ROYAUME DU MAROC

ADMINISTRATION

DE LA DEFENSE NATIONALE

DIRECTION GENERALE DE LA SECURITE

DES SYSTEMES D'INFORMATION

DIRECTIVE NATIONALE DE LA SECURITE

DES SYSTEMES D'INFORMATION

Rabat, décembre 2013.

SOMMAIRE

PREAMBULE

Parallèlement au développement des technologies du numérique, on assiste aujourd'hui à la montée en puissance des vulnérabilités des systèmes d'information à cause de la multiplication et la diversification des activités illicites dans le cyberespace et des attaques informatiques qui ont perturbé à maintes reprises le fonctionnement des systèmes d'information et de communication de plusieurs pays.

Face à ces risques et menaces et à l'instar de ce qui se passe dans les pays avancés dans le domaine de la sécurité des systèmes d'information, le Comité Stratégique de la Sécurité des Systèmes d'Information (CSSSI) institué par le décret n° 2-11-508 du 21 septembre 2011 a adopté en date du 05 décembre 2012 la stratégie nationale de la cyber sécurité.

Cette stratégie a pour objectifs de doter nos systèmes d'information d'une capacité de défense et de résilience, à même de créer les conditions d'un environnement de confiance et de sécurité propice au développement de la société de l'information.

Afin de rendre opérationnelles les orientations et directives inscrites dans la stratégie susmentionnée, le Comité Stratégique a approuvé lors de la même réunion le plan d'actions 2013 de la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI).

Dans ce plan d'actions figure un ensemble de programmes déclinés en actions. Une des principales actions prise consiste à élaborer et mettre en œuvre une Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) avec pour objectifs d'élever et d'homogénéiser le niveau de protection et le niveau de maturité de la sécurité de l'ensemble des systèmes d'information des administrations et organismes publics ainsi que des infrastructures d'importance vitale (désignés dans la suite du document sous le terme « entité »).

La DNSSI décrit les mesures de sécurité organisationnelles et techniques qui doivent être appliquées par les administrations et organismes publics ainsi que les infrastructures d'importance vitale.

Pour arrêter les règles de la DNSSI, la DGSSI s'est inspirée de la norme marocaine NM ISO/CEI27002:2009 et s'est basée sur les résultats de l'enquête menée au mois de juillet 2013 auprès d'un échantillon représentatif d'administrations et organismes publics et d'opérateurs d'importance vitale.

Cette directive, appelée à évoluer et à être complétée par des dispositifs d'applications, constitue aujourd'hui la première référence nationale qui fixe les objectifs et les règles de SSI.

Ce socle de règles minimales peut être enrichi pour certains usages. Les mesures complémentaires nécessaires sont définies par les autorités concernées et partagées par la suite avec la DGSSI.

Pour la mise en œuvre de cette directive, chaque entité concernée définit un plan d'actions, élabore les mesures organisationnelles et techniques nécessaires et assure le suivi permanent.

En outre, chaque entité fait remonter au Centre de veille, de détection et de réponse aux attaques informatiques (ma-CERT) relevant de la DGSSI, les incidents significatifs constatés ainsi que le descriptif des dispositions mises en œuvre pour les résoudre.

Le suivi de la mise en œuvre de la DNSSI est sanctionné par l'élaboration d'un bilan annuel mesurant le degré de maturité atteint par l'entité concernée. Ce bilan est transmis à la DGSSI, qui consolidera une synthèse servant à la prise de décision du CSSSI, notamment pour arrêter le périmètre des audits à effectuer par la DGSSI.

Enfin, et dans le cadre des opérations de sensibilisation à la DNSSI, la DGSSI organisera un séminaire au profit des responsables de sa mise en œuvre au niveau des différentes entités. Cette sensibilisation prendra également la forme de contacts permanents avec lesdits responsables.

PREMIERE PARTIE: DISPOSITIONS GENERALES

La présente partie fixe les conditions de mise en œuvre de la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI).

1. PRINCIPES DIRECTEURS

La DNSSI s'appuie sur les principes directeurs suivants, issus de la Stratégie Nationale de la cyber sécurité, validée par le CSSSI en date du 05 décembre 2012:

- P1. Structure organisationnelle : Mettre en place une structure organisationnelle dédiée à la SSI au niveau de chaque entité pour inclure les volets préventifs et réactifs nécessaires à la cyber sécurité;

- P2. Cartographie des systèmes d'information : Tenir et mettre à jour une cartographie précise des systèmes d'information des entités ;

- P3. Budget de la sécurité des systèmes d'information : Quantifier et planifier le budget consacré à la sécurité des systèmes d'information de chaque entité, tant dans les volets investissements que moyens humains, et son rapport au budget global des systèmes d'information;

- P4.Contrôle des administrateurs : Contrôler et tracer les opérations de gestion et d'administration des systèmes d'information des entités;

- P5. Protection de l'information : Protéger les informations en suivant un ensemble de règles de sécurité précisées dans ce document;

- P6. Formation et sensibilisation : Former et sensibiliser le personnel, notamment les administrateurs systèmes et réseaux et les utilisateurs des systèmes d'information, de leurs droits et devoirs ;

- P7. Hébergement national des données sensibles : Héberger sur le territoire national les informations des entités, qui sont sensibles au regard de leur confidentialité, de leur intégrité ou de leur disponibilité.

2. CHAMP D'APPLICATION

La DNSSI s'applique à tous les systèmes d'information des administrations, des organismes publics et des infrastructures d'importance vitale.

La DNSSI s'adresse à l'ensemble du personnel de ces entités ainsi que les tiers (contractants, etc.).

3. DATE D'ENTREE EN VIGUEUR

La DNSSI entre en vigueur dès sa publication.

4. DISPOSITIONS TRANSITOIRES

La mise en application de la DNSSI s'effectue selon les règles suivantes :

- Les SI des entités doivent être en conformité totale dans les 3 ans suivant la publication de la DNSSI;

- Les entités devront avoir défini un plan d'actions de mise en conformité avec la DNSSI au plus tard une année après sa publication. Ce plan d'actions tiendra compte des impacts sur les activités, et des moyens financiers et humains à mettre en œuvre. Un calendrier de mise en conformité sera établi indiquant les mesures immédiates, les mesures à court terme et les mesures atteignables à moyen terme.

5. CONFORMITE JURIDIQUE ET REGLEMENTAIRE

Les exigences légales et réglementaires doivent être identifiées et documentées pour chaque système d'information des entités. Ces exigences peuvent concerner les éléments suivants:

- Protection des données à caractère personnel;
- Les dispositions en matière de certification électronique et de cryptographie;
- Respect de la propriété intellectuelle (par exemple : conservation des preuves d'achat des logiciels, nombre maximum autorisé d'utilisateurs sur un système, information du personnel sur les problématiques juridiques);
- Archivage légal, etc.

6. MISE EN APPLICATIONDE LA DNSSI

Pour la mise en application de la DNSSI, chaque entité établit son plan d'actions de mise en conformité avec la DNSSI précité à l'article 4.

Ainsi chaque entité doit:

- Désigner un responsable de la sécurité des systèmes d'information (RSSI) ;

- Etablir un inventaire de ses systèmes d'information, et en évaluer la sensibilité;

- Conduire une analyse de risques pour ses systèmes d'information, et veiller à la définition des mesures de sécurité applicables;

- Conduire des actions de sensibilisation et de formation à la sécurité des systèmes d'information et participer aux actions entreprises dans ce sens par la DGSSI ;

- Conduire des actions régulières de contrôle du niveau de sécurité des systèmes d'information et de son périmètre et mettre en œuvre les actions correctives nécessaires;

- Mesurer la résilience de leurs SI par des audits internes et le cas échéant de simulation d'exercices, etc.

