. La sensibilisation jouera un rôle de prévention (faire prendre conscience des enjeux de la sécurité des systèmes d'information) mais aussi un rôle réactif (que faire en cas d'incident).*

Règles

REG 4-1 : Un programme de sensibilisation et de formation à la sécurité des systèmes d'information doit être élaboré, revu et régulièrement mis à jour.

REG 4-2 : Ce programme doit être cohérent avec la politique de sécurité de l'organisme.

REG 4-3 : Ce programme doit prendre en compte les différents niveaux de responsabilités des membres de l'organisme.

REG 4-4 : Ce programme doit être mis à jour régulièrement afin de prendre en compte les nouveaux agents et les enseignements tirés des incidents liés à la sécurité de l'information déjà survenus.

REG 4-5 : Ce programme doit faire apparaître clairement l'engagement de la direction sur la problématique de la sécurité des systèmes d'information.

REG 4-6 : Un programme de formation continue doit être mis en place pour les agents qui sont chargés de veiller à l'application effective de la politique de sécurité, afin qu'ils soient informés sur les menaces et vulnérabilités les plus récentes (veille technologique).

III. ACQUISITION ET DEVELOPPEMENT DES SYSTEMES D'INFORMATION DE L'ETAT DU SENEGAL

Objectif 5 : *Intégrer la sécurité durant tout le cycle de vie des systèmes d'information de l'organisme : il s'agit notamment de spécifier les exigences liées à la sécurité de l'information lors de l'acquisition et du développement de nouveaux systèmes d'information.*

III.1 Acquisition de nouveaux systèmes

Règle

Intégrer la sécurité à l'entame de chaque projet d'acquisition de nouveaux systèmes d'information, en mettant en place une procédure qui permet de réduire les risques en adoptant la mesure suivante :

REG 5-1 : Il faut prendre en compte les exigences liées :

- au contrôle d'accès et à la sensibilisation des utilisateurs sur leurs responsabilités ;
- à la protection pour ce qui concerne la disponibilité, la confidentialité et l'intégrité de l'information et des systèmes d'information ;
- à la journalisation, la surveillance et la détection de fuite de données.

III.2 Développement de logiciels

Règles

Il s'agit d'adopter une méthodologie de développement sécurisé et de veiller à sa mise en œuvre effective en appliquant les mesures suivantes :

REG 5-2 : Sécuriser les locaux utilisés pour le développement de logiciels et appliquer les recommandations relatives à la sécurité du langage choisi, notamment dans les phases de conception, du choix des référentiels, du contrôle des versions et de la correction du code source.

REG 5-3 : Appliquer les normes et standards en vigueur sur le développement sécurisé d'applications (ISO, IEC, ...).

REG 5-4 : En cas d'externalisation du développement de logiciels, le maître d'œuvre doit se conformer aux exigences de sécurité citées supra mais aussi considérer les problèmes relatifs aux licences d'utilisation, à la qualité du développement et aux tests de la sécurité à réaliser pendant le développement.

V. GESTION DES ACTIFS

Objectif 6 : *Les actifs de l'organisme, notamment en matière de système d'information, doivent être identifiés et affectés à des responsables qui doivent en assurer la protection.*

IV.1 Inventaire et responsabilités relatifs aux actifs

Règles

REG 6-1 : Procéder à un inventaire précis des actifs de l'organisme afin de les identifier et le mettre à jour.

REG 6-2 : Affecter les actifs à des responsables désignés et qui sont chargés d'assurer leur sécurité (classification, protection et contrôle d'accès).

REG 6-3 : Identifier, documenter, et mettre en œuvre des règles d'utilisation correcte de l'information, des actifs associés à l'information et des moyens de traitement de l'information.

REG 6-4 : Veiller à la restitution effective des actifs dans leur totalité, en cas de fin de contrat ou de mission.

REG 6-5 : Procéder à une classification des informations suivant leur sensibilité et leur caractère sensible (cf. Instruction présidentielle n° 0303 /PR du 16 juillet 2003).

IV.2 Manipulation des supports d'information

Règles

REG 6-6 : Les informations stockées dans des supports amovibles doivent être protégées contre toute divulgation, modification ou destruction.

REG 6-7 : Pour les matériels qui doivent être mis au rebut, il faut procéder à un effacement sécurisé des données qui y sont stockées tel que défini par l'Instruction présidentielle n° 0303 /PR du 16 juillet 2003.

VI. RELATION AVEC LES FOURNISSEURS

Objectif 7 : *Garantir la protection des actifs de l'organisme accessibles aux fournisseurs.*

La sécurité des systèmes d'information de l'organisme englobe tous les aspects, notamment organisationnel, technique, physique et environnemental. A ce titre, tous les intervenants qui ont accès aux systèmes d'information sont concernés par leur sécurité. Ainsi, les prestataires de service, qui sont amenés à intervenir dans les systèmes d'information, doivent se conformer à la politique de sécurité pour assurer la confidentialité, l'intégrité et la disponibilité des données de l'information et des systèmes d'information.

V.1 Sécurité de l'information dans la relation avec les fournisseurs

Règles

REG 7-1 : Mettre en place une politique de sécurité applicable aux différents fournisseurs (logistique, finance, informatique, …).

REG 7-2 : Mettre en œuvre des procédures permettant de surveiller la conformité aux exigences de sécurité de l'information pour chaque fournisseur.

REG 7-3 : Mettre en place un programme de sensibilisation du personnel en contact avec les fournisseurs sur les règles de sécurité applicables à ces derniers ainsi que sur le niveau d'accès aux systèmes d'information.

REG 7-4 : Mettre en place une charte de sécurité signée par les différentes parties qui doivent s'engager à en respecter scrupuleusement les clauses.

REG 7-5 : Rappeler les exigences légales et réglementaires sur les lois relatives à la protection des données à caractère personnel, sur les droits d'auteur et sur la propriété intellectuelle, et veiller à leur respect.

REG 7-6 : Mettre en place un point focal qui sera chargé de communiquer sur les questions de sécurité avec les fournisseurs.

V.2 Prestations de service et sécurité de l'information

Règles

REG 7-7 : Tous les intervenants doivent être pris en compte, notamment les sous-traitants qui travaillent pour le compte de fournisseurs.

