الـجـمـهـورية الـجـزائـريـــة الـديـمـقـراطـية الـشـعـبـيـة

وزارة البريد والمواصلات السلكية واللاسلكية

2020

Référentiel National de Sécurité de l'Information

Ministère de la Poste et des Télécommunications (MPT)
www.mpt.gov.dz

L06-Version Finale du RNSI 2020

مؤسسة دعم تطوير الرقمنة

Contributeurs

1. Équipe Projet

NOM & PRÉNOM	PROFIL	RÔLE
Mr Abdelbasset Zerrouki	Expert Sécurité de l'Information, Directeur Sécurité de l'Information / Entreprise d'Appui au Développement du Numérique (EADN)	Chef de projet Technique/Rédacteur
Mr ZOUAOUINE Hicham	Expert Sécurité de l'information Cybersecurity Manager / EADN	Membre/Rédacteur
Mr GUENAOUI Fetheddine	Expert Gouvernance de la Sécurité de l'Information / EADN	Membre/Rédacteur
Mr AKBI Farid	Expert Sécurité de l'information.	Membre/Rédacteur
Mr DERHAB Abdelouahid	Expert Gouvernance de la Sécurité de l'Information, Chercheur.	Membre/Rédacteur
Mr. Chelghoum Habib	Ingénieur Sécurité de l'Information (EADN)	Membre.
Mr. Serrir Abderraouf	Ingénieur Sécurité de l'Information (EADN)	Membre.
Mr. ZEMAM Zoubir	Ingénieur Qualité (EADN)	Revue Qualité

2. Représentants des Organismes Publics

NOM & PRÉNOM	ORGANISME
ABBOU Loubna	*Ministère du Tourisme - MT*
ABROUS LAMIA	*Ministère de la formation et de l'enseignement professionnels - MFEP*
ACHOUR Nabil	*SONATRACH - Ministère de l'Energie*
AKEB Mohammed	*Ministère des Ressources en Eau (MRE)*
ALANE Abdelkader	*Ministère de la Communication - MC*
ALLOUANI Akram	*Ministère de l'Energie - ME*
AMARA Ghalem	*Ministère de l'Education Nationale - MEN*
ANIBA Souleyman	*Ministère de la Poste et des Télécommunications - MPT*
ANSAR Belgacem	*Direction générale des Impôts - MF*
ARAB Anouar	*Ministère de la Jeunesse et des Sports - MSJ*
BAKIR Nadia	*Ministère du Travail de l'Emploi et de la Sécurité Sociale - MTESS*
BEKHTI Hamza	*Ministère de la Poste et des Télécommunications - MPT*
BELACEL Kaddour	*Ministère de la Santé de la Population et de la Réforme Hospitalière - MSPRH*
BELBERKANI Noureddine	*Ministère des Affaires Etrangères - MAE*
BELFENDES Faysal	*Commandement de la Gendarmerie Nationale - CGN*
BELFERD Lotfi	*Direction Générale de la Sûreté Nationale - DGSN*
BELFODIL AMINE	*SONATRACH - Ministère de l'Energie (DSI)*
BELFRITAS ABOUELKHEYR	*Centre National d'Intégration des Innovations Pédagogiques et de Développement des Technologies de l'Information et de la Communication en Education (CNIIPDTICE) - MEN*

BELGHOUL Bilal	*Ministère des Affaires Etrangères - MAE*
BELHADJ AISSAA Naila	*Agence Nationale de la Promotion et du Développement des Parcs Technologiques -ANPT*
BELHAMRA HADJIRA	*DIRECTION GENERALE DE LA FONCTION PUBLIQUE ET DE LA REFORME ADMINISTRATIVE*
BENARBIA Sid Ahmed	*Agence Nationale de la Promotion et du Développement des Parcs Technologiques -ANPT*
BENCHEIKH Ahlem	*Algérie Poste - MPT*
BENNAOUM Abdelkader	*Algérie Télécom (Direction de sécurité des systèmes d'information) - MPT*
BOUALI Ali	*Ministère de la Santé de la Population et de la Réforme Hospitalière - MSPRH*
BOUDISSA Abdelmoumen	*El Djazair Information Technology - ELIT - Groupe SONELGAZ*
BOUDJADI Mohamed	*Ministère de l'Enseignement Supérieur et de la Recherche Scientifique - MESRS*
BOUKETTA Adel	*Algérie Télécom (Direction de sécurité des systèmes d'information) - MPT*
BOUKRIA Smail	*La Direction Générale de la Fonction Publique et de la Réforme Administrative - DGFRRA*
BOUKRIT SAMI	*Ministère des Affaires Etrangères - MAE*
BOUNOUA Amel	*SONATRACH - Ministère de l'Energie*
BOUZRINA Sid Ali	*Ministère de la Justice - MJ*
CHARIFI MOHAMED Salim	*Ministère de la Jeunesse et des Sports - MSJ*
CHEBBAB Miloud	*Ministère des Travaux Publics et des Transports - MTPT*
CHERFAOUI FAZZIA	*Ministère des finances – MF / Direction générale de la comptabilité / D – informatique.*
DADI HAMOU Abdelkrim	*Entreprise d'Appui au Développement du Numérique - EADN*
DALI Mustapha	*Ministère de l'Agriculture, du Développement Rural et de la Pêche- MADRP*
DERRIDJ Lamia	*COMMISSION DE REGULATION DE L'ELECTRICITE ET DU GAZ (CREG)*
DJAHNIT ABDESSELAM	*Ministère du Commerce - MC*
DJEDDI Doudja	*Ministère de la Solidarité Nationale, de la Famille et de la Condition de la Femme - MSNFCF*
GHERBOUDJ Faycel	*Ministère de l'Intérieur, des Collectivités Locales et de l'Aménagement du Territoire - MICLAT*
HADDADJI Samir	*Direction Générale de la Sûreté Nationale - DGSN*
HADDED Samira	*Ministère des Finances - MF (DSI)*
HADJIEDJ Mahfoud	*Ministère Des Moudjahidine Et Ayants Droit - MMAD*
HAMMOUCE Imene	*El Djazair Information Technology - ELIT - Groupe SONELGAZ*
HAZAZI FAYCEL	*Ministère de l'Industrie - MI*
HEMIS Mustapha	*Ministère de la Poste et des Télécommunications - MPT*
HOUAMED Nassima	*Direction Générale Des Impôts - Ministère des Finances*
KANOUNE Yahia	*Ministère de l'Intérieur, des Collectivités Locales et de l'Aménagement du Territoire - MICLAT*
KHELLADI Abdelghani	*Ministère de l'Éducation Nationale - MEN*
Kheroubi ARAIBI Sifeddine	*Ministère de la Poste et des Télécommunications - MPT*
KOUICI Nordine	*Ministère de la Défense Nationale - MDN*

LAIDOUDI Lyassine	*Ministère de l'Industrie et des Mines - MIM*
LAOUIR Mohamed	*Ministère de la Communication - MC*
LATEB Adbelhamid	*Ministère des Ressources en Eau (MRE)*
LAZIROU Dalila	*Ministère de l'Industrie et des Mines - MIM*
LEBCIR Fahima	*La Direction Générale de la Fonction Publique et de la Réforme Administrative - DGFRRA*
LEHANINE Fouzia	*SONATRACH - Ministère de l'Energie*
LOUAGUENOUNI Madjid	*Ministère des Ressources en Eau (MRE)*
LOUNACI Leila	*Ministère de la pèche et des produits halieutiques - MPPH*
MEDAOUAR Naima	*Ministère des Travaux Publics et des Transports - MTPT*
MEDELLEL Wissem	*Caisse nationale des assurances sociales - CNAS*
MEHENNI khadidja	*Ministère des Relations avec le Parlement - MRP*
MENNAS Abdelhamid	*Direction Générale du Domaine National - DGDN*
MESROURI Yacine	*Ministère du Tourisme - MT*
OUAMMAR Lamia	*Ministère des Affaires religieuses et des Waqfs - MARW*
OULD ALI Atmane	*Ministère de la Justice - MJ*
OUSLIHA Amina	*Ministère de la culture*
RECHID Abdelatif	*Ministère de la formation et de l'enseignement professionnels - MFEP*
SADEK Houari	*MINISTERE DES RELATIONS AVEC LE PARLEMENT - MRP*
SADEK Houari	*Ministère des Relations avec le Parlement - MRP*
SALHI Samir	*Algérie Police - MPT*
SAMET Abdelkader	*Ministère des Affaires Etrangères - MAE*
SEDDIK Mohamed	*Ministère de la Poste et des Télécommunications - MPT*
SILARBI Larbi	*Ministre de l'Habitat, de l'Urbanisme et de la Ville - MHUV*
SILEM Rabah	*Ministère des Finances - MF*
SLIMANI Younes	*Ministère des Affaires religieuses et des Waqfs - MARW*
TIZOUIAR Tarik	*Ministère de la Défense Nationale - MDN*
YOUCEF KHOUDJA	*Direction Générale de la Sûreté Nationale - DGSN*
ZELLAGUI Khadidja	*Ministère de la pèche et des produits halieutiques - MPPH*

Acronymes et abréviations

Acronyme	Signification
RNSI	Référentiel National de Sécurité de l'Information
eGov	Le gouvernement électronique
TIC	Technologies de l'Information et de Communication
ISO	International Standards Organisation (Français : Organisation internationale de normalisation)
IEC	International Electrotechnical Commission (Français : Commission électrotechnique internationale)
NIST	National Institute of Standards and Technology (USA)
GDPR	General Data Protection Regulation
RGPD	Règlement Général sur la Protection des Données
CIS	Center of Internet Security
RSSI	Responsables de la Sécurité des Systèmes d'Information
GSI	Gouvernance de la Sécurité de l'Information
CSI	Comité de Sécurité de l'Information
CD	Comité de Direction
PCA	Plan de continuité d'activités
DPIA	Data Protection Impact Assessment (Français : Analyse d'impact relative à la protection des données).
PIN	Personal Identification Number
IP	Internet Protocol
DLP	Data Leak Prevention
IaaS	Infrastructure As a Service
PaaS	Product As a Service
SaaS	Security As a Service
AGCE	Autorité Gouvernemental de Certification Electronique
AECE	Autorité Economique de Certification Electronique
CP	Certificate Policy (Français : Politique de Certificats)
PKI	Public Key Infrastructure Infrastructure (Français : Clés Publiques ou PKI)
MSP	Modules de Sécurité Physique
HSM	Hardware Security Module
IoT	Internet of Things (Français : Internet des Objets)
CERT	Computer Emergency Response Team (Français : Equipe de réponse aux incidents de sécurité).
DRP	Disaster Recovery Plan
NDA	Non-Disclosure Agreement (Français : Accord de Confidentialité ou Accord de Non Divulgation)
OTP	One Time Password (Mot de passe à usage unique)
SSDLC	Secure Software Developement Life Cycle (Français : Intégrer la sécurité dans le cycle de vie du développement des logiciels)
SLA	Service Level Agreement (Français : Accord de Niveau de Service)
DMZ	Demilitarized Zone (en Français : Une zone démilitarisée)

Table des matières

1 Préambule.

Dans les dernières années, l'Algérie a connu une évolution rapide dans le domaine des technologies de l'information et de la communication, ce qui représente une condition nécessaire pour la transformation vers l'économie numérique et l'adoption d'une approche E-Gouvernement centrée autour du citoyen. Cependant, cette transformation nécessite la sécurisation et la protection de tous les systèmes numériques ainsi que leurs flux d'information.

Les menaces potentielles des cyber-attaques contre les technologies de l'information et de la communication ont provoqué des pertes économiques et un climat d'insécurité et d'incertitude envers les services numériques. Ceci appelle à appliquer des contremesures qui protègent les organismes et les infrastructures critiques, préservent les intérêts vitaux du pays et renforcent la sécurité nationale.

Dans ce contexte, le présent Référentiel National de Sécurité de l'Information (RNSI) vise à établir une gouvernance et une approche commune de la sécurité de l'information au sein des organismes publics. Il définit aussi les exigences minimales en matière de sécurité qui permettent de gérer, résister et réduire l'impact des menaces qui peuvent survenir. Le RNSI présente aussi les contrôles de sécurité et les bonnes pratiques à adopter par les organismes publics, tout en focalisant sur la formation et la sensibilisation des usagers aux risques encourus, et l'évaluation périodiques des contrôles afin d'assurer la satisfaction continue des exigences de sécurité et la conformité aux obligations réglementaires.

2 Mise à jour du Référentiel National de Sécurité de l'informatique 2016.

Sur instruction du Premier Ministère, un groupe multisectoriel dirigé par le Ministère de la Poste, des Télécommunications, des Technologies et du Numérique (MPTTN), a développé en 2016 le Référentiel National de Sécurité Informatique (RNSI 2016). Ce référentiel est le premier guide regroupant les lignes directrices et les bonnes pratiques en matière de sécurisation des informations et des systèmes d'information. Il couvre plusieurs domaines de la sécurité afin de garantir une protection adéquate des systèmes d'information des organismes publics.
Avec la diversification et l'évolution des menaces cybernétiques ainsi que les nouvelles exigences de la législation et la réglementations Algériennes en matière de la sécurité de l'information, il est important de mettre à jour la première version du RNSI 2016 en vue de prendre en charge les nouveaux risques liés à la transformation digitale que connait plusieurs secteurs névralgiques et au passage vers le gouvernement électronique (eGov).

3 Cadre normatif du référentiel.

L'élaboration du nouveau Référentiel National de Sécurité de l'Information (RNSI 2020) repose sur les meilleures pratiques internationales et les standards connus en matière de la sécurité de l'information, à savoir :

Norme / Standard / Bonnes pratiques	Description
ISO / IEC 27001:2013	Norme internationale de sécurité des systèmes d'information de l'ISO et la CEI. Cette norme spécifie les exigences relatives à l'établissement, la mise en œuvre, la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation.
ISO / IEC 27002:2013	La norme ISO/CEI 27002 est une norme internationale concernant la sécurité de l'information, donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information.
ISO / IEC 27005:2018	Décrit les grandes lignes d'une gestion des risques. Elle est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques.
ISO/IEC 22301:2019	Cette norme décrie les exigences de systèmes de management de la continuité d'activité.
ISO/IEC 22313:2012	Cette norme décrie les lignes directrices de systèmes de management de la continuité d'activité.
ISO/IEC 27035-1 :2016	Gestion des incidents de sécurité de l'information — Partie 1: Principes de la gestion des incidents
ISO/IEC 27035-2 :2016	Gestion des incidents de sécurité de l'information — Partie 2: Lignes directrices pour planifier et préparer une réponse aux incidents.
ISO/IEC 27701:2019	Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices.
ISO / IEC 27015:2015	Cette norme décrie les lignes directrices pour le management de la sécurité de l'information pour les services financiers.
NIST 800-53 Revision 4	Décrie les contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations fédérales USA.
GDPR 2016 (General Data Protection Regulation)	RGPD (Règlement Général sur la Protection des Données) est un règlement de l'union européenne, qui constitue le texte de référence en matière de protection des données à caractère personnel.
CIS 20 Critical Controls (version 7.1).	Le Centre pour la sécurité Internet, Contrôles de sécurité essentiels pour une cyberdéfense efficace, est une publication des meilleures pratiques en matière de sécurité informatique.

4 Cadre Légal et Réglementaire du référentiel.

Texte légal ou réglementation.	**Références.**
Dispositif national de la sécurité des systèmes d'information.	Décret présidentiel n° 20-05 du 24 Joumada El Oula 1441 correspondant au 20 janvier 2020 portant mise en place d'un dispositif national de la sécurité des systèmes d'information.
Réglementation relative aux mesures cryptographiques.	Décret exécutif n°16-61 du 02 Joumada El Oula 1437 correspondant au 11 février 2016 modifiant et complétant le décret exécutif n° 09-410 du 23 Dhou El-Hidja 1430 correspondant au 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles.
Les règles générales relatives à la poste et aux communications électroniques	Loi n°18-04 du 24 Chaâbane 1439 correspondant au 10 mai 2018 fixant les règles générales relatives à la poste et aux communications électroniques.
Propriété intellectuelle (Les logiciels)	Ordonnance n°03-05 du 19 Joumada EL Oula 1424 correspondant au 19 juillet 2003 relative aux droits d'auteur et aux droits voisins.
Certification électronique	Loi n°15-04 du 11 Rabie Ethani 1436 correspondant au 1er Février 2015 fixant les règles générales relatives à la signature et à la certification électroniques. Décret n°2016-134 du 17 Rajab 1437 correspondant au 25 avril 2016 fixant l'organisation, le fonctionnement et les missions des services techniques et administratifs de l'Autorité nationale de certification électronique. Décret n°2016-135 du 17 Rajab 1437 correspondant au 25 avril 2016 fixant la nature, la composition, l'organisation et le fonctionnement de l'Autorité gouvernementale de certification électronique.
Protection des données à caractère personnel.	Loi n° 18-07 du 25 Ramadhan 1439 correspondant au 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel.
Les infractions liées aux technologies de l'information et de la communication	Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 05 aout 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.
Lutte contre la cybercriminalité.	Décret présidentiel n° 14-252 du 13 Dhou El Kaada 1435 correspondant au 8 septembre 2014 portant ratification de la convention arabe pour la lutte contre la cybercriminalité.

5 Objectif du Référentiel National de Sécurité de l'Information 2020.

Le Référentiel National de Sécurité de l'Information (RNSI 2020) a pour objectif de fournir un cadre et un ensemble de prérequis qui permettront d'élaborer et d'implémenter la politique de sécurité des systèmes d'information au sein des organismes à caractère public et leurs sous-tutelles.

Les recommandations contenues dans ce document fournissent une approche de sécurisation de l'information basée sur la gestion des risques en ce qui concerne la confidentialité, l'intégrité et la disponibilité des informations.

Les objectifs du référentiel perceptibles à travers ses différents domaines sont :

- Augmenter le niveau de sécurité des systèmes d'information et la protection des informations des organismes par la mise en place des contrôles de sécurité adéquats ;
- Adopter une approche basée sur l'appréciation des risques lors de l'implémentation des contrôles de sécurité ;
- Définir les rôles et responsabilités appropriées en matière de protection des informations.

6 Champs d'application du RNSI 2020 (périmètre).

Ce référentiel s'applique aux administrations et secteurs publics. (Instruction n°02/PM du 03 Juillet 2016, portant mise en œuvre du Référentiel National Normalisé de Sécurité Informatique), ainsi que toute infrastructure hébergée sur le territoire national et traitant de l'information sensible selon les législations et règlementations en vigueur.

7 Applicabilité des contrôles du référentiel.

Les contrôles de sécurité mentionnés dans ce référentiel sont conçus pour répondre aux besoins de sécurité de l'information de toutes les administrations et secteurs publics faisant partie du champ d'application.

Les contrôles varient en termes d'applicabilité d'un secteur à un autre en prenant en considération, l'aspect organisationnel, les règlements internes, la nature de l'activité et les technologies déployées. Toutefois, il est indispensable d'élaborer une déclaration d'applicabilité justifiant l'insertion ou l'exclusion d'une mesure de sécurité à la base du résultat des appréciations des risques.

8 Suivi de la mise en œuvre du référentiel

Objectif : Garantir le suivi de mise en œuvre du référentiel national de sécurité de l'information.

Afin de garantir la mise en place du référentiel,

1. Chaque département ministériel doit mette en place un comité de suivi sectoriel qui regroupe les Responsables de la Sécurité des Systèmes d'Information (RSSI) des organismes du secteur, présidé par le RSSI du département ministériel. Chaque comité de suivi sectoriel doit suivre l'évolution de la mise en œuvre du RNSI dans le secteur ;

2. Chaque organisme du secteur doit mette en place un comité de suivi de mise en œuvre du RNSI présidé par le RSSI de l'organisme ;

3. Le RSSI de chaque organisme doit analyser les différentes informations qui lui sont parvenues, élaborer un rapport contenant ses conclusions et remarques et le transmettre à sa hiérarchie et au comité de suivi sectoriel ;

4. Un outil d'évaluation et de conformité (RNSI2020_AssessmentToolkit_Vx) sera mise en place afin de réglementer le processus d'évaluation et de mesure de l'engagement des organismes quant à l'application des exigences dudit référentiel.