Lors de l'élaboration du plan de mise en œuvre pluriannuelle de la DNSSI, les entités doivent prendre en considération plusieurs critères pour prioriser les règles de sécurité à adopter : impact de la mesure sur la sécurité du SI (poids donné pour chaque règle dans le document), coût estimatif de mise en œuvre, capacités techniques et humaines disponibles, complexité.

Il peut être nécessaire, dans certains cas spécifiques, de déroger à des règles énoncées par la DNSSI. Il appartient alors à l'autorité de l'entité concernée de leur substituer formellement des règles particulières.

Pour chacune de ces règles, la dérogation, motivée et justifiée, doit être expressément accordée par le RSSI de l'entité concernée. La décision de dérogation accompagnée de la justification est tenue à la disposition de la DGSSI.

7. SUIVI DE L'APPLICATION DE LA DNSSI

La DGSSI met à la disposition de chaque entité un tableau de bord pour le suivi de l'application de la DNSSI ainsi que les guides techniques d'implémentation des différentes règles de sécurité.

Chaque entité élabore son bilan annuel de mise en application de la DNSSI en se basant sur ledit tableau de bord, et le soumet annuellement à la DGSSI.

Le bilan annuel constitue une synthèse de l'état d'avancement de l'organisation en sécurité et de l'application des règles édictées par la DNSSI. Ce bilan comprend également un récapitulatif des actions réalisées pour la mise en conformité à la DNSSI, et une synthèse des incidents traités, des éventuels audits diligentés et des exercices menés.

8. EVOLUTIONS DE LA DNSSI

La DGSSI élabore les évolutions de la DNSSI, en liaison avec les administrations, organismes publics et infrastructures d'importance vitale, en prenant en compte:

- Les résultats d'analyses de risques ;
- Les évolutions des menaces et les retours d'expérience des traitements d'incidents ;
- Les évolutions des contextes organisationnel, juridique, réglementaire et technologique.

DEUXIEME PARTIE: OBJECTIFS ET REGLES DE SECURITE

Cette seconde partie traite les objectifs et les règles permettant de contribuer à la réalisation des principes directeurs et s'organise sous la forme des chapitres cités ci-dessous:

- Politique de sécurité de l'information;
- Organisation de la sécurité;
- Gestion des biens;
- Sécurité liée aux ressources humaines;
- Sécurité physique et environnementale;
- Gestion de l'exploitation et des télécommunications;
- Contrôle d'accès;
- Acquisition, développement et maintenance;
- Gestion des incidents;
- Gestion de la continuité d'activités;
- Conformité.

A chaque règle est associé :

- Un poids allant de 1 à 4 et qui traduit le niveau d'impact croissant de son non-respect sur le SI en termes de disponibilité, d'intégrité, de confidentialité ou de de traçabilité;
- Le(s)responsable(s) concerné(s)devant veiller à l'implémenter et/ou la faire respecter notamment la Direction Générale, le Secrétariat général, la Direction SI, RSSI….etc.).

Les entités doivent implémenter les règles selon un classement de sensibilité A, B ou C arrêté en commun entre l'entité et la DGSSI. Ces classes sont définies comme suit :

Classe A: Systèmes d'information sur lesquels une atteinte à la confidentialité, à l'intégrité ou à la disponibilité peut entraîner un impact **catastrophique** sur la capacité de l'entité à remplir les missions vitales pour la nation dont elle est chargée, sur ses biens essentiels, ou sur les individus.

Classe B : Systèmes d'information sur lesquels une atteinte à la confidentialité, à l'intégrité ou à la disponibilité peut entraîner un impact **Important** sur la capacité de l'entité à remplir ses missions assignées vis à vis des services de l'Etat fournis par cette entité, sur ses biens sensibles, ou sur les individus.

Classe C : Systèmes d'information sur lesquels une atteinte à la confidentialité, à l'intégrité ou à la disponibilité peut entraîner un impact **limité** sur les services offerts par l'entité, sur ses biens sensibles, ou sur les individus.

L'applicabilité d'une règle dépend de la classe du SI selon l'échelle suivante :

- Non applicable « N/A » : signifie que l'entité disposant d'un SI relevant de la classe peut ne pas appliquer la règle ;
- "applicable" : signifie que l'entité disposant d'un SI relevant de la classe doit appliquer la règle de sécurité;
- "=" : pour indiquer que les exigences d'une classe sont égales à celles d'une autre classe inférieure ;
- «+» et «++» : pour indiquer que les exigences d'une classe sont supérieures à celles d'une autre classe inférieure.

1. POLITIQUE DE SECURITE

Objectif O.1: Apporter à la sécurité de l'information une orientation et un soutien de la part du management de l'entité, conformément aux exigences de la DNSSI.

DS-CONF : Conformité avec la DNSSI

Chaque entité doit se conformer avec les exigences contenues dans le document de la DNSSI. Pour ce faire, il faut :

- Organiser et coordonner l'application de la DNSSI au sein des entités ;
- Formaliser et tenir à jour les documents d'application (Plan d'actions, règles spécifiques, procédures et charte);
- Budgétiser les projets de sécurité ;
- Et établir un calendrier précisant les étapes d'application de la DNSSI.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Secrétariat Général ou Direction Générale, DIRECTION SI, RSSI

DS-BESOIN : Besoins de sécurité

Chaque entité doit définir les besoins en matière de confidentialité, disponibilité, intégrité et traçabilité pour chaque processus dans le système d'information.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Secrétariat Général ou Direction Générale, DIRECTION SI, RSSI

DS-EXAM : Examen de la DNSSI

Le RSSI doit réexaminer régulièrement l'application des mesures de la DNSSI.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	=	=	RSSI

DS-TDB : Tableaux de bord

Le RSSI doit se servir d'un tableau de bord de la sécurité des systèmes d'information pour assurer le suivi de la bonne application des règles de la DNSSI.

Le tableau de bord est fourni par la DGSSI et devra permettre aux entités de s'auto-évaluer et calculer annuellement les écarts par rapport aux règles de la DNSSI.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	+	=	RSSI

2. ORGANISATION DE LA SECURITE

2.1. ORGANISATION INTERNE

Objectif O.2: Mettre en place au sein de l'entité une organisation adéquate garantissant une gestion préventive et réactive de la sécurité de l'information.

ORG-INTER-DIR : Implication de la direction

La hiérarchie de chaque entité doit valider les documents d'application de la DNSSI et définir les rôles et responsabilités en matière de SSI.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Secrétariat Général, Direction Générale

ORG-INTER-RSSI : Désignation d'un RSSI

Chaque entité est tenue de désigner un RSSI dont les tâches sont définies dans une fiche de poste. Eu égard à la nature de sa mission et afin de lui garantir l'indépendance requise, il est recommandé de rattacher le RSSI au Secrétariat Général ou à la Direction Générale.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Secrétariat Général, Direction Générale

ORG-INTER-AUT : Relations avec les autorités compétentes en SSI

Chaque entité doit entretenir des relations étroites avec la DGSSI autorité compétente en matière de SSI.

Le RSSI doit remonter à la DGSSI tout incident ayant un impact majeur sur la sécurité des systèmes d'information.

Dans ce cadre, il est tenu de partager avec la DGSSI les mécanismes mis en place pour traiter cet incident et à défaut de saisir la DGSSI afin de l'assister dans sa résolution.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	+	=	Secrétariat Général, Direction Générale, Direction SI, RSSI

2.2. TIERS

Objectif O.3: Assurer la sécurité de l'information et des moyens de traitement de l'information de l'entité, consultés, opérés, communiqués ou gérés par des tiers.

ORG-TIER-EXIG : Exigences vis-à-vis des tiers

Les exigences de sécurité (performances, disponibilité, ...) et les niveaux de service voulus doivent être inclus de façon précise dans les contrats conclus.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Secrétariat Général ou Direction Générale, DIRECTION SI

ORG-TIER-RISQ : Risques émanant des tiers

Chaque entité doit gérer les risques particuliers qui peuvent provenir des tiers en contrôlant et limitant strictement leurs droits. Elle doit s'assurer que les dispositions réglementaires et contractuelles, relatives à la sécurité des systèmes d'information, sont formalisées et appliquées.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	=	=	DIRECTION SI, RSSI

ORG-TIER-EXTER : Externalisation

En cas d'externalisation, des procédures qui planifient les transitions sont nécessaires et le respect de la DNSSI par le tiers est primordial.