REG 7-8 : Les clauses contractuelles entre les fournisseurs et l'entité doivent intégrer toute la chaîne d'approvisionnement informatique : conformité avec les normes relatives à la sécurité des produits informatiques, publication des exigences de sécurité satisfaites par leurs produits et en fournir la preuve.

REG 7-9 : Mettre en œuvre des procédures d'audit sur les prestations effectuées par les fournisseurs ainsi que sur la qualité de ces services.

VII. SECURITE PHYSIQUE

VI.1 Zones sécurisées

Objectif 8 : *Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisme.*

1. Périmètres de sécurité physique

Des périmètres de sécurité physique doivent être définis et utilisés pour protéger les zones contenant l'information sensible c'est-à-dire relevant notamment de secret de défense nationale et les moyens de traitement de l'information. Les mesures suivantes doivent mises en œuvre à cet effet.

Règles

REG 8-1 : Tous les centres de données, les salles des serveurs, les salles d'exploitation, les salles de commutation, les installations de stockage, les salles de service et les salles des équipements réseau doivent être considérées comme des zones sécurisées.

REG 8-2 : L'accès à ces zones ne doit être permis qu'au personnel muni d'une autorisation écrite ou d'un badge délivré par le responsable désigné.

L'accès provisoire peut être autorisé à des tiers (personnel extérieur, autre personnel de l'entité,...) après une autorisation écrite du responsable désigné et la récupération des téléphones ou appareils et matériels mobiles. Ce personnel doit être accompagné en permanence par au moins une personne autorisée.

REG 8-3 : Un registre d'accès doit être tenu à l'entrée de chaque zone sécurisée. Il doit contenir l'identité, le but, la signature, l'heure d'entrée et de sortie de toute personne accédant au site.

REG 8-4 : Un agent de sécurité doit être placé à l'entrée de chaque site sensible ; il est chargé des missions suivantes :

- interdiction en permanence de l'accès au personnel non autorisé ;
- inscription au registre d'accès ;
- contrôle des bagages à l'entrée et à la sortie ;
- gestion des alarmes de surveillance ;
- gestion des appels d'urgence ;
- toute autre tâche de sécurité de son ressort.

REG 8-5 : Les zones sécurisées doivent être fermées en dehors des heures de service. Toutes les fenêtres, portes, et issues de secours doivent être verrouillées. Tous les conduits de climatisation, élévateurs …, doivent être munis de grilles métalliques.

REG 8-6 : Tous les droits d'accès doivent être immédiatement révoqués en cas de départ à la retraite de l'agent, de démission, de suspension, de mutation ou de congé de longue durée.

REG 8-7 : Les enregistrements d'accès doivent être régulièrement sauvegardés et conservés pendant une période déterminée.

REG 8-8 : Chaque Agent de Sécurité des Systèmes d'Information (ASSI) doit choisir les techniques et les équipements appropriés sur la base des résultats d'une évaluation de risque physique et d'une analyse des coûts de contre-mesures ou des avantages associés.

2. Contrôle d'entrée physique dans les zones sécurisées

Les zones sécurisées doivent être protégées par des contrôles adéquats à l'entrée afin que seul le personnel autorisé y soit admis. Les règles suivantes doivent être appliquées :

Règles

REG 9-1 : L'entrée est autorisée sur présentation de la carte d'accès visiteur. L'identité du visiteur, le but de sa visite, l'heure d'entrée et de sortie ainsi que toute autre information utile le concernant, doivent être inscrits dans un registre. Il faut authentifier l'identité du visiteur à l'aide d'un moyen approprié.

REG 9-2 : Les visites ne sont pas autorisées en dehors des heures de service ou de pause.

REG 9-3 : Tous les agents doivent porter un moyen d'identification visible ; ils doivent immédiatement aviser le personnel de sécurité s'ils rencontrent des visiteurs non accompagnés et toute personne ne portant pas d'identification visible (exemple : port de badge).

REG 9-4 : L'accès à la salle de serveurs doit être limité aux seules personnes autorisées.

3. Sécurisation des bureaux, des salles et des équipements

Les mesures de sécurité suivantes doivent être appliquées aux bureaux, aux salles et aux équipements.

Règles

REG 10-1 : Les bâtiments doivent être discrets et ne donner que le minimum d'indications sur leur usage, sans signe évident, à l'extérieur comme à l'intérieur, identifiant la présence d'activités de traitement de l'information.

REG 10-2 : Les équipements-clés doivent être installés dans un emplacement non accessible au public. Ils doivent être configurés de manière à empêcher toute fuite d'information sensible, notamment par rayonnement électromagnétique (mise en place de cages de faraday).

REG 10-3 : Les répertoires et les annuaires téléphoniques internes, identifiant les emplacements des moyens de traitement de l'information sensible, ne doivent pas être facilement accessibles sans autorisation.

4. Travail dans les zones sécurisées

Les règles suivantes doivent être appliquées pour le travail dans les zones sécurisées.

Règles

REG 11-1 : Le personnel doit être informé de l'existence de zones sécurisées et qu'il n'y a accès que sur la seule base des principes du besoin d'en connaître et d'utiliser.

REG 11-2 : Le travail sans surveillance dans les zones sécurisées doit être évité pour des raisons de sécurité.

REG 11-3 : Les zones sécurisées inoccupées doivent être physiquement verrouillées et contrôlées périodiquement.

REG 11-4 : L'utilisation d'équipements photo, vidéo, audio ou d'autres dispositifs tels que les caméras intégrées à des appareils mobiles, doit être interdite, sauf autorisation.

5. Zones de livraison et de chargement

Les mesures suivantes doivent être mises en œuvre afin de séparer les zones sécurisées et les zones de livraison et de chargement.

Règles

REG 12-1 : Désigner la zone d'approvisionnement pour les matières entrantes (accès restreint au personnel de livraison).

REG 12-2 : Inspecter les matières entrantes, par des équipements appropriés, pour vérifier la présence éventuelle de substances dangereuses (substances explosives, chimiques, ou autres) avant qu'elles ne quittent la zone de livraison et de chargement.

REG 12-3 : Enregistrer les matières entrantes dès leur arrivée sur le site conformément aux procédures d'enregistrement des actifs.

REG 12-4 : Toute la comptabilité matière doit être effectuée par les directions chargées des équipements dans les différentes entités.