9 Revue et Amélioration continue du document du référentiel

Le présent référentiel fera l'objet d'améliorations continues pour se conformer à la législation ou réglementation Algérienne en cours d'application, en fonction des nouvelles exigences de la sécurité de l'information, menaces cybernétiques, et/ou les résultats de l'application du référentiel dans les différents organismes publics.

10 Gouvernance de la sécurité de l'information

Objectif : Définir et mettre en place l'ensemble des responsabilités et pratiques exercées par la direction (1) afin de soutenir les objectifs de l'organisme à travers l'alignement de la stratégie de la sécurité de l'information avec la stratégie globale de l'organisme, tout en s'assurant que les risques sont gérés de manière appropriée, et vérifier que les ressources de l'organisme sont utilisées de manière optimale.

Activités :

1. Développer la stratégie globale de la sécurité de l'information.
2. Développer les politiques de sécurité de l'organisme.
3. Identifier, mettre en place et surveiller les métriques de sécurité afin de mesurer l'évolution de réalisation des objectifs de sécurité de l'organisme.
4. Vérifier périodiquement la conformité des stratégies et politiques de sécurité à mettre en place avec les normes de sécurité connues.

(1) Aussi équivalent au terme 'Top management'.

10.1 Engagement (anglais : Leadership)

Objectif : Démontrer le degré de l'engagement de la Direction de l'organisme à soutenir les mesures de sécurité visant à protéger son système d'information réalisées par l'ensemble de ses structures et des tiers intervenants avec le présent référentiel.

L'engagement de la direction doit faire preuve de leadership et affirmer son engagement à travers les mesures suivantes :

1. Assurer que la politique de la sécurité de l'information et ses objectifs de sécurités sont établis, mise en place, et alignés avec les objectifs stratégiques de l'organisme ;
2. Assurer l'intégration des exigences du système de gestion de la sécurité de l'information dans les processus métier de l'organisme ;
3. Assurer que les ressources (humaines et financières) nécessaires à la réalisation des objectifs de sécurité de l'information de l'organisme sont disponibles ;
4. Communiquer sur l'importance de l'efficacité des mesures de sécurité mise en place ;
5. Démontrer l'engagement de la direction lors des opérations d'amélioration continue des mesures de sécurité (audit, appréciation des risques, conformité).

10.2 Organisation de la sécurité de l'information

Objectif : Établir un cadre organisationnel et fonctionnel pour initier et vérifier la mise en place de la gestion de la sécurité de l'information au sein de l'organisme en tenant compte de l'envergure de chaque organisme ainsi que ses spécificités organisationnelles et fonctionnelles.

1. La Direction(1) doit identifier, approuver et documenter les structures organisationnelles de la gouvernance de la sécurité de l'information, ainsi que les rôles et les responsabilités qui leur sont liés, et s'engage à soutenir les personnes affectées à ces entités ;
2. Un service chargé de la gouvernance de la sécurité de l'information (GSI) doit être créé indépendamment de la structure chargée de la gestion des systèmes d'information (de préférence directement lié au premier responsable de l'organisme) afin d'éviter tout conflit d'intérêts ;
3. Les rôles, responsabilités et qualifications du responsable du GSI doivent être clairement définis en fonction de la nature de ce poste (ou rôle). Le RSSI assure le rôle du responsable du GSI ;
4. Un comité de Direction (CD) doit être mise en place pour veiller à l'alignement des objectifs de la sécurité de l'information avec les objectifs de l'organisme ;
5. Le CD est présidé par le premier responsable de l'organisme ou un responsable désigné, en tenant compte de l'absence de conflit d'intérêts ;
6. Un comité de sécurité de l'information (CSI) doit être mis en place et attaché fonctionnellement à la CD pour assurer le suivi, ainsi que la mise en œuvre de la stratégie de la sécurité de l'information et valider et contrôler les actions menées par le GSI ;
7. La Direction veille à ce que le responsable de la structure chargée de la gouvernance de la sécurité de l'information soit membre du comité de sécurité de l'information (CSI) ;
8. S'assurer que les tâches et responsabilités incompatibles soient cloisonnées pour limiter les possibilités d'accès, de modification, ou de mauvais usage non autorisés des actifs de l'organisme suivant la disponibilité des ressources.

(1) Aussi équivalent au terme 'Top management'.

10.3 Politique de sécurité de l'information

Objectif : Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction(1), conformément aux exigences métier et aux lois et règlementation en vigueur.

Les contrôles à mettre en place :

1. Le service chargé de la GSI doit élaborer la politique générale ainsi que les politiques spécifiques de la sécurité de l'information (Le contrôle d'accès, Sécurité physique, Sauvegarde, etc.) qui définissent clairement les contrôles et les exigences de la sécurité de l'information ;
2. La politique générale de la sécurité de l'information doit être alignée avec les exigences de la stratégie de l'organisme ;
3. Le service chargé de GSI doit s'assurer que les contrôles et les exigences inclus dans les politiques de sécurité sont mis en œuvre ;
4. La politique globale de la sécurité de l'information doit faire l'objet de l'approbation du premier responsable de l'organisme après la validation du comité de sécurité de l'information (CSI) si ce dernier existe ;
5. La Direction veille à la diffusion des politiques de sécurité aux parties concernées (employés de l'organisme et tiers) ;
6. Les politiques de sécurité doivent être examinées et mises à jour à des intervalles de temps réguliers, ou en cas de modification des exigences législatives, réglementaires et normatives pertinentes. Toute mise à jour doit être documentée et adoptée par la Direction ;
7. Les politiques de la sécurité de l'information doivent être déclinées du présent référentiel, et peuvent être soutenues par les normes, les standards et les bonnes pratiques en matière de sécurité de l'information.

(1) Aussi équivalent au terme 'Top management'.

10.4 Rôles et responsabilités

Les rôles et les responsabilités liés à la sécurité de l'information doivent être établis, validés, communiqués, revus et mis à jour à des intervalles réguliers, ou en cas de modifications apportées aux exigences législatives et réglementaires

10.4.1 Le Responsable de la Sécurité des Systèmes d'Information (RSSI)

Objectif : Désigner la personne qui sera en charge d'aider et de suivre la mise en œuvre des mesures de sécurité dans l'organisme, ainsi que les exigences du Référentiel National de Sécurité de l'Information.

Missions :

1. Élaborer et participer à la rédaction et à la mise à jour régulière des différents documents de sécurité (politiques, procédures, etc.) ;
2. Conseiller la direction(1) sur les choix techniques et organisationnels pour assurer la sécurité des systèmes d'information ;
3. Établir la cartographie des risques liés à la sécurité du système d'information, et veiller à la mise en œuvre des différents plans de remédiation ;
4. Évaluer et contrôler le niveau de sécurité des systèmes d'information de l'organisme ;
5. Participer à la mise en place du plan de continuité d'activité, et l'efficacité du plan de secours informatique ;
6. Élaborer un programme de sensibilisation et de formation sur le thème de la sécurité de l'information à destination du personnel interagissant avec le système d'information ;
7. Mettre en place un accompagnement en faveur des différentes structures afin de garantir l'intégration et l'assimilation de la composante sécurité dans les différentes phases de projet, et après l'entrée en production des systèmes d'information ;
8. Effectuer des missions d'audit et d'investigation, à des intervalles de temps réguliers ou après incident ;
9. Assurer le rôle du responsable de la gouvernance de la sécurité de l'information si nécessaire.

(1) Aussi équivalent au terme 'Top management'.

10.4.2 Comité de Direction (CD)

Objectif : aligner le programme de la sécurité de l'information avec les objectifs et la stratégie de l'organisme en respectant les exigences du référentiel national de sécurité de l'information.
Missions : 1. Assurer l'inclusion des exigences du référentiel dans le processus de gestion de la sécurité de l'information ; 2. Établir les objectifs annuels et la stratégie du programme de sécurité de l'information ; 3. Fournir les ressources adéquates pour le fonctionnement de la gouvernance de la sécurité de l'information ; 4. Contrôler la contribution des différentes structures aux processus de gestion de la sécurité de l'information ; 5. Approuver les projets liés à la sécurité de l'information ; 6. Assurer la communication sur la sécurité de l'information avec les parties prenantes telles que le comité de sécurité de l'information.

10.4.3 Comité de Sécurité de l'information (CSI)

Objectif : Assurer la bonne gestion et le fonctionnement adéquat du programme de sécurité de l'information.
Missions : 1. Assure le pilotage de la gestion de la sécurité de l'information ; 2. Promouvoir la cohérence en sécurité de l'information dans l'organisme ; 3. Valider les différentes politiques de sécurité et la stratégie globale de la sécurité de l'information ; 4. Valider et approuver les mises à jour de l'évaluation des risques liés à la sécurité de l'information ; 5. Assurer le déroulement souple des opérations liés à la sécurité de l'information ; 6. Contrôler la mise en œuvre des mesures de sécurité exigées par le Référentiel National de Sécurité de l'Information. 7. Pilote le processus d'amélioration continue des actions de sécurité dans une démarche transverse et cohérente. 8. Les membres du Comité de Sécurité de l'information doivent allier compétences techniques et connaissance des activités et des enjeux métiers de l'organisme (experts en sécurité, administrateurs des systèmes d'information, responsables métier).

10.5 Relation avec les autorités

Objectif : Mettre en place des procédures spécifiant quand et comment il convient de contacter les autorités compétentes (par exemple, les autorités chargées de l'application des lois, les organismes de réglementation, les autorités de surveillance).

Les contrôles à mettre en place :

1. Définir les modalités de signalement des incidents d'atteinte à la sécurité de l'information (par exemple, en cas de suspicion de violation de la loi, ou une attaque par le biais d'Internet). Entretenir de telles relations devient une exigence afin de favoriser la gestion des incidents ou le processus de planification des mesures d'urgence et de continuité de l'activité ;
2. Entretenir des relations appropriées avec les autorités de régulation, qui seront utiles pour anticiper d'éventuels changements sur le plan juridique ou réglementaire qui devraient être appliqués par l'organisme ;
3. Entretenir des relations appropriées avec les autres autorités concernant les services publics à savoir les collectivités locales, les services d'urgence, les fournisseurs d'électricité, la santé, la sécurité et les unités de protection civile ;
4. Des relations appropriées avec les opérateurs en télécommunication doivent être entretenues ;
5. Des relations appropriées avec les autorités compétentes dans le domaine de la sécurité de l'information doivent être entretenues par la structure en charge de l'organisme.

11 Gestion des risques liés à la sécurité de l'information

Objectif : Assurer une gestion systématique des risques de la sécurité de l'information visant à protéger les actifs informationnels et technologiques conformément aux politiques et procédures de l'organisme, ainsi qu'aux exigences législatives et réglementaires en vigueur.

11.1 Gouvernance liée à la gestion des risques :

Objectif : Assurer que les risques liés à la sécurité de l'information de l'organisme sont pris en charge et maintenus à un niveau acceptable en identifiant les vulnérabilités présentes, les menaces ainsi que leurs conséquences (impacts) potentielles sur les actifs, et de proposer les actions correctives nécessaires.

Contrôles :

1. Le service chargé de la GSI doit adopter, documenter et appliquer une méthodologie et des procédures de gestion des risques liés à la sécurité de l'information de l'organisme conformément aux exigences des métiers en matière de confidentialité, de disponibilité et d'intégrité ;

2. La méthodologie et les procédures de gestion des risques doivent être revues et mises à jour régulièrement, ou en cas de changements significatifs des exigences législatives, réglementaires, ou normatives ;

3. La méthodologie de gestion des risques et ses révisions, doivent être approuvées par le premier responsable de l'organisme ;

4. La méthodologie de gestion des risques doit tenir compte de l'aspect communication, surveillance et revue des risques ;

5. L'appréciation des risques de sécurité de l'information doit être faite à des intervalles réguliers, ou dans les cas des changements significatifs tels que :
   - Lancement de nouveaux projets ;
   - Nouvelle relation avec tiers partie ;
   - Lancement de nouveaux produits et services techniques ;
   - Acquisition de nouvelles technologies ;

6. Les résultats d'appréciation des risques doivent être revus et validés par le premier responsable de l'organisme.

11.2 Conception des contrôles de sécurité :

Objectif : Concevoir les contrôles de sécurité adéquats en adoptant une approche basée sur l'évaluation des risques (anglais : risk-based), et s'assurer que la documentation requise est rédigée.

Contrôles :

1. Avant de décrire les processus et les contrôles de sécurité, il est indispensable de procéder à leurs conceptions en prenant en considération :
    - Les objectifs du contrôle ;
    - Les éléments d'entrée ;
    - Les rôles et les responsabilités des principaux intervenants ;
    - L'interdépendance des processus ;
    - Les ressources nécessaires aux opérations,
    - La liste des évidences ;
    - Les indicateurs de mesure ainsi que ses éléments de sortie.
2. Le service chargé de la GSI doit documenter les différents contrôles de sécurité liés au Référentiel National de Sécurité de l'Information.

12 Évaluation des contrôles de sécurité de l'information

Objectif : Veiller à ce que les contrôles de sécurité de l'information de l'organisme soient mis en œuvre et fonctionnent conformément aux politiques et procédures internes, ainsi qu'aux exigences législatives et réglementaires en vigueur.

Contrôles :

1. Le service chargé de la GSI doit examiner périodiquement l'application des contrôles de sécurité en évaluant leur performance, efficacité, efficience et leur conformité aux exigences de sécurité des politiques de sécurité de l'organisme ;

2. Les contrôles de sécurité doivent être mesurés périodiquement en appliquant les métriques adéquates ;

3. L'application de contrôles de sécurité dans l'entité peut être examinée par des parties indépendantes du service de gestion de la sécurité (tel que le service d'audit interne de l'organisme), à condition que l'audit soit effectué de manière indépendante, conformément aux normes d'audit ;

4. Les résultats de l'audit de sécurité doivent être documentés et présentés au comité de la sécurité de l'information (CSI), qui à son tour le communique à la Direction ;

5. Il convient d'utiliser l'outil d'évaluation et de conformité aux exigences du Référentiel National de Sécurité de l'Information renseigné et mis à jour (**RNSI2020_AssessmentToolkit_Vx**) ;

6. L'organisme doit documenter et conserver les résultats des revues.

13 Documents liés à la sécurité de l'information

Objectif : Dans le cadre de la mise en œuvre et le suivi du référentiel national de sécurité de l'information, une liste minimale de documents liés à la sécurité de l'information est exigée, à savoir :

1. La politique de sécurité des systèmes d'information ;
2. Les politiques spécifiques de sécurité (développement sécurisé, ressource humaine, classification de l'information, sécurité physique et environnementale, gestion des incidents, etc.) ;
3. La description du processus et de la méthodologie de gestion des risques liés à la sécurité de l'information, ainsi que la cartographie des risques ;
4. Le plan de traitement des risques approuvé par la Direction ;
5. La déclaration d'applicabilité des contrôles ;
6. L'organisation et les rôles liés à la sécurité de l'information ;
7. Les résultats de la surveillance et de la mesure d'efficacité des contrôles (tableau de bord opérationnel, tactique et stratégique) ;
8. Le programme d'audit dédié à la sécurité de l'information ;
9. Les rapports d'audit liés à la sécurité de l'information et les résultats des tests d'intrusion ;
10. Le plan de continuité d'activités (PCA) ;
11. Les plans de reprise après sinistre suivant les différents scénarios de menaces qui pèsent à l'organisme ;
12. L'outil d'évaluation et de conformité aux exigences du Référentiel National de Sécurité de l'Information renseigné et mis à jour (**RNSI2020_AssessmentToolkit_Vx**).

14 Domaines de sécurité dans le RNSI 2020

14.1 DOMAINE 1 - Gestion des actifs

14.1.1 Responsabilités relatives aux actifs.

Objectif : Identifier les actifs associés à l'information et aux moyens de traitement de l'information de l'organisme et définir les responsabilités appropriées en matière de protection.

14.1.1.1 Inventaire des actifs :

1. L'organisme doit maintenir un inventaire complet, précis, documenté, cohérent et à jour des actifs informationnels ;
2. Les actifs ayant accès à des informations ou manipulant des moyens de traitement des informations au sein de l'organisme doivent être identifiés et inventoriés ;
3. Les dépendances entre les différents actifs doivent être clairement identifiées.

14.1.1.2 Propriétaire de l'actif :

1. Les individus ou toutes autres entités ayant des capacités de gestion et ou décisionnelles des actifs peuvent être désignés comme responsables d'actifs ;
2. Un propriétaire de l'actif doit être désigné lors de la création de l'actif ou de son transfert vers l'organisme ;
3. Les actifs identifiés et inventoriés au sein de l'organisme doivent être affectés à des personnes ou des entités ;
4. Des tâches de gestion peuvent être déléguées, par exemple à une entité ou personne, qui veille en permanence au bon fonctionnement des actifs durant leur cycle de vie, mais la responsabilité incombe au propriétaire ;
5. Le propriétaire des actifs doit remplir les fonctions suivantes :
   - S'assurer et confirmer que l'actif est inventorié ;
   - Vérifier et revoir périodiquement les restrictions d'accès et la classification des actifs, en se basant sur les politiques de classification et de contrôle d'accès validées ;
   - Conduire régulièrement une analyse des risques sur les actifs pour appliquer les contrôles de sécurité adéquats pour réduire les risques à un niveau acceptable par l'organisme.

14.1.1.3 Utilisation adéquate des actifs :

1. Des règles d'utilisation adéquate des informations, des actifs doivent être élaborées, validées, documentées et mises en œuvre ;
2. Les employés et les partenaires (fournisseurs, clients, prestataires, …) manipulant ou ayant accès aux actifs de l'organisme, doivent être informés et sensibilisés des exigences de sécurité des informations, des actifs et des moyens de traitement des informations de l'organisme. Ils doivent être responsables de l'utilisation de ces actifs.

14.1.1.4 Restitution et destruction des actifs :

1. Une procédure de restitution et de destruction des actifs doit être formalisée et documentée en adéquation avec les politiques et procédures de sécurité de l'organisme, ainsi que les lois en vigueur ;
2. Tous les employés et partenaires doivent restituer tous les actifs de l'organisme en leur possession lors de la cessation de leur emploi, contrat ou convention ;
3. En cas de réforme de tout équipement disposant d'un support de stockage, des procédures de destruction définitive des données doivent être élaborées. Lorsque les impératifs de sécurité l'imposent, les supports de stockage doivent être détruits.

14.1.2 Classification de l'information.

Objectif : Déterminer le niveau de protection qui devrait être appliqué aux informations et aux actifs.

14.1.2.1 Classification de l'information :

1. Les informations de l'organisme ainsi que les actifs doivent être classifiés en tenant en considération les exigences légales, la nature, la valeur, la criticité et la sensibilité à la divulgation ou à la modification non autorisée de cette information ;
2. La classification et les mesures de protection des informations doivent prendre en considération les exigences métier de l'organisme pour partager ou restreindre l'information ;
3. Les actifs autres que des informations peuvent également être classifiés, et ce, en conformité avec la classification des informations qui sont stockées, traitées ou manipulées par ces actifs ;
4. Chaque niveau de classification doit être associé à des procédures de gestion et de traitement, ainsi que les mesures de protection des actifs qui lui sont propres;
5. La classification doit être inclue dans les processus de gestion de l'organisme ;

6. Le schéma de classification des informations et des actifs associés doit être cohérent et documenté pour tout l'organisme ;
7. Les employés doivent être informés des niveaux de classification des actifs et des procédures y afférentes pour appliquer les mêmes règles de classification et de protection ;
8. Les résultats de classification devraient indiquer la valeur des actifs en fonction de leur sensibilité et leur criticité au sein de l'organisme, notamment en termes de confidentialité, d'intégrité et de disponibilité.