Toute externalisation de service applicatif d'une entité doit faire l'objet d'un contrat sous droit marocain. Le contrat intégrera impérativement des engagements de protection de l'information, d'auditabilité et de réversibilité.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	MOA, DIRECTION SI, RSSI

ORG-TIER-HEBERG : Hébergement

L'hébergement des données sensibles des entités sur le territoire national est obligatoire.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	Secrétariat général ou Direction générale, MOA/MOE, DIRECTION SI

3. GESTION DES BIENS

3.1. RESPONSABILITES RELATIVES AUX BIENS

Objectif O.4: Inventorier tous les biens et leur attribuer un propriétaire.

RESP-BIEN-INV : Inventaire des biens

Un inventaire des ressources informatiques (matériels et logiciels) doit être réalisé et mis à jour régulièrement, intégrant notamment:

- ✓ La liste des composants matériels (avec n° de série) et logiciels (avec n° de licence) de la configuration ;
- ✓ La version du système d'exploitation et les correctifs appliqués ;
- ✓ L'identification de l'utilisateur dans le cas d'un poste de travail.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	=	=	DIRECTION SI

RESP-BIEN-CARTO : Cartographie SI

Chaque entité doit tenir et mettre à jour une cartographie de son SI en se basant sur l'inventaire des ressources informatiques.

La cartographie précise les composants matériels et logiciels, les centres informatiques et les architectures des réseaux sur lesquels sont identifiés les points névralgiques.

L'architecture réseau doit être décrite et formalisée à travers des schémas d'architecture et des configurations (protocoles, moyens de protection actifs et passifs, matrice des flux, etc.), maintenus au fil des évolutions apportées aux SI.

Les documents de cartographie sont sensibles. Ils feront l'objet d'une protection adaptée.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	DIRECTION SI

RESP-BIEN-PROP : Propriétaires des biens

Il est recommandé d'attribuer formellement chaque information et moyens de traitement de l'information à un propriétaire. Ce dernier est la personne ou l'entité ayant accepté la responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l'utilisation et de la protection des biens.

A ce propriétaire peut être affecté, un processus métier, un ensemble défini d'activités, une application ou un ensemble défini de données.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	+	=	RSSI

3.2. CLASSIFICATION DES INFORMATIONS

Objectif O.5: Classer les informations en termes d'exigences légales, de sensibilité et de criticité, afin de garantir un niveau de protection approprié.

CLASSIF-INFO-ECH : Echelle de classification

Tout document doit être classifié selon son niveau de sensibilité en termes de confidentialité.

L'attribution du niveau de sensibilité doit s'appuyer sur une échelle constituée des niveaux de sensibilité allant du document public au document très confidentiel.

Poids	Classes cibles			Responsables
4	C	B	A	
	Applicable	+	=	DIRECTION SI, RSSI, Utilisateur

CLASSIF-INFO- MES : Protection des informations

Chaque entité doit mettre en place les mesures adéquates au niveau de sensibilité des informations manipulées, en termes de : marquage, diffusion, stockage ou destruction, transmission… et les formaliser dans une procédure de classification des informations.

Un ensemble de mesures doivent entre autres s'appliquer:

- Les informations doivent porter de manière visible l'indication de leur niveau de sensibilité;
- La diffusion d'une information peut être :

- ✓ Possible dans le cas d'informations publiques après autorisation de publication auprès du responsable ;
- ✓ Ou libre en interne de l'administration ou l'organisme public;
- ✓ Ou bien seules les personnes mentionnées sur la liste de diffusion ont le droit de détenir le document.

- Des règles de stockage sur poste de travail, poste nomade, sur le réseau local ou bien des documents papiers doivent être bien identifiées.
- Les impressions de documents sensibles doivent faire l'objet d'un usage de moyens sécurisés d'impression et d'une récupération immédiate des documents imprimés.

Poids	Classes cibles			Responsables
4	C	B	A	DIRECTION SI, RSSI, Utilisateur
	applicable	+	=	

CLASSIF-INFO-EXAM: Examen de la classification

Il faut revoir périodiquement les classifications d'informations et l'application des règles contenues dans la procédure de classification des informations.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	+	=	RSSI

4. SECURITE LIEE AUX RESSOURCES HUMAINES

Objectif O.6: Garantir que le personnel, les contractants et les utilisateurs tiers connaissent leurs obligations en matière de SSI.

4.1. AVANT LE RECRUTEMENT

RH-AVT-ENQ: Personnel de confiance

Le personnel appelé à travailler au sein de l'entité sur des tâches sensibles doit faire l'objet d'une attention particulière.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	=	=	Secrétariat Général ou Direction Générale

RH-AVT- CONFID : Engagement de confidentialité

Une clause de confidentialité dans la charte d'utilisation des SI doit être signée par les nouveaux employés, précisant l'obligation de respecter l'ensemble des règles de sécurité en vigueur.

Poids	Classes cibles			Responsables
4	C	B	A	RSSI, Utilisateur
	applicable	+	=	

4.2. APRES LE RECRUTEMENT

RH-PDT- FORM : Formation du personnel

Chaque entité doit organiser régulièrement des sessions de formation et de sensibilisation au profit de ses employés en matière de SSI. La DGSSI organisera annuellement des sessions de formation et de sensibilisation.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	=	=	Secrétariat Général ou Direction Générale, DIRECTION SI, RSSI

4.3. A L'ISSUE DU CONTRAT OU EN CAS DE CHANGEMENT DE POSITION

RH-FIN-REST: Restitution des biens

Un processus formalisé de restitution des biens doit être mis en place dès lors qu'il s'agit d'un cas de départ, de cessation, de changement de fonction, de mutation d'un employé ou d'un personnel non permanent (stagiaires par exemple).

Afin de préserver l'intégrité et la confidentialité des informations, l'entité doit veiller à la formalisation d'une procédure de passation de consignes (transmission de données sous format papier et électronique) et de transfert éventuel des biens, en coordination avec le Service des Ressources Humaines (SRH).

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	=	=	Secrétariat Général ou Direction Générale, DIRECTION SI, SRH, RSSI

RH-FIN-ACC : Retrait des accès

Il faut établir un retrait des droits d'accès au système d'information en cas de départ, de cessation, de changement de fonction, ou de mutation d'un employé ou du personnel non permanent (stagiaires par exemple). Avant ce retrait, le SRH a obligation d'informer le service informatique et plus particulièrement l'administrateur du système et réseau du mouvement de personnel.

Poids	Classes cibles			Responsables
4	C	B	A	
	Applicable	+	=	DIRECTION SI, SRH, Administrateur systèmes et réseaux

5. SECURITE PHYSIQUE

5.1. ZONES SECURISEES

Objectif O.7: Empêcher tout accès physique non autorisé.

PHYS-DECOUP : Découpage des zones

Des zones physiques de sécurité doivent être délimitées pour protéger les systèmes d'information et les moyens de traitement associés, conformément à la classification des biens.

Ce découpage peut se faire selon la typologie suivante *:*

- Zones internes : autorisées uniquement au personnel de l'entité, aux tiers autorisés ou aux visiteurs accompagnés.
- Zones restreintes : autorisées aux personnes habilitées à consulter, à traiter et manipuler des informations ou des équipements sensibles.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Secrétariat Général, Direction Générale

PHYS-SIGNAL : Signalétiques

Les zones physiques de sécurité doivent être identifiées par une signalétique claire, visible et compréhensible.