VI.2 Sécurité des matériels

Objectif 13 : *Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisme.*

1. Emplacement et protection des matériels

Il faut choisir un emplacement approprié pour le matériel et le protéger contre les menaces et les dangers environnementaux et les possibilités d'accès non autorisé.

Règles

REG 13-1 : Les installations sensibles doivent être équipées de systèmes d'alarme périodiquement contrôlés.

REG 13-2 : Tout le matériel doit être installé dans des salles sécurisées. Les portes et les fenêtres ne doivent pas être des moyens d'accès ou de connexion au matériel, de l'extérieur de la zone sécurisée. Des issues de secours doivent être prévues dans tous les sites.

REG 13-3 : Dans tous les sites sensibles, des dispositifs de détection et de lutte contre l'incendie tels que les détecteurs de fumée et les extincteurs, doivent être installés, contrôlés et testés régulièrement.

REG 13-4 : Les sites sensibles doivent être en briques réfractaires et ne doivent contenir aucun matériel inflammable tel que des meubles en bois, des rideaux ou des tapis.

REG 13-5 : Il faut utiliser les spécifications techniques des fabricants des matériels électriques et se conformer aux normes de sécurité électrique des sociétés locales prestataires d'électricité pour empêcher les incendies.

REG 13-6 : Il faut faire inspecter et tester régulièrement les installations électriques pour s'assurer de leur bon fonctionnement (systèmes d'éclairage, interrupteurs, câbles électriques, générateur de secours, …).

REG 13-7 : Une alimentation électrique d'urgence doit être sauvegardée par un générateur de secours.

REG 13-8 : Tous les équipements sensibles doivent disposer d'une alimentation électrique permanente.

REG 13-9 : Le matériel doit être installé sur un support surélevé. Des systèmes de détection de fuite d'eau doivent être installés dans les sites sensibles.

REG 13-10 : Des systèmes de climatisation, de ventilation, d'alimentation en gaz et d'évacuation des eaux usées doivent être installés, entretenus et vérifiés régulièrement pour

empêcher d'éventuels endommagements des actifs et l'interruption des activités de l'entité. Des appareils de mesure de l'humidité et de la température doivent être prévus.

REG 13-11 : Les sites de reprise sur sinistre et de stockage de données doivent être installés à des endroits très éloignés du site principal.

REG 13-12 : Le matériel ou le support de stockage défectueux et les pièces de rechange, mis au rebut, doivent être stockés dans une pièce séparée qui doit être en permanence verrouillée.

REG 13-13 : La salle d'équipements et les racks (système de baie métallique aux dimensions standardisées permettant de monter divers modules électroniques les uns au-dessus des autres) ne doivent comporter aucun signe écrit décrivant leurs noms, leurs buts, les diagrammes de réseau, les numéros de ports, les adresses IP, etc.

REG 13-14 : Les équipements doivent être nettoyés régulièrement pour éviter notamment la poussière.

REG 13-15 : Il doit être strictement interdit d'effectuer des activités autres que celles prévues dans les salles abritant des équipements sensibles.

REG 13-16 : Il doit être strictement interdit de manger, de boire et de fumer à l'intérieur de la zone sécurisée.

2. Sécurité du câblage

Il faut assurer la sécurité des câbles électriques ainsi que les câbles de télécommunication qui transportent les données de l'organisme pour empêcher les interférences, le piratage, leur endommagement ou l'interception des informations par des tiers non autorisés.

Règles

REG 14-1 : Les lignes électriques et les lignes de télécommunication branchées aux systèmes d'information doivent être enterrées autant que faire se peut, par mesure de sécurité.

REG 14-2 : Les câbles électriques doivent être séparés des câbles de télécommunication pour empêcher les interférences.

REG 14-3 : Tous les câbles de télécommunication doivent être fiables et installés dans des conduits. Des câbles redondants doivent être installés pour assurer une reprise rapide des services.

REG 14-4 : Les câbles électriques doivent être installés dans des conduits appropriés.

REG 14-5 : Les panneaux de brassage et les salles des câbles doivent être isolés des zones d'accueil du public avec un accès contrôlé.

REG 14-6 : Les panneaux de répartition électrique ainsi que les chambres de câblage doivent être strictement contrôlés et l'accès limité au personnel autorisé.

REG 14-7 : Tous les sites sensibles doivent être équipés de paratonnerres et de parafoudres pour protéger respectivement les bâtiments et les matériels.

3. Maintenance des matériels

Les mesures suivantes doivent être prises pour entretenir correctement tous les matériels de l'organisme en vue d'assurer leur disponibilité permanente et leur intégrité.

Règles

REG 15-1 : Seul le personnel autorisé doit effectuer le service de maintenance.

REG 15-2 : Les unités de maintenance doivent établir un contrat avec les fournisseurs accrédités, immédiatement après la mise en service du matériel.

REG 15-3 : Les clauses du contrat doivent tenir compte des intérêts de l'organisme. Elles doivent préciser la qualité de service, la disponibilité, le temps de réponse, les politiques de rechange, les modalités de paiement, etc. Le responsable de l'entité doit approuver le contrat.

REG 15-4 : Les unités de maintenance doivent ouvrir un registre pour la traçabilité de leur travail, des paiements effectués, de la qualité, de la performance et de l'expiration du contrat.

REG 15-5 : Le travail effectué par les fournisseurs doit être approuvé, notamment par les administrateurs systèmes, réseaux et de bases de données ; ils doivent tenir un registre, à ce sujet.

REG 15-6 : Les activités de maintenance doivent être effectuées sous une surveillance étroite et adéquate des ASSI. En cas d'intervention d'un prestataire, ils doivent toujours être présents et veiller à ce qu'aucun fichier ou programme de données ne soit copié.

REG 15-7 : Les dossiers de maintenance doivent être conservés pour suivi.

REG 15-8 : En cas de remise d'un équipement pour réparation, les données qui y sont contenues doivent être sauvegardées dans d'autres supports et être supprimées de manière sécurisée.

4. Politique du bureau propre et de l'écran vide

La mise en place d'une politique du bureau propre et de l'écran vide réduit les risques d'accès non autorisés, de perte et d'endommagement de l'information pendant et après les heures de travail. L'utilisation de coffres forts ou d'autres moyens de stockage sécurisés peut également contribuer à la protection de l'information contre les sinistres tels que les incendies, les tremblements de terre et les inondations ou explosions.