14.1.2.2 Étiquetage des actifs :

1. Un ensemble approprié de procédures pour l'étiquetage des actifs informationnels et actifs associés devrait être élaboré et mis en œuvre conformément au schéma de classification de l'information adopté par l'organisme ;
2. L'étiquetage devrait refléter le schéma de classification établi précédemment, et les étiquettes doivent être facilement identifiables ;
3. Les procédures devraient donner des indications notamment sur l'endroit et la manière de fixation des étiquettes des actifs physiques ;
4. Les procédures peuvent définir les cas pour lesquels l'étiquetage n'est pas obligatoire ;
5. Les employés doivent être informés des procédures d'étiquetage.

14.1.3 Manipulation des actifs :

Objectif : Des procédures destinées pour la manipulation des actifs devraient être élaborées, mises en œuvre et communiquées, et ce, conformément aux bonnes pratiques recommandées et à la législation et règlementation en vigueur.

Les contrôles :

1. Élaboration de procédures pour le traitement, le stockage et la communication des informations conformément au schéma de classification de l'information adopté par l'organisme ;
2. La tenue à jour d'un enregistrement des destinataires autorisés à accéder aux actifs de l'organisme ;
3. La protection des actifs de support contenant l'information ;
4. La protection des copies temporaires ou permanentes d'information à un niveau compatible avec le niveau de protection de l'information originale.

14.2 DOMAINE 2 - Protection des données à caractère personnel

Protection des données à caractère personnel

Objectif : Définir les règles de sécurité à suivre lors de la collecte, le traitement, le stockage et la disposition des données personnelles identifiables des employés et des citoyens en conformité avec la législation et règlementation en vigueur.

Les informations personnelles identifiables d'un individu peuvent inclure, entre autres :

- Informations sur une personne telles que le nom, date de naissance, lieu de naissance, informations sur l'emploi, informations sur les antécédents médicaux, informations sur les antécédents judiciaire et informations financières.
- Numéro d'identification personnel tel que le numéro d'identification national, numéros de passeport, permis de conduire, etc.
- Informations de son adresse de résidence / bureau, etc.
- Numéros de téléphone,
- Caractéristique personnelle, par exemple photographies, empreintes digitales ou autres données biométriques,

14.2.1 Exigences pour la gouvernance de la protection des données personnelles

1. Les organismes doivent élaborer les politiques et les procédures de protection des données personnelles, la méthodologie d'audit et de mise en conformité, gestion des incidents en cas de violation de données personnelles, ainsi que le processus de gestion des risques ;
2. Analyse d'impact relative à la protection des données (DPIA : Data Protection Impact Assessment) : les organismes devraient effectuer une analyse DPIA des opérations de traitement envisagées, lorsque le traitement risque de générer des risques élevés pour la vie privée ;
3. Identifier les activités principales de l'organisme qui nécessitent la collecte et le traitement des données personnelles. Le traitement prévu doit préciser :
    - Le responsable du traitement ;
    - La finalité du traitement ;
    - Les personnes concernées ;
    - Les tiers auxquels ces données peuvent être communiquées ;
    - Les catégories de données utilisées et leurs origines ;
    - Identifier les actifs concernés par le traitement des données à caractère personnel ;
    - Les personnes qui ont accès aux données ;
    - Les restrictions des accès aux données ;
    - La durée de conservation des données personnelles (suivant la politique de l'organisme et la réglementation en vigueur) ;
    - Les mesures à prendre pour assurer la sécurité des données et du traitement.

4. Les données personnelles ne doivent être conservées que pendant la période nécessaire aux fins pour lesquelles elles ont été collectées et traitées ;
5. Les données personnelles collectées doivent être exactes, complètes et à jour ;
6. Appréciation des risques liés aux traitements des données à caractère personnel :
   - Identifier les impacts potentiels de ses risques ;
   - Identifier les sources de risque et les menaces ;
   - Déterminer les mesures existantes ou prévues pour la diminution de ses risques ;
   - Mettre en œuvre et vérifier les mesures prévues.
7. Le responsable de collecte et de traitement des données personnelles doit notifier les parties intéressées des cas de violation de données ;
8. Les organismes doivent assurer des programmes de formation de sensibilisation au tour des risques liés aux données personnelles, surveiller et évaluer régulièrement la mise en œuvre de ces programmes, et au besoin ajuster les pratiques pour assurer la conformité aux exigences de sécurité ;
9. La traçabilité des opérations de traitement des données à caractère personnel doit être garantie ;
10. La protection de la vie privée dès la conception, Privacy by Design en anglais : les considérations de protection de la vie privée doivent être prises en compte dès la conception du produit ou du service amené à collecter, traiter ou utiliser des données à caractère personnel.

14.2.2 Exigences de sécurité pour la personne concernée

(La personne concernée : toute personne physique dont les données à caractère personnel font l'objet d'un traitement)

1. Le traitement des données personnelles doit se faire dans le cadre du respect de la dignité humaine, de la vie privée, des libertés publiques et ne doit pas porter atteinte aux droits des personnes, à leur honneur et à leur réputation ;
2. Donner à la personne concernée une information claire et complète concernant le traitement de leurs données personnelles ;
3. Leur permettre de lire et approuver toute politique (si elle existe) en relation avec le traitement de leurs données personnelles ;
4. Donner aux personnes concernées les moyens d'exercer leurs droits sur leurs données, et répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données ;

5. En cas de collecte de données en réseaux ouverts, la personne concernée doit être informée que les données à caractère personnel la concernant peuvent circuler sur les réseaux sans garanties de sécurité et qu'elles risquent d'être lues et utilisées par des tiers non autorisés.

14.2.3 Exigences de sécurité pour le responsable du traitement

(Le responsable du traitement : Personne physique ou morale, publique ou privée ou toute autre entité qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données.)

1. Des mesures techniques et organisationnelles appropriées doivent être appliquées afin d'empêcher l'accès, la destruction, l'utilisation, la modification et la divulgation non autorisées des données à caractère personnel, et ce, en fonction du volume et de la sensibilité des données, et de la taille et de la complexité de l'organisme et du coût des outils disponibles ;
2. Lorsque le traitement des données à caractère personnel sur les réseaux de communications électroniques ouverts au public, entraîne la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à ces données, le fournisseur de services avertit, sans délai, l'autorité concerné et la personne concernée lorsque cette violation peut porter atteinte à sa vie privée ;
3. Ne collecter que les données nécessaires ;
4. Le responsable du traitement doit tenir à jour un inventaire des violations de données à caractère personnel et des mesures prises pour y remédier ;
5. Les informations personnelles identifiables doivent être détruites d'une manière sécurisée conformément aux normes et procédures d'élimination des données.

14.2.4 Exigences de sécurité pour les tierces parties

(Tierces Parties : toute personne physique ou morale, publique ou privée ou toute autre entité autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données.).

1. Les tierces parties concernées par la collecte et le traitement des données personnelles doivent déployer des mesures appropriées pour assurer la sécurité des données et des systèmes, et pour protéger les données personnelles contre la perte, l'accès non autorisé, la destruction, l'utilisation, la modification ou la divulgation ;
2. Les données à caractère personnel objet du traitement ne peuvent être communiquées à un tiers que pour la réalisation de fins directement liées aux fonctions du responsable du traitement et du destinataire et sous réserve du consentement préalable de la personne concernée. Toutefois, ledit consentement n'est pas exigé si le traitement est nécessaire ;

3. Chaque fournisseur de services tient à jour un inventaire des violations de données à caractère personnel et des mesures prises pour y remédier ;
4. L'échange de données entre les administrations/secteurs publics est régi par les mêmes mesures appliquées pour les tierces parties.

14.2.5 Exigences de sécurité concernant le transfert de données vers un pays étranger

1. L'organisme doit identifier des données à caractère personnel qui feront l'objet de transfert vers un pays étranger ;
2. Les données à caractère personnel ne peuvent être transférées vers un pays étranger, que sur autorisation de l'autorité concerné, conformément aux dispositions de la loi en vigueur, et que si ce pays assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet ;
3. Mettre en place les mesures de contrôle et de supervision lors de l'envoi de données sensibles à l'étranger.
4. Il est interdit, dans tous les cas, de communiquer ou de transférer des données à caractère personnel vers un pays étranger, lorsque ce transfert est susceptible de porter atteinte à la sécurité publique ou aux intérêts vitaux du pays.

14.3 DOMAINE 3 - Gestion et contrôle des accès

14.3.1 Gestion et contrôle des accès.

Objectif : Veiller à ce que seules les personnes autorisées ont accès aux informations et aux systèmes d'information de l'organisme.

14.3.1.1 Politique de contrôle d'accès

Pour limiter l'accès à l'information et aux moyens de traitement de l'information en fonction des habilitations, il est nécessaire :

1. D'établir, de documenter et de tenir à jour une politique de contrôle d'accès sur la base des exigences métier et de sécurité de l'information ;
2. L'organisme détermine les règles de contrôle d'accès, des droits d'accès et des restrictions d'accès appropriés aux fonctions spécifiques de l'utilisateur de ces actifs conformément à la politique de sécurité approuvée ;
3. Les contrôles d'accès sont à la fois logiques et physiques et il convient de les envisager conjointement suivant l'approche de défense en profondeur (Anglais : Defence in Depth) ;
4. La politique de contrôle d'accès doit tenir compte des impératifs suivants :
    - Les exigences en matière de sécurité des applications métier ;
    - La cohérence entre la politique des droits d'accès et la politique de classification de l'information ;
    - Le respect de la législation et les obligations contractuelles applicables, relatives à la limitation de l'accès aux données ou aux services ;
    - L'identification et l'authentification des utilisateurs en appliquant la gestion de l'inscription et désinscription des utilisateurs et la gestion des mots de passe ;
    - La gestion des autorisations des utilisateurs en appliquant les principes de : besoin de savoir (anglais : need to know), moindre privilège et séparation des tâches (anglais : Segregation of Duties),
    - La gestion des accès à haut privilège ;
    - La revue régulière des droits d'accès ;
    - L'archivage des enregistrements de tous les événements significatifs relatifs à l'utilisation et à la gestion des identités des utilisateurs.

14.3.1.2 Gestion des accès utilisateurs.

Pour maîtriser l'accès utilisateur par le biais des autorisations et empêcher les accès non autorisés aux informations et aux systèmes d'information, il est nécessaire de mettre en œuvre un processus formel de gestion des accès utilisateur pour attribuer ou révoquer des droits d'accès à tous les types d'utilisateurs, de tous les systèmes et de tous les services d'information.

1. La procédure de gestion des identifiants utilisateur doit inclure :
    - L'obligation d'attribuer à chaque utilisateur un identifiant qui lui est propre ;
    - Les identifiants doivent permettre de relier chaque action effectuée sur le système à un utilisateur unique ;
    - L'utilisation des identifiants communs (anglais : generic accounts) peut être autorisée à titre exceptionnel lorsque les aspects opérationnels liés à l'activité de l'organisme l'exigent ;
    - Les mots de passe doivent respecter la politique de mot de passe arrêtée par l'organisme ;
    - La revue régulière des identifiants des utilisateurs (identifiants nominatifs et identifiants communs). Cette revue concerne les utilisateurs qui sont administrateurs sur les systèmes de l'organisme et les utilisateurs des applications métier ;
    - L'obligation de suppression ou de blocage immédiat des identifiants des utilisateurs qui ont quitté l'organisme d'une façon temporaire ou définitive.

2. Le processus de gestion des accès utilisateur doit inclure :
    - Une procédure formelle de la gestion des accès utilisateur permettant la maitrise des opérations d'attribution ou de révocation des droits d'accès aux systèmes et aux services d'information ;
    - La séparation de tâches pour le contrôle d'accès, par exemple la demande d'accès, l'autorisation d'accès et l'administration des accès ;
    - La vérification que les droits d'accès accordés sont adaptés à la politique d'accès, et qu'ils sont cohérents avec les autres exigences telles que la séparation des rôles ;
    - L'adaptation des droits d'accès des utilisateurs qui ont changés de fonction ou de poste ;
    - La tenue à jour d'un enregistrement centralisé de tous les droits d'accès accordés aux identifiants utilisateurs ;
    - La revue régulière des droits d'accès des systèmes ou des services d'information.

14.3.1.3 Gestion des contrôles d'accès aux réseaux de l'organisme

Pour que les utilisateurs ne puissent avoir accès qu'aux ressources réseau pour lesquels ils ont reçu une autorisation formelle, il est nécessaire de définir une politique relative à l'utilisation des réseaux et des services y afférents, cette politique de gestion des contrôles d'accès au réseau doit définir :

1. Un descriptif des ressources réseaux existantes ;
2. Les moyens utilisés pour accéder aux réseaux ;
3. Les exigences d'authentification de l'utilisateur pour l'accès aux différentes ressources réseaux ;
4. Les procédures d'autorisation désignant les personnes autorisées à accéder aux ressources réseaux ;
5. Les procédures et mesures de gestion destinées à protéger l'accès aux ressources réseaux.

14.3.2 Gestion des comptes à privilèges

Objectif : L'organisme doit mettre en place les mesures nécessaires pour restreindre et contrôler l'attribution et l'utilisation des privilèges élevés d'accès.

14.3.2.1 Identification des comptes à privilèges :

- Le processus d'approvisionnement des privilèges (octroi, suppression, élévation des privilèges, etc.) doit être documenté conformément aux exigences de la politique de contrôle d'accès de l'organisme ;
- L'accès aux informations et systèmes d'information de l'organisme doit se faire en respectant le principe du moindre privilège (anglais : least privilege) ;
- Les personnes qui auront besoin d'accès aux ressources de l'organisme avec privilèges doivent avoir les autorisations nécessaires (cas des administrateurs) ;
- Maintenir une liste/enregistrements à jour des comptes avec privilèges.

14.3.2.2 Détection des comptes à privilèges :

Conduire à intervalle régulier des scans sur l'infrastructure et les systèmes d'information de l'organisme pour identifier les comptes avec privilèges à tous les niveaux (réseau, système, application, base de données).

14.3.2.3 Protection des comptes à privilèges :

- Limiter l'utilisation des comptes avec privilèges uniquement à des tâches administratives et d'une manière temporaire ;

- S'assurer que les activités liées aux accès avec privilèges sont enregistrées dans des journaux d'évènements ;
- Utiliser les différentes méthodes d'authentification forte lors des accès avec des comptes avec privilèges (exemple : authentification à deux facteurs) ;
- Les accès avec privilèges doivent se faire via des identifiants utilisateurs différents des identifiants utilisateurs employés pour les tâches ordinaires (Exemples : accès aux applications bureautiques, messagerie, accès à l'internet) ;
- Sensibiliser les utilisateurs sur les risques liés aux accès avec privilèges.

14.3.2.4 Supervision des comptes à privilèges :

- Superviser régulièrement les comptes à privilèges.

14.3.3 Gestion des informations secrètes d'authentification

Objectif : Rendre les utilisateurs responsables de l'utilisation et la protection de leurs informations secrètes d'authentification.

1. Pour préserver la confidentialité de l'authentification secrète, une politique pourla définition, l'utilisation et la transmission des informations secrètes d'authentification (mot de passe, code PIN…) doit être établie ;
2. Préserver la confidentialité des informations secrètes d'authentification pour les identifiants génériques d'administration partagés en ce qui concerne les identifiants génériques d'administration ;
3. Procéder au changement des informations secrètes d'authentification par défaut définies par les constructeurs et éditeurs après installation des systèmes ou logiciels ;
4. Les utilisateurs doivent changer régulièrement leurs mots de passe suivant la politique de gestion des mots de passe de l'organisme ;
5. Les utilisateurs doivent être sensibilisés sur les risques liés à la mauvaise manipulation des informations secrètes d'authentification, et sont tenus d'appliquer les mesures et pratiques de cette politique.

14.3.4 Gestion des Accès à distance (anglais : Remote Access)

Objectif : S'assurer que les contrôles adéquats sont en place pour maitriser les risques liés à tout type d'accès distant (employés, fournisseurs, consultants, etc.) en dehors du périmètre de sécurité.

Une politique des accès à distance est à implémenter pour prendre en charge les risques supplémentaires que pose l'accès aux ressources internes en dehors du périmètre de sécurité de l'organisme ainsi que les conditions et les restrictions d'utilisation.

14.4 DOMAINE 4 - Sécurité des appareils mobiles

Sécurité des appareils mobiles.

Objectif : Établir les règles et les lignes directrices pour une utilisation sécurisée des appareils mobiles (ordinateurs portables ou LAPTOP, tablettes, téléphones mobiles, cartes à puces, etc.).

14.4.1 Politique ou procédure d'utilisation des appareils mobiles :

1. Une politique et procédures relatives à l'utilisation et à la gestion sécurisée des appareils mobiles doivent être définies et revues périodiquement.

   Cette politique doit prendre en charge :

   - La protection physique ;
   - Les contrôles d'accès ;
   - Les techniques cryptographiques ;
   - Les sauvegardes et effacement des données (anglais : data wipe) ;
   - La protection antivirus.

2. Cette politique doit également inclure des règles et des conseils sur la connexion des appareils mobiles aux réseaux de l'organisme et des conseils sur l'utilisation de ces appareils dans des lieux publics ;

3. Cette politique doit tenir en compte de l'utilisation des appareils personnels dans le périmètre de sécurité de l'organisme et les risques y afférents (Anglais : Bring Your Own Device - BYOD) ;

4. Les employés doivent être sensibilisés sur les meilleures pratiques et mesures de sécurité et sur les risques relatifs à l'utilisation des appareils mobiles.

14.4.2 L'inventaire des appareils mobiles :

1. L'organisme doit identifier par des outils manuels ou automatiques tous les appareils mobiles qui sont utilisés par les employés et les tierces parties pour maitriser les risques liés à leur utilisation ;
2. L'organisme doit gérer et mettre à jour un inventaire détaillé de tous les appareils mobiles qui accèdent aux ressources de l'organisme.

14.4.3 Exigences pour un usage sécurisé des appareils mobiles :

1. Identifier le niveau de protection nécessaire des appareils mobiles selon le niveau de classification des informations stockées et traitées ;
2. Approuver chaque connexion d'un appareil mobile au réseau interne selon la politique d'utilisation des appareils mobiles ;
3. Prendre des précautions particulières lors d'utilisation des appareils mobiles pour que les données ne soient pas compromises. La politique de contrôle d'accès doit

prendre en compte les risques liés à l'usage des équipements mobiles dans des environnements non protégés (cas de réseaux publics) ;

4. Utiliser, dans la mesure de possible, des techniques cryptographiques pour protéger la confidentialité et l'intégrité des données sur les appareils mobiles suivant la politique de cryptographie de l'organisme ;
5. Protéger l'accès aux appareils mobiles par des mécanismes d'authentification forts (Mots de passe complexes, codes de sécurité, empreintes digitales, reconnaissance faciale, etc.) ;
6. Appliquer les dernières mises à jour stables du système d'exploitation et/ou matériel (Micrologiciel ou firmware) suivant la politique de l'organisme ;
7. Il est recommandé d'échanger les documents classifiés de l'organisme via des serveurs de fichiers sécurisés, ou par messagerie électronique de l'organisme ;
8. Configurer un mécanisme de suppression des données après un nombre déterminé de tentatives d'accès échoués sur les appareils mobiles qui contiennent des informations sensibles et classifiées.

14.4.4 Mesures à suivre pour maitriser les risques liés au vol ou perte des appareils mobiles :

1. Porter les appareils mobiles comme bagage à main lors des voyages ;
2. Activer dans la mesure du possible un mécanisme de localisation des appareils pour faciliter leur localisation en cas de perte ou vol ;
3. Utiliser des technologies d'effacement à distance pour désactiver et supprimer les données dans le cas de perte ou vol des appareils mobiles ;
4. Utiliser des mesures de blocage à distance des appareils mobiles en cas de perte ou de vol ;
5. Dans le cas de perte ou vol de tout appareil mobile contenant des données métier :
    - Signaler immédiatement le vol ou la perte aux services de sécurité de l'organisme et autorités concernées, selon la politique de l'organisme ;
    - Ouvrir un incident de sécurité et le documenter conformément à la procédure de gestion des incidents de sécurité.