Poids	Classes cibles			Responsables
1	C	B	A	
	applicable	=	=	Service des moyens généraux, RSSI

PHYS-PROC : Procédure de contrôle d'accès

Il faut formaliser la procédure de contrôle d'accès physique, la valider par le management et tenir le personnel au courant de son contenu.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	=	=	Secrétariat Général, Direction Générale, RSSI

PHYS-PUBLIC- RES : Accès réseau

Tout accès réseau installé dans une zone d'accueil du public doit être filtré ou isolé dureté du réseau informatique des entités.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Administrateur systèmes et réseaux, RSSI

PHYS-PUBLIC-INFO.SENS : Informations sensibles

Dans l'éventualité où une entité traite exceptionnellement des informations sensibles dans des zones publiques, des mesures spécifiques doivent être mises en place, notamment en matière de protection audiovisuelle, ainsi qu'en matière de protection des informations stockées sur les supports.

.Poids	Classes cibles			Responsables
3	C	B	A	
	N/A	applicable	+	RSSI, Utilisateur

PHYS-INTER/RESTR-DISPO : Dispositif de contrôle d'accès

Les entités sont tenues à mettre en place un dispositif de contrôle d'accès physique individualisé dans les zones restreintes. Pour accéder à ces zones, les tiers doivent être obligatoirement accompagnés.

Poids	Classes cibles			Responsables
	C	B	A	
4	applicable	+	=	DIRECTION SI, RSSI

PHYS-INTER/RESTR-TRACE : Traçabilité des accès

Chaque entité doit assurer la traçabilité des accès du personnel et des visiteurs externes aux zones restreintes, et conserver les enregistrements pour une durée d'au moins trois mois.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	Secrétariat Général, Direction Générale, DIRECTION SI, RSSI

PHYS-INTER/RESTR- VIDEOPROT : Vidéo protection

Les zones restreintes doivent être équipées de vidéo protection. Les enregistrements ne doivent être manipulés que par un nombre limité de personnes habilitées à cet effet.

Poids	Classes cibles			Responsables
3	C	B	A	
	N/A	applicable	+	Secrétariat Général, Direction Générale, DIRECTION SI, RSSI

PHYS-ENVIR-INCEN.FUM : Détecteurs d'incendie

Les zones restreintes doivent être équipés de systèmes de détection d'incendie.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Service des moyens généraux, DIRECTION SI, RSSI

PHYS-ENVIR-INCEN.EXTINCT: Extincteurs de feu

Les zones restreintes doivent être protégées par une installation d'extinction automatique d'incendie.

Poids	Classes cibles			Responsables
4	C	B	A	
	N/A	applicable	+	Service des moyens généraux, DIRECTION SI, RSSI

PHYS-ENVIR-EAU: Dégâts des eaux

Afin de se protéger des dégâts des eaux, tout équipement sensible ne doit pas être placé en rez-de-chaussée ou sous-sol. Si c'est le cas, il est nécessaire de prendre les mesures techniques adéquates.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	+	++	Service des moyens généraux, DIRECTION SI, RSSI

5.2. SECURITE DU MATERIEL

Objectif O8 : Empêcher la perte, l'endommagement ou la compromission des biens et l'interruption des activités de l'entité.

PHYS-MAT- CABL : Sécurité du câblage

Les câbles électriques et de transmission de données (courant fort et courant faible), connectés aux infrastructures de traitement de l'information doivent être identifiés (étiquetés), documentés et séparés (câbles déroulés en faisceaux clairs et non emmêlés) afin d'empêcher toute interférence électromagnétique et tout piégeage.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	DIRECTION SI, RSSI

PHYS-MAT-OND : Onduleurs

Les équipements informatiques et de téléphonie doivent être protégés des variations et des microcoupures d'électricité par des onduleurs.

Poids	Classes cibles			Responsables
4	C	B	A	
	Applicable	=	=	Service des moyens généraux, DIRECTION SI, RSSI

PHYS-MAT-ELECTROG : Groupe électrogène

Les équipements informatiques et de téléphonie doivent être secourus par un groupe électrogène.

Poids	Classes cibles			Responsables
2	C	B	A	
	N/A	applicable	=	Service des moyens généraux, DIRECTION SI, RSSI

PHYS-MAT-CLIM : Climatisation

Les zones abritant des systèmes d'information doivent être équipées de systèmes de climatisation.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Service des moyens généraux, DIRECTION SI, RSSI

PHYS-MAT-MAINT : Maintenance des équipements de sécurité

Le bon fonctionnement des équipements de sécurité (extincteurs, climatisation, détecteur d'incendie, onduleur, groupe électrogène, etc.) doit être contrôlé périodiquement.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	=	+	Service des moyens généraux, DIRECTION SI, RSSI

PHYS-MAT-MAINT. DELAI : Délai d'intervention

Un délai d'intervention adapté en cas de défaillance doit être précisé dans les contrats de maintenance des équipements de sécurité (extincteurs, climatisation, détecteur d'incendie et d'eau, onduleur, groupe électrogène, etc.).

Poids	Classes cibles			Responsables
2	C	B	A	
	N/A	applicable	+	Service des moyens généraux, DIRECTION SI, RSSI

PHYS-MAT-REB: Mise au rebut

Une procédure de mise au rebut des ressources informatiques doit être mise en place afin d'effacer les données présentes sur les disques durs ou la mémoire intégrée de manière sécurisée.

Dans le cas de données sensibles, la destruction de la ressource peut s'avérer nécessaire de manière à empêcher toute tentative de récupération.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	+	++	RSSI

6. GESTION DE L'EXPLOITATION ET DES TELECOMMUNICATIONS

6.1. PROCEDURES ET RESPONSABILITES LIEES A L'EXPLOITATION

Objectif O.9: Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information et gérer les actions d'administration du SI.

EXP-PROC-FORMEL : Procédures d'exploitation

Chaque entité doit documenter les procédures d'exploitation des moyens de traitement de l'information, les rendre disponibles, les expliquer à toute personne ayant besoin d'en connaître et les maintenir à jour.

Les procédures d'exploitation essentielles sont :

• Les procédures d'administration et de sécurisation des actifs critiques du système d'information ;
• Les procédures de sauvegarde (pour définir les mesures en place pour assurer et contrôler les sauvegardes) ;
• Les procédures de gestion des accès et des habilitations (pour décrire les mécanismes de gestion et de protection des accès) ;
• Les procédures de gestion des incidents (pour définir les processus de gestion des différents incidents) ;
• Les procédures de gestion des correctifs (pour définir les actions nécessaires au maintien à jour et en condition de sécurité des systèmes).

Toute modification dans les procédures d'exploitation doit faire l'objet du cycle: demande, validation, application, contrôles a posteriori.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	Administrateur systèmes et réseaux, MOE/MOA, RSSI

EXP-PROC-OIA- ACC : Accès aux outils et interfaces d'administration

L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	RSSI, Administrateur systèmes et réseaux

EXP-PROC-ADMIN-TRACE : Traçabilité des actions d'administration

Les actions d'administration doivent être tracées. Pour cela les comptes d'administration doivent être nominatifs pour assurer une imputabilité des actions.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	DIRECTION SI, RSSI

EXP-PROC-ADMIN- DIST : Administration à distance

Les actions d'administration à distance sur les ressources locales doivent s'appuyer sur des protocoles d'administration sécurisés.

Des mesures de sécurité spécifiques doivent être définies et respectées (accord explicite de l'utilisateur au moment d'un accès distant, traçabilité, etc.).

Poids	Classes cibles			Responsables
4	C	B	A	
	N/A	applicable	+	DIRECTION SI, Administrateur systèmes et réseaux, RSSI

EXP-PROC-ADMIN- CENTR : Centralisation

Il convient que les administrateurs systèmes et réseaux utilisent des outils centralisés, permettant l'automatisation et la supervision des traitements quotidiens, offrant une vue globale et pertinente sur le SI.