Règles

REG 16-1 : Les supports amovibles de stockage de données sensibles tels que les disques durs, les disquettes, les bandes magnétiques, les CDROM, les DVD, les Blu-ray, les clés USB, les cartes SD, les cartes à puces …, doivent être conservés dans un coffre ou une armoire au même titre que les documents et correspondances sensibles sur support papier.

REG 16-2 : Après les heures de travail ou en l'absence des utilisateurs, les clefs des locaux, des coffres et des armoires doivent être gardées dans un endroit sûr accessible aux seules personnes autorisées. Toute sortie de clé doit être contrôlée, et les personnes autorisées doivent être désignées par l'autorité responsable.

REG 16-3 : Les fichiers contenant des informations classifiées et qui sont périmées doivent être effacés. Cette destruction ne doit pas être uniquement logique mais elle doit être accompagnée d'un effacement physique pour prévenir toute possibilité de lecture.

REG 16-4 : Les documents contenant des informations sensibles ou classifiées doivent être immédiatement retirés des imprimantes, des photocopieuses, des scanneurs, des appareils de télécopie après leur utilisation.

REG 16-5 : En l'absence de leurs utilisateurs, les ordinateurs et les terminaux doivent être déconnectés ou protégés par un verrouillage automatique (délai court) de l'écran ou du clavier contrôlé par un mot de passe ou un autre mécanisme d'authentification.

REG 16-6 : L'utilisation non autorisée des photocopieurs et autres appareils de reproduction (par exemple les scanneurs ou les appareils photo numériques) doit être strictement interdite.

REG 16-7 : Il faut utiliser des imprimantes dotées d'une fonction d'identification par code personnel, afin que seules les personnes ayant initiés une tâche d'impression puissent récupérer leurs documents imprimés et uniquement lorsqu'elles se trouvent à proximité de l'imprimante.

VIII. SECURITE LOGIQUE

La sécurité logique complète la sécurité physique. Son objectif est de protéger les systèmes d'information contre l'intrusion et d'assurer la confidentialité des données.

La sécurité logique est composée de la sécurité des accès, de la sécurité des applicatifs et de la sécurité des échanges.

VII.1 Sécurité des accès (Principes du besoin d'en connaître et d'utiliser)

Objectif 17 : *Il faut mettre en œuvre une politique de la sécurité des accès basée sur les exigences métier et de sécurité de l'information : un accès au système d'information et aux données, basé respectivement sur les principes du besoin d'en connaître et du besoin d'utiliser et, partant, du moindre privilège. Chaque utilisateur n'a accès qu'au système d'information et aux données dont il a besoin pour accomplir les tâches qui lui sont assignées.*

Règles

Il faut fixer les règles autorisant ou non l'établissement de connexion entre l'organisme et l'extérieur, ou entre zones dans l'organisme, pour une bonne politique de sécurité des accès :

REG 17-1 : Spécifier les mesures de sécurité pour les applications métier.

REG 17-2 : Appliquer le principe du besoin d'en connaître : « Nul ne peut, du seul fait de son grade ou son titre, avoir accès aux informations sensibles s'il n'est pas habilité et s'il n'a pas besoin d'en connaître pour réaliser ses tâches (différentes tâches ou fonctions impliquent des besoins d'en connaître différents, d'où des profils d'accès différents) ».

REG 17-3 : Appliquer le principe du besoin d'utiliser : « Nul ne peut, du seul fait de son grade ou son titre, avoir accès aux moyens de traitement des informations sensibles, s'il n'est pas habilité et s'il n'a pas besoin de les utiliser pour accomplir son travail (matériels informatiques, applications, procédures, salles) ».

REG 17-4 : Effectuer un cloisonnement des rôles pour le contrôle des accès.

REG 17-5 : Mettre à jour régulièrement les droits d'accès attribués aux utilisateurs.

REG 17-6 : Revoir régulièrement les privilèges et les droits d'accès en cas de changement de poste de travail.

VII.2 Sécurité des applicatifs

Objectif 18 : *Le contrôle d'accès doit prendre en compte les applications système et les applications métiers. L'accès à ces applications doit être limité conformément à la politique de contrôle d'accès.*

Règles

REG 18-1 : Un mécanisme permettant de contrôler l'accès aux fonctions d'application système doit être mis en place.

REG 18-2 : Les droits d'accès des utilisateurs doivent être contrôlés (lecture, écriture, suppression, …).

REG 18-3 : Il faut restreindre l'accès aux applications par un mécanisme de connexion sécurisée.

REG 18-4 : Une technologie d'authentification forte doit être utilisée lorsque les données sont classifiées.

REG 18-5 : Il faut limiter le nombre de connexions non autorisées aux applications.

REG 18-6 : Il ne faut pas afficher d'informations qui peuvent fournir des indications lors d'une tentative de connexion non autorisée.

REG 18-7 : Les mots de passe par défaut doivent être changés impérativement.

REG 18-8 : Il faut mettre en place un système de contrôle des tentatives de connexion automatique et fermer les sessions inactives au bout d'un certain temps d'inactivité. Toutes les tentatives de connexion doivent être journalisées.

REG 18-9 : Les mots de passe doivent être robustes. Ils ne doivent pas être transmis en clair. Il faut les changer régulièrement suivant une périodicité définie.

REG 18-10 : Il faut prévenir rigoureusement et interdire formellement l'installation de logiciels sans l'autorisation de l'Agent de la Sécurité des Systèmes d'Information (ASSI).

REG 18-11 : Les applications ou utilitaires non indispensables doivent être désinstallées.

REG 18-12 : L'accès au code source des applications doit être contrôlé afin d'en assurer l'intégrité.

VII.3 Sécurité des échanges

Objectif 19 : Assurer la sécurité des données échangées dans les réseaux de communication. Se conformer aux recommandations de la Commission nationale de cryptologie pour le choix des algorithmes de chiffrement et de signature numérique.

Règles

Les services de réseau comprennent la fourniture de connexion, les services de réseau privé, les réseaux à valeur ajoutée et les solutions de management de la sécurité des réseaux comme les pare-feux et les systèmes de détection d'intrusion. Ces services peuvent aller du simple octroi d'une bande passante non gérée à des offres complexes à valeur ajoutée.