14.4.5 Mesures de sécurité liées à l'accès aux systèmes de messagerie à partir des appareils mobiles.

Dans le cas d'accès à la messagerie de l'organisme, les contrôles suivants doivent être envisagés :

1. **Contrôle technique** : Les paramètres du serveur de messagerie doivent être configurés pour empêcher les employés de configurer le client de messagerie officiel sur un smartphone qui ne figure pas dans l'inventaire des appareils mobiles. L'accès doit se faire via des mécanismes sécurisés ;

2. **Contrôle procédural :** Les employés doivent obtenir l'approbation du responsable pour la synchronisation de leurs emails sur un appareil mobile (Téléphone mobile, tablette) ;
3. **Contrôle Administratif :** La charte informatique doit contenir une clause de réception des emails professionnels sur les appareils mobiles. Les employés doivent respecter les conditions d'utilisation ;
4. **Sensibilisation :** Les employés doivent être informés et sensibilisés sur les meilleures pratiques et mesures de sécurité relatives à l'utilisation des emails professionnels sur des appareils mobiles.

14.4.6 Fin de vie des appareils mobiles (anglais : device disposal) :

1. L'organisme doit procéder à un effacement total des données de l'appareil mobile (anglais : data wipe) suivant la politique en vigueur, et cela lors de chaque changement de propriétaire ou dans le cas de fin d'usage (vente, don, ou envoi pour recyclage) ;
2. Procéder à la destruction physique de l'appareil mobile en utilisant les outils appropriés et certifiés.

14.4.7 Sauvegardes externes des données :

1. L'organisme doit évaluer les risques liés à la possibilité que les données stockées dans les appareils mobiles (données personnelles ou métier) soient sauvegardées dans le Cloud, ou dans des supports de stockage externe tels que les disques amovibles.

14.5 DOMAINE 5 - Sécurité des réseaux

14.5.1 Gestion de la sécurité des réseaux

Objectif : Protéger l'information et les systèmes d'information sur le réseau contre les risques qui peuvent impacter les objectifs de sécurité de l'organisme.

14.5.1.1 Gestion des réseaux.

L'organisme doit mettre en place une politique et procédures associées qui doivent prendre en charge les mécanismes de conception et de gestion sécurisées de l'infrastructure réseau, notamment :

1. Les définitions des tâches / rôles / responsabilités des acteurs impliqués dans la gestion et la configuration des ressources réseau de l'organisme ;
2. La définition des règles de conception d'une architecture réseau qui garantissent les performances et la sécurité des systèmes, des utilisateurs et des transactions ;
3. Le maintien à jour de la documentation du réseau qui inclue au minimum :
   - Un diagramme déterminant la topologie du réseau, les équipements réseaux, et toutes les connexions autorisées ;
   - Un diagramme logique qui détaille les services et les serveurs critiques ;
   - La configuration de tous les équipements réseaux.
4. La gestion de la sécurité physique et logique des équipements réseaux :
   - Gestion des accès physiques ;
   - Gestion des accès logiques par des mécanismes d'authentification (administrateurs et équipements réseaux), d'autorisation et de traçabilité lors de l'administration des périphériques réseau ;
   - Durcissement de la configuration des équipements ;
   - Gestion des correctifs et des configurations ;
5. Assurer que les systèmes, les processus, et les utilisateurs n'ont accès qu'aux ressources réseau nécessaires à l'exécution de leurs tâches ;
6. Conduire à intervalle régulier des tests de vérification afin de s'assurer que les mesures de sécurité sont conformes à la politique de sécurité de l'organisme :
   - Vérification de la configuration des équipements réseaux ;
   - Tests d'intrusions ;
   - Des audits de conformité.
7. Assurer la journalisation (Logs) et la surveillance centralisée des équipements et trafic réseaux ;

8. Gérer les changements de la topologie du réseau et des équipements réseaux (Etude et validation) ;
9. Prendre en charge la sécurité des réseaux sans fil de l'organisme.

14.5.1.2 Conception du réseau

1. Architecture du réseau :
   - L'organisme doit élaborer, appliquer et maintenir une architecture réseau qui permet de faire face aux besoins toujours grandissant en capacité et en sécurité ;
   - L'architecture doit prendre en considération le model de défense multicouches;
   - Les mécanismes de sécurité des équipements réseaux doivent être intégrés et exploités afin de : prévenir/ralentir/contenir et détecter les attaques réseaux.
2. Segmentation du réseau :
   - Une politique de segmentation du réseau doit être établie pour cloisonner les différents groupes de services, d'informations et d'utilisateurs, et aussi pour réduire les surfaces d'attaques ;
   - Le cloisonnement peut être physique ou logique ;
3. L'organisme doit élaborer, appliquer et maintenir une stratégie de détection et de prévention d'intrusion.

14.5.2 Transmission des données qui transitent dans le réseau.

Objectif : Protéger les données qui transitent dans le réseau afin de garantir leur intégrité et leur confidentialité.

14.5.2.1 Contrôle de la distribution et transmission des données

1. Les organismes doivent gérer l'échange de données électroniques afin de s'assurer que les exigences de sécurité (confidentialité, intégrité, etc.) relatives au niveau de classification sont maintenues durant le processus de transfert ;
2. Les organismes doivent mettre en œuvre les contrôles et les procédures techniques permettant de garantir que les données et les informations ne peuvent être échangées qu'après autorisation ;
3. L'utilisation de protocoles sécurisés doit être privilégiée lors de la transmission des données.

14.5.2.2 Contrôle des Transactions en ligne

1. Lorsque les organismes acceptent ou initient des transactions en ligne, ils doivent mettre en œuvre des contrôles, et vérifier que les contrôles existent pour :
   - Valider l'identité des parties impliquées dans la transaction ;
   - Si nécessaire, obtenir l'approbation appropriée pour la transaction ;
   - Protéger les données confidentielles utilisées lors de la transaction ;
   - Assurer l'intégrité de la transaction ;
   - Obtenir la preuve que la transaction s'est achevée correctement ;
   - Empêcher la relecture non autorisée ou accidentelle d'une transaction, de sorte qu'elle ne puisse être reproduite.
2. Les méthodes pour mettre en œuvre les contrôles ci-dessus dépendent de la nature de la transaction et du niveau du risque identifié. Elles peuvent inclure sans s'y limiter:
   - L'utilisation des signatures électroniques issues d'un tiers de confiance où d'un prestataire de services de signature électronique conformément à la législation et la réglementation en vigueur ;
   - L'utilisation des techniques d'authentification forte, telle que l'authentification multi-facteurs ;
   - Chiffrement des données échangées par le biais de protocoles sécurisés ;
   - Journalisation des transactions dans un lieu sécurisé.

14.5.3 Messagerie et Communication sur Internet

Objectif : Protéger de manière appropriée l'information transitant par la messagerie électronique, et mettre en place les mesures nécessaires pour maintenir la sécurité du système de messagerie de l'organisme à un niveau acceptable.

14.5.3.1 Responsabilités de l'utilisateur

1. L'organisme doit mettre en place une politique d'utilisation appropriée et sécurisée de l'Internet et de la messagerie électronique ;
2. L'utilisateur doit être sensibilisé sur cette politique et de ses responsabilités.

14.5.3.2 Filtrage des contenus inappropriés et/ou Dangereux Provenant d'Internet.

L'organisme doit mettre en place un dispositif permettant de :

1. Contrôler et sécuriser la navigation Internet et l'échange d'information sur internet ;
2. Filtrer les contenus inappropriés et/ou dangereux provenant d'Internet ;
3. Contrôler et sécuriser son système de messagerie électronique.

14.5.4 Sécurisation des communications

Objectif : Sécuriser les communications à caractère confidentiel.

1. La transmission des informations confidentielles par un canal de communication non sécurisé doit être strictement interdite ;
2. Lors des échanges de données confidentielles par voix sur IP, les mesures de sécurité appropriées doivent être mises en place ;
3. L'échange de données confidentielles de l'organisme sur les plateformes de voix sur IP, hébergées en dehors du territoire national, est interdit ;
4. Toutes les données confidentielles de l'organisme doivent être chiffrées lors de la transmission à travers les réseaux sans fil ou publics.

14.5.5 Mesures de sécurité à respecter en cas de déplacement à l'étranger.

Objectif : Prémunir les missionnaires contre les risques de sécurité encourus lors des déplacements à l'étranger.

1. Supprimer toutes les données professionnelles sensibles, non nécessaires à la mission, de tous les terminaux et supports de stockage amovibles avant tout déplacement à l'étranger ;
2. Le missionnaire doit garder sur lui en permanence son terminal professionnel ainsi que les supports de stockage ;
3. Le missionnaire doit désactiver les fonctions de communication sans fil tel que le Wi-Fi et le Bluetooth des appareils mobiles lorsque celle-ci ne sont pas nécessaires ;
4. Il est interdit d'utiliser des terminaux (ordinateurs, tablettes...) publics ou partagés pour accéder au compte de messagerie professionnelle ou aux applications métier ;
5. Interdire formellement le transfert par un étranger de documents via des supports de stockage amovibles. Tout échange de document doit se faire exclusivement par courriel ;
6. Informer la hiérarchie et la représentation diplomatique algérienne en cas d'inspection ou de saisie des équipements informatiques par des autorités étrangères lors des missions à l'étranger ;
7. Exiger aux missionnaires de mentionner dans leurs comptes rendus la liste des objets connectés offerts lors de leur déplacement ;
8. Interdire l'utilisation des équipements offerts lors d'un déplacement à l'étranger à des fins professionnelles ;
9. Le missionnaire doit changer les mots de passe utilisés pendant la mission.

14.6 DOMAINE 6 - Sécurité des systèmes d'information

Sécurité des systèmes d'information.

Objectif : S'assurer que les exigences de sécurité sont établies et intégrées fonctionnellement dans les systèmes d'information tout au long de leur cycle de vie. C.à.d. lors de l'acquisition, le développement et la maintenance de ces derniers.

14.6.1 Gouvernance de la sécurité des systèmes d'information

Définir une politique pour la gestion de l'acquisition, la mise à jour et le développement des produits et services informatiques. Cette politique doit s'appliquer également au service de conseil et à la sous-traitance de projets informatiques ou d'activités connexes.

14.6.2 Acquisition, développement et maintenance des systèmes d'information :

1. Mesures à mettre en œuvre des exigences de sécurité :

- Les exigences de sécurité doivent être identifiées à l'aide de diverses méthodes, telles que les guides de bonnes pratiques et politiques, la modélisation des menaces et correction des vulnérabilités. Les résultats de l'identification des exigences doivent être documentés en fusionnant tous les points de vue de toutes les parties prenantes ;
- Assurer leur alignement avec les objectifs métiers de l'organisme ;
- Elles doivent être approuvées par le responsable métier approprié ou son équivalent ;
- Elles doivent être incluses dans l'énoncé des besoins métier et techniques ;
- Les exigences de sécurité doivent être incluses pour les nouveaux systèmes d'information ou les changements apportés aux systèmes d'information existants ;
- Tenir compte des prérequis de mesures de sécurité identifiés lors de l'analyse des risques ;
- Décrire la manière de vérification afin de s'assurer que les exigences de sécurité soient respectées ;
- Chaque nouvelle acquisition d'un système, un processus de test de sécurité formel doit être appliqué ;
- Lorsque les fonctionnalités de sécurité d'un produit ou d'une mise à jour proposée ne répondent pas aux exigences spécifiées, le risque introduit et les contrôles associés doivent être réexaminés avant l'achat du produit.

1. **Changements apportés aux logiciels et applications :** Lors de développement ou de mise à jour d'un système d'information l'organisme doit :
    - Développer une procédure de gestion des changements (code source, versions, Configuration, etc.) ;
    - Garder une trace de tous les changements ;
    - Conserver une copie de chaque version du logiciel en adoptant les procédures appropriées de vérification de l'intégrité ;
    - S'assurer que toutes les documentations pertinentes sont à jour ;
    - Assurer une planification adéquate pour effectuer la mise en œuvre des modifications au bon moment ;
    - Définir clairement qui est autorisé à approuver les changements apportés aux logiciels / applications ;
    - Les changements doivent être testés dans un environnement de test avant la mise en production ;
    - L'organisme doit assurer une revue technique des applications après les modifications du système d'exploitation soit par l'installation des correctifs soit par des changements de configuration ;
2. **Gestion des mises à jour des systèmes :** Un processus de gestion des mises à jour des systèmes doit être suivi, ceci afin d'assurer que :
    - Les correctifs et les mises à jour sont testés, approuvés et appliqués ;
    - Les versions des logiciels utilisés sont prises en charge (supportées) par le fournisseur ;
    - Hormis les correctifs fournis par le fournisseur, les logiciels métier ne doivent pas être modifiés sauf dans des circonstances particulières (par exemple, lorsque cela est nécessaire pour une activité critique).

14.6.3 Principes d'ingénierie de la sécurité des systèmes d'information

Les propriétaires des systèmes d'information doivent :

1. Veiller à ce que des procédures d'ingénierie de système d'information sécurisées basées sur les principes d'ingénierie de sécurité soient établies, documentées et appliquées ;
2. S'assurer que les principes d'ingénierie de la sécurité sont revus et mis à jour régulièrement.
3. Veiller à ce que la sécurité soit intégrée à toutes les couches de l'architecture : métier, applications, données et technologies ;

4. Assurer un équilibre entre le besoin de sécurité de l'information et le besoin d'accessibilité à l'information ;
5. Analyser les nouvelles technologies pour détecter les risques de sécurité et revoir la conception par rapport aux modèles d'attaque connus.

14.6.4 Sécurité des logiciels :

1. Contrôler l'installation de logiciels sur des systèmes opérationnels en implémentant les mesures suivantes :
    - Autoriser l'installation du logiciel seulement par les administrateurs autorisés ;
    - Empêcher l'installation des logiciels par les utilisateurs, à moins que leur rôle / besoin métier le justifie ;
    - Garder une copie originale de chaque logiciel installé, y compris les versions précédentes ;
    - Avoir un journal d'évènement de toutes les installations de logiciels ;
    - Établir les procédures de sauvegarde et de restauration, et les tester régulièrement.
2. Protection des données de test en implémentant les mesures suivantes :
    - Utiliser des échantillons de données pour tester les applications ;
    - Veiller à ce que les données de test ne contiennent pas des informations à caractère personnel. En cas de nécessité, appliquer les filtres adéquats ;
    - Limiter le transfert de données réelles de l'environnement de production vers l'environnement de test ;
    - Supprimer d'une manière sécurisée toutes les données de test immédiatement après la fin des tests ;
    - Garder une trace de toute copie / suppression de données de/entre l'environnement de production et l'environnement de test.
3. Protection du code source des applicatifs :
    - Définir une politique de contrôle d'accès au code source ;
    - Définir et réviser périodiquement les autorisations d'accès au code source ;
    - Utiliser des logiciels de gestion des versions ;
    - Maintenir un journal d'évènements de tous les accès.

14.6.5 Utilisation correcte des applications

Pour éviter les erreurs, la perte, les modifications non autorisées ou l'utilisation abusive d'informations dans les applications ; l'organisme doit :

1. Valider la saisie des données (Input data validation) dans les applications pour s'assurer que ces données sont correctes et appropriées ;
2. Incorporer des contrôles de validation dans les applications pour détecter toute corruption d'informations par le biais d'erreurs de traitement ou d'actes délibérés ;
3. Garantir l'authenticité et l'intégrité des messages dans les applications ;
4. Valider les données en sortie (data output validation) des applications.

14.6.6 Développement externalisé des logiciels

1. Le développement externalisé des logiciels doit être surveillé et contrôlé par l'organisme. Veuillez, vous référer à "La sécurité des tierces parties" pour plus de détails.
2. Quand le développement des logiciels est sous-traité, les points suivants doivent être considérés :
    - Définir une politique de codage sécurisé ;
    - Définir un processus d'assurance qualité (Quality Assurance) ;
    - Inclure dans le contrat d'acquisition de logiciel une clause obligeant les tierces parties à se conformer à la politique de codage sécurisé ;
    - Réviser le code source pour identifier les vulnérabilités potentielles et / ou le code malveillant ou le code non conforme aux fonctionnalités requises.

14.7 DOMAINE 7 - Sécurité liée à l'exploitation

Sécurité liée à l'exploitation
Objectif : Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.

14.7.1 Procédures d'exploitation documentées :

Les procédures d'exploitation du système d'information doivent être documentées et mises à disposition de tous les utilisateurs concernés. Parmi ces documents :

1. Installation et configuration des Software et Hardware ;
2. Les procédures de sauvegarde et de récupération (Backup/Recovery) ;
3. Plan de reprise après sinistre (Disaster Recovery Plan) ;
4. La procédure de supervision ;
5. Les procédures de test et de vérification.

14.7.2 Gestion des changements

Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sur les objectifs de la sécurité de l'information (confidentialité, intégrité et disponibilité) doivent être contrôlés. Il faut tenir compte des points suivants :

1. Le processus de gestion des changements doit être défini, approuvé et mis en œuvre ;
2. La mise en conformité avec le processus de gestion des changements doit être régulièrement supervisée ;
3. Les rôles et responsabilités relatifs à la gestion des changements doivent être clairement définis et approuvés ;
4. Les demandes de changements doivent être approuvées par toutes les parties prenantes et spécialement celles des fonctions métiers ;
5. Les exigences en matière de sécurité doivent être vérifiées pour chaque changement pour maitriser les risques qui peuvent surgir ;
6. La mise en place maîtrisée d'un processus de modification d'urgence permettant une mise en œuvre rapide et contrôlée des modifications nécessitées par la résolution d'un incident ;
7. La conservation d'un journal d'audit contenant toutes les informations pertinentes des changements effectués.

14.7.3 Dimensionnement

L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système. Les points suivants sont à considérer :

1. Identification des exigences de dimensionnement et besoins en capacité en tenant compte du caractère critique du système concerné pour l'organisme ;
2. Définition et mise en œuvre des mesures de détection pour détecter les problèmes en temps voulu ;
3. Surveillance et réglage des systèmes (anglais : tuning) pour améliorer leur disponibilité et leur efficacité ;
4. Identification et analyse des tendances et évolution d'utilisation des ressources clés, en particulier en ce qui concerne les applications métier ou les outils de gestion des systèmes d'information ;
5. Prévision des futurs besoins en matière de dimensionnement et exigences de capacité en tenant compte des nouvelles exigences métier et système ;
6. Création d'un plan documenté du dimensionnement (capacité et d'ajustement).

14.7.4 Séparation des environnements de développement, de test et d'exploitation

Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou des changements non autorisés dans l'environnement de production. Parmi les points à considérer :

1. Définir et de documenter les règles concernant le passage des logiciels du stade de développement au stade d'exploitation ;
2. Ne pas procéder à des tests sur des systèmes en production.
3. Ne pas copier de données sensibles dans l'environnement de test.

14.7.5 Protection contre les logiciels malveillants

Il convient de mettre en œuvre des mesures de détection, de prévention et de récupération, conjuguées à une sensibilisation des utilisateurs adaptée, pour se protéger contre les logiciels malveillants.

14.7.6 Sauvegarde des informations :

Établir une politique de sauvegarde destinée à définir les exigences de l'organisme en matière de sauvegarde de l'information et des systèmes d'information.

14.8 DOMAINE 8 - Sécurité des Systèmes d'Information Critiques

Sécurité des Systèmes d'Information Critiques.
Objectif : S'assurer que toutes les mesures de sécurité sont implémentées dans les systèmes critiques de l'organisme. Dans le cas de défaillance dans leur application, cela pourrait avoir des conséquences importantes pour la survie des organismes.