Poids	Classes cibles			Responsables
3	C	B	A	
	N/A	applicable	+	Administrateur systèmes et réseaux

6.2. ACCEPTATION DU SYSTEME

Objectif O.10:Réduire le plus possible le risque de pannes du système.

EXP-SYS-CONFIG : Configuration système

Les systèmes d'exploitation et les logiciels doivent être configurés et mis à jour selon des procédures formalisées (tests de non régression, compatibilité avec les logiciels métiers, etc.).

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Administrateur systèmes et réseaux

EXP-SYS-ANAL: Dimensionnement

Des analyses régulières du bon dimensionnement des systèmes et des réseaux (capacité mémoire, bande passante, temps de réponse, …) doivent être réalisées dans le but de mener les actions de redimensionnement améliorant la disponibilité du SI.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	+	++	Administrateur systèmes et réseaux

6.3. PROTECTION CONTRE LES CODES MALVEILLANTS

Objectif O.11: Protéger l'intégrité des logiciels et de l'information.

EXP-PROTEC-CODE.MALVEIL : Protection contre codes malveillants

Des logiciels de protection contre les codes malveillants ou solution antivirale doivent être installés et mis à jour sur l'ensemble des serveurs, postes de travail et équipements de mobilité.

Le personnel doit être informé sur les actions à mener en cas d'attaque par des codes malveillants (alerte, actions de confinement, déclenchement de processus de gestion de crise, etc.).

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	DIRECTION SI, RSSI

EXP-PROTEC-NAVIG : Sécurité du navigateur

Une configuration sécurisée du navigateur Internet doit être déployée sur l'ensemble des serveurs et des postes de travail pour tout accès Internet ou Intranet.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	+	++	Administrateur systèmes et réseaux

6.4. SAUVEGARDE DES INFORMATIONS

Objectif O.12: Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information

EXP-SAUV-PROC : Procédure de sauvegarde

Chaque entité doit mettre en place des procédures de sauvegarde qui précisent pour chaque système d'information :

- La nature des sauvegardes (complète, incrémentale, déduplication, …) ;
- La fréquence (journalière, hebdomadaire, mensuelle, …) ;
- Le type de support (sur disque, sur bande, Logs SGBD).

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Administrateur systèmes et réseaux, RSSI

EXP-SAUV-RESTAUR : Restauration

Chaque entité doit s'assurer périodiquement que les données sauvegardées peuvent être restaurées en temps voulu.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	MOE/MOA, Administrateur systèmes et réseaux

EXP-SAUV-PHYS : Sécurité physique des sauvegardes

Les supports de sauvegarde doivent être protégés physiquement. Et il convient de les placer à un endroit pour échapper aux dommages d'un sinistre sur le site principal. Pour ce faire, il faut se conformer aux bonnes pratiques en vigueur dans ce domaine.

Poids	Classes cibles			Responsables
3	C	B	A	
	N/A	Applicable	=	DIRECTION SI, RSSI

EXP-SAUV-SENSI: Sauvegarde sensible

Les données sensibles doivent être sauvegardées de manière chiffrée. Cela nécessite une saine gestion des clés de chiffrement.

Poids	Classes cibles			Responsables
4	C	B	A	
	Applicable	+	++	Administrateur systèmes et réseaux, RSSI

6.5. GESTION DE LA SECURITE DES RESEAUX

Objectif O.13: Assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle ils s'appuient.

EXP-RES-CONFIG : Configuration des équipements réseaux

Les configurations opérationnelles des équipements de communication et filtrage doivent être durcies notamment par rapport aux versions natives des fournisseurs par le changement des mots de passe et certificats, et la fermeture des services et des ports non nécessaires.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Administrateur systèmes et réseaux

EXP-RES-RSF : Sécurité des réseaux sans fil

Le déploiement du réseau sans fil doit être limité et doit faire l'objet d'une étude de sécurité spécifique.

Il est fortement conseillé de cloisonner le réseau sans fil du reste du réseau: une passerelle maîtrisée doit être mise en place permettant de tracer les accès et de restreindre les échanges aux seuls flux nécessaires.

Poids	Classes cibles			Responsables
3	C	B	A	
	Applicable	=	=	RSSI, Administrateur systèmes et réseaux

6.6. MANIPULATION DES SUPPORTS

Objectif O.14: Contrôler et protéger les supports amovibles et nomades.

EXP-NOM/AMOV-GEST : Gestion des supports amovibles

Il ne faut activer l'exécution automatique des supports amovibles que pour des impératifs de service.

L'accès aux supports amovibles doit faire l'objet d'un traitement adapté (chiffrement, contrôle anti-virus, etc.) surtout lorsqu'ils contiennent de l'information sensible.

Les supports amovibles doivent être fournis aux utilisateurs par les entités. Leur utilisation doit être encadrée par la charte d'utilisation des SI.

Poids	Classes cibles			Responsables
4	C	B	A	
	Applicable	=	+	Administrateur systèmes et réseaux

EXP-NOM/AMOV-STOCK : Sécurité physique des postes nomades et supports amovibles

Il faut stocker les postes nomades et les supports amovibles contenant des données sensibles dans des locaux protégés et tenir un registre de ces supports.

En cas d'utilisation de ces postes hors des locaux de travail (mission, conférence, réunion, etc.) une procédure formalisée doit être prévue pour leur protection.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	+	++	Secrétariat Général, Direction Générale, RSSI

EXP-NOM/AMOV-MES: Mesures de sécurité sur postes nomades et supports amovibles

Les postes nomades et les supports amovibles doivent être tous soumis aux mêmes mesures de sécurité que les autres équipements du parc en termes de mise à jour régulière de l'antivirus, application des correctifs, contrôle de conformité, interdiction des téléchargements à caractère non conforme à la charte d'utilisation des ressources informatiques.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	+	++	Administrateur systèmes et réseaux, RSSI

EXP-AMOV-SENSI : Données sensibles sur supports amovibles

Les données sensibles contenues dans des postes nomades ou des supports amovibles doivent être chiffrées par un dispositif de confiance.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	Administrateur systèmes et réseaux, RSSI

6.7. ÉCHANGE DES INFORMATIONS

Objectif O.15: Assurer la sécurité des échanges des informations et des supports physiques au sein de l'entité et avec un organisme externe.

EXP-ECHG-TELECOM: Les échanges par équipements de télécommunications

Des exigences de confidentialité doivent être définies pour les échanges d'informations sensibles qui transitent par tous types d'équipements de télécommunications (données, voix, audiovisuel, etc.).

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	Secrétariat Général, Direction Générale, Administrateur Systèmes et Réseaux

EXP-ECHG-PHYS.COUR : Supports physiques en transit

Les échanges physiques doivent faire l'objet d'un ensemble de mesures à mettre en place :

- Désigner des coursiers dûment habilités;
- Utiliser un emballage suffisant pour protéger le contenu ;
- Le cas échéant, assurer une livraison en main propre.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	+	=	Secrétariat Général, Direction Générale, Service des moyens généraux

EXP-ECHG-MAIL.PERSO: Usage de la messagerie professionnelle

Chaque entité doit définir dans la charte d'utilisation du SI le bon usage de la messagerie professionnelle. Elle doit expliciter les règles nécessaires pour la sécurité de la messagerie notamment:

- Interdire l'usage de la messagerie professionnelle à des fins personnelles et le renvoi automatique vers une messagerie non maîtrisée ;
- Vérifier la source des e-mails avant d'ouvrir les pièces jointes (attention aux codes exécutables);
- Accéder à distance à la messagerie professionnelle via VPN;
- Chiffrer et signer les messages sensibles par des moyens dédiés.

L'usage d'une messagerie personnelle peut être autorisé dans la mesure où elle est strictement confinée et ne met pas en danger le SI de l'entité.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	RSSI, Utilisateur

EXP-ECHG- MAIL.FILTR : Filtrage des mails

Chaque entité doit veiller à l'application des mécanismes de filtrage du courrier électronique émis et reçu notamment par:

- Contrôle antiviral des pièces jointes, leurs tailles et natures;
- Protection anti-spam;
- Contrôle des en-têtes SMTP.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Administrateur systèmes et réseaux

6.8. SUPERVISION

Objectif O.16:Détecter les traitements non autorisés de l'information.