Pour tous les services de réseau, il convient d'identifier les mécanismes de sécurité, les niveaux de service et les exigences de gestion, et de les intégrer dans les accords de services de réseau, que ces services soient fournis en interne ou qu'ils soient externalisés.

Il faut, par conséquent, prendre des mesures pour garantir aussi bien la sécurité des données échangées que celle des supports de transmission.

REG 19-1 : Il faut mettre en place une politique d'accès aux réseaux de l'entité, qui précise les exigences d'authentification des utilisateurs.

REG 19-2 : Il faut définir les responsabilités et les procédures de gestion des équipements réseau.

REG 19-3 : Les moyens de transmission de l'information doivent être conformes à la législation en vigueur.

REG 19-4 : Il faut mettre en place un mécanisme de surveillance et de journalisation de toutes les activités dans le réseau.

REG 19-5 : Les données transmises via les réseaux publics doivent être protégées selon leur niveau de classification. Il faut utiliser les réseaux de l'Etat, autant que faire se peut, pour transmettre des données hors de l'entité.

REG 19-6 : Les services de réseau doivent, en accord avec le fournisseur, être sécurisés par des fonctions de sécurité : l'authentification, l'intégrité, le chiffrement, la non répudiation et les contrôles de connexion réseau.

REG 19-7 : Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifiques. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, validées par le HFD concerné, doivent être prises dans le cadre de la défense en profondeur.

En particulier, une segmentation du réseau doit être mise en place de façon à limiter, à un périmètre déterminé, les conséquences d'une intrusion depuis la voie radio. A défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil, sur des systèmes d'information manipulant des données sensibles, est proscrit.

REG 19-8 : Il faut effectuer un cloisonnement, physique et/ou logique des réseaux informatiques, suivant un critère bien défini pour séparer les réseaux : par service administratif, par niveau de sécurité, etc.

REG 19-9 : Dans le cas d'une interconnexion avec un autre organisme ou lors de la mutualisation des moyens de traitement de l'information, il faut effectuer une analyse des risques afin de protéger les systèmes contenant des informations sensibles :

a) **Sur le plan des données échangées**, c'est-à-dire pendant la transmission de l'information, des procédures doivent être mises en place pour assurer sa protection:

REG 19-9-1 : Il faut choisir des algorithmes de chiffrement labellisés par la Commission nationale de cryptologie.

REG 19-9-2 : Il faut sensibiliser le personnel sur les risques de divulgation des informations classifiées.

REG 19-9-3 : Il faut sensibiliser le personnel sur les dangers, au plan de la sécurité, de l'utilisation des appareils indiscrets, comme le téléphone et la télécopie, pour échanger des informations sensibles. Il faut utiliser en lieu et place, des téléphones et des fax chiffrés sous réserve des dispositions de la loi n° 2008-41 du 20 août 2008 sur la cryptologie.

REG 19-9-4 : Les données transmises par le biais d'équipements électroniques doivent respecter la législation sur les transactions électroniques et les différents décrets d'application.

REG 19-9-5 : Il faut mettre en place un système d'authentification forte et un système de chiffrement pour sécuriser la messagerie électronique de l'entité.

REG 19-9-6 : Il faut assurer la disponibilité et la fiabilité de la messagerie électronique.

b) **Sur le plan des données stockées**, il faut mettre en place une politique de chiffrement de ces données pour garantir leur confidentialité, leur intégrité et leur authenticité ainsi qu'une politique de gestion des clefs de chiffrement. Ces mesures sont les suivantes :

REG 19-9-7 : Chiffrer une ou plusieurs parties des disques durs des systèmes d'information contenant les informations sensibles.

REG 19-9-8 : Lorsque le matériel ou le système d'information est mis hors service, en plus de l'effacement sécurisé des disques, l'intégralité de ces disques doit être chiffrée pour réduire le risque de divulgation de l'information sensible.

REG 19-9-9 : Il faut utiliser les moyens d'effacement sécurisé des données contenues dans les disques dur labellisés par la Commission nationale de cryptologie.

REG 19-9-10 : Il faut se conformer à la règle **19-9-1** pour le choix des algorithmes de chiffrement.

REG 19-9-11 : Il faut choisir des longueurs de clefs de chiffrement conformes aux recommandations de la Commission nationale de cryptologie.

REG 19-9-12 : Il faut mettre en œuvre une politique rigoureuse de gestion des clefs de chiffrement afin d'en assurer la protection, sans faille, durant tout leur cycle de vie.

REG 19-9-13 : Il faut former les utilisateurs à l'emploi correct des matériels et des logiciels de chiffrement.

VIII. SECURITE DE L'EXPLOITATION

VIII.1 Procédures et responsabilités liées à l'exploitation

1) Procédures d'exploitation documentées

Objectif 20 : *S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.*

Les procédures d'exploitation doivent être documentées et mises à la disposition de tous les utilisateurs concernés.

Règles

REG 20-1 : Des procédures bien documentées doivent être établies pour l'installation et la configuration des systèmes.

REG 20-2 : Une procédure bien documentée de redémarrage et de récupération de chaque système, en cas de défaillance, doit être définie et appliquée.

REG 20-3 : Une procédure bien documentée de sauvegarde et de maintenance, pour chaque système, doit être définie et appliquée.

REG 20-4 : Les contacts du support technique doivent être disponibles et tenus à jour, pour faire face notamment aux difficultés d'exploitation.

REG 20-5 : Les normes de sécurité de l'équipement doivent être documentées et suivies.

REG 20-6 : L'installation de logiciels n'ayant aucun rapport avec les activités de l'entité doit être prohibée.

REG 20-7 : L'utilisation de logiciels non autorisés, et sans une licence authentique, doit être strictement interdite.

REG 20-8 : Les procédures d'exploitation doivent être régulièrement auditées, contrôlées et mises à jour.

2) Gestion des changements

Objectif 21 : *Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information, qui influent sur la sécurité de l'information, doivent être autorisés et contrôlés à travers un processus de gestion de changement avec des mécanismes régulateurs appropriés. Lorsque des changements sont effectués, un journal d'audit, contenant toutes les informations pertinentes, doit être créé et maintenu.*

Règles

REG 21-1 : Il faut identifier et consigner les changements significatifs.