1. Le plan stratégique de sécurité (Schèma Directeur de la stratégie de la sécurité de l'information) doit tenir compte des systèmes critiques de l'organisme, de leur évolutivité en termes de capacité et des exigences de sécurité ;
2. Une cartographie détaillée des systèmes critiques doit être élaborée ;
3. La Direction de l'organisme doit approuver la cartographie des systèmes critiques et désigne les personnes en charge de leur gestion ;
4. Conduire régulièrement une évaluation des risques et des audits de conformité sur les actifs constituant les systèmes d'information critiques ;
5. Appliquer une vérification stricte des antécédents (anglais : screening/background check) sur les employés qui gèrent les systèmes critiques ;
6. Les personnes en charge des systèmes critiques doivent être hautement qualifiées ;
7. Les utilisateurs qui accèdent à ces systèmes doivent utiliser des méthodes d'authentification forte (2-facteurs, biométrie, etc.) ;
8. Un plan de contingence et de résilience doit être établi, documenté et testé régulièrement pour les systèmes identifiés comme critiques ;
9. Organiser régulièrement des cyber-exercices pour tester le degré de préparation et de réponse aux incidents cybernétiques. Le scénario de cet exercice est la simulation des cyber-incidents impactant les systèmes classifiés critiques ;
10. Conduire à intervalle régulier des tests d'intrusions (réseau et application) ;
11. Identifier et classifier les points de sortie des informations afin de minimiser les risques liés aux fuites d'informations (Anglais : Data Leak Prevention-DLP) ;
12. L'organisme doit disposer des moyens pour surveiller les flux échangés dans les systèmes d'information. Ces sondes analysent les flux de communication transitant sur le réseau pour rechercher les événements susceptibles d'affecter la sécurité des SIC ;
13. Dans les centres de données (data center), il est indispensable d'isoler physiquement l'infrastructure des systèmes critiques du reste des systèmes et appliquer de fortes mesures de sécurité physiques (par exemple : Rack avec empreinte digital ou carte à puce) ;
14. La localisation géographique des infrastructures des systèmes critiques de souveraineté doit être discrète dans la limite du possible ;

15. L’intervention des parties externes (fournisseurs, partenaires, consultants, etc.) sur ces systèmes critiques doit être strictement réglementée ;
16. Stockage des composants de rechange pour assurer le fonctionnement pendant les périodes de crise (rupture d’approvisionnement, Evènements hasardeux, fin de contrat avec fournisseur, etc.) ;
17. Utilisation de plusieurs fournisseurs pour l'approvisionnement en matière de composants critiques identifiés.

14.9 DOMAINE 9 - Sécurité des Services Cloud

Sécurité des Services Cloud
Objectif : Sécuriser les informations stockées, traitées et récupérées à travers les services cloud, et veiller à ce que les risques de cyber sécurité liés à ces services cloud sont maitrisés en respectant les obligations légales, réglementaires et contractuelles

14.9.1 Gouvernance liée à l'usage du cloud.

1. Une stratégie doit être définie pour le modèle de déploiement (Public, Privé, hybride) et le type de service (IaaS, PaaS et SaaS) et les données qui doivent être ou pas stockées ou traitées dans les services cloud, en fonction de leurs sensibilité et criticité ;
2. Si le service cloud concerne le traitement, le stockage et la manipulation des données à caractère personnel ; le système de traitement d'information et de stockage des données doit être hébergé dans le territoire national.

14.9.2 Exigences de sécurité pour le demandeur de services cloud :

1. Avant chaque demande de service cloud une analyse des risques doit être effectuée et des mesures de sécurité appropriées doivent être mise en œuvre pour la protection des données contre les attaques cybernétiques (anglais : cyber attacks), la fuite, la perte ou l'indisponibilité des données ;
2. Envisager des méthodes pour récupérer les données lors de la résiliation du contrat avec le fournisseur ;
3. L'utilisation des canaux de communication sécurisés entre les systèmes internes de l'organisme et les services cloud ;
4. Assurer que le fournisseur met en œuvre des mesures de sécurité pour la ségrégation des données et des accès dans un environnement multi-locataire ;
5. Un contrat doit être signé pour chaque service cloud, le contrat inclue, entre autres :
    - La disponibilité de données et fonctionnalités métier ;
    - La protection des données contre les accès non-autorisé ;
    - La gestion des incidents de sécurité ;
    - La propriété et le cycle de vie des données.
6. Comprendre et maintenir l'endroit où l'information soit stockée ou traitée avec les restrictions applicables dans l'environnement cloud ;

7. Assurer un plan de migration des données et des systèmes après la cessation de relation de service ;

8. Assurer que toutes les autres exigences de sécurité identifiées lors de l'analyse des risques sont incluses dans la prestation de service ;

9. Assurer, dans la mesure du possible, le droit de vérifier si les dispositifs de sécurité identifiés lors de l'analyse des risques sont implémentés ;

10. Des accords de niveau de services ou SLA (Service Level Agreement) doivent être signés avec le fournisseur de service cloud, pour chaque service hébergé, suivant la matrice de criticité du service fourni ;

14.9.3 Exigences de sécurité pour le fournisseur de services cloud :

1. Assurer que le fournisseur de services cloud dispose d'un cadre de gouvernance de la sécurité qui coordonne et dirige son approche globale de la gestion du service et des informations qu'il héberge ;

2. Fournir l'assurance qu'à la fin du contrat des services cloud, toutes les données du client sont renvoyées/transférées de manière sécurisée et supprimées de tous les systèmes d'information et les supports de stockage du fournisseur cloud ;

3. Assurer une séparation entre les différents clients des services cloud pour empêcher un consommateur malveillant d'affecter le service ou les données d'un autre client de services ;

4. Le fournisseur de services cloud doit mettre à la disposition de ses clients les outils nécessaires pour les aider à gérer leur service en toute sécurité.

14.10 DOMAINE 10 - Cryptographie

Cryptographie.

Objectif : S'assurer que la confidentialité et l'intégrité des données sensibles ou classifiées sont préservées à travers la mise en place des mesures adéquates de cryptographie en adéquation avec les politiques et procédures de sécurité de l'organisme, ainsi que les lois en vigueur (Algériennes ou internationales).

Les mesures cryptographiques peuvent également garantir :

- **L'authentification :** s'assurer qu'une personne ou une entité est bien ce qu'elle prétend être. Un système d'authentification robuste est essentiel pour protéger l'accès aux systèmes d'information de l'organisme, et
- **La non-répudiation :** permet d'apporter la preuve qu'un utilisateur a exécuté une action, telle que l'envoi d'un message, et l'empêchant ainsi de le nier.

14.10.1 Gouvernance :

1. Une politique générale d'utilisation des mesures cryptographiques et les procédures associées doit être développée, implémentée et mise à jour régulièrement pour fournir des niveaux de protection appropriés aux informations sensibles. Cette politique doit être établie en conformité avec la politique de sécurité générale de l'organisme ;

2. L'organisme doit conduire régulièrement des audits de conformité pour éviter les violations de la réglementation appliquée en Algérie et de toute exigence de sécurité (normes, standards et bonnes pratiques de sécurité) ;

3. Les contrôles cryptographiques doivent être déployés tout en garantissant le respect des exigences légales, réglementaires et contractuelles Algériennes en vigueur ;

4. Les mesures de sécurité cryptographiques doivent être appliquées sur les actifs de l'organisme en se basant sur le schéma global de la classification des données ainsi des résultats de l'appréciation des risques ;

5. Les exigences de sécurité pour les mesures cryptographiques doivent être revues périodiquement et approuvées par la Direction de l'organisme. Cela inclut entre autres :

    - L'approbation des solutions techniques cryptographiques ;
    - La gestion des clés cryptographiques ;
    - Le chiffrement des données sensibles ou classifiées stockées (at-rest) ou transférées (in-transit).

6. Dans le cas où les mesures cryptographiques ne peuvent être appliquées, l'organisme doit mettre en place des contrôles de sécurité compensatoires pour une meilleure maitrise des risques encourus ;

7. L'organisme doit adopter les algorithmes et les normes de cryptage qui ont été testés, approuvés, et qui ont atteint une maturité élevée afin de préserver les objectifs de sécurité de l'information de l'organisme ;

8. Les équipements et logiciels d'encryptions sont considérés comme des équipements sensibles de télécommunication ;

9. L'organisme doit tenir compte de l'impact du chiffrement des informations pour raison d'analyse du contenu (exemple : analyse des messages cryptés, détection de logiciels malveillants) ;

10. En cas d'échange d'informations avec des organismes étrangers hors du pays, l'organisme doit se conformer (si obligation il y'a) aux exigences liées au mesures cryptographiques du pays de l'organisme tiers ;

11. Les employés en charge de la gestion des services cryptographiques doivent disposer des habilitations nécessaires pour exercer dans des fonctions de ce type de postes ;

12. Les fournisseurs ou prestataires de services doivent se conformer aux exigences liées à l'usage des mesures cryptographiques de l'organisme découlant des règlements et des politiques de sécurité en vigueur.

14.10.2 L'autorité de certification de l'organisme :

1. L'autorité de certification électronique racine (1) de l'organisme doit être signée par l'autorité gouvernemental de certification électronique (AGCE) ou l'autorité économique de certification électronique (AECE) une fois fonctionnelles ;

2. L'autorité de certification électronique racine de l'organisme peut être signée par un prestataire (2) de services de certification électronique établi dans un pays étranger, à condition que ce dernier se conforme aux exigences de reconnaissance mutuelle conclue par l'AGCE ou l'AECE ;

3. L'organisme doit élaborer pour chacune de ses autorités de certification (racine et subalternes) une politique de certificats (3) qui détaille l'utilisation des mesures cryptographiques. La politique de certificats (CP) de l'autorité de certification électronique racine de l'organisme doit être approuvée par l'autorité de certification parente, à savoir l'AGCE ou l'AECE.

(1) Infrastructure à Clés Publiques ou PKI (Anglais : Public Key Infrastructure).
(2) Un prestataire de services de certification électronique qui délivre des certificats électroniques qualifiés au profit des intervenants dans la branche gouvernementale ou économique.
(3) Anglais : Certificat Policy (CP).

14.10.3 Protection des données au repos [4] :

Les données au repos sont les données qui sont stockées (sauvegardées ou archivées) dans des supports ou médias physiques tels que les disques dures, bandes magnétiques, disques amovibles, etc.

1. Fournir un niveau de protection élevé basé sur des mesures cryptographiques pour les données sensibles ou classifiées au repos en tenant comptes des résultats de l'appréciation des risques ;

2. Les mises en place des mesures cryptographiques pour les données au repos peuvent également être obligatoires pour les besoins de conformité aux exigences légales et réglementaires.

(4) Anglais: Data at Rest.

14.10.4 Protection des données en transit [5] :

Les données en transit sont les données qui sont transférées d'un endroit/système vers un autre via l'infrastructure réseau privé de l'organisme ou via l'infrastructure réseau publique (Internet).

1. Des mesures de sécurité cryptographique doivent être appliquées sur les données sensibles ou classifiées qui sont en transit ;

2. Lorsqu'aucune mesure de sécurité ne peut être appliquée à l'infrastructure réseau, par exemple lorsque des informations sont transmises sur une infrastructure réseau publique, le cryptage des données sensibles ou classifiées est le seul mécanisme permettant d'éviter que les informations ne soient compromises.

(5) Anglais : Data in-Transit.

14.10.5 Disponibilité des clés et données cryptées :

1. Des moyens doivent être mis en place pour la préservation et la restauration des informations cryptées classifiées ou sensibles pour le besoin d'une investigation ou suite à une indisponibilité ;
2. La mise en place des mesures procédurales et techniques est essentielle pour la préservation des clés de cryptages lors de la récupération des données ;
3. Dans la mesure du possible, les outils de produits cryptographiques doivent fournir un moyen de récupération des données permettant de tenir compte des circonstances dans lesquelles la clé de cryptage est indisponible en raison d'une perte, d'un dommage ou d'une défaillance ;
4. En cas ou les clés cryptographiques sont compromises (exemple : cas d'attaque) ; l'organisme doit informer les parties intéressées et les autorités concernées.

14.10.6 Gestion des clés cryptographiques (Key management)

Objectif : La sécurisation des informations par les mécanismes cryptographiques dépend directement de la force des clés, de l'efficacité des mécanismes et des protocoles associés aux clés et du niveau de protection des clés. Il convient à l'organisme de mettre en place les contrôles administratifs, techniques et physiques pour la protection des clés tout au long de leur cycle de vie.

Contrôles à considérer :

1. Une politique de gestion des clés cryptographiques détaillée ainsi que les procédures associées doivent être élaborées ;
2. Il convient que la politique comporte des exigences de gestion des clés cryptographiques couvrant l'ensemble de leur cycle de vie : génération, stockage, archivage, renouvellement, extraction, attribution, retrait ou révocation et destruction des clés, restauration des clés (Key Recovery) ;
3. Les clés cryptographiques (secrètes et privés) doivent être protégées contre les risques qui peuvent impacter leurs confidentialité, intégrité et disponibilité ;
4. Identifier les différentes opérations ou fonctions concernées par la gestion des clés cryptographiques durant leur cycle de vie dans le système d'information de l'organisme ;
5. Identifier et classifier les différents types de clés cryptographiques en fonction de leurs usages ainsi que le niveau de protection qu'ils assurent ;
6. Il convient de sélectionner les algorithmes de chiffrement, la longueur des clés et les pratiques d'utilisation conformément aux bonnes pratiques. Une gestion appropriée des clés exige des processus sécurisés de génération, de stockage, d'archivage, d'extraction, d'attribution, de retrait et de destruction.

14.10.7 Protection physique des clés de cryptage :

1. Afin de renforcer la protection des clés cryptographiques secrètes et privées, il est fortement recommandé de les protéger physiquement dans des Modules de Sécurité Physique (MSP) et spécifiques tel que les HSM (Hardware Security Module), ou d'autre dispositifs physiques (disques, cartes à puce, etc.) ;
2. Les modules de sécurité physique peuvent être dupliqués si nécessaire pour raison de continuité des services cryptographiques ;
3. Les modules de sécurité physique doivent être hébergés en Algérie ;
4. Les MSP doivent être hébergés dans des emplacements physiques avec le niveau de sécurité adéquat ;
5. L'accès logique aux HSM doit se faire via des mécanismes d'authentification forte ;
6. L'organisme doit effectuer régulièrement des audits de conformité sur les MSP ;
7. La destruction des MSP est régie par la politique interne de l'organisme et de la législation en vigueur.

14.11 DOMAINE 11 - Sécurité Physique

Sécurité Physique

Objectif : Protéger les employés, les informations, les équipements, et l'infrastructure de l'organisme contre les accès physiques non autorisés et les risques environnementaux afin de minimiser les risques d'intrusion, vol, destruction ou altération des ressources.

14.11.1 Gouvernance de la sécurité physique :

1. Une politique de sécurité physique et les procédures associées doivent être développées et approuvées.

14.11.2 Zones sécurisées

Objectif : Définir des périmètres de sécurité pour protéger les zones hébergeant les informations sensibles et systèmes/infrastructure critiques de l'organisme.

1. **Sécurité physique des systèmes :** Limiter l'accès aux centres de données (data center), serveurs, équipements réseaux, et infrastructure au personnel autorisé uniquement en appliquant les contrôles de sécurité physique appropriés ;
2. **Périmètre de sécurité physique** : Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones hébergeant des informations sensibles, systèmes critiques et les moyens de traitement de l'information ;
3. **Contrôles physiques des accès :** Les zones sécurisées doivent être protégées par des contrôles d'accès adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis ;
4. **Sécurisation des bureaux, des salles et des équipements :** Des mesures de sécurité physique aux bureaux, aux salles et aux équipements doivent être conçues et appliquées ;
5. **Protection contre les menaces extérieures et environnementales :** Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être conçues et appliquées ;
6. **Travail dans les zones sécurisées :** Des procédures pour le travail dans les zones sécurisées doivent être conçues et appliquées ;
7. **Zones de livraison et de chargement :** Les points d'accès tels que les zones de livraison, de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux doivent être contrôlés et, si possible, isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

14.11.3 Matériel

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

1. **Emplacement et protection du matériel :** Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibilités d'accès non autorisé ;
2. **Services généraux :** Les matériels doivent être protégés des coupures de courant et autres perturbations dues à une défaillance des services généraux (tels que l'électricité, les télécommunications, l'alimentation en eau, le gaz, l'évacuation des eaux usées, la ventilation, et la climatisation) ;
3. **Sécurité du câblage :** Les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information doivent être protégés contre toute interception ou tout dommage ;
4. **Maintenance du matériel :** Il convient d'entretenir le matériel correctement pour garantir sa disponibilité permanente et son intégrité ;
5. **Sortie des actifs :** Les matériels, les informations ou les logiciels des locaux de l'organisme ne doivent pas sortir sans autorisation préalable ;
6. **Sortie du matériel et des actifs hors des locaux de l'organisme :** Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site ;
7. **Matériel utilisateur laissé sans surveillance :** Les utilisateurs doivent s'assurer que les matériels non surveillés hors des locaux sont dotés d'une protection appropriée ;
8. **Mise au rebut ou recyclage du matériel :** Il convient de vérifier chacun des éléments du matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut ou sa réutilisation.

14.12 DOMAINE 12 - Internet des Objets - Internet Of Things (IoT)

14.12.1 Mesures de sécurité lors de l'acquisition d'un IoT

Lors de l'acquisition d'un IoT par un organisme, un ensemble d'exigences doivent être vérifiées:

1. Avoir toutes les autorisations (homologations) nécessaires auprès des autorités concernées pour l'acquisition et l'exploitation de l'IoT ;
2. S'assurer que l'IoT fonctionne avec la dernière version stable de son système d'exploitation et de son micrologiciels (anglais : firmware) ;
3. S'assurer que l'IoT ne contient pas de vulnérabilité ou défaut connu en exigeant la fourniture éventuelle d'un document de conformité avec les standards en vigueur ;
4. S'assurer que l'IoT peut recevoir des mises à jour logicielles régulières ;
5. S'assurer que l'IoT repose sur des composants logiciels ou micrologiciels capables d'accepter des mises à jour authentifiées et approuvées de manière appropriée par le constructeur ou le fournisseur ;
6. S'assurer que l'IoT n'inclut pas d'informations d'authentification fixes ou codées en dur utilisées pour l'administration à distance, la fourniture de mises à jour ou la communication ;
7. S'assurer que l'IoT utilise des protocoles et des technologies standards non obsolètes.

14.12.2 Mesures de sécurité lors du déploiement d'un IoT

L'IoT est considéré comme un actif de l'organisme, et de ce fait, l'organisme doit mettre en place les mesures de protection nécessaires pour maitriser les risques liés à son utilisation.

1. Changer la configuration par défaut de l'IoT ;
2. La mise en place des IoT sur réseau doit être dans une zone démilitarisé (DMZ) à part autant que possible ;
3. S'assurer de la protection physique des objets ;
4. Activer le cryptage si l'objet le permet ;
5. Changer le nom du compte par défaut ainsi que le mot de passe par un autre plus difficile à deviner ou casser conformément à la politique des pots de passes de l'organisme ;
6. Activer toutes les fonctionnalités de journalisation d'alertes ou de notification sur les événements de sécurité ;
7. Désactiver les services et protocoles inutiles.

14.13 DOMAINE 13 - Surveillance et Journalisation

Gestion de la Surveillance et de la Journalisation
Objectif : Enregistrer les activités des utilisateurs, les exceptions, les défaillances et les événements liés à la sécurité de l'information, générer des preuves et détecter les incidents de sécurité.
1. L'organisme doit définir et mettre en œuvre une politique et procédures de gestion et d'analyse des journaux ainsi que la surveillance des infrastructures et des systèmes d'information ; 2. L'organisme doit arrêter la liste des évènements et des activités qui doivent être créés, tenus à jour, vérifiés régulièrement et archivés ; 3. L'organisme doit mettre en place un système de gestion de la journalisation permettant notamment, d'enregistrer, maintenir et analyser périodiquement les événements liés à la sécurité de l'information, entre autres les activités des utilisateurs et des administrateurs ; 4. Les journaux d'évènements doivent être conservés durant une période préalablement définie afin de faciliter les opérations d'audit et d'investigations, et ce conformément à la législation et régulations en vigueur ; 5. L'organisme doit protéger la confidentialité et l'intégrité des journaux d'évènement et veiller à leur disponibilité ; 6. L'organisme doit veiller à ce que le système de journalisation ne soit accessible que par les personnes autorisées et que toute modification de ses paramètres soit subordonnée à l'autorisation de qui de droit ; 7. Les horloges de l'ensemble des systèmes de traitement de l'information concernés de l'organisme doivent être synchronisées automatiquement sur une source de référence temporelle unique.

