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

(VERSION N° 2 - 2023)

صاحب الجلالة الملك محمد السادس نصره الله

Note de présentation

Le développement du numérique figure depuis plusieurs années à l'ordre du jour de l'action des pouvoirs publics au Maroc. Notre pays a fait le choix, sous la conduite éclairée de Sa Majesté Le Roi, que Dieu L'assiste, d'accorder une place de plus en plus large aux nouvelles technologies de l'information et des communications, eu égard à leur rôle crucial en matière de développement économique et social. La dynamique enregistrée pour l'accélération de la transition numérique nationale s'est vue appuyée par le nouveau modèle de développement qui a consacré le digital comme levier transverse à même d'assurer un développement responsable et inclusif.

Au sein de l'administration publique, des entreprises et établissements publics, collectivités territoriales et infrastructures d'importance vitale privées et publiques, le développement de la digitalisation a déjà été amorcée. Le digital, qui offre en effet un immense potentiel, contribue actuellement de manière forte à la modernisation de ces organisations.

Si la digitalisation s'impose comme un atout incontournable et offre tant d'opportunités en matière de développement économique, de souveraineté et de bonne gouvernance, il n'en demeure pas moins qu'elle est aussi porteuse de risques et de menaces. Une digitalisation accélérée associée à la généralisation du recours aux moyens informatiques offre un terrain propice à la délinquance informatique et aux activités malveillantes.

Pour répondre à cet enjeu, la cybersécurité a fait toujours partie intégrante des stratégies de digitalisation au Maroc. Beaucoup d'efforts ont été déployés pour le renforcement de la sécurité et de la résilience des systèmes d'information au niveau national. La cybersécurité constitue en effet un pilier incontournable pour le développement de la confiance numérique et l'essor des services digitaux.

Dans le cadre de cette vision, une dynamique soutenue a été engagée, depuis la création de la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), pour la mise en place d'un cadre juridique complet qui tiendrait compte des défis auxquels notre pays est confronté dans le domaine de la cybersécurité.

En 2014, la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) a été publiée par la circulaire N° 3/2014 du Chef du Gouvernement. La DNSSI vise comme objectifs d'élever et d'homogénéiser le niveau de protection et de maturité de la sécurité de l'ensemble des systèmes d'information des administrations et organismes publics, ainsi que des infrastructures d'importance vitale.

En 2020, l'arsenal juridique national a été enrichi par la promulgation de la loi n° 05-20 relative à la cybersécurité. Cette loi prévoit un ensemble de mesures de sécurité de nature organisationnelle et technique qui sont destinées à accroître les capacités nationales dans le domaine de la cybersécurité, à accompagner la transition numérique du Royaume et à coordonner l'action de prévention et de protection contre les attaques et incidents de cybersécurité. Le décret n° 2-21-406 pris pour l'application de la loi n° 05-20 a vu ensuite le jour en 2021.

Dans la continuité de ces efforts, et pour tenir compte de l'évolution constante de l'environnement des technologies de l'information et des menaces et risques qui lui sont associés, la DGSSI a procédé, en exécution des **Hautes Instructions Royales**, à la mise à jour de la Directive Nationale de la Sécurité des Systèmes d'Information. La nouvelle Directive tient compte des enseignements tirés des actions de contrôle, d'audit, de gestion et de traitement d'incidents menées notamment par la DGSSI au sein des différents organismes. Elle prend en considération également les changements apportés au cadre juridique et normatif et aux bonnes pratiques applicables dans le domaine de la sécurité des systèmes d'information.

Conformément à la loi n° 05-20 sur la cybersécurité, le champ d'application de la nouvelle version de la Directive couvre les administrations de l'Etat, les établissements et entreprises publics, les personnes morales de droit public, les collectivités territoriales, ainsi que toutes les infrastructures d'importance vitale (IIV) qu'elles soient publiques ou privées.

En substance, cette version passe en revue et actualise l'ensemble des mesures de sécurité que les entités et les IIV doivent mettre en application, tant sur le volet organisationnel que technique. Elle constitue ainsi une référence nationale fixant les objectifs et arrêtant les règles minimales de la sécurité des systèmes d'information applicables auxdites entités et IIV.

Quant aux modalités d'application, les entités et les IIV disposent d'un délai de six (6) mois à compter de la date de sa publication, afin de fixer un calendrier des mesures à mettre en œuvre pour s'y conformer. En outre, un outil d'évaluation de la conformité à la DNSSI a été élaboré par la DGSSI et sera publié sur son site Internet pour que les entités puissent dresser leur bilan de mise en conformité par rapport aux règles prescrites par la Directive.

Cette conformité sera vérifiée également lors des audits des systèmes d'information gérés par les services de la DGSSI ou des auditeurs qualifiés par cette direction.

Sommaire

Préambule

Parallèlement au développement des technologies du numérique, on assiste de plus en plus à la montée des activités illicites dans le cyberespace et à la multiplication des attaques informatiques qui arrivent à exploiter les vulnérabilités des systèmes d'information et à perturber leur fonctionnement.

Face à ces risques et menaces, le Maroc a adopté à partir de 2020 la loi n° 05-20 relative à la cybersécurité ainsi que son décret d'application n° 2-21-406. Ces deux textes visent principalement à définir les mesures de protection et renforcer la sécurité des systèmes d'information (SSI) au niveau national, permettant ainsi de les doter 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 dispositions du cadre juridique en vigueur et en application de l'article 9 du décret précité, la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) a procédé à la mise à jour de la Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI), dont la première version a été mise en application et entérinée en date du 10 Mars 2014 par circulaire n°3/2014 du Chef du Gouvernement.

La nouvelle version de la DNSSI s'applique à tous les systèmes d'information (SI) des administrations de l'État, des collectivités territoriales, des établissements et entreprises publics, toute autre personne morale de droit public désignés dans la loi 05-20 par « entité », et aux SI des infrastructures d'importance vitale (IIV) publiques et privées.

La Directive nationale concerne l'ensemble des personnes physiques ou morales intervenant dans les SI des entités et des IIV, qu'il s'agisse des agents relevant de ces entités et IIV ou bien de tiers (prestataires ou sous-traitants) et de leurs employés.

Elle décrit les mesures de sécurité organisationnelles et techniques qui doivent être appliquées par lesdites entités ou IIV, et constitue un cadre commun de référence qui fixe les objectifs et arrête les règles de la sécurité des systèmes d'information.

Toutefois, ce cadre commun ne devra pas être considéré comme suffisant. Chaque entité ou IIV doit s'appuyer également sur les guides et référentiels élaborés par la DGSSI pour renforcer la résilience et la sécurité de leurs SI.

Aussi, il appartient aux responsables des entités ou des IIV d'adapter les dispositions de la directive au contexte de leurs SI. Globalement, la plupart des règles énoncées constituent des règles de base qui devraient pouvoir être appliquées. Les écarts éventuels de conformité par rapport aux règles édictées doivent, le cas échéant, être dûment motivés et justifiés.

La présente version de la directive a été élaborée en tenant compte notamment :

- de l'évolution des contextes juridique, réglementaire, normatif et technologique.
- des enseignements tirés des actions de contrôles et d'audit menées notamment par la DGSSI;
- des retours d'expérience de la gestion et des traitements d'incidents ;
- des évolutions des menaces et des risques en matière de SSI ;
- des résultats d'analyses de risques menés au sein de certaines entités ou IIV ;

Les objectifs et les règles de sécurité de la DNSSI s'organisent sous la forme des chapitres cités ci-dessous:

- Politique de sécurité des systèmes d'information ;
- Organisation de la sécurité des systèmes d'information ;
- Sécurité des ressources humaines ;
- Gestion des actifs informationnels;
- Contrôle d'accès ;
- Cryptographie ;
- Sécurité physique et environnementale ;
- Sécurité liée à l'exploitation ;
- Sécurité des communications ;
- Acquisition, développement et maintenance des systèmes d'information ;
- Relations avec les fournisseurs ;
- Gestion des incidents de cybersécurité ;
- Gestion de la continuité de l'activité ;
- Conformité.