REG 21-2 : Il faut planifier les changements et la phase de test.

REG 21-3 : Il faut apprécier les incidences potentielles de ces changements sur la sécurité de l'information.

REG 21-4 : Une procédure d'autorisation formelle des changements proposés doit être mise en œuvre.

REG 21-5 : Il faut vérifier que les exigences de sécurité de l'information sont respectées.

REG 21-6 : Il faut transmettre les informations détaillées sur les changements apportés à toutes les personnes concernées.

REG 21-7 : Il faut mettre en œuvre les procédures de repli, incluant les procédures et les responsabilités en cas d'abandon et de récupération, suite à l'échec des changements ou à des événements imprévus.

REG 21-8 : Il faut mettre en place un processus de modification d'urgence permettant une mise en œuvre rapide et contrôlée des modifications requises par la résolution d'un incident.

3) Séparation des environnements de développement, de test et d'exploitation

Objectif 22 : *Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.*

Un niveau de séparation entre les environnements d'exploitation, de test et de développement doit être déterminé et mis en œuvre pour éviter les problèmes d'exploitation.

Règles

REG 22-1 : Les règles concernant le passage des logiciels du stade de développement au stade d'exploitation doivent être définies et documentées.

REG 22-2 : Il faut exécuter les logiciels de développement et les logiciels d'exploitation sur des systèmes informatiques différents et dans des domaines ou des répertoires différents.

REG 22-3 : Il faut tester les modifications à apporter aux systèmes et aux applications dans un environnement de test avant de les appliquer aux systèmes en exploitation.

REG 22-4 : Les activités de développement doivent être séparées des activités de test.

REG 22-5 : Les compilateurs, les éditeurs et les autres outils de développement ou les utilitaires systèmes ne doivent pas être accessibles depuis les systèmes en exploitation, lorsqu'ils ne sont pas nécessaires.

REG 22-6 : Les utilisateurs doivent utiliser des profils différents pour les systèmes en exploitation et les systèmes de test, et les menus doivent afficher les messages d'identification adéquats pour réduire le risque d'erreur.

REG 22-7 : Il ne faut pas copier de données sensibles dans l'environnement du système de test, à moins qu'il ne soit doté de mesures de sécurité équivalentes.

VIII.2 Protection contre les logiciels malveillants

Objectif 23 : *Garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.*

Règles

Mesures contre les logiciels malveillants

REG 23-1 : Un outil de protection contre les logiciels malveillants doit être installé sur tous les serveurs, les ordinateurs fixes et les terminaux mobiles.

REG 23-2 : L'utilisateur, ou à défaut, l'administrateur doit prendre toutes les mesures et effectuer les paramétrages nécessaires pour la mise à jour de l'outil (cf. REG 23-1) en vue de son fonctionnement efficient.

REG 23-3 : Il faut installer et mettre à jour régulièrement les logiciels de détection et de réparation pour analyser les ordinateurs et les supports (analyse des fichiers sur le réseau et sur les courriers électroniques). Ces opérations doivent inclure notamment l'analyse des fichiers reçus ou téléchargés, ainsi que celle des pièces jointes, attachées aux courriers électroniques, et l'analyse des pages web pour s'assurer de l'absence de logiciels malveillants.

REG 23-4 : En cas de détection de logiciels malveillants, une alerte doit être diffusée dans l'ensemble de l'entité.

REG 23-5 : Les courriers électroniques suspects, avec ou sans pièces jointes, ne doivent pas être ouverts.

REG 23-6 : Des anti-spams doivent être installés sur les serveurs de messagerie. Des listes noires en temps réel doivent être utilisées pour bloquer les spams.

REG 23-7 : Des filtres de contenus doivent être installés pour empêcher l'utilisation de sites web malveillants ou suspectés en tant que tels.

REG 23-8 : Etablir des procédures de continuité d'activités de l'organisme, après une attaque par logiciels malveillants, comprenant les sauvegardes de tous les logiciels et données nécessaires ainsi que les dispositions de sauvegarde.

REG 23-9 : Les utilisateurs doivent veiller à se protéger de l'introduction de logiciels malveillants qui peuvent contourner les mesures de protection habituelles, lors des opérations de maintenance et de dépannage.

REG 23-10 : Il faut s'assurer que les bulletins d'alerte concernant les logiciels malveillants sont exacts et informatifs, et proviennent de sources qualifiées (publications réputées, sites internet fiables, éditeurs de logiciels contre les logiciels malveillants) pour distinguer les canulars des menaces réelles. Tous les utilisateurs doivent être informés de l'existence de canulars et de la marche à suivre s'ils en découvrent.

VIII.3 Sauvegarde

Objectif 24 : *Une politique de sauvegarde pour faire face aux pertes de données de l'organisme doit être établie.*

La sauvegarde de l'information consiste à réaliser des copies de données, de logiciels et d'images système, et à les tester régulièrement conformément à une politique établie. Le mode et les équipements de sauvegarde doivent garantir une sécurité suffisante pour une exploitation ultérieure, en cas de sinistre et de défaillance du support.

Règles

REG 24-1 : Les données des utilisateurs, les configurations, les fichiers système et les messages électroniques doivent être périodiquement sauvegardés dans des serveurs dédiés, sur site et/ou hors site ou dans des supports de stockage amovibles.

REG 24-2 : La fréquence recommandée de sauvegarde est définie comme suit:

- sauvegarde incrémentielle quotidienne des données sensibles des utilisateurs ;

- sauvegarde complète, par semaine, des données non sensibles des utilisateurs ;
- sauvegarde complète, par semaine, des données du système;
- sauvegarde complète, par semaine, de la configuration du système et du réseau;
- sauvegarde régulière des informations stockées sur les serveurs centraux par l'administrateur système.

REG 24-3 : Le stockage en ligne gratuit, offert par certains prestataires privés, doit être interdit.

REG 24-4 : Il faut protéger les données sensibles sauvegardées en les chiffrant avec des moyens de chiffrement labellisés par la Commission nationale de cryptologie.

REG 24-5 : Les locaux de stockage des données sensibles doivent être sécurisés.

REG 24-6 : Les supports de stockage des données sauvegardées doivent être étiquetés selon une convention standard qui doit être suivie dans toute l'entité. L'étiquetage recommandé doit inclure le nom du site, le nom de la machine, le nom du lecteur, les données, la date et l'heure de sauvegarde, etc.