EXP-SUPERV-MAINT : Traçabilité des actions de maintenance

Les interventions de maintenance sur les ressources informatiques de l'entité doivent être tracées par le service informatique. Ces traces sont à conserver pendant une durée d'au

moins trois mois et ce tout en déployant les mesures nécessaires pour assurer leur intégrité.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	Administrateur Systèmes et Réseaux, RSSI

EXP-SUPERV-JOURNAL: Journalisation des événements

Chaque entité doit mettre en place un journal répertoriant les événements de sécurité pour garantir la détection des problèmes liés au système d'information. Ces journaux doivent être analysés périodiquement et les actions à mener doivent être bien définies.

Les journaux d'événements peuvent notamment recenser les éléments suivants :

- Connexions au système (succès et échecs) ;
- Modification de paramètres de sécurité, de privilèges, de comptes utilisateurs, de groupes, etc. ;
- Événements système (arrêt / redémarrage de processus système sensibles) ;
- Accès/modification de données système ;
- Échec lors d'un accès à une ressource (fichier système, objet, réseau, etc.) ;
- Application des correctifs de sécurité ;
- Actions d'administration et de prise de main à distance ;
- Journaux du logiciel antivirus (si présent) : activation/désactivation, mises à jour, détection de codes malveillants, etc.

Ces journaux doivent être régulièrement sauvegardés.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	Administrateur systèmes et réseaux, RSSI

EXP-SUPERV-SYNCHRON : Synchronisation

Les serveurs doivent être synchronisés sur la même base de temps. Pour ce faire, il est nécessaire d'utiliser le service NTP de confiance (Network Time Protocol).

Le bon paramétrage des horloges est important, car il influe sur la précision des journaux d'événements qui peuvent être utilisés lors d'investigations. Des journaux imprécis peuvent porter atteinte à la crédibilité des traces.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Administrateur systèmes et réseaux

7. CONTROLE D'ACCES

7.1. GESTION DE L'ACCES UTILISATEUR

Objectif O.17: Maîtriser l'accès à l'information par l'application d'une politique du moindre privilège

ACC-UTILIS-IDF/AUTH : identification et authentification

L'accès des utilisateurs aux ressources (réseaux, système d'exploitation ou applications informatiques) passe obligatoirement par une identification et une authentification individuelle. Et les droits particuliers (super-utilisateur, Administrateur systèmes et réseaux,…) doivent être parfaitement identifiés, limités (nombre et droits) et justifiés.

Il convient de mettre à la disposition des utilisateurs une fiche d'habilitation écrite précisant leurs droits d'accès.

Un utilisateur doit disposer des droits nécessaires à l'exercice de son métier. Il ne doit pas, par contre, disposer de privilèges d'administration sur son poste de travail.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	DIRECTION SI, RSSI

ACC-UTILIS - MULTIUTILIS : Les sessions multiutilisateurs

Dans le cas de comptes multiutilisateurs (compte fonctionnel par exemple), la traçabilité des utilisateurs doit être assurée (par un cahier de suivi par exemple).

Poids	Classes cibles			Responsables
4	C	B	A	
	N/A	applicable	+	Administrateur Systèmes et Réseaux, RSSI

ACC-UTILIS-MDP : Gestion des mots de passe

Les règles de gestion des mots de passe doivent être définies et appliquées, en particulier:

- La structure (complexité minimale) ;
- Le changement périodique ;
- La suppression en cas de suspicion de compromission ;
- La réinitialisation.

Un contrôle automatisé de la robustesse des mots de passe doit être déployé.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Administrateur Systèmes et Réseaux, RSSI

ACC-UTILIS-EXAM : Examen des droits d'accès

Un examen périodique des droits attribués est nécessaire en s'appuyant sur l'inventaire des applications et des ressources utilisées.

Suite à cet examen, les comptes des utilisateurs ayant, à titre d'exemple, quitté l'entité, ou les comptes redondants doivent être supprimés.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	SRH, Administrateur Systèmes et Réseaux, RSSI

7.2. CONTROLE D'ACCES AU RESEAU

Objectif O.18: Empêcher les accès non autorisés aux services disponibles sur le réseau.

ACC-DISTANT-AUT: Utilisateurs distants autorisés

L'accès d'utilisateurs distants ne doit être réalisable que par des personnes autorisés et bien définies.

Des mesures d'authentification fortes par l'usage de protocoles sécurisés pour ce type de connexions sont nécessaires lors d'échanges sensibles.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Administrateur systèmes et réseaux

ACC-DISTANT-CHIFFR: Tunnelisation

Il faut chiffrer les connexions à distance par des protocoles sécurisés (IPSEC, SSL, SSH,..).

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Administrateur systèmes et réseaux

ACC-PORT-DIS : Ports d'accès distants

Il convient de désactiver ou de retirer les ports d'accès à distance inutiles installés sur un ordinateur ou un équipement en réseau.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Administrateur systèmes et réseaux

ACC-PORT-CONFIG : Ports de configuration

Les ports de diagnostic et de configuration ne doivent être accessibles qu'après accord du responsable du service informatique et cela pour la stricte durée nécessaire au traitement.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	Administrateur systèmes et réseaux

ACC-RES-SEG : Segmentation réseau

Il est recommandé de segmenter le réseau selon la sensibilité des données qu'il transporte.
La segmentation du réseau se fait par la mise en œuvre de zones démilitarisées (DMZ), et de réseaux locaux virtuels (VLAN) appropriés.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	=	=	DIRECTION SI, Administrateur systèmes et réseaux

ACC-RES- SEG.PROTEC : Protection des zones segmentées

Les zones segmentées doivent être protégées l'une des autres par la mise en place de règles de filtrage strictes des flux applicatifs et d'administration. La liste des règles de filtrage doit être documentée et tenue à jour.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	DIRECTION SI, Administrateur systèmes et réseaux

7.3. CONTROLE D'ACCES AUX APPLICATIONS ET A L'INFORMATION

Objectif O.19 : Empêcher les accès non autorisés aux informations stockées dans les applications.

ACC-APP-SENSI : Accès aux applications sensibles

Les applications sensibles doivent être protégées par des mécanismes de restriction des accès (login/mot de passe spécifiques, règles de filtrage et d'accès, plages horaires de connexions).

Les applications critiques doivent fonctionner sur des environnements informatiques dédiés (serveur spécifique…) et des architectures durcies (redondance, bascules, résilience, résistance aux attaques en déni de service, etc.).

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	+	DIRECTION SI, Administrateur systèmes et réseaux, RSSI

8. ACQUISITION, DEVELOPPEMENT ET MAINTENANCE

8.1. EXIGENCES DE SECURITE APPLICABLES AUX SYSTEMES D'INFORMATION

Objectif O.20: Veiller à ce que la sécurité fasse partie intégrante dans les projets de développement des systèmes d'information.

DEV-EXIG-PROJ : Exigences de sécurité dans les projets de développement

La sécurité doit être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	DIRECTION SI, MOE/MOA, RSSI

8.2. BON FONCTIONNEMENT DES APPLICATIONS

.

Objectif O. 21: Empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des informations dans les applications.

DEV-FONCT- ENTREE : Validation des données d'entrée

Les données en entrée des applications doivent faire l'objet d'un autocontrôle formel ou d'un contrôle de saisie indépendant afin de détecter des erreurs comme :

- les valeurs hors intervalle;
- les caractères invalides dans les champs de données;
- les données manquantes ou incomplètes;
- non-respect des limites inférieures et supérieures en termes de volume;
- paramètre de mesures de sécurité non autorisés ou incohérents.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	=	=	MOE/MOA, Utilisateur

DEV-FCT- INTERN : Traitements internes

Il convient d'inclure des fonctions de sécurité (programmation défensive) dans les applications afin de détecter les éventuelles altérations de l'information dues à des erreurs de traitement ou des actes délibérés.

Afin d'empêcher les attaques, il est nécessaire de respecter les préconisations des référentiels de développement sécurisé en fonction des langages choisis.

Poids	Classes cibles			Responsables
1	C	B	A	
	applicable	=	=	DIRECTION SI, MOE/MOA

DEV-FCT- SORT : Validation des données de sortie

Des contrôles de validation automatiques des traitements sensibles doivent être effectués pour s'assurer que les résultats sont cohérents et fiables.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	+	=	MOE/MOA

8.3. MESURES CRYPTOGRAPHIQUES

Objectif O.22: protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques.

DEV-CRYPTO-FICH: Mesures cryptographiques sur les fichiers et les transactions

Il faut définir les fichiers et les transactions devant être protégés par des solutions de chiffrement et/ou de signature électronique au niveau de l'architecture applicative.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	+	=	MOE/MOA, Utilisateur

DEV-CRYPTO-PKI : Système de gestion des clés

Il faut utiliser un système de gestion des clés (PKI). Une procédure de recouvrement des clés en cas de perte ou altération est nécessaire.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	DIRECTION SI, MOE/MOA, RSSI

8.4. SECURITE DES FICHIERS SYSTEME

Objectif O.23: Mener les développements logiciels selon une méthodologie de sécurisation du code source pour son intégrité.

DEV-CODE : Sécurité du code source

Il est recommandé de contrôler l'accès au code source du programme (restriction des droits, sources conservées hors des systèmes opérationnels, bibliothèques soumises à autorisation, etc.).

Poids	Classes cibles			Responsables
3	C	B	A	
	N/A	applicable	=	MOE/MOA

8.5. SECURITE EN MATIERE DE DEVELOPPEMENT ET D'ASSISTANCE TECHNIQUE

Objectif O.24: Empêcher toute possibilité de fuite d'informations.

DEV-FUITE : Fuite d'informations

Il faut limiter les fuites d'informations au niveau applicatif et mettre en place des contrôles adaptés (les développeurs doivent faire en sorte, par exemple, que les messages d'erreur renvoyés ne soient pas trop détaillés et avoir une vision commune de la gestion des exceptions).

Poids	Classes cibles			Responsables
3	C	B	A	
	N/A	applicable	+	MOE/MOA

8.6. GESTION DES VULNERABILITES TECHNIQUES

Objectif O.25:Réduire les risques liés à l'exploitation des vulnérabilités techniques ayant fait l'objet d'une publication.

DEV-VULN : Mesures aux vulnérabilités techniques

Des études de vulnérabilités système et applicative (scans des systèmes et des réseaux, tests d'intrusion) doivent être périodiquement menées. Cela nécessite une attention permanente sur les bulletins publiés par le ma-CERT.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	RSSI, Administrateur systèmes et réseaux

9. GESTION DES INCIDENTS

Objectif O. 26 : Garantir que le mode de notification des événements et failles liés à la sécurité de l'information permette la mise en œuvre d'une action corrective, dans les meilleurs délais.

9.1. SIGNALEMENT DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

INCID-SIGNAL : Signalement des événements liés à la sécurité des systèmes d'information

Une procédure de signalement d'incidents doit être formalisée. Celle-ci définit les mesures correspondantes à la remontée d'un événement par les employés : Il faut que l'ensemble des personnes impliquées dans la maintenance, l'exploitation, l'administration ou l'utilisation du système puisse noter et signaler dans les meilleurs délais tout dysfonctionnement de sécurité observé ou soupçonné dans l'usage normal du système et pouvant porter atteinte aux données ou au système lui-même.

Chaque incident de sécurité doit faire l'objet de la création d'un ticket d'incident permettant de gérer et de suivre sa résolution.

Pour les incidents significatifs, ceux-ci doivent être signalés au ma-CERT relevant de la DGSSI.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	DIRECTION SI, RSSI

9.2. GESTION DES AMELIORATIONS ET INCIDENTS LIES A LA SECURITE DE L'INFORMATION

INCID-PROC : Procédure de gestion des incidents

Les procédures de gestion d'incidents doivent couvrir les différents types d'incidents de sécurité (erreurs, sinistres naturels, malveillances, dénis de service, infections virales, intrusion, sabotage, saturation, etc.).

Chaque entité doit gérer les tickets d'incidents de sécurité.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	++	DIRECTION SI, RSSI

INCID-ACTION : Collecte de traces

En cas d'attaque suspectée, le principe essentiel est de ne rien faire pouvant entraver le travail d'investigation (effacer ou altérer des traces) ou avertir l'attaquant. La déconnexion physique des réseaux extérieurs peut s'avérer nécessaire pour sauvegarder une activité ou des données éphémères.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	+	=	Utilisateur

INCID-REACT : Réaction aux incidents

Dès qu'une alerte dommageable se déclenche, l'entité doit mobiliser les ressources internes et/ou externes pour réagir efficacement à ce type d'alerte.

Les alertes peuvent provenir soit d'un éditeur ou fournisseur, soit du centre de veille, de détection et de réponses aux attaques informatiques (ma-CERT) relevant de la DGSSI.

Dans ce dernier cas, l'entité accuse réception de l'alerte et transmet par la suite, si elle est impactée par cette alerte, un compte rendu d'exécution à la DGSSI.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	+	Secrétariat Général, Direction Générale, DIRECTION SI, RSSI

INCID-REP: Répertoire d'incidents

La typologie et la description des incidents doivent être localement enregistrées dans une base permettant un enrichissement progressif ainsi qu'un accès sélectif facile pour effectuer le traitement et le suivi des divers incidents futurs.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	=	=	RSSI

10. GESTION DU PLAN DE CONTINUITE DE L'ACTIVITE

Objectif O.27: Neutraliser les interruptions des activités de l'entité, protéger les processus métier cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.

10.1. ASPECTS DE LA SECURITE DE L'INFORMATION EN MATIERE DE GESTION DE LA CONTINUITE DE L'ACTIVITE

CONTINU-BIA : Continuité de l'activité et appréciation du risque

Il faut établir une analyse d'impacts sur l'activité de l'entité, qui consiste à:

- Identifier les activités et processus critiques ;
- Analyser les risques lies aux activités et processus;
- Analyser les impacts qui résulteraient d'un arrêt de ces activités et processus critiques ;
- Déterminer comment ces impacts évolueraient dans le temps en cas d'arrêt prolongé ;
- Etablir le temps d'arrêt ou d'indisponibilité maximum supportable des activités critiques ;
- Identifier et considérer toute activité critique dépendant des fournisseurs et autres tiers ;
- Estimer le délai cible de rétablissement des activités après un sinistre ;
- Estimer les ressources humaines, techniques et logistiques que chaque activité critique requiert pour sa reprise ;

Dans ce cadre, un questionnaire doit être mis à la disposition des responsables d'activités pour dérouler semestriellement cette opération.

Poids	Classes cibles			Responsables
4	C	B	A	
	N/A	applicable	+	Secrétariat Général, Direction Générale, DIRECTION SI, RSSI

CONTINU-ACT: Plan de Continuité et de Reprise d'Activité (PCA/PRA)

Le PCA/PRA doit regrouper l'ensemble des solutions pour pallier tous les arrêts des processus critiques et applications sensibles.

Chaque entité doit préparer un plan technique de continuité et de reprise d'activités intégrant l'ensemble des solutions de secours informatique (sauvegarde, site de secours, bascule, résilience des réseaux, redondance matérielle et logicielle, etc.).

Toute personne en charge d'une action relevant du PCA/PRA doit connaître précisément son rôle et ce qu'elle doit faire concrètement en cas de sinistre. Elle doit également comprendre la finalité recherchée, afin d'inscrire son action dans la cohérence globale de l'entité.