Pour la mise en application de cette directive, les entités et les IIV doivent définir un calendrier de mise en conformité au plus tard six (6) mois après sa publication. Ce calendrier doit être établi en indiquant les mesures immédiates, les mesures à court terme et les mesures atteignables à moyen terme.

Annuellement, chaque entité ou IIV dresse son bilan de mise en application de la DNSSI en se basant sur l'outil d'évaluation de la conformité à la DNSSI élaboré par la DGSSI et publié sur son site Internet. Le bilan annuel constitue une synthèse de l'état d'avancement de la mise en conformité par rapport aux règles édictées par la DNSSI. A la demande de la DGSSI, les entités et les IIV lui transmettent ledit bilan.

Orientations de la direction en matière de sécurité des systèmes d'information

Objectif 1 : *Apporter à la sécurité des systèmes d'information (SI) une orientation et un soutien de la part de la direction de l'entité ou de l'IIV, conformément aux exigences métier et aux lois, règlements, directives et référentiels en vigueur.*

POL-RISQUE : Analyse de risque

Chaque entité ou IIV doit identifier les besoins de sécurité en matière de confidentialité, disponibilité et intégrité pour chaque processus supporté par le système d'information et procéder à une analyse des risques de sécurité liés à ce système d'information.

POL-FORMEL : Politique de sécurité des systèmes d'information

Chaque entité ou IIV doit définir une politique en matière de sécurité des SI qui soit approuvée par un niveau hiérarchique élevé (ex. : secrétariat général, direction générale, …) et qui décrit les règles qui doivent être adoptées pour gérer les besoins identifiés de sécurité des SI.

Cette politique doit être déclinée au besoin en politiques spécifiques par domaine ou par aspect de sécurité.

La politique de sécurité des SI doit être élaborée en se basant sur une analyse de risques, et doit être diffusée et communiquée au personnel et aux tiers concernés et mise à jour régulièrement.

POL-PAS : Plan d'actions de la sécurité des SI

Chaque entité ou IIV doit définir un plan d'actions pour la mise en conformité avec sa politique de sécurité des SI. Ce plan d'actions tiendra compte des impacts sur les activités, et des moyens financiers et humains à mettre en œuvre en indiquant les mesures à court terme et les mesures atteignables à moyen terme.

POL-TDB : Tableau de bord de la sécurité des SI

Chaque entité ou IIV doit élaborer et se servir d'un tableau de bord de la sécurité des SI pour assurer le suivi de la bonne application des règles édictées dans sa politique de sécurité.

Le tableau de bord doit se baser sur des indicateurs permettant le suivi de la mise en œuvre des règles de sécurité des SI propres à l'entité ou à l'IIV.

ORGANISATION DE LA SECURITE DES SYSTEMES D'INFORMATION

Organisation interne

Objectif 2 : *Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité du SI au sein de l'entité ou de l'IIV.*

ORG-INTER-GOUV : Gouvernance de la sécurité des SI

Chaque entité ou IIV doit mettre en place une gouvernance appropriée de la sécurité des SI avec l'implication notamment d'un niveau hiérarchique élevé (ex. : secrétariat général, direction générale, …) de l'entité ou de l'IIV, et ce afin de définir les orientations stratégiques en matière de sécurité des SI et assurer le suivi de l'avancement de l'ensemble des projets y afférents.

ORG-INTER-RSSI : Désignation d'un responsable de la sécurité des SI (RSSI)

Les règles applicables à la désignation et aux missions du RSSI sont fixées par la loi n° 05-20 relative à la cybersécurité et son décret d'application.

Tout changement de l'identité et des coordonnées du RSSI doit être porté à la connaissance de la DGSSI.

ORG-INTER-RESP : Attribution des rôles et responsabilités

Chaque entité ou IIV doit définir et attribuer les rôles et responsabilités des différents acteurs en matière de sécurité des SI.

Cette attribution doit tenir compte de la séparation entre les tâches et les domaines de responsabilité incompatibles.

Télétravail

Objectif 3 : *Assurer la sécurité du système d'information de l'entité ou de l'IIV en cas d'adoption du télétravail.*

ORG-TELETRAV-SEC : Télétravail sécurisé

Chaque entité ou IIV doit prendre les mesures adéquates, en fonction du moyen d'accès, pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.

A cet effet, une politique ou des procédures claires précisant les systèmes accessibles et les mesures de sécurité applicables, doivent être définies, validées par la hiérarchie, communiquées et tenues à jour pour une mise en œuvre appropriée du télétravail.

SECURITE DES RESSOURCES HUMAINES

Avant l'embauche

Objectif 4 : *S'assurer que le personnel et les contractuels comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'entité ou l'IIV envisage de leur confier.*

RH-AVT-PERSON : Personnel de confiance

A l'embauche, des vérifications des informations des candidats appelés à travailler sur des tâches sensibles au sein de l'entité ou de l'IIV doivent être réalisées conformément à la réglementation, à l'éthique, et proportionnellement aux exigences métier et à la classification des actifs informationnels accessibles.

RH-AVT-COND : Termes et conditions d'embauche

Les accords contractuels avec les employés et les sous-traitants doivent préciser leurs responsabilités et celles de l'entité ou de l'IIV en matière de sécurité des SI.

Après l'embauche

Objectif 5 : *S'assurer que les employés et les contractuels sont conscients de leurs responsabilités en matière de sécurité des SI et qu'ils assument ces responsabilités.*

RH-APRES-FORM : Formation et sensibilisation du personnel

Chaque entité ou IIV doit organiser régulièrement, selon un programme préétabli, des sessions de formation et de sensibilisation au profit de son personnel en matière de sécurité des SI.

Rupture, terme ou modification du contrat de travail

Objectif 6 : *Protéger les intérêts de l'entité ou de l'IIV dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail.*

RH-FIN-GEST : Gestion des mutations et départs

Afin de préserver la confidentialité et l'intégrité de l'information, chaque entité ou IIV doit formaliser et mettre en place une procédure de gestion des mutations ou des départs qui couvre notamment :

- *La notification au service informatique par le service des ressources humaines de tout mouvement du personnel ;*
- *La passation des consignes ;*
- *La restitution des biens informatiques ;*
- *Le retrait ou la modification des accès aux SI.*

GESTION DES ACTIFS INFORMATIONNELS

Responsabilités relatives aux actifs informationnels

Objectif 7 : *Identifier les actifs informationnels de l'entité ou de l'IIV et définir les responsabilités appropriées en matière de protection.*

ACTIF-RESP-INV : Inventaire des actifs

Un inventaire des actifs informationnels (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);*
- *la version du système d'exploitation et les correctifs appliqués ;*
- *l'identification de l'utilisateur final si applicable (poste de travail, téléphonie IP, imprimante, ...).*

ACTIF-RESP-PROP : Propriétaires des actifs

Chaque actif informationnel doit être attribué formellement à un propriétaire qui a la responsabilité de la gestion des actifs informationnels qui lui sont attribués (inventaire, classification, protection, destruction, réforme ...) tout au long de leurs cycles de vie.

ACTIF-RESP-CHARTE : Charte d'utilisation du SI

Une charte d'utilisation du SI doit être élaborée en conformité avec la politique de sécurité des SI en vigueur. Elle doit être validée par la hiérarchie, communiqué et signée ou acceptée par les utilisateurs.

Cette charte doit contenir, entre autres :

- *Un rappel des exigences législatives et réglementaires applicables dans le contexte de l'entité ou de l'IIV ;*
- *Les règles générales d'utilisation des ressources informatiques ;*
- *Les éléments de sensibilisation des utilisateurs ;*
- *Les clauses de confidentialité des informations manipulées ;*
- *Les réflexes à adopter en cas d'incident ou de suspicion d'incident de cybersécurité et les règles à respecter notamment l'obligation de déclarer tout incident de cybersécurité à la DGSSI ;*
- *La charte d'utilisation du SI constitue un élément opposable en cas de manquement grave.*

ACTIF-RESP-CARTO : Cartographie SI

Chaque entité ou IIV doit tenir et mettre à jour une cartographie de son SI qui précise les composants matériels et logiciels ainsi que les architectures des réseaux sur lesquels sont identifiés les centres de données et les différents sites desservis.

Les documents de cartographie doivent être maintenus au fil des évolutions apportées aux SI et faire l'objet d'une protection adaptée.

Classification des actifs informationnels

Objectif 8 : *S'assurer que les actifs informationnels bénéficient d'un niveau de protection approprié conforme à leur importance pour l'entité ou pour l'IIV.*

ACTIF-CLASSIF-INFO : Classification

Chaque entité ou IIV doit classifier ses actifs informationnels selon leur niveau de sensibilité en termes de confidentialité, d'intégrité et de disponibilité, et ce sur la base d'une échelle d'impacts fixée par l'entité ou par l'IIV et qui tient compte notamment de sa taille, de son importance, de ses missions, de son domaine d'activités, de ses exigences métiers, de ses propres enjeux de sécurité et des obligations légales, règlementaires, contractuelles ou normatives qui lui sont applicables. Le résultat de cette classification traduit la valeur des actifs informationnels en fonction de leur sensibilité et de leur caractère critique pour l'entité ou pour l'IIV.

En parallèle, l'entité ou l'IIV doit procéder à la classification des mêmes actifs informationnels et SI selon le référentiel de la classification des actifs informationnels et SI fixé par la loi n° 05.20 et son décret d'application. L'objectif de cette classification est d'identifier les SI sensibles et les données sensibles au sens de la loi précitée.

ACTIF-CLASSIF-MES : Mesures de protection des informations

Sur la base des résultats de ces classifications, chaque entité ou IIV doit mettre en place les mesures de sécurité proportionnelles à la sensibilité des actifs et les formaliser dans une procédure de classification des actifs informationnels.

L'entité ou l'IIV doit également se conformer aux dispositions pertinentes de la loi n° 05-20 relative à la cybersécurité et son décret d'application et appliquer les mesures de protection définies dans les référentiels élaborés par la DGSSI.

ACTIF-CLASSIF-EXAM : Examen de la classification

Chaque entité ou IIV doit revoir la classification de ses actifs informationnels et de ses SI au moins une fois tous les trois ans et à chaque fois que nécessaire. Les mesures de protection doivent évoluer en fonction de la nouvelle classification.

Manipulation des supports et gestion des appareils mobiles

Objectif 9 : *Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'entité ou de l'IIV stockée sur des supports et assurer la sécurité de l'utilisation des appareils mobiles.*

ACTIF-SUP-AMOV : Gestion des supports amovibles

Chaque entité ou IIV doit mettre en place des mesures appropriées pour la gestion des supports amovibles notamment :

- *la désactivation de leur exécution automatique, sauf dans des cas exceptionnels liés à des impératifs de service ;*
- *leur conservation dans des locaux protégés et l'adoption de mesures adaptées tel que le chiffrement, le contrôle anti-virus, etc. surtout lorsqu'ils contiennent des données sensibles ;*

ACTIF-SUP-MOBIL : Politique en matière d'appareils mobiles

Les règles de sécurité destinées à gérer les risques découlant de l'utilisation des appareils mobiles doivent faire partie intégrante de la politique de sécurité des SI de l'entité ou de l'IIV.

ACTIF-SUP-NOMAD : Postes nomades

Les postes nomades 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 et interdiction des téléchargements à caractère non conforme à la charte d'utilisation du SI.

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.

ACTIF-SUP-REB : Mise au rebut ou recyclage des supports

Une procédure de mise au rebut ou de recyclage des supports doit être mise en place afin d'effacer de manière sécurisée les données présentes sur tous type de support (les disques durs, les mémoires intégrées, …).

Dans le cas de données sensibles, la destruction du support ou sa démagnétisation si applicable, peut s'avérer nécessaire de manière à empêcher toute tentative de récupération.

CONTROLE D'ACCES

Exigences métier en matière de contrôle d'accès

Objectif 10 : *Limiter l'accès à l'information et aux moyens de traitement de l'information.*

ACC-EXIG-POL : Politique de contrôle d'accès

Chaque entité ou IIV est tenue d'établir, de documenter et de revoir une politique de contrôle d'accès aux systèmes, réseaux et services sur la base des exigences métier et de sécurité de l'information en respectant le principe du moindre privilège.

Gestion de l'accès utilisateur

Objectif 11 : *Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.*

ACC-UTILIS-ENREGIS/DESINSCRI : Enregistrement et désinscription des utilisateurs

Chaque entité ou IIV doit mettre en œuvre une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à permettre l'attribution de droits d'accès.

Cette procédure impose notamment :

- *la création d'identifiants utilisateurs uniques ;*
- *la suppression ou le blocage immédiats des identifiants des utilisateurs qui ont quitté l'organisation ;*
- *la détection périodique des identifiants utilisateurs redondants, suivie de leur suppression ou de leur blocage ;*
- *l'assurance que des identifiants utilisateurs redondants ne sont pas attribués à d'autres utilisateurs.*

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.

Les droits particuliers (super-utilisateur, Administrateur systèmes et réseaux, ...) doivent être parfaitement identifiés, limités (nombre et droits) et justifiés.

ACC-UTILIS-HABILIT : Gestion des habilitations

Chaque entité ou IIV est tenue de mettre en place une matrice d'habilitations qui précise pour chaque utilisateur ses droits d'accès sur les différents systèmes et services du SI.

ACC-UTILIS-GENERIQ : Gestion des comptes génériques

Chaque entité ou IIV est tenue de créer des comptes nominatifs pour les utilisateurs permettant de les relier à leurs actions et de les leur imputer.

Lorsque les aspects opérationnels liés à l'activité de l'entité ou de l'IIV exigent l'utilisation de comptes génériques, ces comptes doivent être approuvés, documentés et inventoriés.

ACC-UTILIS-REVUE : Revue des droits d'accès

Une revue périodique des droits attribués est nécessaire, au moins une fois par an, en s'appuyant sur l'inventaire des applications et des ressources utilisées, ainsi que sur la matrice des habilitations.

Suite à cet examen, les corrections nécessaires doivent être apportées.

Contrôle d'accès aux systèmes et aux applications

Objectif 12 : *Empêcher les accès non autorisés aux systèmes et aux applications.*

ACC-SYS/APP-ACC : Accès aux systèmes et applications

Les systèmes et applications doivent être protégés par des mécanismes adaptés de restriction des accès (login/mot de passe, authentification forte, règles de filtrage et d'accès, plages horaires de connexions) conformément à la politique de contrôle d'accès de l'entité ou de l'IIV.