REG 24-7 : Un test de restauration doit être effectué périodiquement pour vérifier l'intégrité des données sauvegardées. La fréquence de ces tests doit être proportionnelle au degré de sensibilité des systèmes.

REG 24-8 : Les archives des données sauvegardées doivent être conservées pendant une durée déterminée, conformément aux lois et règlements en vigueur. Pour empêcher la perte des données archivées, à cause de l'obsolescence des moyens utilisés, celles-ci doivent être réécrites en utilisant les techniques modernes d'archivage. La décision de reconversion doit être prise par l'Agent de Sécurité des Systèmes d'Information (ASSI).

VIII.4 Journalisation et surveillance

Objectif 25 : *Enregistrer les événements et générer des preuves.*

Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et revus régulièrement.

Dans ce cadre, des mesures appropriées doivent aussi être prises pour prévenir l'accès non autorisé aux données sensibles et aux données à caractère personnel contenues dans les journaux

d'évènements. En outre, les administrateurs systèmes ne doivent pas avoir la possibilité d'effacer ou de désactiver les journaux concernant leurs propres activités.

Règles

REG 25-1 : Les journaux d'événements doivent contenir les informations suivantes :

- les identifiants des utilisateurs ;
- les activités du système ;
- la date, l'heure et les détails relatifs aux événements significatifs (exemple : ouvertures et fermetures de sessions) ;
- l'identité ou l'emplacement du terminal si possible et l'identifiant du système ;
- les enregistrements des tentatives d'accès au système réussies ainsi que celles avortées ;
- les enregistrements des tentatives d'accès aux données et autres ressources, réussies ou avortées ;
- les modifications apportées à la configuration du système ;
- l'utilisation des privilèges ;
- l'emploi des utilitaires et des applications ;
- les fichiers qui ont fait l'objet d'un accès et la nature de l'accès ;
- les adresses et les protocoles du réseau ;
- les alarmes déclenchées par le système de contrôle d'accès.

REG 25-2 : Les moyens de journalisation et l'information journalisée doivent être protégés contre les risques de falsification et les risques d'accès non autorisés.

REG 25-3 : Les fichiers de journalisation doivent être analysés par des outils automatiques destinés à cet effet.

REG 25-4 : Il faut journaliser les activités de l'administrateur système et les activités de l'opérateur système, protéger et revoir régulièrement les journaux.

REG 25-5 : Un système de détection des intrusions hors du contrôle des administrateurs système et réseau doit être utilisé pour vérifier la conformité des activités d'administration système et réseau.

REG 25-6 : Les journaux doivent être vérifiés de façon permanente.

REG 25-7 : Tous les événements majeurs doivent être enregistrés sur n'importe quel ordinateur ou système manipulant des données sensibles, y compris, mais sans s'y limiter, les échecs de connexion, les modifications de données, l'utilisation de comptes privilégiés, les changements de mode d'accès, les modifications apportées aux logiciels installés ou au

système d'exploitation et les modifications apportées aux autorisations accordées aux utilisateurs.

VIII.5 Synchronisation des horloges

Objectif 26 : *Synchroniser les horloges de l'ensemble des systèmes de traitement de l'information sur une source de référence temporelle unique.*

Règles

REG 26-1 : Toutes les horloges système, les horloges des ordinateurs et des périphériques réseau doivent être synchronisées à un serveur de temps central.

REG 26-2 : Le serveur de temps doit être doublé d'un serveur de secours installé dans un endroit sécurisé.

REG 26-3 : Les utilisateurs ne doivent pas être en mesure de changer la date, les paramètres du fuseau horaire ainsi que les paramètres de synchronisation du temps ou de l'horloge du système.

VIII.6 Installation de logiciels sur les systèmes en exploitation

Objectif 27 : *Mettre en œuvre des procédures pour contrôler l'installation de logiciels sur les systèmes en exploitation*

Les systèmes en exploitation doivent être examinés et testés lorsque des changements surviennent. Les modifications de logiciels doivent être autorisées avec une analyse d'impact appropriée.

Des procédures pour contrôler les installations de logiciels sur les systèmes en exploitation doivent être mises en œuvre.

REG 27-1 : La mise à jour des logiciels en exploitation, des applications et des bibliothèques des programmes doit être effectuée par des administrateurs qualifiés après autorisation du responsable de l'entité ou de l'AQSSI.

REG 27-2 : Les correctifs doivent être recommandés par les administrateurs système ou par les éditeurs du logiciel.

REG 27-3 : Les correctifs doivent être appliqués sur un site de test, et si aucune anomalie n'est constatée, ils sont appliqués sur le site de production. Les correctifs critiques doivent avoir une haute priorité et être immédiatement installés.

REG 27-4 : Les responsables des processus dépendants d'un logiciel doivent être informés avant l'application d'un correctif critique.

REG 27-5 : Une sauvegarde complète doit être effectuée avant l'application d'un correctif.

REG 27-6 : Les correctifs doivent être installés manuellement sur les systèmes qui ne sont pas connectés à internet.

REG 27-7 : Les ordinateurs qui sont connectés à internet doivent être configurés pour télécharger automatiquement les mises à jour recommandées. Les ordinateurs qui ne sont pas connectés à internet doivent être mis à jour manuellement.

REG 27-8 : Les mises à niveau, mises à jour et correctifs doivent être journalisés par l'administrateur système dans un registre.

REG 27-9 : Si l'application automatique d'un correctif ou d'une mise à jour affecte négativement les systèmes, il faut rétablir les systèmes originaux à partir des sauvegardes.

IX. CLOUD COMPUTING, APPAREILS MOBILES ET TELETRAVAIL

De nos jours, les systèmes d'information deviennent de plus en plus flexibles en raison de l'adoption de nouvelles technologies telles que :

- le Cloud computing (ou informatique en nuage) qui consiste généralement à exploiter via internet des ressources et des applications distantes ;
- l'utilisation des terminaux mobiles (ex: portables, smartphones, tablettes, …) pour accéder à un système d'information de l'entité.