14.14 DOMAINE 14 - Gestion des Incidents de sécurité

Gestion des Incidents de sécurité.

Objectif : Garantir que toutes les violations ou faiblesses de sécurité signalées sont traitées et que des contrôles d'atténuation sont mis en place pour empêcher leur réapparition.

14.14.1 Gouvernance de la gestion des incidents de sécurité :

1. L'organisme doit établir une politique et/ou procédures pour gérer la réponse aux incidents de sécurité de l'information ;
2. Cette politique doit inclure des procédures d'identification, de signalement, d'enregistrement, d'intervention et d'escalade des incidents afin de garantir une réaction rapide, efficace et ordonnée aux incidents de sécurité ;
3. La politique doit contenir une définition claire d'un incident ou un évènement de sécurité ;
4. Il convient de créer une équipe de réponse aux incidents de sécurité pour une meilleure prise en charge des incidents (anglais : CERT- Computer Emergency Response Team). Parmi les tâches du CERT :
    - Centralisation des demandes d'assistance à la suite des incidents de sécurité (attaques) sur les réseaux et les systèmes d'information : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;
    - Traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CERT, contribution à des études techniques spécifiques ;
    - Établissement et maintenance d'une base de données des vulnérabilités ;
    - Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences ;
    - Coordination éventuelle avec les autres organismes (hors du domaine d'action) : opérateurs et fournisseurs d'accès à Internet, CERT sectoriel et national.

14.14.2 Identification des Incidents :

1. L'organisme doit définir des lignes directrices pour aider les utilisateurs à identifier et signaler les incidents ;
2. Identifier les données pertinentes à collecter avant, pendant et après un incident de sécurité.

14.14.3 Déclaration des incidents :

Tous les utilisateurs des systèmes d'information, y compris les tiers, doivent signaler immédiatement toute atteinte à la sécurité, tentative de violation et toute faille de sécurité des systèmes d'information.

Identifier un point de contact central pour la déclaration des incidents de sécurité.

1. **Déclaration des incidents à l'entité responsable de la gestion des incidents dans l'organisme.**

    - Les utilisateurs doivent signaler les incidents de sécurité de l'information au service centralisé interne de gestion des incidents ;
    - Définir un prototype de déclaration des incidents en interne qui contient toutes les informations nécessaires pour assurer un suivi efficace ;
    - Toute déclaration d'incident reçu par l'autorité interne doit être traitée en tenant compte de la nature et de la gravité de l'incident ;
    - Toutes les données relatives à l'incident doivent être sécurisées et conservées correctement. Ces données peuvent être nécessaires à titre de preuve lors de l'enquête ;
    - Les incidents doivent être communiqués au CERT sectoriel et/ou national (s'ils existent).

2. **Déclaration des incidents aux autorités externes.**

    - Seul un responsable désigné doit être autorisé à signaler les incidents à des entités externes, en termes d'exigences légales et / ou réglementaires ;
    - Avant chaque déclaration aux autorités externes les facteurs ci-dessous doivent être considérés :
        - Exigences légales, statutaires et réglementaires imposant à l'organisme de signaler l'incident ;
        - L'impact potentiel de l'atteinte à l'image de marque de l'organisme ;
        - Valeur de l'information perdue.
    - Il peut être nécessaire de donner aux services d'autorité externe un accès aux communications interceptées, aux activités de surveillance et aux preuves. Une diligence raisonnable doit être exercée pour vérifier la bonne foi de la commande, les circonstances dans lesquelles la commande est émise et les implications juridiques. Cet accès, surveillance, interception ne seront autorisés qu'avec l'approbation de l'entité concernée dans l'organisme.

14.14.4 Enregistrement des incidents de sécurité de l'information

1. Chaque incident déclaré doit être enregistré avec un identifiant unique pour faciliter le suivi ;
2. Définir les prérequis d'un enregistrement d'incidents de sécurité de l'information ;
3. Conserver (enregistrer) et présenter les informations conformément aux dispositions légales relatives à la présentation de preuves auprès des juridictions compétentes ;
4. L'enregistrement des informations est nécessaire pour tous les incidents de sécurité en cours d'investigation ;
5. Les enregistrements doivent être conservés d'une manière sécurise et la période de rétention doit être définie selon les obligations légales et réglementaires.

14.14.5 Analyse et réponse aux incidents :

1. Les incidents doivent être évalués sur la base de la catégorie, d'impact et de la fréquence ;
2. Définir les ressources et les capacités requises pour le traitement de l'incident ;
3. La collecte des preuves peut nécessiter une visite sur site ou la prise de contact avec du personnel interne ou externe possédant l'expertise requise pour obtenir les informations requises ;
4. Effectuer des tests de capacité de réponse aux incidents de sécurité et comparer les résultats aux résultats attendus afin d'identifier les lacunes et les faiblesses à corriger.

14.14.6 Reprise d'activité après incidents de sécurité.

1. En fonction de la nature de l'incident et en fonction du plan d'action élaboré, l'ensemble du personnel et l'équipe de la sécurité de l'information doivent être contactés pour la reprise des activités ;
2. La récupération impliquera l'identification et l'élimination des causes de l'incident. Cela pourrait impliquer une série d'activités, notamment la mise en œuvre de contrôles de sécurité supplémentaires, l'installation de nouveaux correctifs, la restauration de sauvegardes et la reconfiguration de dispositifs de sécurité.

14.14.7 Prévention des incidents

1. Une fois la reprise des activités est terminée, une analyse détaillée doit être réalisée pour identifier les points forts et les points faibles de l'infrastructure et des processus existants ;
2. Des contrôles de sécurité supplémentaires (contrôles préventifs) doivent être envisagés pour éviter la récurrence de l'incident ;
3. Effectuer une évaluation de l'adéquation des contrôles de sécurité préventifs proposés / mis en œuvre. Si nécessaire, les politiques, normes, procédures et directives de sécurité doivent être révisées.

14.14.8 Collecte de preuves et enquêtes d'investigation (anglais : Forensic).

1. L'organisme doit identifier les exigences légales et réglementation applicables pour la collecte des preuves ;
2. Le service légal et les services de conformité doivent être consultés dans le cas où l'incident de sécurité implique la collecte des preuves. Les preuves incluent, des systèmes informatiques, des documents papier et des périphériques informatiques ;
3. En cas de preuves électroniques, l'organisme doit envisager de faire appel aux services d'un spécialiste d'enquête sur les fraudes et de règlement des litiges disposant d'une expertise adéquate en criminalistique informatique ;
4. L'organisme doit établir des procédures pour la collecte des preuves en prenant en compte :
    - Chaine de responsabilité (anglais : chain of custody) ;
    - L'intégrité de la preuve ;
    - Rôles et responsabilités du personnel impliqué ;
    - Les compétences du personnel ;
    - La documentation de la collecte des preuves.

14.15 DOMAINE 15 - Gestion de la continuité des activités

Gestion de la continuité des activités

Objectif : Assurer la continuité et la reprise des activités critiques et des systèmes d'information, et limiter l'impact d'un désastre sur les personnes, les processus et les infrastructures pour faire face aux menaces qui pèsent sur la continuité des opérations et des systèmes d'information.

14.15.1 Gouvernance de la gestion de la continuité des activités

1. Une politique et un plan de continuité des activités (PCA) doivent être établies ;
2. L'organisme doit élaborer et mettre en œuvre un plan de continuité et de reprise d'activité basé sur les scénarios de risques ;
3. La gestion des risques liés à la continuité des activités doit être alignée avec les politiques et procédures de gestion des risques de l'organisme ;
4. Le plan de continuité des activités doit définir des catégories de désastre en fonction de leurs gravités et localisation. Pour chaque catégorie, une structure spécifique de gestion de crise et de continuité doit être définie ;
5. Le plan doit identifier toutes les comités nécessaires pour une gestion efficace de la continuité et de la reprise des activités ;
6. Les rôles et responsabilités des parties prenantes doivent être clairement définis et communiqués ;
7. Le plan de continuité des activités doit inclure toutes les obligations légales et contractuelles à respecter en termes de continuité des activités et disponibilité de l'information ;
8. Le plan doit inclure des exigences en matière de la sécurité de l'information et des mesures de protection appropriées afin de garantir une reprise des activités avec un niveau de sécurité acceptable ;
9. Ajouter des clauses contractuelles pour les services fournis par des tierces parties pour garantir une continuité des activités des services fournis en cas de désastre ;
10. Le plan de continuité des activités et de reprise après sinistre doit être mis en œuvre, testé et mis à jour périodiquement ;
11. Définir des indicateurs de performance afin d'assurer le suivi de mis en œuvre du plan.

14.15.2 Formation et sensibilisation du personnel :

1. Pour que le plan de continuité et de reprise des activités soit efficace, les parties prenantes et le personnel concerné doivent être formés au fonctionnement du plan et les processus opérationnels connexes.

14.15.3 Test du plan de continuité et de reprise des activités après sinistre :

1. Une procédure de test du plan de continuité et de reprise des activités après sinistre (Angais : DRP : Disaster Recovery Plan) doit être établie ;

2. Des exercices de test doivent être effectués périodiquement selon la procédure de test par les équipes chargées afin de vérifier la pertinence du plan. Cela permettra de se familiariser avec les procédures de reprise avant qu'un sinistre ne se produise ;

3. Une variété de techniques de tests doit être utilisée afin de garantir que le plan fonctionne tel que prévu ;

4. Définir des indicateurs de performance afin de tester l'efficacité des tests et du plan ;

5. Toutes les parties prenantes impliquées dans le plan de continuité et de reprise des activités doivent participer aux tests du plan ;

6. Tester les installations et les services des fournisseurs (garantissant que les produits et services fournis par des tiers respectent les engagements contractés).

14.15.4 Maintenance et mise à jour du plan de continuité et de reprise des activités

1. Le plan de reprise d'activités doit être conçu pour respecter le délai de reprise prévu et le niveau de disponibilité définit par le métier ;

2. Le plan de continuité et de reprise des activités doit être revu périodiquement ou suite à un changement majeur tel que :
    - Changement des stratégies ou objectifs métier ;
    - Changement des lois ;
    - Changement ou identification de nouveaux risques ;
    - Changement de l'organigramme de l'organisme ;
    - Changement des architectures systèmes ou réseaux ;
    - Changement et/ou migration des systèmes (exemple : cas d'un upgrade).
    - Changement de localisation des installations et ressources ;
    - Changement des fournisseurs ou clients clé.

3. Le plan doit être mis à jour selon les résultats des évaluations des tests de reprise ;

4. Les coordonnées des personnes fournies dans le plan de reprise doivent être vérifiées périodiquement pour s'assurer que les modifications sont apportées.

14.16 DOMAINE 16 - Ressources humaines

Ressources Humains.

Objectif : L'organisme devrait intégrer les exigences en matière de sécurité de l'information dans ses processus de gestion des ressources humaines, et veiller à ce que les parties prenantes soient conscientes des menaces de sécurité de l'information ainsi que leurs rôles et responsabilité avant, pendant et après le contrat de travail.

14.16.1 Gouvernance

1. Une politique et des procédures associées doivent être développées pour intégrer les exigences de sécurités dans les processus de gestion des ressources humaines avant, durant et après le contrat de travail ;
2. Établir un règlement intérieur, et s'assurer que les employés, fournisseurs ou tierces parties doivent accepter et signer le contrat de travail et le règlement intérieur ;
3. Définir clairement dans le contrat d'embauche et dans le règlement intérieur les rôles et responsabilités en termes de la sécurité de l'information ;
4. Surveiller, mesurer et évaluer périodiquement l'efficacité des processus de gestion des ressources humaines.
5. Établir et diffuser des chartes d'utilisation des ressources informatiques (voir annexe 2).

14.16.2 Mesures à considérer avant le recrutement de la ressource humaine

Chaque organisme doit effectuer des vérifications avant chaque recrutement pour les employés internes, tierces parties et fournisseurs de services pour pouvoir accéder ou manipuler les informations et les systèmes d'information de l'organisme.

Chaque organisme doit :

1. Définir une procédure pour la vérification des antécédents (références, l'historique de travail, casier judiciaire, certificats professionnels ou diplôme académiques, etc.). La procédure doit être alignée avec les prérequis métier et obligations légales et règlementaires, et doit définir les critères et les limitations de la vérification ;
2. Pour les recrutements à travers des partenaires tierces, exiger contractuellement la vérification des antécédents, et avoir la possibilité de vérifier les enregistrements de cette vérification d'une manière aléatoire dans le cas où cela s'avère nécessaire.

14.16.3 Confidentialité et accords de non divulgation :

Tous les employés (y compris les employés temporaires), les fournisseurs et les tierces parties doivent :

1. Lire et approuver la charte (ou politique) d'utilisation des ressources informatiques de l'organisme (voir annexe 2) ;
2. Signer un accord de confidentialité ou Accord de non divulgation (Anglais : Non-Disclosure Agreement / NDA) avant d'avoir un accès aux ressources de l'organisme.

14.16.4 Formation et sensibilisation sur les menaces cybernétiques :

1. Définir un plan de communication et un mécanisme de sensibilisation pour informer tous les employés, les fournisseurs et les tierces parties des politiques et procédures de sécurité de l'organisme auxquelles ils doivent se conformer ;
2. Mettre en place et exécuter régulièrement un programme de sensibilisation aux risques liés à l'usage des TIC et à la sécurité de l'information et aux menaces cybernétiques. Ce programme doit couvrir tous les employés de l'organisme ainsi que les utilisateurs des tierces parties ;
3. Maintenir et mettre à jour un registre des utilisateurs formés et sensibilisés à la sécurité de l'information ;
4. Tester et évaluer l'efficacité du programme de formation et sensibilisation pour identifier les points à améliorer.

14.16.5 Processus disciplinaire

1. Définir un processus disciplinaire formel pour les violations de la sécurité de l'information conformément aux exigences légales et réglementaires ;
2. Définir et communiquer d'une manière claire une liste illustrant les violations de la sécurité de l'information aux employés, fournisseurs et tierces parties.

14.16.6 Rupture, terme ou modification du contrat de travail

1. Les utilisateurs (salariés ou contractants) doivent restituer tous les actifs en leur possession à l'issue de la rupture, du terme ou de la modification du contrat de travail ;
2. Les droits d'accès des utilisateurs doivent être révoqués lors de la cessation de leur emploi, de leur engagement, de leur contrat.

14.17 DOMAINE 17 - Sécurité liée à l'usage des Réseaux Sociaux

Sécurité liée à l'usage des Réseaux Sociaux (Anglais : Social Media)

Objectif : L'organisme qui utilise les réseaux sociaux dans ses activités doit mettre les mesures de sécurité nécessaires à tous les niveaux (stratégique, tactiques et opérationnel) pour mieux maitriser les risques liés à l'usage des réseaux sociaux.

14.17.1 Mesures à suivre par les organismes qui possèdent des comptes métier dans les réseaux sociaux

1. Une politique d'usage des réseaux sociaux doit être établie et régulièrement revue pour être conforme aux lois et exigences en matière de régulation et de sécurité ;
2. La politique d'usage des réseaux sociaux doit être lue et approuvée par les parties prenantes (Utilisateurs finaux, administrateurs, etc.) ;
3. L'organisme doit évaluer quelles plateformes de réseaux sociaux, sont appropriées pour soutenir la stratégie globale et les objectifs de l'organisme ;
4. Les comptes réseaux sociaux de l'organisme doivent être identifiés et classifiés ;
5. S'assurer que seuls les utilisateurs autorisés ont accès aux comptes de réseaux sociaux de l'organisme, et que l'accès est immédiatement révoqué dès qu'il n'est plus requis ;
6. Faire des compagnes de sensibilisation sur les risques liés à l'usage des réseaux sociaux ;
7. L'organisme se réserve le droit de surveiller, interdire, restreindre, bloquer, supprimer ou de suspendre à ses employés l'accès à tout site de réseau social, à tout moment à sa seule discrétion si cela n'est pas conforme aux politiques et législation en vigueur ;
8. S'assurer que le plan de réponse aux incidents de sécurité (Anglais : Security Incident Response Plan) tien en compte les attaques des réseaux sociaux ;
9. Le contenu doit être revu régulièrement, et des contrôles de contenu doivent être implémentés afin de détecter les contenus inappropriés et qui peuvent aussi contenir du code malveillant ;
10. Mettre en place un mécanisme de prédiction, détection et de protection contre les bots (comptes réseaux sociaux autonomes et automatisés) qui sont utilisés par exemple pour influencer les opinions publiques sur un sujet particulier ;
11. Les activités des administrateurs qui gèrent les comptes des réseaux sociaux de l'organisme doivent être enregistrées conformément à la politique interne de l'organisme.

14.17.2 Sécurité du profil de l'organisme sur les réseaux sociaux

1. Le profil de l'organisme et le compte d'utilisateur sur les réseaux sociaux doivent être gérés par une équipe autorisée ;
2. Le profil de l'organisme sur les réseaux sociaux doit être créé qu'après l'approbation de l'autorité appropriée ;
3. La présence de profil de l'organisme sur les réseaux sociaux doit être autorisée que pour la promotion des produits et services de l'organisme ;
4. Pour l'approbation et le téléchargement du contenu, une procédure de gestion de contenu doit être référée ;
5. Il convient d'afficher un message d'avertissement sur les profils réseaux sociaux de l'organisme dans afin de sensibiliser les utilisateurs à ne pas partager d'informations personnelles et confidentielles.

14.17.3 Mesures à suivre par les organismes qui autorisent ses employés à accéder aux réseaux sociaux dans le milieu du travail :

1. Les employés autorisés à accéder aux réseaux sociaux dans le périmètre de sécurité de l'organisme doivent lire et approuver la politique d'usage sûre des réseaux sociaux de l'organisme ;
2. Ne pas divulguer d'informations personnelles sensibles, c'est-à-dire : adresse personnelle, informations financières, numéro de téléphone ;
3. Les postes de travail des utilisateurs qui accèdent aux réseaux sociaux doivent être surveillés et supervisés avec les outils adéquats ;
4. Les employés ayant des comptes personnels sur les réseaux sociaux ne doivent pas utiliser le même profil pour communiquer directement ou indirectement au nom de l'organisme ;
5. Les employés de l'organisme doivent assumés toutes responsabilités liées à la sécurité, à la confidentialité et les risques inhérents à l'envoi de contenu sur les réseaux sociaux ;
6. Les utilisateurs des réseaux sociaux doivent protégés leurs comptes avec les mécanismes d'authentifications fortes (2-factors, OTP, fingerprint, etc.).
7. Les employés ne doivent pas mettre dans leurs profils le détail de leur fonction, ni le nom de leur employeur, ni les équipements qui sont en train de gérer, et plus spécialement :
    - Ceux qui possèdent des privilèges élevés,
    - Ceux qui travaillent dans des systèmes critiques
    - Ceux qui travaillent dans des projets secrets d'État.

14.17.4 Pour les employés de l'organisme qui possèdent des comptes personnels dans les réseaux sociaux.

1. Les utilisateurs des réseaux sociaux doivent protéger leurs comptes personnels avec les mécanismes d'authentification fortes (2-factors, OTP, fingerprint, etc.) ;
2. Être conscient des dangers encourus lors de l'utilisation des réseaux sociaux tels que les risques liés au cyber-espionnage et crimes cybernétiques ;
3. S'assurer que les mesures de sécurité (mise à jour système et logiciel, antimalware, contrôles d'accès, etc.) sont en place sur les machines à partir desquels les employés accèdent aux réseaux sociaux ;
4. Ne pas utiliser des emails de l'organisme pour créer des comptes sur les réseaux sociaux ;
5. Les employés doivent utiliser des mots de passe différents de ceux utilisés pour accéder aux ressources de l'organisme ;
6. Se méfier des liens partagés ou des pièces jointes, notamment via des services de messagerie directe offerts dans les réseaux sociaux ;
7. Reporter tout incident de sécurité qui peut surgir à l'organisme.