Poids	Classes cibles			Responsables
4	C	B	A	
	N/A	applicable	=	DIRECTION SI, RSSI, Administrateur systèmes et réseaux, MOA/MOE, Utilisateur

CONTINU-TEST.PLAN : Mise à l'essai des PCA/PRA

Un plan de test technique (tests de restauration des systèmes, des applications, des données ou des communications, etc.) doit être mis en œuvre annuellement.

Poids	Classes cibles			Responsables
4	C	B	A	
	N/A	applicable	+	DIRECTION SI, RSSI, Administrateur systèmes et réseaux

CONTINU-TEST.EX/SCEN : Exercices et Scenarios

L'organisation d'exercice de crise est recommandée. Les différents tests sur les moyens de secours permettent de formaliser différents scénarios possibles.

Poids	Classes cibles			Responsables
2	C	B	A	
	N/A	applicable	+	DIRECTION SI, RSSI, Administrateur systèmes et réseaux

11. CONFORMITE

Objectif O.28: Eviter toute violation des obligations légales, réglementaires, statutaires, ou contractuelles et des exigences de sécurité.

11.1. CONFORMITE AVEC LES EXIGENCES LEGALES

CONF-EXIG : Identification de la législation en vigueur

L'ensemble des exigences réglementaires, légales et contractuelles, doit être explicitement identifié et son application par l'entité doit figurer dans la charte SI décrite ci-après.

Poids	Classes cibles			Responsables
3	C	B	A	
	applicable	=	=	Secrétariat Général, Direction Générale, RSSI

CONF-LIC: Droits de propriété intellectuelle

Il est strictement interdit d'utiliser tout logiciel non accompagné d'une licence en règle.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Administrateur systèmes et réseaux

CONF-ARCH: Protection des archives

Les responsabilités et les procédures à appliquer doivent être mises en place afin de protéger les archives de l'entité conformément à la législation en vigueur.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	=	=	Secrétariat Général, Direction Générale, RSSI

CONF-DONNEE. PERSO: Protection des données personnelles

Les données à caractère personnelles doivent être traitées en respectant les dispositions législatives et réglementaires en vigueur.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Secrétariat Général, Direction Générale, RSSI

CONF-CRYPTO: Réglementation relative aux mesures cryptographiques

Le RSSI s'assure du respect des dispositions du cadre normatif relatif à la mise en œuvre des mesures cryptographiques.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	RSSI

11.2. CONFORMITE AVEC LA POLITIQUE ET NORMES DE SECURITE ET CONFORMITE TECHNIQUE

CONF-DNSSI : Vérification de la conformité avec la DNSSI

Il faut contrôler régulièrement la mise en œuvre du plan d'application des règles de la DNSSI.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	=	=	RSSI

CONF-CHART.SI: Charte d'utilisation SI

Une charte de sécurité du SI, destinée au personnel, doit être élaborée en conformité avec la DNSSI. Elle traite de la sécurité du poste de travail, des accès réseaux (email, internet, …) et des consignes d'utilisation des moyens SI tel que la messagerie professionnelle.

Cette charte doit être validée par la hiérarchie et signée par les utilisateurs. Elle constitue un élément opposable en cas de manquement grave.

La charte du SI doit contenir, entre autres :

- Les règles générales d'utilisation des ressources informatiques;
- Des éléments de sensibilisation des utilisateurs : confidentialité des informations manipulées, etc. ;
- Les réflexes à adopter en cas d'incident ou de suspicion d'incident ;
- Les règles relatives à l'utilisation de données privées sur le réseau et le statut des dispositifs privés (supports amovibles, postes nomades, smartphone, etc.).

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	=	=	RSSI, Utilisateur

CONF-RGS : Vérification de la conformité avec le RGS

Il faut veiller à terme à l'application du référentiel général de la sécurité en cours d'élaboration.

Poids	Classes cibles			Responsables
2	C	B	A	
	applicable	=	=	RSSI

11.3. PRISES EN COMPTE DE L'AUDIT DU SYSTEME D'INFORMATION

Objectif O.29: Mener des opérations d'audit et capitaliser sur les résultats obtenus.

CONF-AUDIT : Audit du système d'information

Les modalités de déroulement des opérations d'audit déployées par l'entité doivent être bien définies par le RSSI (accès aux équipements, contrôles et traitements admis, effacement des données sensibles, marquage de certaines opérations, et habilitation des auditeurs, etc.).

Chaque opération d'audit donne lieu à des recommandations. Celles-ci sont mises en œuvre dans le cadre du plan d'actions.

Ces audits doivent être réalisés au moins une fois tous les deux ans. Les rapports y afférents doivent être communiqués à la DGSSI.

Poids	Classes cibles			Responsables
4	C	B	A	
	applicable	=	=	Secrétariat Général, Direction Générale, RSSI

GLOSSAIRE

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

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

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

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

Cyber sécurité
Situation recherchée pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises.

Cyberespace
Ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs.

Certificat électronique
Est un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.

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

Zone démilitarisée (DMZ)
Zone qui se situe entre un réseau interne et un réseau public qui permet d'isoler certains serveurs de l'organisme à usage public (serveurs Web, FTP, …), généralement contrôlée par un Firewall ou pare-feu.

Dysfonctionnement
Ecart par rapport à la situation normale ou au processus normal. Il peut être provoqué par des facteurs internes ou externes.

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

Information sensible
Une information sensible, est une information dont la compromission, l'altération, le détournement ou la destruction, est de nature à nuire à la continuité du fonctionnement ou mettant en danger le patrimoine informationnel de l'organisme et des services de l'Etat.

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

Intégrité

Objectif de sécurité qui consiste à empêcher, ou tout du moins à détecter, toute altération non autorisée de données. Par altération on entend toute modification, suppression partielle ou insertion d'information. Cet objectif peut être assuré par la signature électronique.

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

Ma-CERT
Centre de Veille, de Détection et de Réaction aux Attaques Informatiques au Maroc.

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

Mesure
Moyen de gérer un risque, et pouvant être de nature administrative, technique, gestionnaire ou juridique.

Non répudiation
Objectif de sécurité qui permet de garantir qu'une transaction ne peut être niée.

Normes
Document de référence contenant des spécifications techniques précises destiné à être utilisé comme règles ou lignes directrices.

Network Time Protocol (NTP)
Protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure.

Plan de Continuité d'Activité (PCA)
Vise à assurer et maintenir la continuité de l'activité à plein régime ou en mode dégradé, en cas de désastre ou panne informatique majeure touchant le SI. Il permet de garantir la survie de l'organisme en préparant à l'avance la continuité des activités désignées comme stratégiques Au contraire du PRA, le PCA n'autorise pas de coupure intégrale du service : la continuité, au moins partielle doit être assurée. Ce plan traite essentiellement des activités "métier", le secours de moyens informatique ne constitue que l'un de ces aspects.

Infrastructure de clés publiques (PKI)
Ensemble de composants physiques, logiciels, procédures et documents visant à gérer le cycle de vie des clés cryptographiques et leurs certificats.

Plan de reprise d'activité(PRA)
Vise à permettre la reprise de l'activité, à plein régime ou en mode dégradé, au bout d'un certain temps. Il permet la remise en service des infrastructures et des applications nécessaires pour revenir à une situation nominale le plus rapidement possible sur le plan informatique, il décrit la cinématique globale du redémarrage du SI après interruption. Bien que différents, on considère généralement que le PRA est une partie intégrante du PCA.

Réseau privé virtuel (VPN)
Technique d'interconnexion de réseaux locaux permettant de chiffrer les communications pour en conserver la confidentialité.

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

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

Tiers
Personne ou organisme reconnu(e) comme indépendant(e) des parties concernées.

Vulnérabilité
Faille de sécurité dans un programme ou sur un système informatique.