ACC-SYS/APP-PRIVIL : Gestion des accès à privilèges

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

L'inventaire des comptes à privilège doit être tenu à jour.

ACC-SYS/APP-MDP : Gestion des mots de passe

Chaque entité ou IIV est tenue de formaliser une politique de gestion des mots de passe qui définit les règles applicables aux mots de passe, en particulier :

- *la structure (complexité minimale) ;*
- *le changement périodique ;*
- *la suppression en cas de suspicion de compromission ;*
- *la réinitialisation ;*

Un processus de contrôle de l'application de ces règles doit être déployé.

CRYPTOGRAPHIE

Mesures cryptographiques

Objectif 13 : *Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et l'intégrité de l'information.*

CRYPTO-MES-POL : Politique d'utilisation des mesures cryptographiques

En cas de recours à la cryptographie, l'entité ou l'IIV doit élaborer et mettre en œuvre une politique d'utilisation de mesures cryptographiques en vue de protéger l'information.

Cette politique doit spécifier notamment les exigences en matière de certificats de signature ou de chiffrement (délai maximum de validité, algorithme, longueurs de clés, etc..) ou en matière de connexions chiffrées (protocoles autorisés).

CRYPTO-MES-GESTCLE : Gestion des clés cryptographiques

Chaque entité ou IIV utilisant des clés cryptographiques doit élaborer et mettre en œuvre une procédure encadrant leur utilisation et leur protection tout au long de leur cycle de vie (génération, stockage, archivage, extraction, attribution, retrait et destruction).

SECURITE PHYSIQUE ET ENVIRONNEMENTALE

Zones sécurisées

Objectif 14 : *Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'entité ou de l'IIV.*

PHYS-ZONE-DELIMIT : Délimitation des zones

Des zones physiques de sécurité doivent être délimitées pour protéger les SI et les moyens de traitement associés.

Cette délimitation peut se faire selon la typologie suivante :

- *zones publiques : autorisées à toute personne.*
- *zones internes : autorisées uniquement au personnel de l'entité ou de l'IIV, aux tiers autorisés ou aux visiteurs accompagnés.*
- *zones restreintes : accessibles uniquement aux personnes de l'entité ou de l'IIV habilitées à consulter, à traiter et manipuler des informations ou des équipements classifiés, et le cas échéant aux tiers autorisés et accompagnés.*

PHYS-ZONE-PROC : Procédures de contrôle d'accès

Chaque entité ou IIV doit formaliser les procédures de contrôle d'accès physique à ses locaux en mettant en place les mécanismes nécessaires pour leur application. Ces procédures doivent être validées par la hiérarchie et le personnel doit être tenu au courant de leurs contenus.

PHYS-ZONE-DISPO : Dispositif de contrôle d'accès

Les entités ou les IIV sont tenues de mettre en place un dispositif de contrôle d'accès physique individualisé dans les zones restreintes.

Ce dispositif doit assurer la traçabilité des accès du personnel et des tiers autorisés et accompagnés aux zones restreintes, et conserver les enregistrements pour une durée d'au moins trois mois.

PHYS-ZONE-VIDEOPROT : Vidéo protection

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

PHYS-ZONE-INCEN : Sécurité incendie

Les zones abritant des systèmes de traitement de l'information doivent être équipées de systèmes adaptés pour la détection et l'extinction d'incendies.

PHYS-ZONE -EAU : Dégâts des eaux

Les moyens de traitement de l'information doivent être placés dans des locaux à l'abri des risques des dégâts des eaux.

Matériels

Objectif 15 : *Empêcher la perte, l'endommagement, le vol ou la compromission des actifs informationnels et l'interruption des activités de l'entité ou de l'IIV.*

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. Les câbles doivent être déroulés en faisceaux clairs et non emmêlés.

PHYS-MAT-OND : Onduleurs

Les équipements de traitement de l'information doivent être protégés des variations et des microcoupures d'électricité par des onduleurs à capacité adaptée.

PHYS-MAT-ELECTROG : Groupe électrogène

En cas de besoins accrus de disponibilité des SI, l'entité ou l'IIV peut faire recours à un groupe électrogène pour pallier les interruptions prolongées du courant électrique.

PHYS-MAT-CLIM : Climatisation

Les zones abritant des moyens de traitement de l'information (salles des machines, datacenter…etc.) doivent être équipées de systèmes de climatisation pour réguler au besoin la température et l'humidité.

PHYS-MAT-EQUIP : Entretien des équipements de sécurité environnementale

Les équipements de sécurité environnementale (extincteurs, climatisations, détecteurs d'incendie, onduleurs, groupes électrogènes, etc.) doivent être correctement entretenus pour assurer leur bon fonctionnement.

Un délai d'intervention adapté en cas de défaillance doit être précisé dans les contrats de maintenance des équipements de sécurité environnementale.

PHYS-MAT-HORSLOC : Sécurité du matériel et des actifs hors les locaux

Chaque entité ou IIV doit appliquer des mesures de sécurité à tous types d'équipements informatiques et supports destinés à être transportés et utilisés hors des lieux de travail habituel, afin de les protéger notamment contre les risques de vol, d'endommagement ou d'intrusion.

SECURITE LIEE A L'EXPLOITATION

Procédures et responsabilités liées à l'exploitation

Objectif 16 : *S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.*

EXP-PROC-CHANG : Gestion des changements

Tout changement apporté au SI doit suivre une procédure formelle respectant le cycle : demande, validation, application et contrôle à posteriori.

En effet, chaque entité ou IIV doit contrôler tout changement qui influe sur la sécurité du SI, en tenant compte des éléments suivants :

- *L'identification et la planification des changements significatifs ;*
- *L'appréciation des incidences potentielles de ces changements sur la sécurité de l'information ;*
- *L'autorisation formelle des changements proposés ;*
- *La transmission des informations détaillées sur les changements apportés à toutes les personnes concernées.*

EXP- PROC-CAP : Gestion des capacités

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 à même de garantir ou d'améliorer la disponibilité du SI.

EXP-PROC-ENVIR : Séparation des environnements

Les environnements de développement, de test et de production doivent être séparés pour réduire notamment les risques d'accès ou de changements non autorisés dans les trois environnements.

Protection contre les logiciels malveillants

Objectif 17 : *Garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.*

EXP-PROTEC-MALVEIL : Protection contre les logiciels malveillants

Des solutions de protection contre les logiciels malveillants doivent être installées et mises à jour sur l'ensemble des serveurs, postes de travail et appareils mobiles.

Sauvegarde

Objectif 18 : *Se protéger contre la perte de données.*

EXP-SAUV-PROC : Procédures de sauvegarde

Chaque entité ou IIV 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) ;*
- *Les données sensibles devant être sauvegardées de manière chiffrée.*

EXP-SAUV-RESTAUR : Restauration

Chaque entité ou IIV doit tester régulièrement les supports de sauvegarde en s'assurant que les données sauvegardées peuvent être restaurées en temps voulu conformément à une procédure de restauration documentée.

EXP-SAUV-SEC : Sécurité des sauvegardes

Chaque entité ou IIV doit protéger physiquement les supports de sauvegarde en les plaçant à un endroit protégé (Armoire ignifuge) ou en les externalisant sur un site suffisamment distant du site principal.

Journalisation et surveillance

Objectif 19 : *Enregistrer les événements et générer des preuves.*

EXP-JOURN/SURV-JOURNAL : Journalisation des événements

Chaque entité ou IIV doit mener une étude pour identifier les journaux à collecter des différentes sources (serveurs, équipements de sécurité, équipements réseaux, applications, postes de travail, etc.) en fonction des risques et incidents redoutés par l'entité ou par l'IIV. Elle doit mettre en place un journal répertoriant les événements de sécurité à collecter. Ces journaux doivent être analysés périodiquement et les actions à mener doivent être bien définies.

Ces journaux doivent être centralisés et protégés contre les risques de falsification ou d'accès non autorisé. Ils doivent être conservés pour une durée minimale de six mois.

EXP-JOURN/SURV-PRIVIL : Traçabilité des actions des comptes à privilège

Les actions des administrateurs système et des opérateurs système doivent être tracées. Pour cela leurs comptes doivent être nominatifs pour assurer l'imputabilité de leurs actions.

EXP-JOURN/SURV-MAINT : Traçabilité des actions de maintenance

Les interventions de maintenance sur les ressources informatiques de l'entité ou de l'IIV 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.

EXP-JOURN/SURV-SYNCHRON : Synchronisation des horloges

Pour assurer la précision des journaux d'événements qui peuvent être utilisés lors des investigations, les actifs doivent être synchronisés sur la même base de temps, à savoir : le service NTP de confiance (Network Time Protocol).

EXP-JOURN/SURV-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.

EXP-JOURN/SURV-CENTR : Centralisation

L'entité ou l'IIV doit mettre en place de manière centralisée les moyens appropriés de supervision et de détection pour le traitement continu des événements de sécurité prévus par la loi n°05-20 relative à la cybersécurité.

Maîtrise des logiciels en exploitation et gestion des vulnérabilités techniques

Objectif 20 : *Garantir l'intégrité des systèmes en exploitation et empêcher toute exploitation des vulnérabilités techniques.*

EXP-SYS-CONFIG : Configuration système

Chaque entité ou IIV doit documenter les procédures d'administration et de configuration sécurisée des actifs du système d'information, les rendre disponibles, les expliquer à toute personne ayant besoin de les connaître et les maintenir à jour.

Les configurations doivent être sauvegardées en lieu sûr après chaque changement.

EXP-SYS-DURC : Durcissement des configurations

Les configurations des équipements et systèmes doivent être durcies notamment par rapport aux versions natives des fournisseurs (le changement des mots de passe par défaut et des certificats, la fermeture des services et des ports non nécessaires, etc..).

Les procédures et guides de durcissement pour les différents types d'actifs doivent être documentés et tenus à jours.

EXP-VULN-INSTALL : Restrictions liées à l'installation de logiciels

Chaque entité ou IIV doit définir et mettre en place un processus de contrôle des logiciels que les utilisateurs peuvent installer ainsi que des privilèges qui leurs sont accordés en tenant compte de leurs fonctions.

EXP-VULN-GEST : Gestion des vulnérabilités techniques

Chaque entité ou IIV doit être tenue informée en temps voulu des vulnérabilités techniques des systèmes d'information en exploitation, d'évaluer son exposition à ces vulnérabilités et de prendre les mesures appropriées pour traiter le risque associé.

Une procédure de gestion des vulnérabilités doit être mise en place en prenant en compte principalement les éléments suivants :

- *L'inventaire des actifs informationnels en service ;*

- *Les rôles et responsabilités associés à la gestion des vulnérabilités ;*
- *Les délais d'intervention ;*
- *Les modalités de corrections (Application de correctifs, cloisonnement, …).*
- *Les vulnérabilités jugées critiques doivent être portées à la connaissance de la DGSSI.*

EXP-VULN-CORRECT : Gestion des correctifs

Chaque entité ou IIV doit définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité.

Un processus de gestion des correctifs propre à chaque système ou applicatif doit être défini et adapté suivant les contraintes et le niveau d'exposition du système.

Considérations sur l'audit du système d'information

Objectif 21 : *Réduire au minimum l'incidence des activités d'audit sur les systèmes en exploitation.*

EXP-AUDIT-MES : Mesures relatives à l'audit du système d'information

Les modalités de déroulement des opérations d'audit déployées par l'entité ou par l'IIV doivent être bien définies (accès aux équipements, contrôles et traitements admis, consultation des données, habilitation des auditeurs, etc.).

Les exigences et activités d'audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations qui pourraient être subies par les processus métier.

Certaines règles applicables à l'audit des systèmes d'information sensibles sont définies par la loi n° 05-20 et ses textes d'application.

SECURITE DES COMMUNICATIONS

Management de la sécurité des réseaux

Objectif 22 : *Garantir la protection des informations sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.*

COM-MANAG-CLOISON : Cloisonnement du réseau

Chaque entité ou IIV est tenue de cloisonner son réseau en zones (zone publique, zone utilisateurs, zone serveurs, etc.) selon la classification et les niveaux de sensibilité des actifs informationnels connectés.

COM-MANAG-FILTRAGE : Filtrage des flux

Le trafic entrant et sortant de chaque zone réseau doit être soumis à des règles strictes de filtrage conformément à la politique de contrôle d'accès et à la classification des données traitées.

La liste des règles de filtrage doit être documentée et tenue à jour.

COM-MANAG-SYSAUT : Systèmes autorisés sur le réseau

L'entité ou l'IIV doit mettre en place les moyens et mécanismes nécessaires pour s'assurer que seuls les équipements autorisés peuvent être connectés au réseau interne de l'entité ou de l'IIV.

COM-MANAG-DISTANT : Accès distants

L'accès distant ne doit être réalisable que par des personnes autorisées et bien définies et à partir de moyens maitrisés.

Des mesures d'authentification adaptées et l'usage de protocoles sécurisés pour ce type de connexions sont nécessaires.

COM-MANAG-TUNEL : Tunnelisation chiffrée

Chaque entité ou IIV doit mettre en place des mécanismes de chiffrement pour la protection des tunnels de connexion à distance lorsque l'accès se fait à travers un réseau public.

COM-MANAG-RSF : Sécurité des réseaux sans fil

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

Le réseau sans fil doit être cloisonné 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.

Des moyens d'authentification adaptés doivent être mis en place pour limiter l'accès aux réseaux sans fil aux seules personnes autorisées.

Transfert de l'information

Objectif 23 : *Maintenir la sécurité de l'information transférée au sein de l'entité ou de l'IIV et vers l'extérieur.*

COM-TRANS-FICHIER : Usage des transferts par fichiers

Des moyens adaptés doivent être mis en place pour la protection des informations qui transitent à travers tout type de moyens de communication (serveurs de fichier, partage ou stockage Cloud, etc.) contre l'interception, la reproduction, la modification, les erreurs d'acheminement ou la destruction.

COM-TRANS-MESS : Usage de la messagerie électronique

Chaque entité ou IIV doit formaliser et mettre en œuvre les règles de bon usage nécessaires pour la sécurité de la messagerie électronique notamment :

- *le chiffrement et la signature des messages sensibles par des moyens adaptés ;*
- *l'accès à distance à la messagerie professionnelle via un canal sécurisé ;*
- *la vérification de la source des courriers électroniques avant d'ouvrir les pièces jointes;*
- *l'interdiction de l'usage de la messagerie professionnelle à des fins personnelles ;*
- *l'interdiction du renvoi automatique vers une messagerie non maîtrisée, sauf autorisation expresse pour des raisons exceptionnelles.*

COM-TRANS-FILTR : Filtrage des mails

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

- *le contrôle antiviral des pièces jointes, leurs tailles et natures ;*
- *la protection anti-spam ;*
- *le contrôle des entêtes SMTP.*

ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION

Exigences de sécurité applicables aux systèmes d'information

Objectif 24 : *Veiller à ce que la sécurité fasse partie intégrante des SI tout au long de leur cycle de vie.*

DEV-EXIG-PROJET : Sécurité de l'information dans la gestion de projet

Chaque entité ou IIV doit traiter la sécurité de l'information dans la gestion de tous types de projets SI. A ce titre, la sécurité doit être intégrée à toutes les phases du cycle de vie du projet de manière à s'assurer notamment que :

- *une appréciation du risque, liée à la sécurité de l'information, soit effectuée au commencement du projet pour identifier les exigences de sécurité ;*
- *les objectifs en matière de sécurité de l'information soient intégrés aux objectifs du projet et pris en compte dès la conception ;*
- *la vérification de la sécurité soit intégrée dans les tests d'acceptation.*

DEV-EXIG-TRANSAC : Protection des transactions liées aux services d'application

Chaque entité ou IIV doit identifier les fichiers et les transactions devant être protégés par des solutions de chiffrement et/ou de signature électronique au niveau de l'architecture applicative.

Sécurité des processus de développement et d'assistance technique

Objectif 25 : *S'assurer que la sécurité de l'information est mise en œuvre dans le cadre du cycle de développement des SI conformément aux référentiels et guides en vigueur.*

DEV-PROC-POL : Politique de développement sécurisé

Chaque entité ou IIV doit élaborer et mettre en place, conformément aux guides et référentiels élaborés par la DGSSI, une politique de développement sécurisé des logiciels et des systèmes, qui définit notamment :

- *les exigences de sécurité de l'environnement de développement ;*
- *les exigences de sécurité dans la phase de conception ;*
- *les points de contrôle de la sécurité aux différentes étapes clés du projet ;*
- *les référentiels de développement sécurisé à utiliser ;*
- *les règles de protection du code source et le contrôle des versions.*

DEV-PROC-CHANG : Contrôle des changements apportés au système dans le cycle de développement

Les changements apportés au SI dans le cycle de développement doivent être contrôlés en utilisant des procédures formelles.

A cet effet, chaque entité ou IIV doit mener une appréciation du risque pour analyser les incidences des changements apportés au SI dans le cycle de développement et se limiter aux changements nécessaires.

Lorsque les changements sont apportés, chaque entité ou IIV doit revoir et tester les applications métiers critiques afin de vérifier tout impact sur l'activité ou sur la sécurité.

DEV-PROC-ENVIR : Environnement de développement sécurisé

Chaque entité ou IIV doit veiller à ce que les environnements de développement soient sécurisés, de manière à tenir compte notamment de :

- *la sensibilité des données traitées, stockées et en transit ;*
- *les exigences internes et externes découlant des politiques et référentiels en vigueur ;*
- *le niveau de fiabilité du personnel travaillant dans l'environnement ;*
- *le contrôle d'accès aux environnements ;*
- *la séparation des différents environnements de développement ;*
- *le degré d'externalisation associée à la tâche de développement.*

DEV-PROC-TEST : Test de la sécurité du système

Chaque entité ou IIV doit assurer la réalisation des tests de la sécurité durant le cycle de développement conformément à la politique de développement sécurisé de l'entité ou de l'IIV et aux guides et référentiels élaborés par la DGSSI.

DEV-PROC-CODE : Protection du code source des programmes

Un contrôle strict de l'accès au code source des programmes et aux éléments associés tels que les exigences de conception, les spécifications, les programmes de vérification et de validation, doit être mis en place.

DEV-PROC-DONNEE : Protection des données de test

Lorsque des données d'exploitation sont utilisées pour les besoins d'un test, il est nécessaire notamment de :

- *respecter les procédures d'accès qui s'appliquent aux systèmes d'applications en exploitation ;*
- *obtenir une autorisation pour copier des informations d'exploitation dans un environnement de test ;*
- *effacer les informations d'exploitation d'un environnement de test immédiatement après la fin des tests ;*
- *journaliser toute reproduction et utilisation de l'information d'exploitation.*

En outre, lorsque les données d'exploitation sont de nature sensible, elles ne doivent pas être utilisées sans qu'il ne soit procédé à leur anonymisation.

RELATIONS AVEC LES FOURNISSEURS

Sécurité de l'information dans les relations avec les fournisseurs

Objectif 26 : *Garantir la protection des actifs de l'entité ou de l'IIV accessibles aux fournisseurs.*

FOURNIS-REL-RISQ : Risques émanant des fournisseurs

Chaque entité ou IIV doit identifier les risques de sécurité liés aux interventions des fournisseurs et des prestataires.

FOURNIS-REL-POL : Politique de sécurité de l'information dans les relations avec les fournisseurs

Chaque entité ou IIV doit mettre en place une politique qui définit les mesures de sécurité spécifiques applicables aux fournisseurs et aux prestataires.

FOURNIS-REL-EXIG : Exigences contractuelles

Les contrats conclus doivent prévoir les exigences de l'entité ou de l'IIV en termes de sécurité et de niveaux de service. Les fournisseurs et les prestataires sont tenus conformément aux contrats conclus de respecter la politique de sécurité des SI de l'entité ou de l'IIV.

Des clauses d'auditabilité et de réversibilité sont à prévoir lorsqu'il s'agit de contrats d'externalisation, et ce conformément aux dispositions de la loi n°05-20 relative à la cybersécurité.

Gestion de la prestation du service

Objectif 27 : *Maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les fournisseurs.*

FOURNIS-GEST-SURVEIL : Surveillance et revue des services des fournisseurs

Chaque entité ou IIV doit surveiller, revoir et auditer à intervalles réguliers les prestations assurées par les fournisseurs, afin de s'assurer que les clauses portant sur la sécurité de l'information prévues dans les contrats sont respectées et que les éventuels incidents sont correctement gérés.

GESTION DES INCIDENTS DE CYBERSECURITE

Traitement et réponse aux incidents de cybersécurité

Objectif 28 : *Garantir une méthode cohérente et efficace de détection et de traitement des incidents de cybersécurité, incluant la communication des événements et des failles liés à la sécurité.*

INCID-GEST-PROC : Procédures et responsabilités en matière de gestion des incidents

Les procédures de gestion d'incidents doivent couvrir les différents types d'incidents affectant la sécurité ou le fonctionnement du système (erreurs, dysfonctionnement, sinistres naturels, malveillances, dénis de service, infections virales, intrusion, sabotage, saturation, etc.) et définir les moyens de signalement et de suivi d'incidents.

Les responsabilités de gestion des incidents de cybersécurité doivent être définies pour garantir que lesdites procédures soient développées et communiquées au sein de l'entité ou de l'IIV.

INCID-GEST-CAT: Catégorisation et classification des incidents

Chaque entité ou IIV doit définir les différentes catégories d'incidents susceptibles d'affecter la sécurité du SI ainsi que l'échelle de classification de ces incidents selon l'impact induit.

INCID-GEST-SIGNAL : Signalement des événements

L'ensemble des personnes impliquées dans la maintenance, l'exploitation, l'administration ou l'utilisation du système doivent être en mesure de noter et signaler dans les meilleurs délais tout dysfonctionnement observé ou soupçonné dans l'usage normal du système et pouvant porter atteinte aux données ou au système lui-même.

La procédure de gestion des incidents doit garantir que le signalement soit remonté aux autorités compétentes selon les exigences législatives et réglementaires en vigueur.

INCID-GEST-QUALIF : Qualification des événements

Chaque entité ou IIV doit pouvoir évaluer chaque évènement afin de pouvoir décider s'il s'agit d'un incident lié à la sécurité du SI et de déterminer sa catégorie. Dans ce cas, la criticité de cet incident doit être appréciée selon une échelle de classification des incidents de cybersécurité basée sur la sensibilité du service impacté et sur l'impact induit.

INCID-GEST-REPONSE : Réponse aux incidents liés à la sécurité des SI

Dès qu'un incident de cybersécurité est confirmé, chaque entité ou IIV doit attribuer les rôles et responsabilités aux différents membres de l'équipe d'intervention interne, externe ou mixte, et s'assurer que toutes les tâches concernant la réponse sont correctement réalisées et journalisées conformément à une procédure de réponse formalisée.

INCID-GEST-ALERT : Réaction aux alertes liés à la sécurité des SI

Chaque entité ou IIV doit mobiliser les ressources internes et/ou externes pour réagir efficacement aux alertes liées à la sécurité des SI.

Ces 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 ou l'IIV 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.

INCID-GEST-REP : Répertoire d'incidents

La typologie et la description des incidents de cybersécurité 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.

INCID-GEST-PREUV : Recueil des preuves

En cas d'attaque suspectée, chaque entité ou IIV doit définir et appliquer les procédures relatives :

- *aux processus de recherche, de reconnaissance et de documentation des preuves potentielles ;*
- *au recueil des éléments physiques pouvant contenir des preuves potentielles ;*
- *au processus de création de copie de données ;*
- *à la protection et la sauvegarde de l'intégrité et l'état d'origine des preuves potentielles.*

GESTION DE LA CONTINUITE DE L'ACTIVITE

Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité

Objectif 29 : *Neutraliser les interruptions des activités de l'entité ou de l'IIV, protéger les processus métier cruciaux des effets causés par les défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.*

CONTINU-BIA : Analyse d'impact sur l'activité

Chaque entité ou IIV est tenue d'établir une analyse d'impacts sur son activité, qui consiste à :

- *identifier les activités et processus critiques ;*
- *analyser les risques liés 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 ;*
- *établir le temps d'arrêt ou d'indisponibilité maximum supportable des activités critiques ;*
- *identifier et considérer toute activité critique dépendant d'autres entités ou IIV, des fournisseurs et d'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.*

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

Chaque entité ou IIV doit préparer un plan de continuité et de reprise d'activités intégrant l'ensemble des solutions pour pallier les arrêts des processus et applications critiques. Il doit porter notamment sur des solutions de secours informatique (sauvegarde, site de secours, bascule, résilience des réseaux, redondance matérielle et logicielle, etc.).

Le PCA/PRA doit décrire de manière précise les rôles et les responsabilités de tous les intervenants en cas de sinistre.

CONTINU-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.

CONTINU-EXERCICE : Exercices et Scenarios

Chaque entité ou IIV est tenue d'organiser de manière régulière des exercices de crise afin de tester le PCA/PRA.

CONFORMITE

Conformité aux obligations légales et réglementaires

Objectif 30 : *Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité des SI.*

CONF-OBLIG-IDF : Identification de la législation en vigueur

L'arsenal légal, réglementaire, normatif et contractuel auquel l'entité ou l'IIV est soumise doit être clairement identifié. La politique de sécurité des SI doit faire référence à cet arsenal et mettre l'accent sur l'obligation de s'y conformer.

CONF-OBLIG-CYBERSEC : Conformité à la réglementation liée à la cybersécurité

Chaque entité ou IIV doit veiller à ce que la gestion de la sécurité ses SI soit conforme au cadre juridique applicable en matière de cybersécurité notamment la loi n° 05-20 relative à la cybersécurité et le décret n° 2-21-406 pris pour son application.

CONF-OBLIG-INTELLECT : Droits de propriété intellectuelle

Chaque entité ou IIV doit veiller au respect des droits de propriété intellectuelle notamment en interdisant l'utilisation de tout logiciel non doté d'une licence d'utilisation valide.

CONF-OBLIG-PERSO : Protection des données personnelles

Chaque entité ou IIV doit veiller au respect de la législation relative à la protection des données à caractère personnel notamment la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et les textes pris pour son application.

CONF-OBLIG-CRYPTO : Réglementation relative aux mesures cryptographiques

Chaque entité ou IIV doit veiller au respect des dispositions légales, réglementaires et normatives se rapportant au recours à des mesures cryptographiques.

Revue de la sécurité de l'information

Objectif 31 : *Garantir que la sécurité des SI est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles*

CONF-REVU-SSI : Vérification de la conformité de la sécurité des SI

Chaque entité ou IIV doit auditer régulièrement la conformité de la sécurité de ses systèmes d'information.

Chaque opération d'audit doit donner lieu à des recommandations. Celles-ci doivent être mises en œuvre dans le cadre de plans d'actions en concertation avec les structures concernées.

A sa demande, les rapports d'audit peuvent être mis à la disposition de la DGSSI.

Annexe : Glossaire

Actif informationnel

Toute ressource tel que le matériel, le logiciel, la donnée ou la procédure, qui compose un système d'information.

Analyse des risques

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

Audit

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

Cloisonnement du réseau

Technique ayant pour objectif de diviser un réseau informatique en plusieurs sous-réseaux. Le cloisonnement est principalement utilisé afin d'augmenter les performances globales du réseau et améliorer sa sécurité, 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.

Cybersécurité

L'ensemble de mesures, procédures, concepts de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques, et technologies permettant à un système d'information de résister à des évènements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ce système offre ou qu'il rend accessibles.

Cyberespace

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

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.

Dysfonctionnement

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

Environnement de développement

Englobe les personnes, les processus et la technologie associés au développement et à l'intégration du système.

Filtrage

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

Incident de cybersécurité

Un ou plusieurs événements indésirables ou inattendus liés à la sécurité des SI et présentant une forte probabilité de compromettre les activités d'une entité ou d'une IIV, ou de menacer la sécurité de ses systèmes d'information.

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.

Journaux d'événements

Ils sont utilisés pour détecter des incidents de sécurité. Les journaux sont consultés et analysés en temps réel. Ils sont également employés pour retrouver les traces d'un incident de sécurité et permettre de comprendre le cheminement d'une attaque et d'évaluer son impact.

Les catégories de journaux contiennent différents types d'informations en fonction de l'objectif de la journalisation : sécurité informatique, audits, conformité aux réglementations, etc.

Menace

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

Mesure

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

Moyen de traitement de l'information

Tout système, service ou infrastructure de traitement de l'information, ou le local les abritant.

Network Time Protocol (NTP)

Protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure.

Opérateurs système

Une personne qui exécute des programmes et des routine spécifiques au système d'information.

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'entité ou de l'IIV 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 informatiques ne constitue que l'un de ces aspects.

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.

Principe du moindre privilège

Principe qui consiste à limiter les droits / habilitations de tout individu sur le SI aux seules applications / données qui lui sont nécessaires dans le cadre de ses missions.

Système de gestion de clés cryptographiques

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

Système d'information (SI)

Un ensemble organisé de ressources telles que les personnels, matériels, logiciels, données et procédures qui permettent de collecter, de classifier, de traiter et de diffuser 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.

Liste des règles par chapitre

POLITIQUES DE SECURITE DES SYSTEMES D'INFORMATION

POL-RISQUE : Analyse de risque
POL-FORMEL : Politiques de sécurité des systèmes d'information
POL-PAS : Plan d'actions de la sécurité des SI
POL-TDB : Tableau de bord de la sécurité des

ORGANISATION DE LA SECURITE DES SYSTEMES D'INFORMATION

ORG-INTER-GOUV : Gouvernance de la sécurité des SI
ORG-INTER-RSSI : Désignation d'un RSSI
ORG-INTER-RESP : Attribution des rôles et responsabilités
ORG-TELETRAV-SEC: Télétravail sécurisé

SECURITE DES RESSOURCES HUMAINES

RH-AVT- PERSON : Personnel de confiance
RH-AVT- COND : Termes et conditions d'embauche
RH-APRES- FORM: Formation et sensibilisation du personnel
RH-FIN-GEST : Gestion des mutations et départs

GESTION DES ACTIFS INFORMATIONNELS

ACTIF-RESP-INV : Inventaire des actifs
ACTIF-RESP-PROP : Propriétaires des actifs
ACTIF-RESP-CHARTE : Charte d'utilisation SI
ACTIF- RESP-CARTO : Cartographie SI
ACTIF- CLASSIF-INFO : Classification
ACTIF- CLASSIF-MES : Mesures de protection des informations
ACTIF- CLASSIF- EXAM : Examen de la classification
ACTIF-SUP-AMOV : Gestion des supports amovibles
ACTIF-SUP-MOBIL : Politique en matière d'appareils mobiles
ACTIF-SUP-NOMAD : Postes nomades
ACTIF-SUP-REB : Mise au rebut ou recyclage des supports

CONTROLE D'ACCES

ACC-EXIG-POL : Politique de contrôle d'accès
ACC-UTILIS-ENREGIS/DESINSCRI : Enregistrement et désinscription des utilisateurs
ACC-UTILIS-IDF/AUTH : Identification et authentification
ACC-UTILIS-HABILIT : Gestion des habilitations
ACC-UTILIS-GENERIQ : Gestion des comptes génériques
ACC-UTILIS-REVUE : Revue des droits d'accès
ACC-SYS/APP-ACC : Accès aux systèmes et applications
ACC-SYS/APP-PRIVIL : Gestion des accès à privilèges
ACC-SYS/APP-MDP : Gestion des mots de passe

CRYPTOGRAPHIE

CRYPTO-MES-POL : Politique d'utilisation des mesures cryptographiques
CRYPTO-MES-GESTCLE: Gestion des clés cryptographiques

SECURITE PHYSIQUE ET ENVIRONNEMENTALE

PHYS-ZONE-DELIMIT : Délimitation des zones
PHYS-ZONE-PROC : Procédures de contrôle d'accès
PHYS-ZONE-DISPO : Dispositif de contrôle d'accès
PHYS-ZONE- VIDEOPROT : Vidéo protection
PHYS-ZONE-INCEN : Sécurité incendie
PHYS-ZONE-EAU : Dégâts des eaux
PHYS-MAT- CABL : Sécurité du câblage
PHYS-MAT-OND : Onduleurs
PHYS-MAT-ELECTROG : Groupe électrogène
PHYS-MAT-CLIM : Climatisation
PHYS-MAT-EQUIP : Entretien des équipements de sécurité environnementale
PHYS-MAT-HORSLOC : Sécurité du matériel et des actifs hors les locaux

SECURITE LIEE A L'EXPLOITATION

EXP-PROC-CHANG : Gestion des changements
EXP- PROC-CAP : Gestion des capacités
EXP-PROC-ENVIR : Séparation des environnements
EXP-PROTEC-MALVEIL : Protection contre les logiciels malveillants
EXP-SAUV-PROC : Procédures de sauvegarde
EXP-SAUV-RESTAUR : Restauration
EXP-SAUV-SEC : Sécurité des sauvegardes
EXP- JOURN/SURV-JOURNAL : Journalisation des événements
EXP- JOURN/SURV-PRIVIL : Traçabilité des actions des comptes à privilège
EXP-JOURN/SURV-MAINT : Traçabilité des actions de maintenance
EXP- JOURN/SURV -SYNCHRON : Synchronisation des horloges
EXP- JOURN/SURV -DIST : Administration à distance
EXP- JOURN/SURV - CENTR : Centralisation
EXP-SYS-CONFIG : Configuration système
EXP-SYS-DURC : Durcissement des configurations
EXP-VULN-INSTALL : Restrictions liées à l'installation de logiciels
EXP-VULN-GEST : Gestion des vulnérabilités techniques
EXP-VULN-CORRECT : Gestion des correctifs
EXP-AUDIT-MES : Mesures relatives à l'audit du système d'information

SECURITE DES COMMUNICATIONS

COM-MANAG-CLOISON : Cloisonnement du réseau
COM-MANAG-FILTRAGE : Filtrage des flux
COM-MANAG-SYSAUT : Systèmes autorisés sur le réseau
COM-MANAG-DISTANT : Accès distants
COM-MANAG-TUNEL : Tunnelisation chiffrée
COM-MANAG-RSF : Sécurité des réseaux sans fil
COM-TRANS-FICHIER : Usage des transferts par fichiers
COM-TRANS-MESS : Usage de la messagerie électronique
COM-TRANS- FILTR : Filtrage des mails

ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION

DEV-EXIG-PROJET : Sécurité de l'information dans la gestion de projet
DEV-EXIG-TRANSAC : Protection des transactions liées aux services d'application
DEV-PROC-POL : Politique de développement sécurisé
DEV-PROC-CHANG : Contrôle des changements apportés au système dans le cycle de développement
DEV-PROC-ENVIR : Environnement de développement sécurisé
DEV-PROC-TEST : Test de la sécurité du système
DEV-PROC-CODE : Protection du code source des programmes
DEV-PROC-DONNEE : Protection des données de test

RELATIONS AVEC LES FOURNISSEURS

FOURNIS-REL-RISQ : Risques émanant des fournisseurs
FOURNIS-REL-POL : Politique de sécurité de l'information dans les relations avec les fournisseurs
FOURNIS-REL-EXIG : Exigences contractuelles
FOURNIS-GEST-SURVEIL : Surveillance et revue des services des fournisseurs

GESTION DES INCIDENTS LIES A LA SECURITE DES SYSTEMES D'INFORMATION

INCID-GEST- PROC : Procédures et responsabilités en matière de gestion des incidents
INCID-GEST-CAT : Catégorisation et classification des incidents
INCID-GEST-SIGNAL : Signalement des événements
INCID-GEST-QUALIF : Qualification des événements
INCID-GEST-REPONSE : Réponse aux incidents liés à la sécurité des SI
INCID-GEST-ALERT : Réaction aux alertes liés à la sécurité des SI
INCID-GEST-REP : Répertoire d'incidents
INCID-GEST-PREUV : Recueil des preuves

GESTION DU PLAN DE CONTINUITE DE L'ACTIVITE

CONTINU-BIA : Analyse d'impact sur l'activité
CONTINU-ACT : Plan de Continuité et de Reprise d'Activité (PCA/PRA)
CONTINU-PLAN : Mise à l'essai des PCA/PRA
CONTINU-EXERCICE : Exercices et Scenarios

CONFORMITE

CONF-OBLIG-IDF : Identification de la législation en vigueur
CONF-OBLIG-CYBERSEC : Conformité à la réglementation liée à la cybersécurité
CONF-OBLIG-INTELLECT : Droits de propriété intellectuelle
CONF-OBLIG-PERSO : Protection des données personnelles
CONF-OBLIG-CRYPTO : Réglementation relative aux mesures cryptographiques
CONF-REVU-SSI : Vérification de la conformité de la sécurité des SI