14.18 DOMAINE 18 – Intégration de la sécurité durant le cycle de vie de développement des logiciels

Intégration de la sécurité durant le cycle de vie de développement des logiciels (anglais : Secure Software Development Life Cycle - SSDLC)
Objectif : Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut également des exigences pour le développement sécurisé.
Contrôles : 1. Un politique de développement sécurisé des applications doit être établie et revue régulièrement ; 2. L'attribution des rôles et des droits d'accès spécifiques, doit être limitée et l'utilisation de ces droits doit être contrôlée ; 3. La désignation d'une personne ayant le rôle « Propriétaire de l'application » qui aura la responsabilité du système développé (évolution, documentation, point de contact, ...) est indispensable ; 4. Lors de nouveaux développements ou d'extension du système d'information, les mesures de sécurité tant techniques qu'opérationnelles doivent être analysées, définies et formalisées ; 5. Dès le commencement de tout projet, il faut réaliser une analyse des risques encourus dans le cadre du traitement des informations compte tenu de leur catégorisation/classification ; 6. Lors de l'élaboration du planning, il est impératif de tenir compte du temps et des moyens nécessaires à l'implémentation des exigences de sécurité ; 7. Lors du développement des applications, une attention particulière doit être consacrée à l'intégrité des données, par la validation des données dès leur introduction, par la sécurisation du traitement interne et par la validation des données de sortie. La traçabilité auditée des données doit être intégrée ; 8. Le code source doit être conforme aux bonnes pratiques de codage (programmation structurée, code commenté, interdiction du codage en dur des mots de passe, etc.) ; 9. Lors du développement des applications, il doit être tenu compte des points faibles de sécurité inhérents aux langages de programmation. La vérification des logiciels par des tiers, autres que les développeurs, constitue une méthode pour réduire ces risques ; 10. Pendant le développement des applications, une gestion procédurale des versions du logiciel et la sécurisation des accès aux bibliothèques software doivent être appliquées ;

11. Des mesures maximales doivent être prises pour éviter que des canaux de communication secrets et des malwares ne se cachent dans les logiciels développés ;
12. Une séparation doit exister tant au niveau des environnements de développement, test, production, qu'au niveau des responsabilités au sein du projet le tout sous la supervision d'un seul et unique responsable : le chef de projet ;
13. Les données de test doivent être manipulées avec précaution de manière à éviter tout danger lié à leur confidentialité. Seules des données de tests spécialement prévues à des fins de développement, seront utilisées ;
14. Dans chaque phase de développement, une attention particulière doit être accordée aux mesures de protection appliquées au traitement des données manipulées en fonction de leur classification ;
15. Une attention particulière doit être accordée à la protection des données liées aux paramètres cryptographiques (clés, certificats, …) qui ne doivent jamais être enregistrées sous une forme non sécurisée ;
16. Les exigences relatives à la sécurisation des accès (identification, authentification et autorisation) doivent être définies et documentées avant d'entamer le développement. Le niveau de sécurisation des accès doit être adapté au degré de confidentialité des données traitées et aux menaces potentielles sur la base d'une analyse des risques. Ces accès, seront tracés et enregistrés ;
17. Tout accès aux données personnelles et confidentielles doit être enregistré. Les spécifications d'un projet détermineront comment l'accès, l'utilisation des systèmes et des applications doivent être enregistrés pour détecter toute violation aux règles de sécurité en vigueur ;
18. En cas de sous-traitance de l'activité de développement, il faut contractualiser les aspects de sécurités, les aspects de confidentialité et de continuité ;
19. Une communication efficace et constructive doit être établie entre les différentes parties concernées par le projet (équipes internes impliquées et fournisseurs inclus) afin de permettre de respecter les principes décrits dans le Référentiel National de Sécurité de l'Information ;
20. Si jugé nécessaire, l'application développée doit permettre d'effectuer les opérations de sauvegarde et de restauration, ceci comprend l'ensemble des informations traitées, et la documentation y relative (codes sources, programmes, documents techniques, etc.) ;
21. Tout au long de la vie du projet, une documentation (documentation technique, procédures, manuels, etc.) doit être développée et maintenue.

14.19 DOMAINE 19 - Exigences de Sécurité pour les projets de technologie de l'information (TIC)

Exigences de Sécurité pour les projets de technologie de l'information (TIC).
Objectif : S'assurer que les exigences en matière de sécurité de l'information sont prises en charge durant le cycle de vie des projets de l'organisme conformément à la politique de sécurité et aux exigences réglementaires et législatives en vigueur.

Contrôles :

1. La sécurité de l'information doit être considérée dans toutes les phases de la gestion des projets, quel que soit le type de projet concerné ;
2. Les exigences de sécurité de l'information doivent être :
    - Incluses dans la méthodologie et les procédures de gestion des projets et de gestion des changements pour garantir que les risques de sécurité sont identifiés et traités dans le cycle de vie technique du projet ou du changement ;
    - Intégrées dès les premières phases des projets. Les contrôles introduits durant la phase de conception sont nettement moins coûteux à mettre en œuvre et à maintenir que ceux inclus durant ou après la phase de réalisation ;
    - Établies clairement durant l'élaboration des cahiers de charges avant la phase de réalisation pour une meilleure maitrise des risques.
3. Les risques cybernétiques doivent être rajoutés dans le registre des risques du projet et doivent être suivis régulièrement ;
    - Les exigences en matière de sécurité pour la gestion de projet et les changements apportés aux actifs informationnels et techniques de l'organisme doivent couvrir au minimum les éléments suivants :
    - Évaluer et traiter les vulnérabilités ;
    - Procéder à un examen des paramètres de configuration, durcissement (Hardening en anglais), ainsi qu'à la mise à jour logicielle avant la phase de mise en production et lors des changements ;
    - Réviser périodiquement les exigences en matière de sécurité de l'information dans la gestion de projet.
4. Pour tous les projets, il convient de traiter et de revoir régulièrement les incidences sur la sécurité de l'information ;
5. Les rôles et responsabilités en matière de sécurité des informations doivent être identifiées et attribuées à des fonctions spécifiques définies dans les méthodes de gestion de projet.

14.20 DOMAINE 20 - Relation avec les tierces parties

Relation avec les tierces parties
Objectif : Définir les mesures à déployer par l'organisme lorsqu'il fait appel à un prestataire de services ; afin de s'assurer qu'ils ne représentent pas un élément de risque additionnel.

14.20.1 Gouvernance des contacts avec les prestataires de services (tierces parties, anglais : Third Parties) :

1. Établir et documenter les exigences de sécurité liées à l'accès des prestataires de services aux actifs de l'organisme pour une meilleure maitrise des risques. Ces exigences de sécurité peuvent être présentées dans une politique de contrats avec de tierces parties ;
2. Les cahiers des charges d'acquisition des solutions matérielles ou logicielles, doivent être en conformité avec le Référentiel National de Sécurité de l'Information.

14.20.2 Exigences de sécurité à appliquer par les organismes demandeurs de services :

1. Une évaluation des risques doit être effectuée pour identifier les exigences de sécurité, et mettre en place les contrôles appropriés avant d'accorder l'accès à une partie externe ;
2. Les exigences en matière de sécurité de l'information visant à atténuer les risques liés à l'accès aux actifs de l'organisme doivent être convenues avec le prestataire de services et documentées ;
3. L'organisme doit s'assurer que les partenaires respectent les objectifs de sécurité convenus, les politiques de sécurités, les normes et les procédures de sécurité adoptées, ainsi que la législation et réglementation en vigueur ;
4. Surveiller régulièrement les accès des tierces parties aux informations et aux systèmes d'information de l'organisme ;
5. Établir un plan de communication avec les tierces parties (fournisseurs, prestataires contractants, partenaires) en cas des incidents de sécurité (cyberattaques) ;
6. Limiter les informations partagées avec les fournisseurs ;
7. Pour les systèmes d'information critiques, contracter avec un ensemble diversifié de fournisseurs pour l'approvisionnement des produits software ou hardware ;
8. Les procédures de continuité du traitement en cas d'incapacité du fournisseur à fournir ses produits ou services doivent être prises en compte dans le contrat.
9. Il convient que le prestataire de service étranger doit avoir une représentation sur le territoire Algérien.

14.20.3 Exigences de sécurité à appliquer par les fournisseurs de services :

1. Une charte fournisseur doit être élaborée et signée par l'intervenant du prestataire avant chaque intervention sur site ou à distance ;
2. Le fournisseur s'engage vis-à-vis de la confidentialité des informations auxquelles son personnel peut avoir accès. Chaque personne concernée (intervenant sur site ou à distance) signe un accord individuel de confidentialité (Anglais : NDA ou Non Disclosure Agreement) ;
3. L'accès au système d'information de l'organisme de la part de personnels d'organismes extérieurs doit être limité et contrôlé conformément à la politique générale d'accès aux moyens informatiques de l'organisme ;
4. Le fournisseur doit sensibiliser les personnes autorisées sur les bonnes pratiques et la conformité aux exigences de sécurité de l'organisme demandeur de services ;
5. Le fournisseur de services doit conserver une visibilité sur les activités de sécurité telles que la gestion du changement, l'identification des vulnérabilités et les réponses aux incidents de sécurité des informations ;
6. Les modifications apportées à la fourniture de services et produits par les tierces parties, notamment les changements des politiques, procédures et contrôles existants en matière de sécurité de l'information, doivent être communiquées à l'organisme impacté.

Annexe 1
Les 20 Domaines de Sécurité dans le RNSI 2020

Codification des domaines :

Code du domaine		Domaines (Français)	Domains (Anglais)
1	AM	Gestion des actifs	Asset Management
2	PDP	Protection des données à caractère personnel.	Personal Data Protection.
3	ACM	Gestion et contrôle des accès.	Access Control Management
4	MDS	Sécurité des appareils mobiles	Mobile Devices Security
5	NTSEC	Sécurité des réseaux	Network Security
6	SYSEC	Sécurité des systèmes d'information	System Security
7	OPSEC	Sécurité liée à l'exploitation	Operation Security Controls
8	SCS	Sécurité des Système d'information critiques	Security of Critical Systems
9	CLDSEC	Sécurité des services cloud	Cloud Security
10	CRYPT	Cryptographie.	Cryptography
11	PHYSEC	Sécurité Physique	Physical Security
12	SECIOT	Internet des Objets	Internet Of Things (IoT)
13	LMO	Surveillance et Journalisation	Loggings and Monotoring
14	SECIM	Gestion des Incidents de sécurité	Security Incident Management
15	BCM	Gestion de la continuité des activités	Business Continuity Management
16	SECRH	Ressources humaines	Human Resources
17	SMSEC	Sécurité liée à l'usage des Réseaux Sociaux	Social Media Security
18	SSDLC	Intégration de la sécurité durant le cycle de vie de développement des logiciels	Secure Software Development life cycle (SSDLC)
19	SECPRJ	Exigences de Sécurité pour les projets de technologie de l'information	Security Requirements for IT Projects.
20	CTP	Relation avec les tierces parties.	Contact with Third Parties

Annexe 2 - Modèle de charte informatique

Charte de sécurité informatique

Préambule

L'organisme met à la disposition des utilisateurs des moyens informatiques afin de leur permettre d'accomplir les missions qui leurs sont assignées. Une mauvaise utilisation de ces moyens augmente les risques d'atteinte à la sécurité des systèmes d'information de l'organisme.

Dans le cadre de la mise en place du référentiel national de sécurité de l'information, il a été décidé d'élaborer une charte de sécurité informatique afin de garantir un seuil minimal de sécurité.

Article 1 : Objet

La présente charte a pour objet de définir les conditions et modalités d'utilisation des ressources informatiques de ***« l'organisme ».*** Elle définit également les règles de sécurité que les utilisateurs doivent respecter.

Article 2 : Champ d'application

La présente charte s'applique à toute personne ayant accès, de manière permanente ou temporaire, aux ressources informatiques de ***« l'organisme »***.

Article 3 : de la propriété des ressources informatiques

- Toutes les ressources informatiques mises à la disposition des utilisateurs sont la propriété exclusive de ***l'organisme*** ;
- Toutes les données hébergées dans les équipements de ***l'organisme*** ou transitant dans ses réseaux sont la propriété exclusive de ***l'organisme***.

Article 4 : Conditions d'accès aux ressources et au réseau informatique

Tout accès aux ressources et réseaux informatiques de ***l'organisme*** est soumis à une procédure d'authentification préalable.

Article 5 : responsabilité de l'utilisateur

L'utilisateur est seul responsable de toute utilisation des moyens d'authentification mis à sa disposition par ***l'organisme***

Article 6 : protection des moyens d'authentification

Afin de préserver les moyens d'authentification mis à sa disposition, l'utilisateur doit :

- Veiller à la protection et à la préservation de ses informations secrètes d'authentification ;
- Changer périodiquement ses informations secrètes d'authentification ;

Il est strictement interdit de communiquer ses informations secrètes d'authentification aux tiers.

Article 7 : Utilisation des ressources informatiques

- Les ressources informatiques de l'organisme ne peuvent être utilisées qu'à des fins professionnelles ;
- L'utilisateur doit préserver les ressources et les moyens informatiques mis à sa disposition ;
- L'utilisateur n'est pas autorisé à installer ou à déployer des applications ou des logiciels sur les moyens ou les ressources informatiques mis à sa disposition ;
- En cas de défaillance de ces moyens ou ressources, il doit informer immédiatement la structure en charge de la maintenance.

Article 8 : Obligations de l'organisme vers les utilisateurs

L'organisme doit :

- Mettre à disposition de l'utilisateur les ressources informatiques nécessaire à l'exécution des missions qui lui incombent ;
- Garantir le bon fonctionnement et la disponibilité des ressources informatiques ;
- Maintenir la qualité du service fourni aux utilisateurs dans la limite des moyens alloués ;
- Informer les utilisateurs des procédures et des politiques applicables en matière de ressources informatiques ;
- Mettre en œuvre les moyens nécessaires pour assurer la confidentialité et l'intégrité des documents et des échanges électroniques des utilisateurs ;
- Informer les utilisateurs que les activités sur le réseau et les systèmes font l'objet d'une surveillance automatisée ;
- Sensibiliser les utilisateurs sur les risques liés à la sécurité informatique.

Article 9 : Obligations de l'utilisateur

L'utilisateur doit :

- Respecter les lois et règlements en vigueur ;
- Respecter la présente charte ainsi que les différentes procédures et politiques de l'organisme ;
- Appliquer scrupuleusement les mesures et les directives de sécurité informatique de l'organisme ;
- Ne pas utiliser ou tenter d'utiliser les comptes d'autrui ;
- Signaler sans délai tout fonctionnement suspect ou incident de sécurité.

Article 10 : de la sécurité et de la protection du poste de travail

L'utilisateur doit respecter scrupuleusement les consignes de sécurité suivantes :

- Verrouiller l'accès au poste de travail en cas d'absence, même temporaire ;

- Alerter les services techniques en cas de découverte d'un nouvel équipement connecté au poste de travail ;
- S'assurer que son poste de travail dispose d'un antivirus, et informer le service concerné de toute alerte de sécurité ;
- Ne jamais connecter des équipements personnels au poste de travail ;
- Scanner tous les supports amovibles connectés au poste de travail avant de les utiliser ;
- Eteindre l'ordinateur pendant les périodes d'inactivité prolongée (nuit, weekend, vacances,) ;
- Ne pas intervenir physiquement sur le matériel (ouvrir les unités centrales, …).

Article 11 : de l'utilisation de la messagerie électronique professionnelle

L'organisme met à la disposition des utilisateurs des comptes de messageries électroniques qui leurs permettent d'émettre et de recevoir des messages électroniques à caractère professionnel.

La messagerie professionnelle ne peut être utilisée qu'à des fins professionnelles. A cet effet, il est strictement interdit de :

- L'utiliser à des fins personnelles ou partisanes ;
- L'utiliser pour l'enregistrement sur les réseaux sociaux, les forums et les sites web ;
- Ouvrir les pièces jointes et/ou les liens hypertexte transmis à partir d'adresses mail inconnues ;
- Ouvrir la boite mail professionnelle à partir des espaces communautaires d'accès à internet notamment les cybers café ;

Lorsque les missions de l'utilisateur nécessitent son enregistrement sur les réseaux sociaux, les forums ou les sites web, une adresse mail dédiée à cet effet lui est attribuée après avis favorable de l'autorité habilitée.

L'utilisateur doit faire preuve de vigilance lors de l'utilisation des courriers électroniques et ceci en s'assurant que :

- L'adresse du destinataire est bien formulée ;
- Le destinataire est habilité à accéder au contenu transmis ;
- Les bonnes pièces jointes ont été rattachée au document.

Il est strictement interdit d'utiliser les adresses mail personnelles pour la transmission des documents professionnels ;

Article 12 : de l'utilisation d'internet

Les utilisateurs ayant accès à internet s'engage à :

- Ne pas utiliser intentionnellement ce service à des fins malveillantes, obscènes, frauduleuses, haineuses, diffamatoires, pornographiques ou illégales ;
- Ne pas fournir des informations liées à leur fonction, grade ou responsabilité sur les réseaux sociaux ;

- Ne pas surcharger le réseau de l'organisme ;
- Faire preuve de prudence lors du téléchargement des fichiers, et s'assurer de les scanner par un antivirus.

Article 13 : des appareils mobiles et de supports de stockage

L'utilisateur doit :

- Signaler, à la hiérarchie dans l'immédiat, toute perte ou vol d'un appareil mobile ou support de stockage professionnel ;
- Verrouiller toujours les appareils mobiles lorsqu'ils ne sont pas utilisés ;
- Désactiver les fonctions Wi-Fi et Bluetooth des appareils lorsque celles-ci ne sont pas nécessaires ;
- Interdiction formelle pour toute personne étrangère à l'organisme de transférer des documents par support amovible, tout échange de document doit se faire par courriel. Dans le cas où le volume de données exige le recours à un support amovible, ce dernier doit être analysé par les services compétents avant toute utilisation ;
- Chiffrer les données confidentielles contenues dans des appareils mobiles et des supports de stockage ;
- Lors des déplacements professionnels, l'utilisateur doit garder ses appareils mobiles et supports de stockage amovible sur soi.

Article 14 : mesures de sécurité à appliquer lors des déplacements à l'étranger

- Il est interdit d'utiliser des terminaux (ordinateurs, tablettes.) publics ou partagés pour accéder au compte de messagerie professionnelle ou aux applications métier ;
- Le missionnaire doit garder sur lui, en permanence, son terminal professionnel ainsi que les supports de stockage ;
- Le missionnaire doit désactiver les fonctions de communication sans fil tel que le Wi-Fi et le Bluetooth des appareils lorsque celle-ci ne sont pas nécessaires ;
- Le missionnaire doit supprimer toutes les données professionnelles sensibles, non nécessaire à la mission, de tous les supports amovibles avant tout déplacement à l'étranger ;
- Le missionnaire doit informer la hiérarchie et la représentation diplomatique algérienne en cas d'inspection ou de saisie des équipements informatiques par des autorités étrangères lors des missions à l'étranger ;
- Il est interdit d'utiliser des équipements offerts lors d'un déplacement à l'étranger à des fins professionnelles ;
- Le missionnaire doit mentionner dans les comptes rendus de la mission, la liste des objets connectés offerts lors du déplacement ;

- Il est formellement interdit qu'un transfert des documents par un étranger se fasse via des supports de stockage amovibles. Tout échange de document doit se faire exclusivement par courriel ;
- Le missionnaire doit changer les mots de passe utilisés pendant la mission.

Article 15 : fin de la relation liant l'utilisateur à l'organisme

- Lorsque la relation liant l'utilisateur à l'organisme prend fin, l'utilisateur doit restituer à l'organisme toutes les ressources informatiques matérielles mises à sa disposition ;
- L'organisme procédera à la suppression de l'ensemble des accès logiques de l'utilisateur aux ressources informatiques mises à sa disposition par l'organisme.

Article 16 : gestion des incidents

En cas d'incident pouvant affecter la sécurité, l'organisme peut :

- Déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation ;
- Isoler ou neutraliser provisoirement toute donnée ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information ;
- Prévenir le responsable hiérarchique.

Article 17 : du non-respect de la charte

Le non-respect des règles définies dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entrainer à son encontre des mesures disciplinaires proportionnelles à la gravité des faits constatés.