Objectif 28 : *Permettre au personnel de mieux appréhender les problèmes de sécurité relatifs au Cloud computing, à l'utilisation des appareils mobiles et au télétravail.*

Règles

L'accès à distance au réseau de l'organisme n'est pas sans risques pour la sécurité de l'information. Il convient donc de prendre les mesures suivantes :

REG 28-1 : Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

REG 28-2 : L'hébergement des données sensibles de l'Administration sur le territoire national est obligatoire, sauf accord du HFD, et dérogation dûment motivée et précisée dans la décision d'homologation.

REG 28-3 : Sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'information, notamment les risques encourus dans le cadre du télétravail et de l'utilisation des terminaux mobiles dans les lieux publics, les aéroports, les chambres d'hôtel, les salles de congrès, de réunions, de conférences et dans d'autres zones non sécurisées.

REG 28-4 : Les appareils mobiles doivent être physiquement protégés contre le vol, en cas de déplacement des utilisateurs. Ils doivent être mis sous clé et dotés de systèmes de verrouillage spéciaux.

REG 28-5 : Mettre en place une politique de contrôle d'accès, protéger les appareils mobiles contre les logiciels malveillants, effectuer des sauvegardes et éviter l'installation d'applications non approuvées.

REG 28-6 : Empêcher la compromission et la divulgation des informations sensibles stockées et traitées par les appareils mobiles en utilisant les algorithmes de chiffrement labellisés par la Commission nationale de cryptologie.

REG 28-7 : Veiller à ce que les appareils mobiles de l'organisme ne soient utilisés que pour des usages professionnels.

REG 28-9 : Mettre en place un mécanisme d'effacement des données, en cas de perte d'appareils mobiles.

REG 28-8 : Eviter de se connecter au réseau de l'organisme par l'intermédiaire de réseaux sans fil non sécurisés.

REG 28-10 : Procéder au contrôle des appareils mobiles durant tout leur cycle de vie.

IX. GESTION DES INCIDENTS

Objectif 29 : *Etablir et mettre en place une procédure de gestion des incidents liés à la sécurité des systèmes d'information incluant la communication des événements et des failles de sécurité.*

Règles

REG 29-1 : Mettre en œuvre des procédures de surveillance, de détection, d'analyse et de signalement des événements et des incidents concernant les activités des réseaux.

REG 29-2 : Mettre en place, au sein de l'entité, une structure d'alerte et de réaction rapide à tout incident relatif à la sécurité des systèmes d'information, composée d'un personnel qualifié avec un point focal qui sert d'interlocuteur entre l'entité et les autres centres de gestion des incidents.

REG 29-3 : Les structures d'alerte et de réaction rapide doivent remonter tout incident lié à la sécurité des systèmes d'information de l'entité et les signaler aux organismes compétents (l'Agence De l'Informatique de l'Etat (ADIE), le Service Technique Central des Chiffres et de la Sécurité des Systèmes d'Information (STCC-SSI), l'Autorité de Régulation des Télécommunications et des Postes (ARTP) ...). Les actions à mener doivent être coordonnées afin d'enrayer les attaques et d'assurer la continuité du fonctionnement des systèmes d'information.

REG 29-4 : Un système de redondance des moyens de traitement de l'information doit être mis en place en vue d'en garantir la disponibilité.

REG 29-5 : Il faut revoir régulièrement le plan de continuité d'activités pour prendre en compte les changements intervenus dans le système d'information afin d'en maintenir la validité et l'efficacité.

REG 29-6 : Il faut tester périodiquement le plan afin de s'assurer de sa fiabilité.

REG 29-7 : Les utilisateurs doivent être formés sur les actions à mener en cas de violation de la politique de sécurité.

REG 29-8 : Les utilisateurs doivent être formés à la détection des actions suspectes ou anormales pouvant présager un incident lié à la sécurité des systèmes d'information (dysfonctionnements ou comportements anormaux du système d'information).

REG 29-9 : La procédure de réponse aux incidents doit comprendre : une phase de recueil et d'analyse des preuves, une communication détaillée sur l'incident survenu, la méthode de traitement utilisée, etc.

REG 29-10 : La procédure relative au recueil de preuves doit prendre en compte les éléments suivants :

a) la chaîne de traçabilité ;
b) les aptitudes et la sécurité du personnel pour effectuer la collecte des preuves numériques ;
c) les fonctions et les responsabilités du personnel ;
d) la documentation ;
e) les séances d'information.

Il faut appliquer la norme ISO/CEI 27037 qui fournit les lignes directrices concernant l'identification, l'acquisition et la protection des preuves numériques.

REG 29-11 : Il faut déterminer la typologie des incidents de sécurité, et en tirer tous les enseignements nécessaires.

XI. AUDIT ET CONFORMITE

Objectif 30 : *Eviter toute violation des dispositions législatives et réglementaires relatives à la sécurité des systèmes d'information.*

Règles

REG 30-1 : Il faut effectuer des audits pour s'assurer que les objectifs de sécurité sont atteints et que les politiques de sécurité sont conformes aux normes de sécurité en vigueur. Les rapports d'audit doivent être communiqués à la Commission nationale de cryptologie.

REG 30-2 : Les auditeurs des systèmes d'information de l'entité doivent être compétents.

REG 30-3 : Les auditeurs doivent établir des rapports d'audit à l'attention, notamment du Haut Fonctionnaire de Défense (HFD) accompagnés de recommandations à mettre en œuvre pour corriger les éventuelles anomalies. En cas de violation flagrante des procédures, des sanctions doivent être prises conformément aux textes en vigueur. Les rapports d'audit doivent être communiqués à la Commission nationale de cryptologie qui fera un rapport de synthèse à l'attention du Président de la République.

REG 30-4 : Toutes les structures auditées doivent appliquer les mesures proposées et faire leurs rapports de conformité.

REG 30-5 : Il faut se conformer aux lois et règlements concernant l'utilisation, l'importation, l'exportation et la fourniture des moyens et des prestations de cryptologie, les droits de propriété intellectuelle, la protection de la vie privée et des données à caractère personnel, la cybercriminalité et, partant, la cybersécurité.

REG 30-6 : La Commission nationale de cryptologie publie et met à jour régulièrement les normes de sécurité auxquelles doivent se conformer tous les systèmes d'information de l'Etat du Sénégal.

REG 30-7 : Des rapports complets doivent être communiqués aux autorités compétentes des entités de telle sorte que des mesures puissent être prises lors de la planification de futurs projets sur la base de l'expérience actuelle.