Sous réserve que soit informé le responsable hiérarchique, les responsables de la sécurité informatiques peuvent :

- Avertir un utilisateur ;
- Limiter ou retirer provisoirement les accès d'un utilisateur ;
- Effacer, comprimer ou isoler toute données ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'information.

Sans préjudice des sanctions disciplinaire le contrevenant aux dispositions de la présente charte peut faire l'objet de poursuites judiciaires.

Article 18 : entrée en vigueur

Cette Charte entre vigueur dès sa signature par l'utilisateur. Tout refus de signature interdira l'accès de l'utilisateur aux ressources informatiques de l'organisme.

Annexe 3 - Glossaire des termes

Termes en Français	Termes en Anglais	Définition
Acceptation du risque	Risk acceptance	Décision argumentée en faveur de la prise d'un risque
Accès sans fil	Wi-Fi	Technologie de réseau informatique sans fil pouvant fonctionner pour construire un réseau interne accédant à Internet à haut débit. Cette technologie est basée sur la norme IEEE 802.11 (ISO/CEI 8802-11).
Actif	Asset	Tout ce qui est tangible ou intangible et qui a de la valeur pour l'organisation. Il existe de nombreux types d'actifs, dont certains comprennent des éléments évidents, tels que : des personnes, des machines, des services publics, des brevets, des logiciels et des services. Le terme peut également inclure des éléments moins évidents, tels que : les informations et les caractéristiques (par exemple, la réputation et l'image publique de l'organisation, ainsi que les compétences et les connaissances).
Actif informationnel	Information asset	Toute connaissance ou donnée, tangible ou non, ayant une valeur pour l'organisation, telle que l'information ou les systèmes d'information.
Analyse du risque	Risk analysis	Le processus systématique pour comprendre la nature du risque et déduire son niveau.
Appareil mobile	Mobile device	Un appareil informatique ou de communication portable doté d'une capacité de stockage d'informations pouvant être utilisé à partir d'un emplacement non fixe. Les appareils mobiles comprennent les téléphones mobiles, les smartphones, les appareils électroniques portables, les assistants numériques personnels, les ordinateurs portables, les netbooks, les tablettes et autres appareils portables connectés à Internet.
Apportez votre propre appareil	BYOD: Bring Your Own Device	Ce terme fait référence à la politique de l'organisation qui permet (en tout ou en partie) à ses employés d'apporter leurs appareils personnels (ordinateurs portables, tablettes et smartphones) dans les locaux de l'organisation et d'utiliser ces appareils pour accéder aux réseaux, informations, applications et systèmes de l'organisation dont l'accès est restreint.
Appréciation du risque	Risk assessment	Ensemble du processus d'identification du risque, d'analyse du risque et d'évaluation du risque.
Attaque	Attack	Tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'utiliser sans autorisation un actif, ou de faire un usage non autorisé de celui-ci
Attaques cybernétiques	Cyber Attack	Exploitation intentionnelle des systèmes informatiques, réseaux des organisations dont le travail dépend des TIC numériques, afin de causer des dommages.
Atténuation des risques	Risk mitigation	Mesures prises pour réduire la probabilité, les conséquences négatives, ou les deux, associées à un risque.
Audit	Audit	Revue et examen indépendants des enregistrements et des activités pour évaluer l'efficacité des contrôles de cybersécurité et garantir la conformité aux politiques établies, aux procédures opérationnelles et aux exigences standard, légales et réglementaires pertinentes.
Authenticité	Authenticity	Propriété selon laquelle une entité est ce qu'elle revendique être
Authentification / identification	Authentication / identification	L'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire

		reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.
Authentification multi-facteurs	Multi-Factor Authentication (MFA)	Système de sécurité qui vérifie l'identité de l'utilisateur, qui nécessite l'utilisation de plusieurs éléments distincts des mécanismes de vérification de l'identité. Les mécanismes de vérification comprennent plusieurs éléments : • Connaissance (quelque chose que seul l'utilisateur sait « comme un mot de passe »). • Possession (propriété exclusive de l'utilisateur «tel qu'un programme, un appareil générant des numéros aléatoires ou des SMS ») pour les enregistrements de connexion, appelés : mot de passe à usage unique. • Caractéristiques inhérentes (caractéristiques de l'utilisateur uniquement, telles que les empreintes digitales). "
Autorisation	Authorization	La définition et la vérification des droits d'accès aux ressources, liées à la sécurité de l'information et des actifs techniques de l'organisation en général et au contrôle de l'accès en particulier.
Besoin de savoir	Need–to–know	Le principe qui consiste à ne communiquer à une personne que les informations dont elle a besoin pour remplir son rôle.
Classification	Classification	La catégorisation d'informations ou de systèmes en fonction du niveau d'impact métier associé à cette information ou système.
Classification des données et informations	Data and Information Classification	Définition du niveau de sensibilité des données et des informations qui entraînent des contrôles de sécurité pour chaque niveau de classification. Les niveaux de sensibilité des données et des informations sont définis selon des catégories prédéfinies dans lesquelles les données et les informations sont créées, modifiées, améliorées, stockées ou transmises. Le niveau de classification est une indication de la valeur ou de l'importance des données et informations de l'organisation.
Cloud Computing	Cloud Computing	Modèle permettant un accès réseau à la demande à un pool partagé de capacités / ressources informatiques configurables (réseaux, serveurs, stockage, applications et services, par exemple) pouvant être rapidement mis en service avec un effort de gestion des opérations ou interaction entre fournisseurs de services minimal. Il permet aux utilisateurs d'accéder aux services basés sur la technologie à partir du cloud sans aucune connaissance, expertise ou contrôle de l'infrastructure qui les supporte. Le modèle de cloud computing est composé de cinq caractéristiques essentielles : libre-service à la demande, accès réseau Universel, mutualisation des ressources indépendante de la localisation, élasticité rapide et service mesuré. Il existe trois types de modèles de prestation de services d'informatique en nuage : logiciels en tant que service (SaaS Software as a Service), plate-forme en tant que service (PaaS Platform as a Service) et infrastructure en tant que service (IaaS : Infrastracture as a Service); Selon l'accès de l'entreprise au cloud computing, il existe quatre modèles : Cloud privé, Cloud communautaire, Cloud public et Cloud hybride. "
Code malveillant, logiciel malveillant	Malicious software, malware	Un programme qui infecte les systèmes, généralement de manière dissimulée, dans le but de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation de la victime, ou de le gêner ou de le perturber victime. Les types de programmes malveillants incluent les virus,

		bombes logiques (logic bomb), les chevaux de Troie (Trojan Hors), Rançongiciel (Ransomware), Outils de dissimulation d'activité (Rootkit), Ver (Worm)
Compétence	Skill	Capacité à appliquer des connaissances et des aptitudes pour obtenir les résultats escomptés
Compromission	Compromise	Divulgation ou obtention d'informations par des personnes non autorisées, ou violation de la politique de cybersécurité de l'organisation suite à la divulgation, au changement, au sabotage ou à la perte de quoi que ce soit, intentionnellement ou non.
Compte privilégié	Privileged account	Un compte privilégié est un compte bénéficiant de droits d'accès étendus qui permettrait à des utilisateurs malveillants de porter plus facilement ou plus gravement atteinte à la sécurité ou au fonctionnement du système d'information, Les comptes privilégiés sont par exemple des comptes d'administrateurs ou des comptes d'utilisateurs disposant de droits à fort impact métier dans une application.
Confidentialité	Confidentiality	Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.
Conservation	Retention	Durée, pendant laquelle les informations, les données, les journaux des événements ou les sauvegardes doivent être conservés, quel que soit le type de support (c.-à-d. Papier et électronique).
Continuité de la sécurité de l'information	Information security Continuity	Processus et procédures visant à assurer la continuité des opérations liées à la sécurité de l'information
Contournement de la politique de sécurité	Security policy bypass	Toute action ayant pour conséquence la mise en échec des règles ou des mécanismes de sécurité mis en place.
Contrôle d'accès	Access Control	Moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les exigences propres à la sécurité et à l'activité métier
Cybercriminalité	Cybercriminality	Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.
Cyberdéfense	Cyberdefence	Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.
Cyberespace	Cyberspace	Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques y compris Internet, les réseaux de communication, les systèmes informatiques et les périphériques connectés à Internet, ainsi que le matériel et les dispositifs de contrôle associés.
Cybersécurité	Cybersecurity	La protection des réseaux, des systèmes informatiques, des systèmes de technologies opérationnelles et de leurs composants matériels et logiciels, de leurs services et des données qu'ils contiennent leur 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 et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.
Défense en profondeur	Defense-in-Depth	Il s'agit d'un concept d'assurance de l'information dans lequel plusieurs niveaux de contrôles de sécurité (défense) sont placés dans un système de technologie de l'information.
Déni de service	Denial of Service (DoS)	Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu (compromission de la disponibilité).

		Remarques : Si l'action est lancée depuis plusieurs sources, il est fréquent de parler de Déni de Service Distribué (DDoS Distributed Denial of Service).
Disponibilité	Availability	L'assurance que les informations, les données, les systèmes et les applications sont disponibles et accessibles par les entités autorisées en cas de besoin.
Evénement de cybersécurité	Cyber security event	Une occurrence identifiée d'un système, d'un service ou d'un état de réseau indiquant une violation possible de la politique de sécurité des informations ou une défaillance des mesures de protection ou une situation inconnue jusqu'alors et pouvant relever de la sécurité.
Externaliser	Outsource	Prendre des dispositions pour qu'un organisme externe prenne en charge une partie des fonctions ou des processus d'un organisme
Faille	Weakness	Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.
Fiabilité	Reliability	Propriété relative à un comportement et à des résultats prévus et cohérents
Filtrage	Filtering	Dispositif permettant de réduire les communications entre deux parties d'un système d'information, par exemple par la déclaration de plages d'adresse réseau autorisées à communiquer entre elles, ou par la déclaration des protocoles autorisés dans cette communication. Dans le cas de TCP ou d'UDP, le filtrage se basera sur un numéro de port.
Gestion des accès privilégiés	Privileged Access Management	Processus de gestion des privilèges à haut risque sur les systèmes nécessitant un traitement spécial afin de minimiser les risques pouvant découler d'une mauvaise utilisation des droits.
Gestion des incidents liés à la sécurité de l'information	Information security incidents management	Ensemble de processus visant à détecter, rapporter, apprécier, gérer et résoudre les incidents liés à la sécurité de l'information, ainsi qu'à en tirer des enseignements.
Gestion des risques	Risk management	Processus consistant à identifier les risques, à évaluer les risques et à prendre des mesures pour réduire les risques à un niveau acceptable.
Gouvernance de la sécurité de l'information	Information security governance	Système par lequel un organisme conduit et supervise les activités liées à la sécurité de l'information.
Hyper Text Transfer Protocol Secure (HTTPS)	Hyper Text Transfer Protocol Secure (HTTPS)	Protocole utilisant le cryptage pour sécuriser les pages Web et les données lors de leur transmission sur le réseau. C'est une version sécurisée du protocole HTTP (Hypertext Text Transfer Protocol).
Identification	Identification	C'est le moyen de vérifier l'identité d'un utilisateur, d'un processus ou d'un appareil, généralement comme condition préalable à l'octroi d'un accès aux ressources d'un système.
Identification des risques	Risk identification	Processus de recherche, de reconnaissance et de description des risques qui comprend l'identification des sources de risque, des événements, de leurs causes et de leurs conséquences potentielles.
Incident de cybersécurité	Cyber security incident	Un ou plusieurs événements indésirables ou inattendus de cybersécurité qui risquent fortement de compromettre les opérations métier et de menacer la sécurité des informations.
Information classifiée	Classified information	Information sensible nécessitant une protection contre la divulgation non autorisée.
Informations sensibles	Sensitive information	Des informations non classifiées ou classifiées identifiées comme nécessitant des protections supplémentaires (par exemple, des informations compartimentées ou des informations marquées pour diffusion limitée.

Infrastructure réseau	Network infrastructure	Infrastructure utilisée pour transporter des informations entre des postes de travail et des serveurs ou d'autres périphériques réseau.
Ingénierie sociale	Social Engineering	Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes. c'est l'exploitation du facteur humain, qui peut être considéré dans certains cas comme un maillon faible de la sécurité du système d'information.
Intégrité	Integrity	Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime.
Intrusion	Intrusion	L'intrusion est le fait, pour une personne ou un objet, de pénétrer dans un espace (physique, logique, relationnel) défini où sa présence n'est pas souhaitée.
Menace	Threat	Cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme
Mesure de sécurité	Security control	Mesure qui modifie un risque. Les mesures de sécurité comprennent tous les processus, politiques, dispositifs, pratiques ou autres actions qui modifient un risque.
Mot de passe	Password	Un mot de passe est un élément de déverrouillage servant dans la vérification de l'identité annoncée d'une personne par un système d'information.
Niveau de risque	Risk level	Importance d'un risque exprimée en termes de combinaison des conséquences et de leur vraisemblance
Non-conformité	Noncompliance	Non-satisfaction d'une exigence
Non-répudiation	Nonrepudiation	Capacité à prouver l'occurrence d'un événement ou d'une action donnée(e) et des entités qui en sont à l'origine.
Objectif d'une mesure de sécurité	Security control objective	Déclaration décrivant ce qui est attendu de la mise en œuvre d'une mesure de sécurité.
Pare-feu	Firewall	Un pare-feu (ou garde-barrière), est un outil permettant de protéger un système informatique connectée à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.
Pare-feu pour Applications Web	Web Application Firewall	Il analyse, filtre, surveille et bloque le trafic Internet à destination et en provenance d'une application Web. Il est également capable de filtrer le contenu d'applications Web spécifiques.
Patch	Patch	Logiciel conçu pour résoudre les problèmes liés à un programme informatique ou à ses données, ou pour la mise à jour de celui-ci. Cela inclut la correction des vulnérabilités de sécurité et autres déficiences du programme, ainsi que l'amélioration de la convivialité ou des performances du logiciel.
Périphérique réseau	Network device	Tout périphérique conçu pour faciliter la communication d'informations destinées à plusieurs utilisateurs. Par exemple : dispositifs cryptographiques, pare-feu, routeurs, commutateurs et concentrateurs.
Point d'accès sans fil	Wireless access point	Un équipement qui permet la communication entre des clients sans fil. C'est généralement aussi le périphérique qui connecte le réseau local sans fil au réseau local câblé.
Principe du moindre privilège	Least Privilege	Un principe de base de la sécurité qui vise à accorder aux utilisateurs uniquement les privilèges d'accès dont ils ont besoin pour s'acquitter de leurs responsabilités officielles.
Procédure	Procedure	Un document avec une description détaillée des étapes nécessaires pour effectuer des opérations ou activités spécifiques conformément aux normes et politiques en

		vigueur. Les procédures peuvent être un sous-ensemble de processus.
Processus	Process	Ensemble d'activités corrélées ou interactives qui transforment des éléments d'entrée en éléments de sortie
Propriétaire du risque	Risk owner	Personne ou entité ayant la responsabilité du risque et ayant autorité pour le gérer
Protocole IP	IP Protocol	La communication sur l'internet est fondée sur un protocole appelé IP pour Internet Protocol qui permet aux ordinateurs de communiquer entre eux. Ce protocole utilise des adresses numériques pour distinguer ces machines et tronçonne la communication en paquets comportant chacun une adresse de source et une adresse de destination. La version la plus couramment employée du protocole est la version IPv4 dans laquelle les adresses sont composées de 4 nombres par exemple 41.111.133.100. Une nouvelle version du protocole est en cours de déploiement : IPv6. Elle utilise des adresses plus longues composées de 8 nombres notés en hexadécimal par exemple 2600 :1005 :b062 :61e4 :74d7 :f292 :802c :fbfd. Enfin IPsec désigne un protocole de chiffrement et de signature des paquets IP.
Récupération	Recovery	Une procédure ou un processus permettant de restaurer ou de contrôler quelque chose qui est suspendu, endommagé ou perdu.
Reprise après sinistre	Disaster Recovery	Programmes, activités et plans conçus pour rétablir les opérations et les services critiques de l'organisme à la suite d'une exposition à des cyber-attaques ou de la perturbation de ces services.
Résilience à la cybersécurité	Cybersecurity Resilience	Capacité globale des organisations à résister aux attaques cybernétiques et à s'en remettre, lorsqu'un dommage est causé.
Risque	Risk	Exposition à un danger, à un préjudice ou à une perte pouvant être rencontrés lorsque une vulnérabilité est exploitée par une menace. Le niveau d'impact sur les services de l'entité, les actifs informationnels ou les individus est le résultat des conséquences potentielles d'une menace et la probabilité que cette menace se produise.
Risques Cybernétiques	Cyber Risks	Risques sur les opérations organisationnelles (y compris la vision, la mission, les fonctions, l'image ou la réputation), les actifs de l'organisation, les individus, d'autres organisations ou le pays en raison d'un potentiel d'accès, d'utilisation, de divulgation, de perturbation, de modification ou de destruction non autorisé d'information et/ou des systèmes d'information.
Sécurisation et renforcement de la configuration	Secure Configuration and Hardening	Protéger, renforcer et configurer les paramètres des ordinateurs, systèmes, applications, périphériques réseau et dispositifs de sécurité afin de résister aux cyberattaques, tels que : l'arrêt ou la modification des comptes par défaut, l'arrêt de services et de ports réseau inutilisés.
Sécurité assurée dès la conception	Security-by Design	Une méthodologie pour le développement de systèmes et de logiciels et la conception de réseaux qui vise à rendre les systèmes, les logiciels et les réseaux exempts de vulnérabilités / faiblesses de cybersécurité et imperméables aux cyberattaques autant que possible, et cela à l'aide de mesures telles que : tests continus, mesures d'authentification et respect des meilleures pratiques de programmation et de conception.
Sécurité de l'information	Information security	Protection des informations et des systèmes d'information contre tout accès, utilisation, divulgation, perturbation,

		modification ou destruction non autorisés afin de garantir la confidentialité, l'intégrité et la disponibilité.
Sécurité de l'information	Information Security	Protection de l'information et des systèmes d'information contre tout accès, utilisation, divulgation, perturbation, modification ou destruction non autorisés afin d'assurer la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.
Sécurité physique	Physical Security	La sécurité physique décrit les mesures de sécurité conçues pour empêcher tout accès non autorisé aux installations, équipements et ressources de l'Organisation, et pour protéger les individus et les biens contre les dommages (tels que l'espionnage, le vol ou les attaques terroristes). La sécurité physique implique l'utilisation de systèmes interconnectés à plusieurs niveaux, y compris la vidéosurveillance, les gardes de sécurité, les limites de sécurité, les verrous, les systèmes de contrôle d'accès et d'autres technologies.
Séparation des tâches	Segregation of Duties	Un principe clé de la cybersécurité est de minimiser les erreurs et les fraudes lors du traitement de tâches spécifiques. Pour ce faire, plusieurs personnes ayant des privilèges différents sont nécessaires pour mener à bien une tâche.
Sous-traitance	Subcontracting	Obtenir des biens ou des services en passant des contrats avec un fournisseur ou un prestataire de services.
Surveillance	Monitoring	Détermination du statut d'un système, d'un processus ou d'une activité
Système de prévention des intrusions	Intrusion Prevention System (IPS)	Système doté de fonctions de détection des intrusions, ainsi que de la capacité de prévenir et d'arrêter des incidents potentiels.
Tâche d'administration	Administrative task	On appelle tâche d'administration d'un système d'information les opérations de configuration et de gestion d'une ressource du système d'information : installation, gestion des configurations, maintenance, évolution du système d'information administré, supervision ou gestion de la sécurité.
Test d'intrusion	Penetration Test	Pratique consistant à tester un système informatique, un réseau, une application Web ou une application mobile afin de détecter les vulnérabilités qu'un attaquant pourrait exploiter.
Tierce partie	Third-Party	Toute organisation qui agit en tant que partie à une relation contractuelle pour fournir des biens ou des services (fournisseurs et prestataires de services compris).
Vulnérabilité	Vulnerability	Faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces